ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ
ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΙΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

ΠΑΙΧΝΙΔΙΑ ΣΟΒΑΡΟΥ ΣΚΟΠΟΥ ΓΙΑ ΤΗΝ ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΤΩΝ ΜΑΘΗΤΩΝ ΣΕ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ: ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΠΙΣΚΟΠΗΣΗ ΚΑΙ ΕΜΠΕΙΡΙΚΗ ΜΕΛΕΤΗ

Διπλωματική Εργασία

της

Γεωργίας Ζεμπίλα

Θεσσαλονίκη, 02/2024

ΠΑΙΧΝΙΔΙΑ ΣΟΒΑΡΟΥ ΣΚΟΠΟΥ ΓΙΑ ΤΗΝ ΕΥΑΙΣΘΗΤΟΠΟΙΗΣΗ ΤΩΝ ΜΑΘΗΤΩΝ ΣΕ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ: ΒΙΒΛΙΟΓΡΑΦΙΚΗ ΕΠΙΣΚΟΠΗΣΗ ΚΑΙ ΕΜΠΕΙΡΙΚΗ ΜΕΛΕΤΗ

Γεωργία Ζεμπίλα

Πτυχίο Εφαρμοσμένης Πληροφορικής, Κατεύθυνση Εφαρμοσμένης Πληροφορικής, Πανεπιστήμιο Μακεδονίας, 2021

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής
Στυλιανός Ξυνόγαλος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 19/02/2024

Ονοματεπώνυμο 1	Ονοματεπώνυμο 2	Ονοματεπώνυμο 3
Στυλιανός Ξυνόγαλος	Θεόδωρος Κασκάλης	Κωνσταντίνος Ψάννης

Γεωργία Ζεμπίλα

Περίληψη

Τα παιχνίδια σοβαρού σκοπού αποτελούν μία κατηγορία παιχνιδιών τα οποία εκτός από την ψυχαγωγία των παικτών επιδιώκουν και άλλους σκοπούς. Ένας από αυτούς είναι η ευαισθητοποίηση τους σε διάφορα θέματα και η αλλαγή της συμπεριφοράς τους. Η εργασία αυτή επικεντρώνεται σε παιχνίδια σοβαρού σκοπού με περιεχόμενο θέματα ασφάλειας και προστασίας των προσωπικών δεδομένων στον κυβερνοχώρο. Η εργασία ερευνά υπάρχοντα παιχνίδια σοβαρού σκοπού με αυτό το περιεχόμενο. Επιπλέον, διερευνά εάν η εφαρμογή παιχνιδιών με αυτή τη θεματική σε μαθητές, μπορεί να συμβάλλει στην ευαισθητοποίηση και την αλλαγή της συμπεριφοράς τους. Κατά τη βιβλιογραφική επισκόπηση πραγματοποιείται ανάλυση της έννοιας της παιχνιδοποίησης και των παιχνιδιών σοβαρού σκοπού. Επιπλέον, αναλύονται παιχνίδια σοβαρού σκοπού με περιεχόμενο την ευαισθητοποίηση σε θέματα ασφάλειας στον κυβερνοχώρο, το ηλεκτρονικό "ψάρεμα", το hacking, τα ζητήματα απορρήτου και την προστασία των προσωπικών δεδομένων. Παράλληλα, εκτός από τον εντοπισμό αυτών των παιχνιδιών, εντοπίζεται σε ποιους απευθύνονται, ποια είναι η εμπειρία των χρηστών και ποια είναι τα μαθησιακά αποτελέσματα από την ενασχόληση τους με αυτά τα παιχνίδια. Κατά την εμπειρική μελέτη, αρχικά αναλύεται ο τρόπος με τον οποίο δημιουργήθηκαν τα ερωτηματολόγια και επιλέχθηκαν τα παιχνίδια τα οποία τέθηκαν σε εφαρμογή σε μαθητές. Από την εμπειρική μελέτη προέκυψε ότι οι μαθητές έχουν θετική στάση απέναντι στη μάθηση μέσω παιχνιδιών και προτιμούν να αξιοποιούνται παιχνίδια ως συμπληρωματικά εργαλεία μάθησης συνδυαστικά με το σχολικό βιβλίο. Επιπλέον, διαπιστώθηκε ότι η στάση των μαθητών πριν την ενασχόληση τους με τα παιχνίδια δεν διαφυλάττει σημαντικά το απόρρητο και τα προσωπικά τους δεδομένα στο διαδίκτυο. Επίσης, προέκυψε ότι η μάθηση βασισμένη σε ψηφιακά παιχνίδια είναι αποτελεσματική ως προς την ανάπτυξη δεξιοτήτων προστασίας στον κυβερνοχώρο. Οι μαθητές δήλωσαν ότι συνέλεξαν πληροφορίες και ότι κινητοποιήθηκαν να αναζητήσουν περισσότερες. Επιπρόσθετα, εξέφρασαν ότι εάν έπαιζαν περισσότερα παιχνίδια με παρόμοιο περιεχόμενο θα μπορούσαν να προστατευτούν καλύτερα στον κυβερνοχώρο. Εν κατακλείδι, τα παιδιά μετά την ενασχόληση τους με τα παιχνίδια ευαισθητοποιήθηκαν σε θέματα ασφάλειας και προστασίας των προσωπικών δεδομένων στο διαδίκτυο και εξέφρασαν ότι χρειάζεται να αλλάξει η συμπεριφορά τους ώστε να προστατεύονται αποτελεσματικότερα.

Λέξεις Κλειδιά:

Παιχνίδια σοβαρού σκοπού, μάθηση βασισμένη σε ψηφιακά παιχνίδια, ευαισθητοποίηση σε θέματα ασφάλειας, προστασία προσωπικών δεδομένων, διαδίκτυο, διαδικτυακό απόρρητο, μαθητές.

Abstract

Serious games are a category of games which, in addition to entertaining the players, pursue other goals. One of the goals is making the players aware of various issues and changing their behavior. This work focuses on serious games dealing with the subject matter of privacy issues and personal data protection in cyberspace. The paper surveys existing serious games with this content. Furthermore, it investigates whether the application of games with this theme to students can contribute to raising awareness and changing their behavior. The literature review analyzes the concept of gamification and serious games. Also, serious games about raising awareness of cyber security issues, phishing, hacking, privacy issues and personal data protection purpose are analyzed. At the same time, in addition to identifying these games, it identifies who they are aimed at, what the user experience is and the learning outcomes from their engagement with these games. During the empirical study, firstly, the way in which the questionnaires were created and the games that were implemented for students were selected. From the empirical study it emerged that students have a positive attitude towards learning through games and prefer to use games as complementary learning tools combined with the textbook. In addition, it was found that the attitude of students before engaging in games did not significantly protect their privacy and personal data online. Digital Game-Based Learning has also been found to be effective in developing cyber protection skills. Students reported learning information and being motivated to seek more. Finally, they expressed that if they played more games with similar content they could be better protected in cyberspace. In conclusion, after playing the games, the children became aware of issues of safety and personal data protection on the internet and expressed the need to change their behavior in order to protect themselves more effectively.

Keywords:

Serious games, Digital Game-Based Learning, security and privacy awareness, personal data privacy, internet, online privacy, students

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

1 Εισαγωγή

1.1 Πρόβλημα – Σημαντικότητα του θέματος

Η διδασκαλία βασισμένη σε παιχνίδια αποτελεί για τους μαθητές έναν ενδιαφέροντα τρόπο ψυχαγωγίας και παράλληλα απόκτησης γνώσεων. Είναι ικανή να αντικαταστήσει τρόπους διδασκαλίας οι οποίοι δεν πετυχαίνουν να κεντρίσουν ιδιαίτερα το ενδιαφέρον των παιδιών. Παράλληλα, είναι γεγονός ότι η χρήση παιχνιδιών σοβαρού σκοπού στην εκπαίδευση και ειδικότερα στο μάθημα της Πληροφορικής στα σχολεία είναι πολύ σημαντική.

Υπάρχουν παιχνίδια τα οποία επικεντρώνονται στην εκμάθηση εννοιών σχετικών με την αλγοριθμική σκέψη, με τον προγραμματισμό, το υλικό και το λογισμικό του Η/Υ, αλλά και παιχνίδια τα οποία δεν στοχεύουν μόνο στην εκμάθηση εννοιών αλλά και στην αλλαγή της συμπεριφοράς των μαθητών και στην ευαισθητοποίηση τους σε σημαντικά ζητήματα. Τα παιχνίδια σοβαρού σκοπού, τα οποία δίνουν έμφαση στην αλλαγή της συμπεριφοράς των μαθητών και στην ευαισθητοποίηση τους σε διάφορα ζητήματα, επικεντρώνονται σε πολλά και διαφορετικά θέματα. Ενδιαφέρον παρουσιάζουν παιχνίδια με θεματικές όπως η αποφυγή του bullying στο σχολείο και γενικότερα στο φυσικό περιβάλλον αλλά και στο διαδικτυακό περιβάλλον (social media κ.α.). Επιπλέον, υπάρχουν παιχνίδια με θεματικές όπως η κακοποίηση ή η σεξουαλική παρενόχληση ή η διακίνηση πορνογραφικού υλικού παιδιών. Παιχνίδια σαν αυτά συμβάλλουν σημαντικά στην κατανόηση των κινδύνων του διαδικτύου. Τέλος, έχουν αναπτυχθεί πολλά παιχνίδια τα οποία στοχεύουν στην αλλαγή της συμπεριφοράς των μαθητών με περιεχόμενο τα προσωπικά τους δεδομένα και την γενικότερη προστασία και διασφάλιση της ιδιωτικότητας και του απορρήτου τους στον κυβερνοχώρο.

Τα τελευταία προαναφερθέντα παιχνίδια σοβαρού σκοπού είναι αυτά στα οποία επικεντρώνεται αυτή η εργασία. Στην παρούσα εργασία δίνεται έμφαση σε παιχνίδια που πραγματεύονται ζητήματα όπως η ασφάλεια στον κυβερνοχώρο, η διαφύλαξη του απορρήτου, τα προσωπικά δεδομένα κ.α.. Αυτό που πραγματικά παρουσιάζει ενδιαφέρον είναι αν η εφαρμογή αυτών των παιχνιδιών στα πλαίσια της εκπαίδευσης είναι ικανή να αλλάξει ουσιαστικά τη στάση των μαθητών απέναντι στα συγκεκριμένα φλέγοντα ζητήματα.

1.2 Σκοπός – Στόχοι

Η παρούσα εργασία ερευνά υπάρχοντα παιχνίδια σοβαρού σκοπού τα οποία επικεντρώνονται σε ζητήματα όπως η ασφάλεια και το απόρρητο στον κυβερνοχώρο, τα προσωπικά δεδομένα κ.α.. Σκοπός αυτής της εργασίας είναι να διερευνηθεί εάν η εφαρμογή υπαρχόντων παιχνιδιών, με θεματικές αυτού του είδους, σε μαθητές είναι ικανή να συμβάλλει στην ευαισθητοποίηση τους στα ζητήματα αυτά και να αλλάξει την υπάρχουσα συμπεριφορά τους στο διαδίκτυο.

Παράλληλα η έρευνα στοχεύει να διαπιστώσει αν οι μαθητές έχουν θετική στάση απέναντι στην εκμάθηση εννοιών μέσω σοβαρών παιχνιδιών. Επιπλέον, η εργασία καλείται να διαπιστώσει την στάση των μαθητών απέναντι στα προσωπικά τους δεδομένα και γενικότερα στην προστασία τους στον κυβερνοχώρο, προτού αυτοί έρθουν σε επαφή με παιχνίδια σοβαρού σκοπού. Τέλος, μέσα από αυτή την έρευνα θα ήταν πολύ χρήσιμο να διαπιστωθεί εάν είναι πραγματικά αποτελεσματική η εφαρμογή παιχνιδιών σοβαρού σκοπού και αν όντως οι μαθητές μετά την ενασχόληση τους με παιχνίδια έχουν ευαισθητοποιηθεί και είναι ικανοί να αλλάξουν την "διαδικτυακή" τους συμπεριφορά.

1.3 Ερωτήματα

1.3.1 Ερωτήματα βιβλιογραφικής επισκόπησης

Τα ερωτήματα της βιβλιογραφικής επισκόπησης είναι τα ακόλουθα:

(Ε.Β.Ε.1) Ποια παιχνίδια σοβαρού σκοπού είναι σχετικά με την ασφάλεια και το απορρήτο στο διαδίκτυο;

(Ε.Β.Ε.2) Σε ποιους απευθύνονται;

(Ε.Β.Ε.3) Ποια είναι οι εμπειρία του χρήστη από αυτά;

(Ε.Β.Ε.4) Ποια είναι τα μαθησιακά αποτελέσματα;

1.3.2 Ερωτήματα εμπειρικής μελέτης

Στο ερευνητικό μέρος η εργασία καλείται να απαντήσει τα ακόλουθα ερωτήματα:

(Ε.Ε.Μ.1.) Ποια είναι η στάση των μαθητών απέναντι στην μάθηση μέσω παιχνιδιών σοβαρού σκοπού;

(Ε.Ε.Μ.2.) Ποια είναι η στάση των μαθητών απέναντι στην προστασία των προσωπικών τους δεδομένων και γενικότερα την προστασία τους στον κυβερνοχώρο;

(Ε.Ε.Μ.3.) Οι μαθητές προτιμούν να μαθαίνουν για την προστασία της ιδιωτικότητας τους μόνο μέσα από παραδοσιακούς τρόπους εκπαίδευσης και το σχολικό βιβλίο, ή συνδυαστικά με παιχνίδια σοβαρού σκοπού;

(Ε.Ε.Μ.4.) Οι μαθητές χρειάζονται βοήθεια για να ασχοληθούν με το διαδικτυακό περιβάλλον (παιχνίδι σοβαρού σκοπού) ή μπορούν να χρησιμοποιήσουν αυτά τα παιχνίδια μόνοι τους εκτός του σχολικού ωραρίου ως συμπληρωματική μάθηση;

(Ε.Ε.Μ.5.) Είναι αποτελεσματική τελικά η εκπαίδευση μέσω της χρήσης παιχνιδιών σοβαρού σκοπού (Digital Game–Based Learning - DGBL) στην ανάπτυξη δεξιοτήτων προστασίας στον κυβερνοχώρο;

(Ε.Ε.Μ.6.) Η εφαρμογή παιχνιδιών σοβαρού σκοπού συμβάλλει στην ευαισθητοποίηση σχετικά με το απόρρητο και στην αλλαγή της συμπεριφοράς;

(Ε.Ε.Μ.7.) Ποια είναι η στάση των μαθητών απέναντι στην ασφάλεια και το απόρρητο στο διαδίκτυο, πριν και ποια μετά την εφαρμογή των παιχνιδιών σοβαρού σκοπού;

1.4 Διάρθρωση της μελέτης

Η παρούσα μελέτη διαρθρώνεται σε 4 κεφάλαια. Το κεφάλαιο 1 αποτελεί την εισαγωγή. Σε αυτό το κεφάλαιο διατυπώνεται το πρόβλημα και η σημαντικότητα του θέματος. Επιπλέον, αναφέρεται ο σκοπός της εργασίας και διατυπώνονται τα ερωτήματα τα οποία θα απαντηθούν είτε στη βιβλιογραφική επισκόπηση είτε στην εμπειρική μελέτη. Τέλος αναγράφεται η διάρθρωση της μελέτης.

Στο κεφάλαιο 2 πραγματοποιείται η βιβλιογραφική επισκόπηση. Εκεί αρχικά εξηγείται η μεθοδολογία της βιβλιογραφικής επισκόπησης. Στη συνέχεια γίνονται γνωστές οι έννοιες της παιχνιδοποίησης και του παιχνιδιού σοβαρού σκοπού. Έπειτα, αναφέρονται παιχνίδια σοβαρού σκοπού σχετικά με την ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο και παιχνίδια σχετικά με το ηλεκτρονικό “ψάρεμα” και το hacking. Παράλληλα, στο δεύτερο κεφάλαιο διατυπώνονται ζητήματα απορρήτου αλλά και παιχνίδια σοβαρού σκοπού με στόχο την ευαισθητοποίηση των ανθρώπων σχετικά με το απόρρητο. Επιπλέον, αναλύονται παιχνίδια σοβαρού σκοπού με περιεχόμενο την προστασία των προσωπικών δεδομένων στο διαδίκτυο. Τέλος, απαντώνται τα ερωτήματα της βιβλιογραφικής επισκόπησης.

Το κεφάλαιο 3 αποτελεί το ερευνητικό κομμάτι της διπλωματικής. Αρχικά εξηγείται η μεθοδολογία της εμπειρικής μελέτης. Στην ενότητα αυτή του κεφαλαίου διατυπώνονται τα παιχνίδια τα οποία επιλέχθηκαν και ο τρόπος με τον οποίο πραγματοποιήθηκε η έρευνα στους μαθητές. Έπειτα, αναλύονται τα αποτελέσματα του ερωτηματολογίου προ-ερωτήσεων. Στην συνέχεια εξετάζονται τα αποτελέσματα που προέκυψαν από την εφαρμογή του ερωτηματολογίου μετά-ερωτήσεων. Τέλος, αναπτύσσονται τα συμπεράσματα τα οποία εξήχθησαν από τα αποτελέσματα των ερωτηματολογίων. Στην ενότητα αυτή του κεφαλαίου απαντώνται, ουσιαστικά, τα ερωτήματα της εμπειρικής μελέτης.

Στο κεφάλαιο 4, το τελευταίο κεφάλαιο, βρίσκεται ο επίλογος της εργασίας. Σε αυτό αναπτύσσονται η σύνοψη και τα συμπεράσματα. Επιπλέον διατυπώνονται τα όρια και οι περιορισμοί, εκεί γίνεται μία σύντομη αναφορά σε κάποιες ατέλειες της έρευνας. Τέλος, αναλύονται μερικές μελλοντικές ιδέες για επέκταση της παρούσας έρευνας.

2 Βιβλιογραφική Επισκόπηση – Θεωρητικό Υπόβαθρο

2.1 Μεθοδολογία της Βιβλιογραφικής επισκόπησης

2.1.1 Εισαγωγή στη μεθοδολογία της βιβλιογραφικής επισκόπησης

Μία συστηματική βιβλιογραφική ανασκόπηση, σύμφωνα με τους Moher et al. (2009), απαντά σε καθορισμένα ερευνητικά ερωτήματα σε ένα πεδίο ακολουθώντας ένα πρωτόκολλο αναζήτησης. Με το πρωτόκολλο αναζήτησης καθορίζονται τα κριτήρια και η στρατηγική αναζήτησης πριν από τη διεξαγωγή της μελέτης για να διασφαλιστούν αμερόληπτα αποτελέσματα. Η παρούσα βιβλιογραφική μελέτη ακολουθεί το πρωτόκολλο PRISMA με στόχο τον προσδιορισμό της στρατηγικής αναζήτησης και της ποιότητας της βιβλιογραφίας.

2.1.2 Ερευνητικά ερωτήματα

Τα ερωτήματα της βιβλιογραφικής επισκόπησης είναι τα ακόλουθα:

(Ε.Β.Ε.1) Ποια παιχνίδια σοβαρού σκοπού είναι σχετικά με την ασφάλεια και το απόρρητο στο διαδίκτυο;

(Ε.Β.Ε.2) Σε ποιους απευθύνονται;

(Ε.Β.Ε.3) Ποια είναι η εμπειρία του χρήστη από αυτά;

(Ε.Β.Ε.4) Ποια είναι τα μαθησιακά αποτελέσματα;

2.1.3 Πηγές δεδομένων και κριτήρια επιλογής

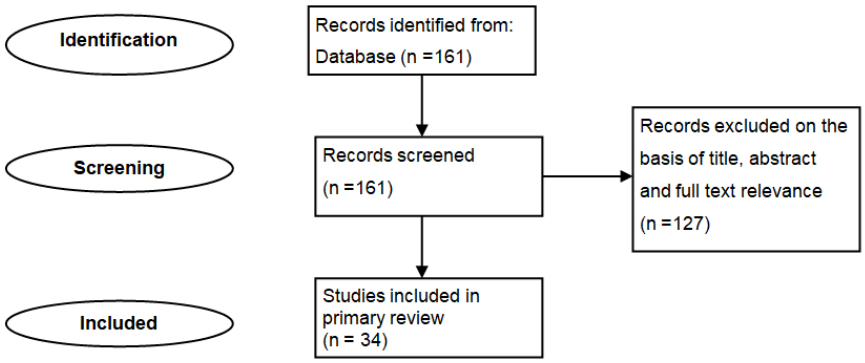
Η βάση δεδομένων η οποία χρησιμοποιήθηκε ήταν η Google Scholar. Για τον εντοπισμό εγγραφών σχετικών με το θέμα των ερευνητικών ερωτημάτων χρησιμοποιήθηκαν λέξεις-κλειδιά. Ο συνδυασμός λέξεων-κλειδιών αποτέλεσε το ερώτημα το οποίο τέθηκε στη βάση δεδομένων. Για τα παιχνίδια σοβαρού σκοπού επιλέχθηκε η λέξη-κλειδί “serious games” και για την ασφάλεια και το απόρρητο επιλέχθηκε η λέξη-κλειδί “online privacy”. Συμπερασματικά, το ερώτημα το οποίο τέθηκε στην βάση δεδομένων Google Scholar ήταν το “serious games” AND “online privacy”. Επιπλέον η τελευταία αναζήτηση στη βάση δεδομένων αυτού του ερωτήματος πραγματοποιήθηκε στις 04/09/2023.

Προκειμένου να προσδιοριστεί το εύρος αναζήτησης μόνο σε σχετικά με τα ερευνητικά ερωτήματα αποτελέσματα τέθηκαν κριτήρια συμπερίληψης και

αποκλεισμού. Το βασικό κριτήριο ένταξης μίας εγγραφής ήταν αυτή να απαντά στην (Ε.Β.Ε.1). Ένα ακόμη κριτήριο ήταν οι εγγραφές να είναι από το 2010-2023.

2.1.4 Επιλογή δεδομένων

Μετά την τελευταία αναζήτηση, 04/09/2023, στη βάση δεδομένων, Google Scholar, βρέθηκαν 161 εγγραφές. Έπειτα, ξεκίνησε η διαδικασία διαλογής τριών φάσεων με βάση τις κατευθυντήριες γραμμές του PRISMA, βλέπε Εικόνα 1. Τα άρθρα αποκλείστηκαν αρχικά με βάση τον τίτλο και την συνάφεια της περίληψης και έπειτα με βάση το κείμενο, σύμφωνα με το βασικό κριτήριο ένταξης αποκλεισμού. Ελέγχθηκε, δηλαδή, αν το εκάστοτε άρθρο απαντά στο ερώτημα (Ε.Β.Ε.1) πρώτα μέσα από τον τίτλο και την περίληψη και στη συνέχεια από το κείμενο. Μετά την ανάγνωση πλήρους κειμένου, 34 άρθρα περιλαμβάνονται στην παρούσα μελέτη.



Εικόνα 1: Διάγραμμα ροής PRISMA

2.2 Η παιχνιδοποίηση και το παιχνίδι σοβαρού σκοπού

2.2.1 Εισαγωγή

Αιώνες τώρα οι άνθρωποι παίζουν παιχνίδια με σκοπό τη διασκέδαση τους. Τα παιχνίδια αυτά έχουν εξελιχθεί μέσα σε αυτούς τους καιρούς. Παράλληλα, σήμερα πολλά από αυτά δεν στοχεύουν αποκλειστικά στη διασκέδαση των παικτών αλλά και σε διαφορετικούς σκοπούς, όπως είναι η διδασκαλία, η μάθηση κ.α.. Έτσι σήμερα πληθώρα παιχνιδιών αποτελούν ένα περιβάλλον το οποίο συχνά αξιοποιείται για μαθησιακούς και εκπαιδευτικούς σκοπούς. Σχετική βιβλιογραφία έχει αναπτυχθεί από τους Treiblmaier et al. (2018).

Αξίζει να αναφερθεί ότι τα πρώτα παιχνίδια υπολογιστών χρησιμοποιούνταν ως προσομοιώσεις για τους στρατιώτες για να δοκιμάσουν πιθανά αποτελέσματα σε

παγκόσμια κλίμακα. Έτσι τα βιντεοπαιχνίδια αποτέλεσαν για τους σχεδιαστές ένα μέσο προσομοίωσης πραγματικών σεναρίων σε εικονικούς χώρους μέσα από διεπαφές και υπολογιστικές διαδικασίες. Τα ψηφιακά παιχνίδια στοιχειοθετούνται σε μία σειρά συστημάτων και αλληλεπιδράσεων που βασίζονται σε κανόνες για την επιμέλεια της εμπειρίας χρήστη, αντίθετα τα αναλογικά παιχνίδια μπορεί να μην βασίζονται σε κώδικα και αλγορίθμους (DeJong, 2020).

2.2.2 Ορισμός της παιχνιδοποίησης και των παιχνιδιών σοβαρού σκοπού

Σύμφωνα με τους Treiblmaier et al. (2020, σ. 134),*"η παιχνιδοποίηση (gamification) ορίζεται ως η χρήση στοιχείων σχεδιασμού παιχνιδιού σε οποιοδήποτε πλαίσιο συστήματος εκτός παιχνιδιού με στόχο να αυξήσει το εσωτερικό και εξωτερικό κίνητρο των χρηστών, να τους βοηθήσει να επεξεργαστούν πληροφορίες, να επιτύχουν καλύτερα τους στόχους ή/και να αλλάξουν τη συμπεριφορά τους"*. Παράλληλα, έχουν προταθεί και άλλοι ορισμοί για την παιχνιδοποίηση, όπως ότι είναι μία διαδικασία "game-thinking" και "game mechanics" με σκοπό την εμπλοκή των παικτών και την επίλυση προβλημάτων, ότι σχετίζεται περισσότερο με τα στοιχεία του παιχνιδιού μίας δραστηριότητας παρά με το παιχνίδι, κ.α.. Η σχετική βιβλιογραφία έχει αναπτυχθεί αρκετά τα τελευταία χρόνια (Treiblmaier et al.(2018); Karagiannis et al.(2020)).

Επιπλέον, σύμφωνα με τους Treiblmaier et al.(2018), είναι σημαντικό να γίνει γνωστό ότι τα παιχνίδια σοβαρού σκοπού (serious games) αποτελούν μία εξειδικευμένη κατηγορία παιχνιδιών τα οποία εκτός από την ψυχαγωγία των παικτών επιδιώκουν και άλλους διαφορετικούς στόχους όπως την εκπαίδευση, στόχους σχετικούς με την πολιτική κ.α.. Επίσης, προσομοιώνουν τις περισσότερες φορές διαδικασίες ή γεγονότα του πραγματικού κόσμου. Συμπερασματικά, το παιχνίδι σοβαρού σκοπού είναι παιχνίδι το οποίο προσομοιώνει καταστάσεις του πραγματικού κόσμου, περιλαμβάνει στοιχεία τα οποία δεν έχουν τα αμιγώς ψυχαγωγικά παιχνίδια και έχει διάφορους στόχους. Υποκατηγορία των παιχνιδιών σοβαρού σκοπού αποτελούν τα εκπαιδευτικά παιχνίδια, τα οποία συμβάλλουν στην απόκτηση γνώσεων ή/και δεξιοτήτων μέσω του παιχνιδιού και έχουν συγκεκριμένο στόχο ο οποίος είναι η εκπαίδευση.

Επιπλέον, πολλοί ειδικοί ισχυρίζονται ότι ένα παιχνίδι σοβαρού σκοπού μπορεί να προσφέρει στους παίκτες αυξημένη αφοσίωση μέσα από τη διαδραστικότητα, τη χρηστικότητα, τη συνεργασία και τον ανταγωνισμό, στοιχεία τα οποία καλό θα ήταν να το διακρίνουν. Παράλληλα, τα παιχνίδια αυτά εκτός από τη μάθηση δίνουν έμφαση και

στη δέσμευση, στη συνεργασία, στην ίδια την ιστορία την οποία πραγματεύονται και στην ευαισθητοποίηση των παικτών (Thieu,2019).

2.2.3 Χρησιμότητα της παιχνιδοποίησης και της μάθησης μέσω παιχνιδιού και τα ζητήματα ηθικής

Σύμφωνα με τους Karagiannis et al. (2020), η παιχνιδοποίηση και η μάθηση μέσω παιχνιδιού (Game-Based Learning) αποτελούν σύγχρονες προσεγγίσεις μάθησης και περιβάλλοντα διδασκαλίας τα οποία ανταποκρίνονται στη θεωρία του Κονστρουκτιβισμού (Constructivism). Σύμφωνα με τον Κονστρουκτιβισμό, τα άτομα δημιουργούν τη γνώση και μαθαίνουν από αυτή. Ουσιαστικά στον Κονστρουκτιβισμό οι άνθρωποι μαθαίνουν μόνο εάν έχουν εσωτερικά κίνητρα και συμμετέχουν στην κατασκευή της γνώσης. Έτσι, γίνεται αντιληπτό, ότι η μάθηση μέσω παιχνιδιού και ιδιαίτερα μέσω ενός ψηφιακού παιχνιδιού (Digital Game-Based Learning) είναι ικανή να δημιουργήσει κίνητρα στα παιδιά για να μάθουν. Επιπρόσθετα, η χρήση οπτικοακουστικών στοιχείων και στοιχείων παιχνιδιού που μοιάζουν με τον πραγματικό κόσμο ενισχύει τη διαδραστικότητα του παίκτη με το περιβάλλον και έχει ως αποτέλεσμα να προάγεται η μάθηση μέσω της εμπειρίας, της αλληλεπίδρασης, της δημιουργίας κινήτρων και της ανάπτυξης δεξιοτήτων σκέψης.

Στόχος της μάθησης μέσω παιχνιδιού είναι να βοηθήσει τον εκπαιδευόμενο να επιτύχει ένα σύνολο μαθησιακών στόχων, μέσω της διαδραστικής εμπειρίας και της ανατροφοδότησης. Υπάρχουν όμως και ηθικά ζητήματα τα οποία θα ήταν ωφέλιμο να συζητηθούν. Η μάθηση μέσω σοβαρών παιχνιδιών επιτρέπει τη μαζική συλλογή δεδομένων σχετικά με τον εκπαιδευόμενο. Αυτά χρησιμοποιούνται για διάφορους σκοπούς, όπως η καταγραφή της προόδου του παίκτη, η ανατροφοδότηση κ.α. (Sandovar et al., 2016).

Τα δεδομένα, αυτά όμως, όπως υποστηρίζουν οι Sandovar et al. (2016), είναι εκτός του ελέγχου του παίκτη. Ένα παράδειγμα για το πόσα δεδομένα παράγονται και συλλέγονται από παιχνίδια είναι το ακόλουθο. Ένα παιχνίδι στρατηγικής πραγματικού χρόνου χρησιμοποιεί τα replay files για να ταξινομήσει τους παίκτες. Ακόμη και αυτά τα αρχεία να μην αποθηκεύονται, φαίνεται ότι το παιχνίδι έχει την ικανότητα να καταγράψει την παραμικρή αλληλεπίδραση του παίκτη με το παιχνίδι. Επίσης, στον χρήστη διατίθενται και στατιστικά δεδομένα τα οποία καθορίζουν την τρέχουσα κατάσταση του παίκτη στο παιχνίδι. Επομένως, γίνεται αντιληπτό ότι τα βιντεοπαιχνίδια

συλλέγουν, συγκεντρώνουν και αποθηκεύουν μεγάλους όγκους δεδομένων παικτών. Για παράδειγμα, στο παιχνίδι Doctor's Cure όλα τα δεδομένα που συλλέγονται για τη μέτρηση της μαθησιακής προόδου των μαθητών παρέχονται στον δάσκαλο. Άρα για να επιτευχθούν οι στόχοι του παιχνιδιού απαιτείται να δημιουργηθούν και να αποθηκευτούν πολλές πληροφορίες στο αρχείο καταγραφής επικοινωνίας μεταξύ μαθητή και δασκάλου. Μεγάλη συλλογή δεδομένων γίνεται σε πολλά παιχνίδια.

Τέλος, ένα άλλο σημείο στο οποίο πρέπει να δοθεί ηθική προσοχή κατά τον σχεδιασμό των σοβαρών παιχνιδιών είναι η μεταφορά των καταστάσεων του πραγματικού κόσμου στο παιχνίδι. Τα παιχνίδια σοβαρού σκοπού αναφέρθηκε ότι προσομοιώνουν εμπειρίες, επομένως η ακρίβεια των σεναρίων, των ενεργειών και των σχολίων μέσα στο παιχνίδι έχουν σημαντικό αντίκτυπο στο πόσο καλά μεταφέρονται οι καταστάσεις στο παιχνίδι (Sandovar et al., 2016).

2.2.4 Ηθικό πλαίσιο σχεδιασμού παιχνίδια σοβαρού σκοπού

Τα παιχνίδια, σύμφωνα με τους Sandovar et al., (2016), είναι περίπλοκα σχεδιασμένα συστήματα όπως περίπλοκη είναι και η μελέτη της ηθικής των ψηφιακών παιχνιδιών. Στα ψηφιακά παιχνίδια η εμπειρία του παίκτη καθορίζεται από τη σχεδίαση και την αλληλεπίδραση του με το παιχνίδι. Υπάρχουν πολλά διαδικτυακά παιχνίδια αλλά δεν είναι βέβαιο ότι όλα είναι ηθικά. Ένα ηθικό παιχνίδι ορίζει τις σχέσεις μεταξύ των παικτών και τα ηθικά όρια που είναι διατεθειμένοι να περάσουν ή όχι. Η ηθική του παιχνιδιού ορίζεται στη σχεδίαση. Αν το παιχνίδι είναι φτιαγμένο να ανταμείβει τον ηθικό παίκτη τότε ο παίκτης μπορεί να παίξει ηθικά. Εάν όμως το παιχνίδι ανταμείβει την ανήθικη συμπεριφορά και την ηθική όχι, τότε ο παίκτης μπορεί να έχει μία διαφορετική συμπεριφορά.

Το γεγονός ότι πολλά διασκεδαστικά παιχνίδια έχουν σχεδιαστεί με σκοπό την αύξηση του κέρδους, τα ξεχωρίζει από τα παιχνίδια σοβαρού σκοπού που στοχεύουν στο να αφυπνίσουν τον παίκτη προσομοιώνοντας εμπειρίες μέσα από έναν ενδιαφέροντα τρόπο μάθησης. Τις περισσότερες φορές τα παιχνίδια σοβαρού σκοπού επιδιώκουν να αλλάξουν την συμπεριφορά των παικτών και γι' αυτόν το λόγο χρειάζεται να διακρίνονται από υψηλό βαθμό ηθικής.

Όπως ειπώθηκε και προηγουμένως, η ηθική των παιχνιδιών ορίζεται στη σχεδίαση. Τα σοβαρά παιχνίδια χρειάζεται κατά τη σχεδίαση να ενσωματώνουν ηθικές

αξίες και όχι προκαταλήψεις. Επομένως, κατά τον σχεδιασμό πρέπει να λαμβάνονται υπόψιν δεοντολογικά ζητήματα και να γίνεται ηθική διαχείριση (Sandovar et al., 2016).

2.2.5 Συμπεράσματα

Υπάρχουν πολλά παιχνίδια τα οποία έχουν ως στόχο τη διασκέδαση των παικτών. Υπάρχουν όμως και παιχνίδια, τα παιχνίδια σοβαρού σκοπού, τα οποία εκτός από τη διασκέδαση επιδιώκουν και άλλους σκοπούς. Στην παιχνιδοποίηση και στη μάθηση μέσω παιχνιδιού χρησιμοποιούνται παιχνίδια σοβαρού σκοπού και αυτό έχει ως αποτέλεσμα να δημιουργούνται κίνητρα στους παίκτες να αποκτήσουν γνώσεις μέσα από αυτά. Η αλληλεπίδραση των παικτών με τα παιχνίδια σοβαρού σκοπού στα πλαίσια της παιχνιδοποίησης είναι ικανή να αναπτύξει τις δεξιότητες της σκέψης και να αλλάξει τη στάση των ατόμων απέναντι σε διάφορα σημαντικά ζητήματα.

2.3 Παιχνίδια σοβαρού σκοπού και Διαδίκτυο

2.3.1 Εισαγωγή

Λαμβάνοντας υπόψιν αυτά τα οποία αναφέρθηκαν προηγουμένως για την μάθηση μέσω παιχνιδιού, και κυρίως μέσω παιχνιδιών σοβαρού σκοπού, γίνεται αντιληπτό ότι αυτές οι προσεγγίσεις μάθησης έχουν μεγάλη αξία στον χώρο της εκπαίδευσης. Ο ρόλος του διδάσκοντα, ο οποίος επιθυμεί να εντάξει στα πλαίσια της διδασκαλίας του παιχνίδια σοβαρού σκοπού, είναι να καθοδηγεί και να βοηθά τα παιδιά να κατακτήσουν τη γνώση και να επιτύχουν τους στόχους τους (Karagiannis et al., 2020).

Τα παιχνίδια σοβαρού σκοπού μπορούν να αξιοποιηθούν ως συμπληρωματικό εργαλείο εκπαίδευσης σε διάφορα μαθήματα ανάλογα με τους σκοπούς και τις ηλικίες για τους οποίους καθένα από αυτά είναι κατασκευασμένο.

Ταυτόχρονα, σύμφωνα με τους Chadwick και Knight (2010), το διαδίκτυο είναι αδιαμφισβήτητα ένα απίστευτο εργαλείο. Παρέχει δυνατότητες επικοινωνίας, μάθησης, διασκέδασης μέσω παιχνιδιών και ψυχαγωγίας με περιεχόμενο από όλο τον κόσμο. Επίσης, είναι χρήσιμο και εύκολο. Αλλά δεν παρέχει μόνο ευκαιρίες, ελλοχεύει και κινδύνους. Ενδεικτικά, ο διαδικτυακός εκφοβισμός, η κλοπή ταυτότητας, οι απάτες, η έκθεση ανηλίκων σε ακατάλληλο περιεχόμενο, είναι κάποιοι από τους κινδύνους του διαδικτύου. Άρα το διαδίκτυο εκτός από χρήσιμο εργαλείο είναι και ένα επικίνδυνο μέρος κυρίως για τα παιδιά, μικρής ηλικίας, αλλά και για τους ενήλικες.

Είναι χρήσιμο, λοιπόν, να υπάρχει ψηφιακός γραμματισμός, ο οποίος μπορεί να πραγματοποιηθεί και μέσα από παιχνίδια ψηφιακού γραμματισμού, όπως υποστηρίζει ο DeJong (2020). Αυτό είναι χρήσιμο για άτομα τα οποία δεν έχουν εύκολη πρόσβαση στην τεχνολογία, ή δεν μπορούν εύκολα να εντοπίσουν τους πόρους. Επιπλέον, τα μικρά παιδιά και οι ηλικιωμένοι μέσα από παιχνίδια ψηφιακού γραμματισμού μπορούν να αποκτήσουν σημαντικές δεξιότητες.

2.3.2 Το πρόβλημα

Η τεχνολογία είναι αναπόσπαστο κομμάτι της καθημερινής ζωής των παιδιών και είναι γνωστό ότι εκτός από πολλά οφέλη κρύβει και κινδύνους. Είναι σημαντικό, λοιπόν, οι μαθητές να γνωρίζουν τόσο τους κινδύνους της τεχνολογίας όσο και τους κινδύνους που συνδέονται με αυτή. Οι κίνδυνοι αυτοί αναπτύσσονται σε σχετική βιβλιογραφία του Thieu (2019).

Σύμφωνα με τους Jaccheri et al. (2017), αν και η ψηφιακή παιδεία των παιδιών έχει αυξηθεί τα τελευταία χρόνια, μιας και η τεχνολογία είναι μέρος της ζωής τους, οι δεξιότητες της ψηφιακής ασφάλειας και του απορρήτου των παιδιών δεν είναι το ίδιο αναπτυγμένες. Η χρήση του διαδικτύου ως μέσο συλλογής και ανταλλαγής πληροφοριών και ιδεών, η ψυχαγωγία και η δικτύωση χρησιμοποιώντας τα μέσα κοινωνικής δικτύωσης προσφέρουν πολλές ευκαιρίες στους χρήστες. Όμως εκτός από ευκαιρίες ελλοχεύουν και κινδύνους.

Οι κίνδυνοι από τη χρήση του διαδικτύου είναι πολλοί και ποικίλοι. Οι διαδικτυακοί κίνδυνοι είναι ένα σύνολο εκούσιων ή ακούσιων εμπειριών οι οποίες αυξάνουν την πιθανότητα πρόκλησης βλάβης στον χρήστη. Τα ζητήματα απορρήτου και οι παραβιάσεις της ιδιωτικής ζωής, ο διαδικτυακός εκφοβισμός και η παρενόχληση, η εκμετάλλευση και η παιδική πορνογραφία είναι κάποιοι από τους κινδύνους του διαδικτύου οι οποίοι χρήζουν ιδιαίτερης προσοχής. Εύκολα συμπεραίνει κανείς ότι ευάλωτα σε αυτούς τους κινδύνους είναι τα παιδιά. Χρειάζονται υποστήριξη ώστε να μάθουν για τους πιθανούς κινδύνους και τις ενδεχόμενες απειλές που μπορεί να κρύβει το διαδίκτυο και έτσι να παραμένουν ασφαλή στον ψηφιακό κόσμο. Η ανάγκη για υποστήριξη επιβεβαιώνεται και από μελέτες οι οποίες αποδεικνύουν την ύπαρξη χάσματος της ψηφιακής γνώσης και της αντίληψης για την ιδιωτικότητα (Jaccheri et al. (2017); DeJong (2020)).

Όπως αναφέρθηκε και προηγουμένως οι ακατάλληλες συμπεριφορές στο διαδίκτυο χρήζουν ιδιαίτερης προσοχής κυρίως από τους νεαρούς. Οι Lareki et al. (2017) υποστηρίζουν ότι εντοπίζεται σε μεγάλο βαθμό το "Grooming" στα παιδιά, το "sexting" στους εφήβους αλλά και γενικότερα ο εθισμός των νεαρών στην τεχνολογία, το διαδίκτυο και τα μέσα κοινωνικής δικτύωσης. Όλα αυτά υποδεικνύουν ακατάλληλες συμπεριφορές, όπως δημοσίευση ακατάλληλων φωτογραφιών, επιβλαβών σχολίων κ.α., από τους νεαρούς που αυξάνουν τις πιθανότητες να εκτεθούν σε κίνδυνο και να πάθουν κάποια βλάβη. Χρειάζεται, λοιπόν, να γνωρίζουν τους κινδύνους και να μάθουν να τους αποφεύγουν.

Οι κίνδυνοι χωρίζονται σε χαμηλού κινδύνου ενέργειες, όπως περιήγηση σε πληροφορίες, ανάγνωση ειδήσεων, προβολή φωτογραφιών, επισκέψεις σε ταξιδιωτικούς και ιατρικούς ιστοτόπους. Επιπλέον, σε ενέργειες μέσου κινδύνου που είναι το άνοιγμα συνημμένων, τα e-mails με συνδέσμους, η λήψη παιχνιδιών κ.α.. Τέλος, σε μεγαλύτερου κινδύνου όπως είναι η αγορά από άγνωστο ιστότοπο, η κοινή χρήση κωδικών πρόσβασης, ο διαδικτυακός τζόγος κ.α.. Όμως οι έφηβοι δυσκολεύονται να διαχωρίσουν το μέγεθος των κινδύνων. Γι' αυτό προτείνεται να εντατικοποιηθεί η εκπαίδευση, σχετικά με τους κινδύνους στον κυβερνοχώρο, στα σχολεία (Lareki et al, 2017).

2.3.3 Αντιμετώπιση του προβλήματος με τη βοήθεια των παιχνιδιών σοβαρού σκοπού

Προηγουμένως υπογραμμίστηκε ότι τα παιχνίδια σοβαρού σκοπού υπάρχουν για να πετύχουν και άλλους στόχους εκτός από την ψυχαγωγία. Ο DeJong (2020) υπογραμμίζει την εκπαιδευτική τους αξία η οποία εκτείνεται και πέρα από το παιχνίδι. Επιπλέον, υποστηρίζει ότι τα παιχνίδια σοβαρού σκοπού δεν μπορούν να είναι απλές παραστάσεις αλλά πρέπει να περιλαμβάνουν και αξίες του παίκτη. Χρειάζεται να είναι καθοδηγούμενα από κανόνες αλλά ταυτόχρονα ελεύθερα και δημιουργικά.

Επαναληπτικά, οι νεαροί χρήστες της τεχνολογίας είναι ιδιαίτερα ευάλωτοι στους κινδύνους τους οποίους αυτή ελλοχεύει. Η έκθεση των νέων, ειδικά των παιδιών μικρής ηλικίας, στον κυβερνοχώρο τους εκθέτει και σε αρνητικές διαδικτυακές εμπειρίες και απειλές. Διαπιστώνεται ότι ο λόγος για τον οποίο είναι ιδιαίτερα ευάλωτοι είναι η έλλειψη καλής ψηφιακής ευεξίας (Allers et al., 2021).

Οι Allers et al. (2021) σημειώνουν ότι η ψηφιακή ευεξία ορίζεται ως η συνολική ευημερία του ατόμου καθώς αλληλεπιδρά με το περιεχόμενο σε ένα ψηφιακό

περιβάλλον και δεν εξαρτάται μόνο από τον τρόπο που το άτομο χρησιμοποιεί την τεχνολογία αλλά επηρεάζεται και από την ικανότητα του να εντοπίζει και να αντιμετωπίζει τους κινδύνους. Παράλληλα, η ψηφιακή ευεξία κάποιου χρήστη είναι υγιής σε μία ψηφιακή κοινωνία εάν ο χρήστης έχει τις ακόλουθες δυνατότητες οι οποίες διασφαλίζουν την ασφάλεια στον ψηφιακό κόσμο. Η υγιής σωματική και ψυχική ευεξία εξασφαλίζεται όταν ο χρήστης μπορεί:

- να διακρίνει τους ψηφιακούς κινδύνους από τις ευκαιρίες
- να ενεργεί υπεύθυνα σε διαδικτυακές καταστάσεις
- να ευθυγραμμίζει τη διαδικτυακή του συμπεριφορά με αξίες εκτός ψηφιακής σύνδεσης

Επίσης, σύμφωνα με τους Allers et al. (2021) είναι δύσκολη για τους νεαρούς, κυρίως για τα παιδιά προσχολικής ηλικίας, η έκθεση σε αυτούς τους κινδύνους καθώς δεν διαθέτουν τα αναγκαία εφόδια, γνώσεις και δεξιότητες, για να προστατευτούν. Αδιαμφισβήτητα υπάρχει αρκετό εκπαιδευτικό υλικό εστιασμένο στην ευαισθητοποίηση των χρηστών για την κυβερνοασφάλεια, όμως δεν ενδιαφέρει, συνήθως, ιδιαίτερα τα παιδιά μικρής ηλικίας. Αυτό έρχεται σε αντίθεση με το γεγονός ότι ο αριθμός των μικρών παιδιών που κάνουν χρήση του διαδικτύου ολοένα και αυξάνεται. Επομένως, αυξάνεται η έκθεση στους κινδύνους αλλά δημιουργείται και η δυνατότητα εκπαίδευσης τους μέσα από το διαδίκτυο. Η εκπαίδευση αυτή μπορεί να επιτευχθεί μέσω της χρήσης παιχνιδιών σοβαρού σκοπού τα οποία επιδιώκουν την προώθηση της ψηφιακής ευεξίας με βιώσιμο τρόπο, αξιοποιώντας το γεγονός ότι τα παιδιά μαθαίνουν παίζοντας παιχνίδια.

Σημασία έχει το παιχνίδι να είναι ένα καλό παιχνίδι, υποστηρίζει σε βιβλιογραφία του ο James (2009). Το καλό παιχνίδι χρειάζεται να έχει τα ακόλουθα χαρακτηριστικά. Πρώτον, να διακρίνεται από σεβασμό και ηθική. Ο σεβασμός αφορά την άμβλυνση των διαφορών, την ανεκτικότητα και την ευγένεια στους ανθρώπους. Η ηθική προϋποθέτει τη δυνατότητα ο άνθρωπος να μπορεί να σκέφτεται τις επιπτώσεις της δράσης του απέναντι στον εαυτό του αλλά και στους άλλους σε πολλαπλά επίπεδα. Δεύτερον, το ηθικό παιχνίδι οφείλει να διακρίνει ρόλους και ευθύνες. Οι παίκτες χρειάζεται να έχουν ρόλους μέσα από τους οποίους θα αναλαμβάνουν ευθύνες. Επίσης, απαραίτητο είναι να διαχωρίζεται ευδιάκριτα το εσωτερικό από το εξωτερικό, χρειάζεται οι παίκτες να γνωρίζουν ότι στο παιχνίδι παίζουν ρόλους και να γνωρίζουν τον εαυτό τους.

Συμπερασματικά, οι Allers et al. (2021) υποστηρίζουν ότι μία πιθανή λύση στο πρόβλημα της έλλειψης ψηφιακής ευεξίας είναι η χρήση παιχνιδιών σοβαρού σκοπού ως εκπαιδευτικά εργαλεία για την εισαγωγή εννοιών που σχετίζονται με την ασφάλεια στον κυβερνοχώρο.

2.3.4 Συμπεράσματα

Επιλογικά, ο διδάσκων θα ήταν ωφέλιμο να επιλέγει προσεγγίσεις μάθησης οι οποίες του επιτρέπουν να αξιοποιήσει τα σοβαρά παιχνίδια ως συμπληρωματικό εργαλείο εκπαίδευσης. Παράλληλα, η ψηφιακή παιδεία είναι πολύ σημαντική διότι το διαδίκτυο χρησιμοποιείται σε μεγάλο βαθμό από νεαρούς οι οποίοι μπορούν να αξιοποιήσουν τις ευκαιρίες που αυτό προσφέρει αλλά παράλληλα είναι ευάλωτοι απέναντι στους κινδύνους του. Γι' αυτό η χρήση ηθικών παιχνιδιών σοβαρού σκοπού σχετικών με την ασφάλεια και το απόρρητο στον κυβερνοχώρο ως εργαλείο εκπαίδευσης είναι πολύ σημαντική.

2.4 Ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο μέσω παιχνιδιών σοβαρού σκοπού

2.4.1 Εισαγωγή

Όπως αναφέρθηκε και στην προηγούμενη ενότητα οι κίνδυνοι στο Διαδίκτυο είναι πολλοί. Για την προστασία από τους κινδύνους οι χρήστες χρειάζεται να έχουν γνώσεις και δεξιότητες ασφάλειας στον κυβερνοχώρο. Κυβερνοασφάλεια είναι η προστασία ψηφιακών συστημάτων και περιουσιακών στοιχείων από εγκλήματα. Η κυβερνοασφάλεια ασχολείται και με την προστασία των δεδομένων από τη χρήση τους για εγκληματικούς σκοπούς, κάτι το οποίο την καθιστά πολύ δύσκολη. Η σχετική βιβλιογραφία έχει αναπτυχθεί τα τελευταία χρόνια (Hill Jr et al. (2020); Hendrix et al.(2016)).

Υπάρχουν πολλά παιχνίδια σοβαρού σκοπού τα οποία πραγματεύονται διάφορα θέματα κυβερνοασφάλειας, όπως η ευαισθητοποίηση για την ασφάλεια, η ασφάλεια δικτύων και ιστού, η κρυπτογραφία και η μηχανική ασφαλούς λογισμικού. Την παρούσα εργασία απασχολούν τα θέματα κυβερνοασφάλειας αναφορικά με την ευαισθητοποίηση για την ασφάλεια. Η επίτευξη κυβερνοασφάλειας με σκοπό τη μείωση των κινδύνων και του κόστους των εγκλημάτων στον κυβερνοχώρο είναι σαφής. Για να επιτευχθεί κυβερνοασφάλεια χρειάζεται οι άνθρωποι να είναι εκπαιδευμένοι, να γνωρίζουν

σύγχρονους τρόπους πρόληψης και να έχουν πρόσβαση σε σύγχρονα εργαλεία. Τα παιχνίδια σοβαρού σκοπού επιτρέπουν στους ανθρώπους να εκπαιδεύονται παίζοντας και έτσι να μάθουν για την ασφάλεια στον κυβερνοχώρο. Η σχετική βιβλιογραφία έχει αναπτυχθεί σημαντικά τα τελευταία χρόνια (Hill Jr et al. (2020); Hendrix et al. (2016)).

2.4.2 Εκπαιδευτικά Εργαλεία Πολυμέσων

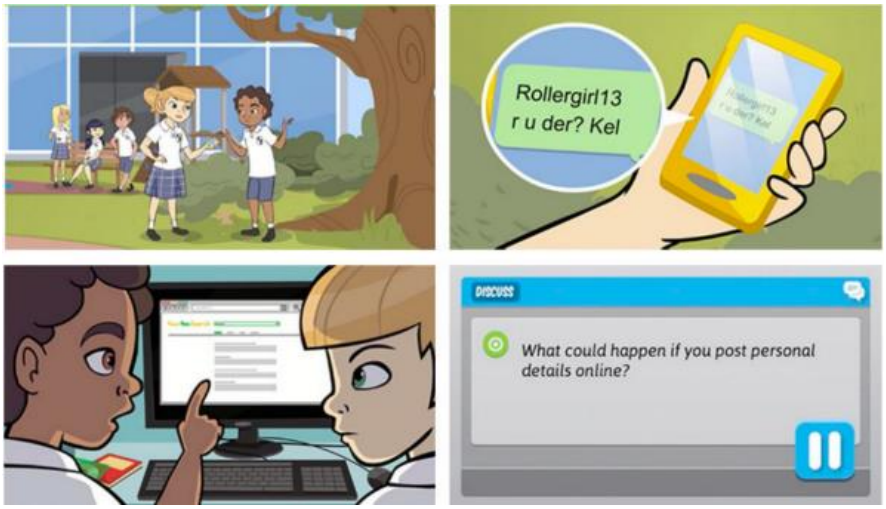
Σύμφωνα με τους Zhang-Kennedy και Chiasson (2021), τα εκπαιδευτικά εργαλεία πολυμέσων είναι μαθησιακό περιεχόμενο το οποίο χρησιμοποιεί περισσότερους από έναν τρόπους επικοινωνίας οι οποίοι μπορεί να περιλαμβάνουν συνδυασμό: κειμένου, εικόνων, ήχου, κινούμενων εικόνων, βίντεο και διαδραστικού περιεχομένου. Τα πολυμέσα αυτά έχουν την δυνατότητα να αυξήσουν τα κίνητρα, την δέσμευση και την κατανόηση του εκπαιδευτικού περιεχομένου του μαθητή.

Υπάρχουν πολλά τέτοια εργαλεία τα οποία αφορούν την ευαισθητοποίηση και την εκπαίδευση για την ασφάλεια στο κυβερνοχώρο. Ο ευρύτερα χρησιμοποιούμενος τύπος εκπαιδευτικών εργαλείων πολυμέσων είναι τα ψηφιακά παιχνίδια, συμπεριλαμβανομένων παιχνιδιών που βασίζονται στο διαδίκτυο και ηλεκτρονικών παιχνιδιών.

Διάφορα είδη παιχνιδιών έχουν σχεδιαστεί για να εξισορροπούν την εκπαίδευση με την ψυχαγωγία και το παιχνίδι. Υπάρχουν παιχνίδια κουίζ τα οποία μπορεί να είναι παραδοσιακά κουίζ έλεγχου γνώσης αλλά μπορεί να είναι εξελιγμένα σαν ερωτήσεις κουίζ που είναι ενσωματωμένες σε άλλες μορφές παιχνιδιών με σκοπό να αυξήσουν την αφοσίωση. Επιπλέον, έχουν δημιουργηθεί και παιχνίδια περιπέτειας τα οποία περιλαμβάνουν παιχνίδια ρόλων (RPG), παιχνίδια περιπέτειας όπου μπορεί κανείς να παίξει μόνος του, παιχνίδια δράσης και παιχνίδια περιπέτειας βασισμένα σε ιστορίες. Επιπρόσθετα, έχουν αναπτυχθεί παιχνίδια προσομοίωσης τα οποία τοποθετούν τους παίκτες σε περιβάλλοντα που έχουν ως στόχο την αναπαραγωγή καταστάσεων του πραγματικού κόσμου. Επίσης, υπάρχουν παιχνίδια στρατηγικής τα οποία εμπλέκουν τους χρήστες σε διαδικασίες λήψης αποφάσεων τακτικής με στόχο να ξεπεράσουν τις προκλήσεις που παρουσιάζονται στον κυβερνοχώρο. Τέλος, υπάρχουν και παιχνίδια δράσης αλλά και καρτών τα οποία ασχολούνται με θέματα του κυβερνοχώρου. Αξίζει να σημειωθεί ότι πολλά από αυτά τα παιχνίδια ταυτίζονται ρητά με το είδος του παιχνιδιού σοβαρού σκοπού. Τα ψηφιακά παιχνίδια συνδυάζουν παράγοντες όπως η διασκέδαση, η

ανατροφοδότηση, η δέσμευση, η επιλογή και η αφήγηση τα οποία μπορούν να συμβάλλουν στην επιτυχία τους.

Ένας ακόμη ευρέως χρησιμοποιούμενος τύπος εργαλείων πολυμέσων είναι οι ταινίες μικρού μήκους, βλέπε Εικόνα 2. Οι περισσότερες από αυτές είναι με τη μορφή κινουμένων σχεδίων δύο διαστάσεων, υπάρχουν και κάποιες οι οποίες είναι ζωντανής δράσης, αλλά και κάποιες τρισδιάστατες ελάχιστες, καθώς σπάνια χρησιμοποιούνται για εκπαίδευση στον κυβερνοχώρο. Οι περισσότερες από αυτές τις ταινίες απευθύνονται σε παιδιά και νεαρούς, πολύ λιγότερες είναι αυτές οι οποίες απευθύνονται σε ενήλικες. Κυρίαρχα θέματα αυτών των ταινιών μικρού μήκους είναι η προστασία των προσωπικών δεδομένων, ο διαδικτυακός εκφοβισμός και η κοινή χρήση εικόνων στο διαδίκτυο. Τα βίντεο αυτά μπορεί να συμπληρώνονται με δραστηριότητες και σχέδια μαθημάτων υπό την καθοδήγηση των δασκάλων. Συνοδευτικοί πόροι τους οποίους μπορεί να χρησιμοποιούν οι δάσκαλοι είναι οδηγοί διδασκαλίας, σχέδια μαθημάτων και άλλοι, πράγμα που υποδηλώνει ότι πρωταρχικός στόχος αυτών των ταινιών είναι να λειτουργούν υποστηρικτικά σε άλλες εκπαιδευτικές προσπάθειες. Ένα ακόμη χαρακτηριστικό αυτών των ταινιών είναι η μικρή τους διάρκεια, η οποία συμβάλλει στην αύξηση της γενικής ευαισθητοποίησης σχετικά με την ασφάλεια στο διαδίκτυο, την ψηφιακή ιθαγένεια, το διαδικτυακό απόρρητο και γενικότερα την ασφάλεια στον κυβερνοχώρο. Με αυτό τον τρόπο επιτυγχάνουν να προσελκύουν τους θεατές. Η μάθηση βασισμένη σε ταινίες έχει οδηγήσει σε μικτά αποτελέσματα κατά την αξιολόγηση της αποτελεσματικότητας. Ορισμένοι ερευνητές υποστηρίζουν ότι με αυτό τον τρόπο προάγεται η κατανόηση ενώ άλλοι ότι μπορεί να αποσπάται η προσοχή από την μαθησιακή δραστηριότητα και συχνά δεν μπορούν να γίνουν ακριβώς αντιληπτά λόγω της περιπλοκότητας ή της ταχύτητας τους. Επιπρόσθετα οι ταινίες δεν προωθούν την αλληλεπίδραση των παικτών με το περιεχόμενο και ανήκουν στην κατηγορία της παθητικής και όχι της ενεργητικής μάθησης. Ωστόσο, συνήθως λόγω της μικρής τους διαρκείας απαιτούν λιγότερο χρόνο από τους χρήστες σε σχέση με άλλα εκπαιδευτικά εργαλεία.



Εικόνα 2: Στιγμιότυπο οθόνης από το “Cybersmart Detectives”, που αποτελεί μέρος της σειράς κινουμένων σχεδίων “Cybersmart Challenge”

Ένας άλλος τύπος εκπαιδευτικών εργαλείων πολυμέσων είναι τα κόμικς. Δεν είναι πολλά σε αριθμό, κάποια είναι για ενήλικες κι άλλα για παιδιά και νεαρούς. Η πρώτη μεγάλη διαδικτυακή προσαρμογή κόμικς για την εκπαίδευση των τελικών χρηστών σχετικά με τους κινδύνους του διαδικτύου είναι το “Security Cartoons”, βλέπε Εικόνα 3. Το “Security Cartoons” δημιουργήθηκε το 2006 με στόχο να αυξήσει την ευαισθητοποίηση και την κατανόηση της ασφάλειας μέσω μίας σειράς σύντομων ασπρόμαυρων κόμικς που ασχολούνται με θέματα όπως το κακόβουλο λογισμικό, η πλαστογράφηση, το ηλεκτρονικό “ψάρεμα”, οι κωδικοί πρόσβασης και η φαρμακοβιομηχανία. Στα θετικά, τα κόμικς μπορούν να προσφέρουν μεγαλύτερη προσβασιμότητα, να συμβάλλουν στην αύξηση της απόδοσης των χρηστών, της κατανόησης και της απομνημόνευσης πληροφοριών ασφαλείας και απορρήτου. Επίσης, χρησιμοποιούνται και για την επισήμανση σημαντικών πληροφοριών απορρήτου σε μία διεπαφή χρήστη. Όμως, τις περισσότερες φορές πρωταρχικός στόχος είναι να ενημερώνουν τους χρήστες και όχι να τους εκπαιδεύουν.

Εικόνα 3: Δείγμα κόμικ από το "Security Cartoons"

Παράλληλα έχουν αναπτυχθεί και "Learning Modules". Ενδεικτικά της "MediaSmarts", το "AdverSmarts" της "Co-Co" με το χαρακτήρα δημητριακών, το "Co-CoCrunch", το "Click if You Agree" με τον χαρακτήρα ρομπότ και το "Privacy Pirates" με τον πειρατικό χαρακτήρα, που στοχεύουν στη βελτίωση του ψηφιακού γραμματισμού και της ψηφιακής παιδείας των παιδιών. Χαρακτηριστικό των μαθησιακών ενοτήτων είναι η ομαδοποίηση πληροφοριών σε κομμάτια που παρουσιάζονται διαδοχικά με σκοπό να βοηθήσουν την απορρόφηση των πληροφοριών από τον μαθητή και βασίζονται ιδιαίτερα στα πολυμέσα για την παροχή εκπαιδευτικού περιεχομένου. Επιπλέον, υποστηρίζουν τόσο την εξατομικευμένη όσο και τη συνεργατική μάθηση με αποτέλεσμα να είναι ιδιαίτερα κατάλληλα σε ένα πλαίσιο τάξης. Αυτό οφείλεται στο γεγονός ότι υπάρχουν πολλά συνοδευτικά εργαλεία και πόροι όπως οδηγοί δασκάλων, σχέδια μαθήματος κ.α.. Αξίζει να σημειωθεί ότι ενότητες μάθησης με διαδραστικά στοιχεία και δραστηριότητες μερικές φορές αναφέρονται ως παιχνίδια αλλά δεν είναι πραγματικά παιχνίδια υπολογιστή, καθώς δεν ενσωματώνονται μηχανισμοί παιχνιδιών που βασίζονται σε κανόνες. Χρησιμοποιούν όμως, μάθηση με βάση το παιχνίδι αυξάνοντας έτσι τα κίνητρα και τη δέσμευση.

Ταυτόχρονα, έχει αναπτυχθεί και ένας άλλος τύπος εργαλείων πολυμέσων τα επιτραπέζια παιχνίδια σχετικά με την ασφάλεια στο κυβερνοχώρο και το απόρρητο. Τα περισσότερα από αυτά χρειάζεται να φορτωθούν, να εκτυπωθούν και να συναρμολογηθούν, υπάρχουν όμως και κάποια σε ψηφιακές εκδόσεις. Όλα είναι παιχνίδια τα οποία μπορούν να παιχτούν από πολλούς παίκτες. Αυτό το πολυμέσο ενθαρρύνει τη συνεργατική μάθηση και τη συζήτηση. Ένα ενδεικτικό επιτραπέζιο παιχνίδι είναι "Control-Alt-Hack", βλέπε Εικόνα 4, το οποίο επικεντρώνεται σε 56

αποστολές που εισάγουν τους παίκτες, οι οποίοι έχουν το ρόλο των ηθικών χάκερς, σε διάφορες έννοιες ασφαλείας. Τα επιτραπέζια με την παραδοσιακή τους μορφή έρχονται σε αντίθεση με τα ψηφιακά παιχνίδια στο γεγονός ότι μπορούν και υποστηρίζουν φυσικές αλληλεπιδράσεις μεταξύ των παικτών. Ένα παιχνίδι το οποίο βρίσκεται σε έναν συγκεκριμένο χώρο είναι πιο πιθανό να ανταποκριθεί στις προσδοκίες των παικτών για κοινωνική αλληλεπίδραση σε σχέση με τα διαδικτυακά παιχνίδια πολλών παικτών. Επιπλέον, τα επιτραπέζια παιχνίδια είναι πιο προσιτά από τα ψηφιακά καθώς μπορούν να παιχτούν και από άτομα με χαμηλή γνώση υπολογιστών και είναι πιο φτηνά στην χρήση τους στην τάξη καθώς δεν απαιτούν εργαστήριο υπολογιστών.

Εικόνα 4: Σετ παιχνιδιού “Control-Alt-Hack”και τράπουλα.

Την παραπάνω βιβλιογραφία για τα εκπαιδευτικά εργαλεία πολυμέσων έχουν αναπτύξει οι Zhang-Kennedy και Chiasson (2021).

2.4.3 Ψηφιακή ευαισθητοποίηση των χρηστών με σκοπό την ηλεκτρονική ασφάλεια μέσω παιχνιδιών σοβαρού σκοπού

2.4.3.1 Εισαγωγή

Σύμφωνα με τους Allers et al. (2021), η κατανόηση του τρόπου διάδοσης της ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο στα παιδιά μπορεί να γίνει εάν αρχικά προσδιοριστεί ο τρόπος με τον οποίο τα παιδιά μαθαίνουν και αναπτύσσουν δεξιότητες. Τα παιδιά μαθαίνουν με πέντε τρόπους:

1. Παρατήρηση: Οπτική μάθηση μέσω παρατήρησης και μίμησης
2. Ακρόαση: Ακουστική μάθηση
3. Εξερεύνηση: Διερευνητική μάθηση
4. Πειραματισμός: Φυσική μάθηση μέσω δοκιμής και λάθους
5. Θέτοντας ερωτήσεις: Διερευνητική μάθηση

Αξίζει να σημειωθεί ότι τα παιδιά μαθαίνουν με διαφορετικούς τρόπους. Κάποια παιδιά ανταποκρίνονται καλύτερα για παράδειγμα μέσω της εξερεύνησης, ενώ άλλα μέσω της παρατήρησης και της ακρόασης. Σίγουρα όμως τα παιδιά και ιδιαίτερα αυτά της προσχολικής ηλικίας μαθαίνουν μέσω του παιχνιδιού. Το παιχνίδι αποτελεί για αυτά έναν διασκεδαστικό τρόπο μάθησης ανεξάρτητα από το ποια μέθοδο διδασκαλίας προτιμούν. Άλλωστε ένα κατάλληλα ρυθμισμένο παιχνίδι δεν χρειάζεται να χρησιμοποιεί αποκλειστικά μία μέθοδο μάθησης αλλά μπορεί να τις συνδυάζει όλες.

2.4.3.2 Το παιχνίδι “Happy Hippo” και η ψηφιακή ευεξία των μικρών παιδιών

Τα παιχνίδια σοβαρού σκοπού μπορούν να αξιοποιηθούν ως πρόσθετο μέσο μετάδοσης γνώσεων και ανάπτυξης δεξιοτήτων. Ωστόσο, σύμφωνα με τους Allers et al. (2021), είναι σημαντικό τα παιχνίδια τα οποία απευθύνονται σε παιδιά, ειδικά προσχολικής ηλικίας, να χαρακτηρίζονται από τέσσερα στοιχεία.

(α) Σαφείς και απλούς στόχους. Οι ξεκάθαρες οδηγίες έχουν ως αποτέλεσμα τα παιδιά να μην διακόπτουν το παιχνίδι.

(β) Ποιοτική ανατροφοδότηση και ανταμοιβές. Η ανατροφοδότηση ενθαρρύνει τα παιδιά όταν κάνουν κάτι ορθά και τα ειδοποιεί όταν κάνουν κάτι λάθος.

(γ) Δομή πρόκλησης. Εδώ λαμβάνεται υπόψη το επίπεδο απόδοσης των παικτών. Το επίπεδο πρόκλησης του παιχνιδιού θα πρέπει να προσαρμόζεται κατάλληλα ώστε να αυξάνεται η δυσκολία του ομαλά.

(δ) Αλληλεπίδραση που βασίζεται στην κίνηση. Αφορά τους φυσικούς τρόπους αλληλεπίδρασης των παιδιών με τις εφαρμογές (πχ οθόνες αφής).

Το παιχνίδι “Happy Hippo” εφαρμόζει αυτά τα τέσσερα στοιχεία. Το “Happy Hippo” είναι ένα παιχνίδι για κινητές συσκευές το οποίο χρησιμεύει ως μέθοδος προώθησης της ευαισθητοποίησης για την ψηφιακή ευεξία των παιδιών προσχολικής ηλικίας. Το παιχνίδι αποτελείται από τέσσερις κύριες σκηνές. Στην πρώτη, ο χρήστης αλληλεπιδρά με το κύριο μενού, βλέπε Εικόνα 5, και μπορεί να επιλέξει ποίημα, κουίζ και το παιχνίδι, που αυτά αποτελούν τις υπόλοιπες σκηνές. Αν ο χρήστης επιλέξει την

σκηνή ποίημα αυτό θα εμφανιστεί στην οθόνη, τα ποιήματα με ευχάριστο τρόπο επιδιώκουν να διαδώσουν στον χρήστη την ευαισθητοποίηση για τους κινδύνους στον κυβερνοχώρο. Τέλος, το ποίημα θέτει κάποια ερωτήματα προβληματισμού στον παίκτη (Allers et al., 2021).

Εικόνα 5: Το κύριο μενού του παιχνιδιού "Happy Hippo"

Έπειτα, αφού ο χρήστης απαντήσει στα ερωτήματα του ποιήματος εισέρχεται στην σκηνή του κουίζ. Μέσα από το κουίζ γίνεται αντιληπτό εάν ο χρήστης κατανοεί ή όχι το πρόβλημα που περιγράφεται στο ποίημα και καλείται να απαντήσει σε τέσσερα ερωτήματα. Η πρόοδος του χρήστη δεν εμποδίζεται, ανεξάρτητα από το αποτέλεσμα που θα φέρει στο κουίζ.

Εικόνα 6: Στιγμιότυπο από το παιχνίδι "Happy Hippo"

Στη συνέχεια ακολουθεί η τελευταία σκηνή του "Happy Hippo" η οποία είναι το παιχνίδι, βλέπε Εικόνα 6. Ο χρήστης ανάλογα με το ποίημα που επέλεξε στην σκηνή ποιήματος παίζει ένα mini παιχνίδι με αντίστοιχη θεματική. Το κάθε mini παιχνίδι είναι διαφορετικό και αποτελεί την τελική ανταμοιβή για την ολοκλήρωση των δύο προηγούμενων σκηνών. Όταν τελειώσει το παιχνίδι εμφανίζεται ένα μήνυμα που

ειδοποιεί τον παίκτη εάν κέρδισε ή έχασε και του δίνεται η επιλογή να ξαναπαίξει ή να επιστρέψει στο κύριο μενού.

Το παιχνίδι αξιολογήθηκε από ειδικούς οι οποίοι είχαν σε γενικές γραμμές θετική στάση απέναντι στο παιχνίδι, επισημαίνοντας ότι υπάρχουν περιθώρια βελτίωσης. Επομένως, το παιχνίδι στους κριτές είχε επιτυχία.

2.4.3.3 Ανάπτυξη δεξιοτήτων ηλεκτρονικής ασφάλειας των παιδιών μέσω του παιχνιδιού "Be smart when online!"

Η ηλεκτρονική ασφάλεια (e-safety), συμφωνα με τις Nicolaidou και Venizelou (2020), των μικρών παιδιών στο διαδίκτυο κεντρίζει το παγκόσμιο ενδιαφέρον. Ως ηλεκτρονική ασφάλεια ορίζεται η ικανότητα ενός ατόμου να ανταποκρίνεται αποτελεσματικά στις προκλήσεις και τις ευκαιρίες που προσφέρει το διαδίκτυο. Αποτελεί μια χρήσιμη δεξιότητα που χρειάζεται να γνωρίσουν τα παιδιά. Η σημαντικότητα της ηλεκτρονικής ασφαλείας αναγνωρίζεται παγκοσμίως, ενώ από το 2004 υπάρχει μία ημέρα αφιερωμένη στην ευαισθητοποίηση σχετικά με τα ζητήματα ηλεκτρονικής ασφαλείας, η "Ημέρα Ασφαλούς Διαδικτύου". Η ασφαλής χρήση του διαδικτύου συμβάλλει στην προστασία των παιδιών από τρεις σημαντικούς κινδύνους που σχετίζονται με τα προσωπικά δεδομένα, τον διαδικτυακό εκφοβισμό και το κακόβουλο λογισμικό.

Το "Be smart when online!", σύμφωνα με βιβλιογραφία των Nicolaidou και Venizelou (2020), στοχεύει στη βελτίωση των δεξιοτήτων ηλεκτρονικής ασφάλειας των παιδιών και στην ικανότητα παρακίνησης. Το παιχνίδι απευθύνεται σε παιδιά ηλικίας 11 με 12 ετών και χωρίζεται σε τρία μέρη. Στο πρώτο οι μαθητές απαντούν σε ένα κουίζ 20 ερωτήσεων-σεναρίων το οποίο επιδιώκει να τους βοηθήσει να αναγνωρίσουν τις υπάρχουσες γνώσεις τους. Στο δεύτερο μέρος υπάρχουν βίντεο, εικόνες, δραστηριότητες και περιοχή συζητήσεων με περιεχόμενο την προστασία των προσωπικών δεδομένων, την αποφυγή του διαδικτυακού εκφοβισμού και την προστασία από τους χάκερς. Εκεί οι μαθητές εξασκούνται και αναπτύσσουν τις δεξιότητες μέσα από τα διαδραστικά κουίζ και τα παιχνίδια. Στο τελευταίο μέρος υπάρχει ένα κουίζ, το οποίο μοιάζει με το αρχικό και επιθυμεί οι μαθητές να πετύχουν μεγαλύτερη βαθμολογία.

Επιλογικά, τα αποτελέσματα του παιχνιδιού έδειξαν ότι η απόδοση των μαθητών αυξήθηκε ως προς την ανάπτυξη των δεξιοτήτων ηλεκτρονικής ασφαλείας. Παράλληλα, οι μαθητές φάνηκαν ικανοποιημένοι από αυτό το μαθησιακό περιβάλλον. Δήλωσαν

επίσης κάποιοι από αυτούς ότι έμαθαν πολλά και σημαντικά πράγματα. Πολλοί δήλωσαν ότι δε χρειάστηκαν βοήθεια για να αλληλεπιδράσουν με το μαθησιακό περιβάλλον.

2.4.3.4 Το παιχνίδι "Internet Safety Game" και η ασφάλεια των μικρών παιδιών στο διαδίκτυο

Ένα παιχνίδι που είναι διαθέσιμο στην πλατφόρμα "Net Smart Kidz" είναι το "Internet Safety Game". Το "Internet Safety Game" είναι ένα διαδικτυακό παιχνίδι για την ασφάλεια στο διαδίκτυο και απευθύνεται σε μικρότερα παιδιά. Το παιχνίδι αποτελείται από ένα περιβάλλον που μοιάζει με επιτραπέζιο παιχνίδι, βλέπε Εικόνα 7. Σκοπός του παιχνιδιού είναι οι παίκτες να συλλέγουν διάφορα αντικείμενα στον πίνακα. Αυτά είναι μέρη πληροφοριών που διδάσκουν στον παίκτη στοιχεία σχετικά με το διαδίκτυο. Έξι είναι τα αντικείμενα που πρέπει να βρεθούν για να κερδίσει ο παίκτης το παιχνίδι. Το παιχνίδι διαπραγματεύεται γεγονότα σχετικά με την μη κοινοποίηση προσωπικών πληροφοριών, όπως όνομα, ηλικία κ.α., στο διαδίκτυο. Πληροφορίες σχετικές με το παιχνίδι αυτό υπάρχουν σε βιβλιογραφία των Roepke και Schroeder (2019).

Εικόνα 7: Στιγμιότυπο από το παιχνίδι "Internet Safety Game"

2.4.3.5 Διδασκαλία του "e-Safety" μέσω του παιχνιδιού "Cyber Smart"

Σύμφωνα με τους Underhay et al.(2016), οι σημερινοί μαθητές είναι πολύ πιθανό να αποτελέσουν θύματα απειλών στον κυβερνοχώρο και γι᾽ αυτό είναι πολύ σημαντικό να γνωρίζουν πως να προστατεύονται. Επίσης, η ενασχόληση με βιντεοπαιχνίδια συμβάλλει στη συγκέντρωση των παιδιών, στη δυνατότητα λήψης αποφάσεων, στην

απόκτηση δεξιοτήτων επίλυσης προβλημάτων, στη λογική σκέψη, τη δημιουργικότητα, την ομαδικότητα και την απόκτηση γνώσεων υπολογιστή.

Καταρχάς, οι μαθητές μπορεί να γίνουν θύματα απειλών διότι δεν γνωρίζουν, οι περισσότεροι, ποιες πληροφορίες ευαίσθητες αποθηκεύουν τα συστήματα υπολογιστών και σε ποιό σημείο του συστήματος είναι αποθηκευμένες. Ταυτόχρονα, το παιχνίδι είναι ένα εύκολα αποδεκτό από τους μαθητές μέσο απόκτησης νέων δεξιοτήτων και εφαρμογής της υπάρχουσας γνώσης. Έτσι, μελετήθηκε ένα παιχνίδι το "Cyber Smart" για την ευαισθητοποίηση σχετικά με το "e-Safety" (ηλεκτρονική ασφάλεια). Προτού οι μαθητές-δείγμα εκτεθούν στο παιχνίδι θα χρειαστεί να απαντήσουν ένα ερωτηματολόγιο έρευνας που θα χρησιμοποιηθεί για τη συλλογή δεδομένων σχετικά με το τι γνωρίζει ένα δείγμα φοιτητών για το "e-Safety" και τα μέτρα που εφαρμόζουν για να προστατεύουν τον εαυτό τους. Στο "e-Safety" και το "Cyber Smart"αναφέρονται σε βιβλιογραφία τους οι Underhay et al.(2016).

Το "Cyber Smart" επιδιώκει ο παίκτης αφού παίξει να ευαισθητοποιηθεί σχετικά με το "e-Safety". Το "Cyber Smart" έχει ως σκηνικό το γραφείο του διαχειριστή συστήματος. Οι παίκτες ως διαχειριστές, χρησιμοποιούν τον υπολογιστή και πειραματίζονται σε θέματα σχετικά με την εφαρμογή του "e-Safety" στο εργαστήριο. Για να νικήσει κανείς στο "Cyber Smart" πρέπει να περάσει όλες τις ενότητες εκμάθησης και να προστατέψει τα δίκτυα και τα συστήματα.

Επιλογικά, διαπιστώθηκε, από τους Underhay et al.(2016), ότι τα παιχνίδια ρόλων στα οποία οι παίκτες αναλαμβάνουν τον ρόλο του διαχειριστή συστήματος που είναι υπεύθυνος για την ασφάλεια και την προστασία δικτύων και συστημάτων είναι πιο δημοφιλή.

2.4.3.6 Το δωμάτιο απόδρασης, "CySecEscape", για την ασφάλεια στον κυβερνοχώρο

Σύμφωνα με τους Löffler et al. (2021), τα τελευταία χρόνια διάφορες διαδραστικές προσεγγίσεις μάθησης έχουν σχεδιαστεί. Μία πολλά υποσχόμενη είναι η προσέγγιση μέσω "escape room". Τα δωμάτια απόδρασης επιδιώκουν την ψυχαγωγία των παικτών μέσα από ομαδική συνεργασία για την αντιμετώπιση διάφορων προκλήσεων οι οποίες μοιάζουν με τον πραγματικό κόσμο. Σε αυτό το δωμάτιο απόδρασης στόχος είναι η αντιμετώπιση προκλήσεων ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο των μικρομεσαίων επιχειρήσεων.

Για την κατασκευή του δωματίου απόδρασης, “CySecEscape 2.0”, αναλύθηκε ο σχεδιασμός των αιθουσών διαφυγής και εντοπίστηκαν τα υπάρχοντα δωμάτια διαφυγής στον τομέα της κυβερνοασφάλειας. Στα δωμάτια απόδρασης οι συμμετέχοντες σχηματίζουν μία ομάδα που προσπαθεί να λύσει γρίφους με τη βοήθεια ενδείξεων και στρατηγικών για να ξεφύγουν από μία περιορισμένη περιοχή σε ένα δεδομένο χρονικό διάστημα. Για την κατασκευή αυτού το παιχνιδιού αναλύθηκαν οι προκλήσεις που αντιμετωπίζουν οι μικρομεσαίες επιχειρήσεις σχετικά με την κυβερνοασφάλεια και ποιες επιπτώσεις έχουν σε αυτές. Το “CySecEscape” ξεκίνησε ως φυσικό δωμάτιο διαφυγής (πρώτη έκδοση), και εξελίχθηκε, λόγω του Covid-19, σε εικονικό (δεύτερη έκδοση). Στους παίκτες παρουσιάζεται η απεικόνιση ενός γραφείου με πολλά αντικείμενα τα οποία μπορούν να μεγεθύνουν, να χειριστούν κ.α.. Επιπλέον, υπάρχει ένα σύνολο δολωμάτων τα οποία κάνουν το παιχνίδι πιο ενδιαφέρον και πιο δύσκολο. Παράλληλα εκτός από την προβλεπόμενη ροή του παιχνιδιού υπάρχει και μία άλλη διαδρομή που μπορεί να ακολουθήσει ο παίκτης για να μάθει πιο εξειδικευμένες γνώσεις. Το παιχνίδι φέρνει τους παίκτες αντιμέτωπους με πραγματικές περιπτώσεις παραβίασης ενός υπολογιστή, όπως ότι η ανάκτηση ενός κωδικού πρόσβασης από τον πηγαίο κώδικα καταδεικνύει την ανάγκη για ασφαλή αποθήκευση κωδικού πρόσβασης μέσω κατακερματισμού.

Το “CySecEscape”, βλέπε Εικόνα 8, απευθύνεται σε ιδιοκτήτες και εργαζομένους μικρομεσαίων επιχειρήσεων με βασικές γνώσεις πληροφορικής. Στόχοι του παιχνιδιού είναι (α) η ευαισθητοποίηση σχετικά με την ασφάλεια στον κυβερνοχώρο και (β) οι συμμετέχοτες να μάθουν τα βασικά στοιχεία της ασφάλειας στο κυβερνοχώρο και τη δυνατότητα εφαρμογής τους. Η ιστορία είναι η διερεύνηση της οικονομικής απάτης σε μία μικρομεσαία επιχείρηση και επιδιώκεται η εύρεση του απατεώνα υπαλλήλου που έχει διαφύγει. Οι παίκτες καλούνται να σώσουν την επιχείρηση σταματώντας την τραπεζική μεταφορά που πραγματοποιεί αυτός ο υπάλληλος.

Εικόνα 8: Στιγμιότυπο από το παιχνίδι “CySecEscape”

Μετά την διττή αξιολόγηση προέκυψε ότι η προσαρμογή του φυσικού παιχνιδιού στον ψηφιακό κόσμο, μετά από λίγες αλλαγές, ήταν πετυχημένη. Επιπλέον, διαπιστώθηκε ότι οι παίκτες έμειναν συγκεντρωμένοι στην οθόνη και εστίασαν σημαντικά στο παιχνίδι. Τέλος, οι συμμετέχοντες αλληλεπίδρασαν με το παιχνίδι και μεταξύ τους δείχνοντας μεγάλο ενδιαφέρον για τις γνώσεις σχετικά με την κυβερνοασφάλεια και αποκτώντας την ικανότητα να τις μεταδώσουν σε άλλους (Löffler et al., 2021).

2.4.3.7 Το παιχνίδι “PASDJO” και οι κωδικοί πρόσβασης

Το “PASDJO” είναι ένα παιχνίδι όπου ο παίκτης βαθμολογεί ένα σύνολο κωδικών πρόσβασης και λαμβάνει ανατροφοδότηση σχετικά με την ποιότητα των κωδικών πρόσβασης. Το παιχνίδι είναι σύντομο και απλό αλλά παρουσιάζει ελλείψεις καθώς δεν αντιμετωπίζει ιδιαίτερα διεξοδικά το θέμα της ισχύος των κωδικών πρόσβασης. Δεν ασχολείται με τα πιθανά μοντέλα αντιπάλου και τους κινδύνους που προκύπτουν από κακούς κωδικούς πρόσβασης. Αυτό είχε ως αποτέλεσμα να μην αποκτώνται γνώσεις και δεξιότητες σχετικές με την κυβερνοασφάλεια (Roepke και Schroeder, 2019).

2.4.3.8 Το παιχνίδι “Security Requirement Education Game” (SREG) και η ασφάλεια στον κυβερνοχώρο

Το “Security Requirement Education Game (SREG)”, κατά τους Hill Jr et al. (2020), είναι ένα παιχνίδι καρτών για πολλούς παίκτες το οποίο επιδιώκει την ανάπτυξη της ασφάλειας στον κυβερνοχώρο. Το “SREG” είναι διαθέσιμο στα αγγλικά και στα κινεζικά. Το παιχνίδι προσομοιάζει ένα πραγματικό περιβάλλον με προβλήματα και παρακινεί τους παίκτες να γνωρίσουν έννοιες σχετικές με την ασφάλεια. Το παιχνίδι

υπόσχεται μέσα από έναν διασκεδαστικό τρόπο να μάθει στους παίκτες έννοιες σχετικές με την ασφάλεια. Τέλος αξιολογήθηκε θετικά από τους παίκτες οι οποίοι ισχυρίστηκαν ότι κατανόησαν την ύπαρξη των τρωτών σημείων και τις επιθέσεις που μπορεί να δεχτεί η ασφάλεια.

2.4.3.9 Το παιχνίδι "Internet Hero" με επίκεντρο το διαδίκτυο

Το "Internet Hero", κατά τους Hill Jr et al. (2020), επιθυμεί να διδάξει στον παίκτη την τεχνική και την κοινωνική βάση του τρόπου χρήσης του διαδικτύου. Επίσης, απευθύνεται σε παιδιά ηλικίας εννέα έως δώδεκα ετών. Ο παίκτης πρέπει να ολοκληρώσει μία σειρά mini παιχνιδιών τα οποία σχετίζονται με τέσσερις δυνατότητες χρήσης του Ιστού, το email, τα κακόβουλα προγράμματα, τα κοινωνικά δίκτυα και τους τύπους σύνδεσης. Οι παίκτες μπορούν να βγάλουν εις πέρας ένα παιχνίδι μόνο εάν κατανοήσουν τις βασικές πτυχές αυτών των τεσσάρων θεματικών. Το παιχνίδι δοκιμάστηκε σε 50 παιδιά και από τα αποτελέσματα προέκυψε ότι υπάρχουν περιθώρια βελτίωσης.

2.4.3.10 Το παιχνίδι "Pomega" με στόχο την ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο

Το "Pomega", κατά τους Hill Jr et al. (2020), είναι ένα παιχνίδι δύο διαστάσεων με στόχο την προώθηση της ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο. Συγκεκριμένα ασχολείται με πέντε θέματα που άπτονται της ευαισθητοποίησης για την ασφάλεια στον κυβερνοχώρο, το phishing, τους κωδικούς πρόσβασης, τα κοινωνικά δίκτυα, την ασφάλεια των κινητών τηλεφώνων και τη φυσική ασφάλεια.

Το "Pomega" δίνει τη δυνατότητα σύνδεσης σε πολλούς χρήστες και είναι μεταφρασμένο στα Αγγλικά και στα Ταϊλανδικά. Οι χρήστες μετά την ενασχόληση τους με το παιχνίδι έλαβαν πιστοποιητικό και αυτό αποτέλεσε παράγοντα που παρακίνησε τα παιδιά να ασχοληθούν με αυτό. Το παιχνίδι απονέμει τα πιστοποιητικά ανάλογα με την πρόοδο των παικτών. Τέλος, από τα αποτελέσματα της αξιολόγησης προέκυψε ότι όλοι οι χρήστες θα μπορούσαν να κερδίσουν υψηλές βαθμολογίες καθώς και ότι οι παίκτες έμειναν ικανοποιημένοι με την ιστορία και τη διεπαφή του "Pomega".

2.4.3.11 Το παιχνίδι "Cyber Air-Strike" και η κυβερνοασφάλεια

Το "Cyber Air-Strike", κατά τους Hill Jr et al. (2020), είναι ένα παιχνίδι δύο διαστάσεων το οποίο επιδιώκει να γνωρίσουν οι παίκτες την κυβερνοασφάλεια.

Ασχολείται με ζητήματα κυβερνοασφάλειας όπως οι επιθέσεις κακόβουλου λογισμικού, το phishing, οι ιοί, οι παραβιάσεις κωδικών πρόσβασης και τα μη εξουσιοδοτημένα δεδομένα. Στοχεύει στην ευαισθητοποίηση των παικτών στα προαναφερθέντα θέματα με διαδραστικό τρόπο.

Η ιστορία του "Cyber Air-Strike" είναι η ακόλουθη: οι παίκτες πρέπει να διανύσουν την πιο μεγάλη απόσταση αεροπορικώς προστατεύοντας το αεροπλάνο τους από τις επιθέσεις κυβερνοασφάλειας. Αυτό μπορούν να το καταφέρουν εάν αποφύγουν τους εχθρούς τους ή αν αξιοποιήσουν συμμάχους. Αξίζει να σημειωθεί ότι "Cyber Air-Strike" δεν έχει δοκιμαστεί σε πραγματικούς παίκτες.

2.4.3.12 Το παιχνίδι "Cyber Detective" και η κυβερνοασφάλεια

Το "Cyber Detective", κατά τους Hill Jr et al. (2020), είναι ένα παιχνίδι λήψης αποφάσεων τριών διαστάσεων. Ο παίκτης πρέπει να παίξει μία σειρά μικρών παιχνιδιών σχετικών με τη κοινή χρήση δεδομένων στα social media, το ηλεκτρονικό "ψάρεμα" και τη δημιουργία ισχυρών κωδικών πρόσβασης. Μετά το κάθε παιχνίδι αναλύεται αν η απόφαση του παίκτη ήταν σωστή ή λανθασμένη.

Στόχος του παιχνιδιού είναι η διδασκαλία της σημαντικότητας της ασφάλειας στον κυβερνοχώρο. Αυτό επιτυγχάνεται μέσα από την ενημέρωση του παίκτη σχετικά με τη συμπεριφορά και τις αποφάσεις του στο κάθε παιχνίδι. Το παιχνίδι δοκιμάστηκε σε εφήβους οι οποίοι διαπίστωσαν ότι αφού έπαιξαν το παιχνίδι απέκτησαν αρκετές γνώσεις σχετικές με την κυβερνοασφάλεια.

2.4.3.13 Το παιχνίδι "Gamified Approach"και οι επιθέσεις κυβερνοασφάλειας

Το "Gamified Approach", κατά τους Hill Jr et al. (2020), επιδιώκει να υποστηρίξει τους παίκτες στην απόκτηση δεξιοτήτων κυβερνοσφάλειας, προστασίας και αντιμετώπισης παραβιάσεων δεδομένων. Το "Gamified Approach" έχει στο επίκεντρο τον επιτιθέμενο. Συγκεκριμένα, στο παιχνίδι επιλέχθηκαν οκτώ τύποι εισβολέων οι οποίοι διακατέχονταν από τα εξής χαρακτηριστικά: κίνητρα, γνώσεις, δεξιότητες και πόρους. Οι οκτώ τύποι εισβολέων και τα χαρακτηριστικά αυτά ενώθηκαν με έξι επιχειρηματικές απόψεις οι οποίες ενίσχυαν αυτά τα χαρακτηριστικά και οδήγησαν στη δημιουργία "avatar" για το παιχνίδι. Το παιχνίδι αυτό επιδιώκει ο παίκτης μέσα από τα μάτια του εισβολέα να μάθει να αντιμετωπίζει μία επίθεση. Τέλος, χρειάζεται να αναφερθεί ότι το παιχνίδι δεν έχει δοκιμαστεί.

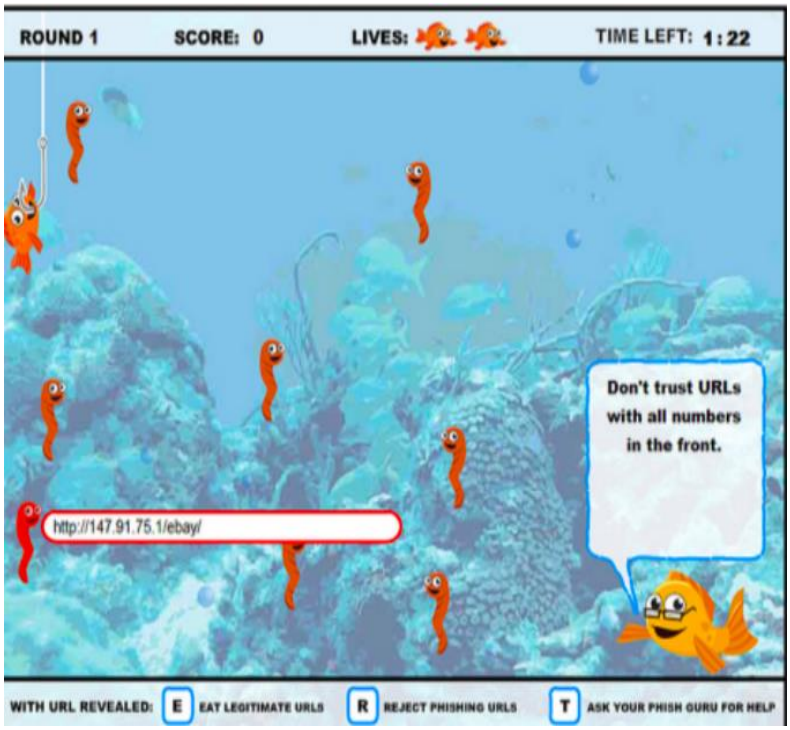
2.4.4 Το Ηλεκτρονικό "Ψάρεμα", το Hacking και τα παιχνίδια σοβαρού σκοπού

2.4.4.1 Το παιχνίδι "Anti-Phishing Educational Game"

Το "Anti-Phishing Educational Game" διδάσκει στους παίκτες πως να αναγνωρίζουν νόμιμες διευθύνσεις "URL" από ψεύτικες. Έτσι επιδιώκει να εκπαιδεύσει τους παίκτες να προλαμβάνουν επιθέσεις phishing. Επίσης, παρέχει συνεχή ανατροφοδότηση με σκοπό να παρακινεί τους χρηστές να βελτιώσουν τη συμπεριφορά τους απέναντι στις απειλές phishing (Hill Jr et al., 2020).

2.4.4.2 Το παιχνίδι "Anti-Phishing Phill"

Το "Anti-Phishing Phill" είναι ένα παιχνίδι το οποίο βασίζεται στον ιστό και διδάσκει στους χρήστες πώς να αναγνωρίζουν διευθύνσεις "URL" ηλεκτρονικού "ψαρέματός" (phishing). Το παιχνίδι αυτό είναι ένα από τα πιο αναγνωρισμένα εργαλεία για την ευαισθητοποίηση σε θέματα πρόληψης ηλεκτρονικού "ψαρέματός". Στο παιχνίδι ο παίκτης λαμβάνει τον ρόλο ενός νεαρού ψαριού, το οποίο ονομάζεται "Phill" και πρέπει να τρώει αληθινά σκουλήκια και να αποφεύγει τα ψεύτικα. Τα αληθινά σκουλήκια αντιπροσωπεύουν διευθύνσεις "URL" νόμιμων ιστοτόπων και τα ψεύτικα αντιπροσωπεύουν διευθύνσεις ηλεκτρονικού "ψαρέματός". Στο παιχνίδι υπάρχει και ο χαρακτήρας του πατέρα του "Phill", ο οποίος είναι ένα έμπειρο ψάρι, το οποίο συμβουλεύει τον παίκτη πώς να αναγνωρίσει τις επιθέσεις ηλεκτρονικού "ψαρέματός", βλέπε Εικόνα 9. Το παιχνίδι αποτελείται από τέσσερις γύρους με αυξανόμενη δυσκολία. Κάθε γύρος εστιάζει σε διαφορετικούς τύπους παραπλανητικών διευθύνσεων "URL". Η σχετική βιβλιογραφία έχει αναπτυχθεί από τους Hendrix et al. (2016) και Zhang-Kennedy και Chiasson (2021).



Εικόνα 9: Στιγμιότυπο από το παιχνίδι "Anti-Phishing Phill". Αριστερά φαίνεται ένα URL και δεξιά το ψάρι που δίνει συμβουλές

2.4.4.3 Το παιχνίδι "What.Hack"

Το "What.Hack", κατά τους Hill Jr et al. (2020), είναι ένα παιχνίδι λήψης αποφάσεων που στοχεύει να διδάξει στους μαθητές μεθόδους κατά του phishing αναπροσαρμόζοντας ρεαλιστικά σενάρια. Το παιχνίδι αναφέρεται σε τρία είδη ηλεκτρονικού "ψαρέματος": επίθεση τομέα, χειραγώγηση "URL" και κακόβουλο συνημμένο (similar domain attack, URL manipulation and malicious attachment). Το παιχνίδι απέφερε θετικά αποτελέσματα ως προς τη βελτίωση της ακρίβειας των παικτών στον εντοπισμό επερχόμενων απειλών.

2.4.4.4 Τα παιχνίδια "Hacknet" και "Uplink"

Το "Hacknet" (Karagiannis, 2022) είναι ένα παιχνίδι υπολογιστή προσομοίωσης Hacking που χρησιμοποιεί ένα Linux bash shell το οποίο αντιπροσωπεύει τα δίκτυα πραγματικού κόσμου και μία πραγματική υποδομή συστήματος. Εκτός από τις εντολές του Linux παρουσιάζεται και ένα σύνολο εργαλείων για δοκιμές διείσδυσης και ηθικό hacking. Συγκεκριμένα, είναι ένα παιχνίδι προσομοίωσης πειρατείας υπολογιστή που δείχνει περιπτώσεις πραγματικών δικτύων και συστημάτων πραγματικού κόσμου. Σε

αυτό παρουσιάζεται ένα σύνολο εργαλείων για ιατροδικαστικές δοκιμές και ηθική παραβίαση, παρόμοια με τα πραγματικά.

Το “Uplink” (Karagiannis, 2022) ασχολείται με την εκμάθηση εντολών δικτύου και τη συμπερίληψη ρεαλιστικών εντολών παρόμοιων με το UNIX μαζί με άλλη βασική ορολογία και χρησιμοποιείται για την εκμάθηση της ασφάλειας στον κυβερνοχώρο.

2.4.4.5 Το παιχνίδι “CyberCIEGE”

Το “CyberCIEGE”, προέρχεται από την “Naval Postgraduate School”, είναι διαθέσιμο για λήψη, και είναι ένα διαδραστικό περιβάλλον όπου οι παίκτες μαθαίνουν για την ασφάλεια του υπολογιστή και του δικτύου. Το “CyberCIEGE”, βλέπε Εικόνα 10, είναι ένα παιχνίδι που εστιάζει σε αμυντικές τακτικές κυβερνοασφάλειας στις οποίες οι συμμετέχοντες έχουν πρόσβαση σε ένα πραγματικό δίκτυο “VPN”. Η συσκευή αναπαραγωγής ενεργεί ως υπάλληλος μίας εταιρείας και υπεύθυνος για τη διαμόρφωση των τειχών προστασίας των “VPN” και άλλων συστημάτων που σχετίζονται με την ασφάλεια. Το παιχνίδι είναι περίπλοκο και έχει διάφορα σενάρια, όπως επιθέσεις που περιλαμβάνουν ιούς, δούρειους ίππους, κακόβουλα συνημμένα ηλεκτρονικού ταχυδρομείου κ.α.. Το παιχνίδι απευθύνεται σε παίκτες με δεξιότητες και γνώσεις cyber security.

Το “CyberCIEGE” επικεντρώθηκε στη γνώση και όχι τόσο στα σημεία εισόδου και στην πολυπλοκότητα. Το παιχνίδι στοχεύει στην αύξηση της ευαισθητοποίησης του εργατικού δυναμικού, προγραμματιστές συστημάτων, λογισμικού, σχεδιαστές συστημάτων και διαχειριστές δικτύου, για την ασφάλεια (Karagiannis (2022); Roepke και Schroeder (2019)).

Εικόνα 10: Στιγμιότυπο από το παιχνίδι “CyberCIEGE”

2.4.4.6 Το παιχνίδι “NITE Team 4” και οι επιθέσεις hacking

Το “NITE Team 4”, σύμφωνα με τον Karagiannis (2022), είναι και αυτό ένα παιχνίδι προσομοίωσης υπολογιστή σε θέματα κυβερνοασφάλειας. Η ιστορία του “NITE Team 4”, βλέπε Εικόνα 11, εξελίσσεται ως εξής: ο παίκτης είναι υπάλληλος μίας εταιρείας που προσλαμβάνει προσωπικό εργατικού δυναμικού ασφαλείας στον κυβερνοχώρο. Το παιχνίδι καλεί τον παίκτη μέσα από ένα αρχικό μήνυμα να αποκρούσει τις διάφορες κυβερνοεπιθέσεις που προέρχονται από χακαρίσματα με σκοπό να κάνει τον κόσμο καλύτερο. Το μήνυμα απεικονίζει την κατάσταση στην οποία μέσα από συμμετοχή σε πραγματικές υποθέσεις αποκτώνται δεξιότητες για την εκτέλεση και την απόκρουση κυβερνοεπιθέσεων. Οι παίκτες σε κάθε στάδιο του παιχνιδιού ανταμείβονται και έτσι έχουν κίνητρα να συνεχίσουν το παιχνίδι ενώ παράλληλα είναι εύκολο να αξιολογηθεί η πρόοδος τους.

Οι περισσότερες αποστολές που τίθενται στον παίκτη σχετίζονται με πραγματικές απειλές και κυβερνοαπειλές. Το παιχνίδι ασχολείται με τα ακόλουθα θέματα: (α) βασικές λειτουργίες τερματικού, (β) ψηφιακή εγκληματολογία, (γ) εισβολή δικτύου, (δ) διοίκηση και έλεγχος, (ε) εκπαίδευση Elite, (στ) ευφυΐα σήματος, (ζ) StringerOSAdvanced. Τα θέματα αναπτύσσονται σε τρία επίπεδα. Αρχικά, ο παίκτης γνωρίζει τις βασικές λειτουργίες τερματικού. Σε αυτό το επίπεδο αναπτύσσονται πρακτικές και αποστολές που βοηθούν τους συμμετέχοντες να μάθουν εργαλεία και εντολές και να εξοικειωθούν με το ψηφιακό περιβάλλον.

Εικόνα 11: Στιγμιότυπο από το παιχνίδι “NITE Team 4”

Έπειτα, στο δεύτερο επίπεδο ο παίκτης μαθαίνει για την ψηφιακή εγκληματολογία μέσα από θέματα όπως η συλλογή πληροφοριών, η απαρίθμηση

καταλόγων και οι επιθέσεις με κωδικό πρόσβασης. Στη συνέχεια, στο επίπεδο τρία ο παίκτης έρχεται σε επαφή με την ενότητα εισβολή δικτύου. Σε αυτό το επίπεδο μαθαίνει πληροφορίες σχετικά με την network infrastructure και τα exploitation tools.

Κατά τη διάρκεια του παιχνιδιού οι παίκτες έρχονται αντιμέτωποι με ρεαλιστικά σενάρια. Καλούνται να αναγνωρίσουν και να συλλέξουν πληροφορίες, να διεισδύσουν σε δίκτυο, να πραγματοποιήσουν διαδικτυακή σάρωση και να ξεκινήσουν επιθέσεις με κωδικό πρόσβασης. Επιπλέον, το "NITE Team 4" παρέχει ανατροφοδότηση στους παίκτες για τα ακόλουθα, (1) την προσοχή που έδειξαν στο παιχνίδι, (2) τη συνάφεια των προϋπαρχουσών γνώσεων με τον στόχο, (3) την αυτοπεποίθηση τους, (4) την αντιληπτή μάθηση, (5) τη σχέση με τον πραγματικό κόσμο και (6) την τεχνική συνάφεια με θεμελιώδη θέματα πληροφορικής.

Η αξιολόγηση του παιχνιδιού έδειξε ότι κάποιοι συμμετέχοντες σημείωσαν πολύ χαμηλή βαθμολογία, ενώ όσοι είχαν ισχυρή βασική γνώση θα μπορούσαν να κατανοήσουν πολλά θέματα κυβερνοασφάλειας που παρουσιάστηκαν στο "NITE Team 4". Επίσης, προέκυψε ότι η απόκτηση γνώσεων μέσα από το παιχνίδι μπορεί να επηρεάσει θετικά και άλλα θέματα πληροφορικής. Επιπρόσθετα, οι παίκτες φάνηκε να εξοικειώθηκαν με τις θεμελιώδεις έννοιες που πραγματεύεται το παιχνίδι. Επιπλέον, οι παίκτες συσχέτισαν σε μεγάλο βαθμό τα σενάρια του παιχνιδιού με την πραγματική ζωή.

Το παρόν παιχνίδι απέδειξε ότι η παιχνιδοποίηση παρακινεί τους μαθητές να ασχοληθούν με την ασφάλεια στον κυβερνοχώρο υπογραμμίζοντας μάλιστα την συναρπαστική της αξία. Οι περισσότεροι παίκτες υποστήριξαν ότι έμαθαν και απέκτησαν δεξιότητες μέσω του παιχνιδιού.

2.4.4.7 Το παιχνίδι προσομοίωσης hacking, "HackLearn" COFELET

Έχει παρατηρηθεί, κατά τους Katsantonis και Mavridis (2021), ότι χρειάζεται να ενισχυθεί η εκπαίδευση της ασφάλειας στον κυβερνοχώρο και ένας τρόπος για να γίνει αυτό είναι η μάθηση που βασίζεται στα παιχνίδια. Για τους σκοπούς αυτούς έχει προταθεί το Conceptual Framework for eLearning and Training (COFELET). Το COFELET καθορίζει τα κύρια στοιχεία που πρέπει να ληφθούν υπόψη για την ανάπτυξη αποτελεσματικών εκπαιδευτικών παιχνιδιών σοβαρού σκοπού κυβερνοασφάλειας, γνωστά και ως παιχνίδια COFELET. Το COFELET στοχεύει τα παιχνίδια να συνδυάζουν παιδαγωγικά στοιχεία και στοιχεία που αντιπροσωπεύουν τις ενέργειες του χρήστη με σκοπό την εκπλήρωση των στόχων των παιχνιδιών.

Με βάση το COFELET αναπτύχθηκε το παιχνίδι “HackLearn”, ένα παιχνίδι κυβερνοασφάλειας. Το “HackLearn”, βλέπε Εικόνα 12, είναι ένα παιχνίδι προσομοίωσης hacking, είναι ένα παιχνίδι σοβαρού σκοπού κυβερνοασφάλειας που βασίζεται σε σύγχρονες θεωρίες μάθησης και πρότυπα κυβερνοασφάλειας. Το “HackLearn” στοχεύει στην παροχή πρακτικών εμπειριών, κυρίως σε επιστήμονες της πληροφορικής, σχετικά με τη χρήση εργαλείων κυβερνοασφάλειας κ.α.. Κατά την πρώτη επαφή του παίκτη με το παιχνίδι παρουσιάζεται σε αυτόν ένα διαδραστικό σενάριο για να τον βοηθήσει να εξοικειωθεί με τη διεπαφή του παιχνιδιού. Το σενάριο που χρησιμοποιείται στο παιχνίδι στοχεύει να κάνει τον εκπαιδευόμενο να κατανοήσει και να εφαρμόσει τα περισσότερα από τα 7 στάδια του CKC μοντέλου για να κάνει μία επίθεση προηγμένης επίμονης απειλής.

Εικόνα 12: Στιγμιότυπο του “HackLearn” και εκμάθηση του hacking

Η αξιολόγηση του παιχνιδιού πραγματοποιήθηκε σε στάδια. Στο πρώτο τέθηκε ένα ερωτηματολόγιο στους παίκτες για να εκτιμηθούν οι υπάρχουσες γνώσεις τους σε θέματα κυβερνοασφάλειας. Στην αξιολόγηση μετά το παιχνίδι οι παίκτες έγραψαν μία αναφορά σχετική με τις δραστηριότητες του παιχνιδιού.

Επιλογικά, σύμφωνα με τα αναλυτικά στοιχεία του παιχνιδιού, ένα υψηλό ποσοστό των φοιτητών ασχολήθηκε με το παιχνίδι και πολλοί από αυτούς το έπαιξαν πολλές φορές για να αυξήσουν την απόδοση τους. Σύμφωνα με αυτούς το παιχνίδι συνέβαλε στην κατανόηση των θεμάτων που πραγματεύεται, είναι ενδιαφέρον, χρήσιμο και δημιουργεί κίνητρα ενασχόλησης. Πολλοί παίκτες του παιχνιδιού δήλωσαν ότι θα ήθελαν στα πανεπιστημιακά μαθήματα να παίζουν και παιχνίδια σοβαρού σκοπού, και συνεπώς προτιμούν να συμμετέχουν ενεργά αξιοποιώντας σύγχρονες μεθόδους διδασκαλίας παρά να είναι παθητικοί δέκτες πληροφοριών. Πολλοί είπαν ότι οι υπάρχουσες γνώσεις τους βοήθησαν να φέρουν εις πέρας τους στόχους του παιχνιδιού.

Γενικά, οι φοιτητές έμειναν αφοσιωμένοι στο παιχνίδι, παρακινήθηκαν και ικανοποιήθηκαν ιδιαίτερα.

2.4.5 Συμπεράσματα

Τα παιχνίδια σοβαρού σκοπού είναι ένας τύπος εργαλείου πολυμέσων και επιτρέπουν στους παίκτες να εκπαιδεύονται παίζοντας και έτσι να μάθουν για την ασφάλεια στον κυβερνοχώρο. Είναι σημαντικό να γίνει κατανοητό ότι τα παιδιά δεν μαθαίνουν όλα με τον ίδιο τρόπο. Άλλα μαθαίνουν καλύτερα μέσω της παρατήρησης και άλλα μέσω της εξερεύνησης. Γενικά όμως, τα παιχνίδια συνδυάζουν πολλές και διαφορετικές μεθόδους μάθησης και έτσι μπορούν να απευθύνονται σε μεγάλο σύνολο παιδιών.

Έχουν αναπτυχθεί διάφορα παιχνίδια τα οποία αφορούν την ψηφιακή ευαισθητοποίηση των χρηστών σχετικά με την κυβερνοασφάλεια. Κάποια απευθύνονται σε μικρά παιδιά, άλλα σε έφηβους και φοιτητές και άλλα σε ενήλικες. Επίσης, ορισμένα από αυτά έχουν δοκιμαστεί και αξιολογηθεί ενώ κάποια όχι. Πλειοψηφικά, από τις αξιολογήσεις προέκυψε ότι μέσα από τα παιχνίδια αυτά οι παίκτες μπορούν να αποκτήσουν ενδιαφέρουσες γνώσεις και να τις μεταδώσουν σε άλλους, μένοντας έτσι, σε γενικές γραμμές, ικανοποιημένοι.

Παράλληλα, έχουν αναπτυχθεί και παιχνίδια με θεματικές όπως το ηλεκτρονικό "ψάρεμα" αλλά και παιχνίδια με επίκεντρο το hacking. Και σε αυτές τις περιπτώσεις, πλειοψηφικά, τα παιχνίδια άφησαν ικανοποιημένους τους παίκτες και τους παρείχαν γνώσεις με διασκεδαστικό τρόπο. Αναφορικά με το hacking, κάποια από τα παιχνίδια είχαν καλύτερη απόδοση σε παίκτες με προϋπάρχουσες γνώσεις.

2.5 Ζητήματα απορρήτου

2.5.1 Εισαγωγή

Έχει διαπιστωθεί, από τον Thieu (2019), ότι οι γνώσεις των εφήβων-μαθητών για το απόρρητο είναι ελλιπείς με αποτέλεσμα το απόρρητο σήμερα να πλήττεται. Τα μέσα κοινωνικής δικτύωσης δεν περιλαμβάνουν πλέον μόνο προσωπικές πληροφορίες όπως το όνομα και η ηλικία αλλά πολλές περισσότερες τις οποίες ενδέχεται ο χρήστης να μην έχει παρατηρήσει.

Για παράδειγμα, σύμφωνα με τον Thieu (2019), πολλοί χρήστες, έφηβοι και μη, δεν παρατηρούν τις πληροφορίες που παρέχουν στο διαδίκτυο σχετικά με το γεωγραφικό

τους απόρρητο. Συγκεκριμένα, δεν γνωρίζουν ότι το Snapchat διαθέτει το “SnapMaps” το οποίο αποτελεί μία δυνατότητα γνωστοποίησης της γεωγραφικής τοποθεσίας που έχει μεγάλη πιθανότητα να παραβιάσει το απόρρητο. Το “SnapMaps”ενημερώνει την τρέχουσα τοποθεσία του χρήστη κάθε φορά που ανοίγει την εφαρμογή και την κάνει διαθέσιμη στην λίστα ανθρώπων που ο χρήστης έχει συμπεριλάβει στους διαδικτυακούς του φίλους. Ποιος όμως μπορεί να είναι σίγουρος ότι αυτές οι πληροφορίες δεν γίνονται γνωστές και σε κάποιον κακόβουλο ο οποίος βλέποντας ότι απουσιάζει ο χρήστης από το σπίτι δεν θα εισβάλει σε αυτό;

2.5.2 Τι είναι το απόρρητο και γιατί σχετίζεται με την ιδιωτική ζωή;

Ως ιδιωτικό απόρρητο, σύμφωνα με τον Thieu (2019), ορίζεται το δικαίωμα να είσαι μόνος ή ελεύθερος από παρεμβάσεις ή εισβολές. Παράλληλα, το απόρρητο των πληροφοριών είναι το δικαίωμα του κάθε ανθρώπου να ελέγχει τα προσωπικά του δεδομένα και τον τρόπο συλλογής και χρήσης τους. Γενικά, η ιδιωτική ζωή αναφέρεται στο δικαίωμα του να είσαι μόνος και ενδέχεται να αντιλαμβάνεται κανείς την ιδιωτικότητα με διαφορετικούς τρόπους.

Η διαφύλαξη του απορρήτου στην Ε.Ε., άρα και στην Ελλάδα, έχει έναν πολύ ισχυρό σύμμαχο, σύμφωνα με τον Thieu (2019), τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR). Ο GDPR έχει κατοχυρώσει, μεταξύ άλλων δικαιωμάτων, το δικαίωμα στους πολίτες να λαμβάνουν μετά από αίτημα όλες τις πληροφορίες τις οποίες έχει συλλέξει μία εταιρεία για αυτούς. Για παράδειγμα, ένας Γάλλος χρήστης της εφαρμογής γνωριμιών “Tinder”, ζήτησε από την εταιρεία να του στείλει τις πληροφορίες (προσωπικά δεδομένα) που κατέχει για αυτόν. Η εταιρεία του έστειλε 800 σελίδες με πληροφορίες, μέσα σε αυτές ήταν και όλες οι συνομιλίες που είχε πραγματοποιήσει ο χρήστης στο “Tinder”. Επιπλέον, αξίζει να αναφερθεί ότι η εταιρεία “IncludeSec”, μία από τις εταιρείες ασφαλείας του απορρήτου της “Tinder”, είχε αποκαλύψει ότι υπήρχε ευπάθεια στην εφαρμογή και ότι κάποιος χάκερ πολύ εύκολα μπορούσε να εντοπίσει την ακριβή τοποθεσία των χρηστών. Το πρόβλημα αυτό βέβαια έχει λυθεί, ενώ, όσο υπήρχε κανένας δεν το αξιοποίησε κακόβουλα. Επομένως, ποιος μπορεί να εγγυηθεί ότι αυτές οι πληροφορίες δεν ενδέχεται να διαρρεύσουν;

Συμπερασματικά, μπορεί εύκολα να διαπιστώσει κανείς ότι είναι σημαντική η ευαισθητοποίηση των ανθρώπων και ιδιαίτερα των ανηλίκων σχετικά με το απόρρητο. Αυτή η ανάγκη αποτελεί και το σημαντικότερο κίνητρο πίσω από τη δημιουργία

παιχνιδιών σοβαρού σκοπού με θέμα το απόρρητο. Όπως αναφέρθηκε και προηγουμένως, τα παιχνίδια σοβαρού σκοπού δεν επιδιώκουν αποκλειστικά να ψυχαγωγήσουν τον χρήστη αλλά και να τον προτρέψουν να αλλάξει τη συμπεριφορά του. Στην παρούσα ενότητα περιγράφονται παιχνίδια τα οποία στοχεύουν στην ευαισθητοποίηση των παικτών σχετικά με το απόρρητο.

2.5.3 Απόρρητο και παιχνίδια σοβαρού σκοπού

2.5.3.1 Εισαγωγή

Από έρευνες, σύμφωνα με τους Papaioannou et al. (2022), έχει διαπιστωθεί ότι οι χρήστες δεν γνωρίζουν πλήρως τα ζητήματα απορρήτου που μπορεί να προκύψουν κατά τη διαδικτυακή τους συμπεριφορά. Επομένως, έχουν διερευνηθεί διάφοροι τρόποι για την αύξηση της ευαισθητοποίησης σχετικά με το απόρρητο. Η ευαισθητοποίηση μπορεί να γίνει μέσω της ενημέρωσης των χρηστών σχετικά με πιθανές απειλές που μπορεί να προκύψουν όταν αποκαλύπτουν μεγάλο όγκο προσωπικών δεδομένων αλλά και μέσω της παροχής εξατομικευμένων προτάσεων απορρήτου.

2.5.3.2 Δωμάτιο απόδρασης για ζητήματα απορρήτου

Τα δωμάτια απόδρασης αποτελούν ένα πολλά υποσχόμενο είδος παιχνιδιού το οποίο μπορεί να αξιοποιηθεί και για εκπαιδευτικούς σκοπούς. Κύριος λόγος της δημοτικότητας τους είναι ότι αποτελούν παιχνίδια συνεργασίας και προκλήσεων. Για την επίτευξη των παραπάνω στόχων έχει προταθεί ένα δωμάτιο απόδρασης το οποίο επιδιώκει την καλλιέργεια της ικανότητας προστασίας της ιδιωτικής ζωής. Οι παίκτες κατά την εισαγωγή τους στο παιχνίδι λαμβάνουν πληροφορίες για την ιστορία μέσα από ένα βίντεο. Σε αυτό το βίντεο παρουσιάζεται ο κεντρικός χαρακτήρας της ιστορίας και αναπτύσσεται η πλοκή. Στο τέλος του βίντεο ένας από τους παίκτες ξυπνά ως χαρακτήρας στο βίντεο, ενώ ο άλλος (άλλοι) που παίζει σε διαφορετική οθόνη αναλαμβάνει τον ρόλο του “φύλακα αγγέλου”. Έπειτα το ρολόι μετράει αντίστροφα και καλεί τους παίκτες να σώσουν τον ήρωα μέσα σε 1 ώρα. Κατά τη διάρκεια του παιχνιδιού οι παίκτες απαντούν σε διάφορα τεστ δεξιοτήτων απορρήτου. Κάποιοι παίκτες κατά τη διάρκεια του παιχνιδιού βοηθούν άλλους με σκοπό να ολοκληρωθούν όλες οι εργασίες που έχουν ως στόχο την προστασία της ιδιωτικότητας του πρωταγωνιστή και τελικά αυτός να σωθεί.

Οι παίκτες, κατά τη διάρκεια του παιχνιδιού, επιδιώκεται να συνειδητοποιήσουν ποιες επιλογές τους ήταν λάθος και να τις διορθώσουν. Αν ο χρόνος τελειώσει και το παιχνίδι δεν έχει ολοκληρωθεί τότε οι παίκτες χάνουν και ο πρωταγωνιστής δεν καταφέρνει να σωθεί. Ο πρωταγωνιστής έχει οδηγηθεί στην αυτοκτονία γιατί έκανε διαδοχικά πολύ σοβαρά λάθη αναφορικά με την προστασία των προσωπικών του δεδομένων. Τα λάθη αυτά τον οδήγησαν στην πλήρη αποκάλυψη της ιδιωτικής του ζωής γι' αυτό και οι παίκτες χρειάζεται να κάνουν σωστές επιλογές ώστε ο ήρωας να μην οδηγηθεί στην απόγνωση. Οι άνω πληροφορίες συλλέχθηκαν από την εργασία των Papaioannou et al. (2022).

2.5.3.3 Το παιχνίδι "Privacy and Security Awareness Training Game"

Το παιχνίδι αυτό είναι ένα παιχνίδι εντοπισμού κινδύνου, στο οποίο ο παίκτης εντοπίζει ζητήματα απορρήτου και ασφάλειας σε ένα γραφείο (Solberg, 2018). Στο παιχνίδι ο παίκτης κάνει κλικ σε σημεία όπου τα πράγματα αποτελούν κίνδυνο απορρήτου ή ασφαλείας και στο τέλος του επιπέδου λαμβάνει μία ανατροφοδότηση για το πόσα εντοπίστηκαν σωστά και πόσα δεν ήταν κίνδυνοι. Ο παίκτης λαμβάνει σχόλια για κάθε κίνδυνο με αποτέλεσμα να μαθαίνει περισσότερες πληροφορίες για κάθε ζήτημα. Τέλος, το παιχνίδι είναι εμπορικό και απευθύνεται σε μεγαλύτερα ηλικιακά άτομα.

2.5.3.4 Το παιχνίδι "Interland - Be Internet Awesome"

Το "Interland – Be Internet Awesome" της Google, σύμφωνα με τους Nahmias et al (2020) περιλαμβάνει ένα πρόγραμμα σπουδών για δασκάλους, πόρους για γονείς και ένα διαδικτυακό παιχνίδι. Το "Interland – Be Internet Awesome" μαθαίνει στα παιδιά κάτι διαφορετικό για το διαδίκτυο, όπως ανησυχίες που σχετίζονται με το απόρρητο, την κοινή χρήση πληροφοριών, τη δημιουργία ισχυρών κωδικών πρόσβασης, τα πλαστά προφίλ και το phishing. Όμως, μετά από ανάλυση διαπιστώθηκε ότι το πρόγραμμα αυτό αν και καλά σχεδιασμένο αντιμετωπίζει κάποια κοινά θέματα ασφαλείας στο διαδίκτυο.

Πιο συγκεκριμένα, το "Interland – Be Internet Awesome", είναι ένα παιχνίδι τριών διαστάσεων το οποίο επιθυμεί να προετοιμάσει τα παιδιά να λαμβάνουν έξυπνες αποφάσεις στο διαδίκτυο. Το παιχνίδι φιλοδοξεί να ενισχύσει τους παίκτες να είναι ασφαλείς και επιτυχημένοι πολίτες στον διαδικτυακό κόσμο. Το παιχνίδι απευθύνεται σε παιδιά δημοτικού. Στο παιχνίδι οι παίκτες ηλικίας δευτέρας με έκτης δημοτικού, κυρίως, εξερευνούν τέσσερα πλωτά νησιά όπου το κάθε ένα από αυτά είναι ένα mini διαφορετικό

παιχνίδι. Επιδιώκει να διδάξει σε αυτά έννοιες όπως ο εκφοβισμός και η καταπολέμηση του, η σημασία ύπαρξης ισχυρών κωδικών πρόσβασης, το phishing και η προσεκτική δημοσίευση στο διαδίκτυο. Σχετική βιβλιογραφία έχει αναπτυχθεί τα τελευταία χρόνια (Hill Jr, et al. (2020); Solberg (2018); Nahmias et al. (2020)).

Σύμφωνα με τον Solberg (2018) το παιχνίδι εστιάζει σε πέντε θεμελιώδεις αρχές (α) μοιραστείτε με προσοχή, (β) μην παραπλανάσθε από ψεύτικα συμβάντα, (γ) προστατέψτε τα μυστικά σας, (δ) είναι ωραίο να είστε ευγενικοί και (ε) όταν έχετε αμφιβολίες να το λέτε. Με αυτό τον τρόπο το παιχνίδι επιδιώκει τα παιδιά να αναπτύξουν κριτική σκέψη, να προστατεύονται από διαδικτυακές απειλές, να μοιράζονται έξυπνα, να είναι ευγενικοί, να σέβονται και να ζητούν βοήθεια.

Επιπλέον, κάθε mini game δίνει την ευκαιρία στον παίκτη να πάρει κακές, καλές και λιγότερο καλές αποφάσεις. Η ύπαρξη διαφόρων λύσεων έχει ως αποτέλεσμα να δίνεται εποικοδομητική ανατροφοδότηση και να υπάρχει πρόοδος των παικτών. Επίσης, παρέχει πιστοποιητικό στους παίκτες μετά την ολοκλήρωση του. Σχετική βιβλιογραφία έχει αναπτυχθεί σημαντικά τα τελευταία χρόνια (Hill Jr, et al. (2020); Solberg (2018); Nahmias et al. (2020)).

2.5.3.5 Το παιχνίδι "Privacy Pirates"

Το "Privacy Pirates" είναι ένα παιχνίδι για παιδιά ηλικίας εφτά έως εννέα ετών που διδάσκει έννοιες σχετικές με το διαδίκτυο. Κατά τη διάρκεια του παιχνιδιού οι παίκτες λαμβάνουν ερωτήσεις σχετικά με το απόρρητο στο διαδίκτυο. Οι σωστές απαντήσεις δίνουν κομμάτια ενός χάρτη θησαυρού. Αυτό το παιχνίδι αποτελεί μία εισαγωγή στο γεγονός ότι οι προσωπικές πληροφορίες έχουν αξία (Solberg (2018).

Μέσα στο παιχνίδι ο παίκτης έχει πρόσβαση σε έναν χαρακτήρα που του παρέχει συμβουλές και ο οποίος είναι μέντορας του και τον παρακινεί όποτε χρειάζεται να ζητήσει βοήθεια από κάποιον να στραφεί σε έναν έμπιστο ενήλικα.

2.5.4 Η ασφάλεια και το απόρρητο των συσκευών

2.5.4.1 Το παιχνίδι "What Can Go Wrong?"

Έχουν αναπτυχθεί διάφορα παιχνίδια σοβαρού σκοπού τα οποία επιδιώκουν την διδασκαλία της ασφάλειας και του απορρήτου συσκευών. Ένα τέτοιο παιχνίδι είναι το "What Can Go Wrong?". Το "What Can Go Wrong?" είναι ένα παιχνίδι λήψης αποφάσεων για την ευαισθητοποίηση του παίκτη σχετικά με το απόρρητο και την

ασφάλεια στις κινητές συσκευές (Hill Jr et al., 2020). Τα ζητήματα που θίγει το συγκεκριμένο παιχνίδι αφορούν το κλείδωμα οθόνης, το phishing, κακόβουλα APKs (Android Packages), και άδειες εφαρμογών. Το παιχνίδι παίζεται από επιτραπέζιο υπολογιστή. Επίσης έχει αξιολογηθεί θετικά ως προς την επίτευξη του στόχου της ευαισθητοποίησης.

2.5.4.2 Το παιχνίδι "Make My Phone Secure!"και οι άδειες χρήσης

Ένα άλλο παιχνίδι που αφορά το απόρρητο του κινητού τηλεφώνου είναι το "Make My Phone Secure!" (Hill Jr et al., 2020). Το παιχνίδι κάνει χρήση τριών σεναρίων αδειών. Το πρώτο σενάριο είναι το "Instagram Hears My Conversations" στο οποίο η εφαρμογή ζητά να είναι ενεργή η λειτουργία του μικροφώνου επιδιώκοντας ενδεχομένως την αποστολή στον χρήστη στοχευμένων διαφημίσεων. Το δεύτερο σενάριο είναι το "Flashlight Could Steal My Data" στο οποίο η εφαρμογή φακού ζήτα πρόσβαση στον χώρο αποθήκευσης του χρήστη. Αυτή η άδεια χρήσης δύναται να επιτρέψει την υποκλοπή δεδομένων χρήσης. Το τρίτο σενάριο είναι το "Shoppingtogo Sends Spam Messages". Το σενάριο αυτό αφορά μία εφαρμογή αγορών η οποία ζητά άδεια πρόσβασης στα στοιχεία επικοινωνίας του χρήστη, ενώ δεν είναι απίθανο να πουλήσει τα στοιχεία επικοινωνίας του χρήστη σε τρίτο. Τέλος, το παιχνίδι αξιολογήθηκε από 20 παίκτες οι οποίοι διαπίστωσαν ότι διασκέδασαν και ενημερώθηκαν σχετικά με τα ζητήματα των σεναρίων.

2.5.4.3 Το παιχνίδι "Be Aware!" που αφορά την ασφάλεια και το απόρρητο συσκευών ATM

Επιπλέον, ένα ακόμα παιχνίδι το οποίο αφορά συσκευή είναι το "Be Aware!", το οποίο είναι ένα παιχνίδι επαυξημένης πραγματικότητας με θεματική την παραβίαση των "ATM" (Hill Jr et al., 2020). Η ιστορία εκτυλίσσεται γύρω από δύο παραβιασμένα "ATM" τα οποία εμφανίζονται μαζί με ένα τρίτο απαραβίαστο. Μέσω της επαυξημένης πραγματικότητας και της κίνησης του κινητού, ο χρήστης καλείται να εντοπίσει το μηχάνημα που δεν είναι παραβιασμένο. Έτσι το παιχνίδι κάνει γνωστές τις έννοιες του "Skimming", της χρήσης κάμερας και συσκευής "Skimming", για την κλοπή των στοιχείων της πιστωτικής κάρτας του θύματος, και του "Credit Card Skimming", της χρήσης συσκευής με σκοπό την κλοπή των στοιχείων της πιστωτικής κάρτας του θύματος. Τέλος, το παιχνίδι δεν έχει αξιολογηθεί.

2.5.4.4 Απόρρητο και έξυπνο ρολόι

Όπως έχει αναφερθεί και παραπάνω, δημοσκοπήσεις έχουν δείξει ότι ο κόσμος ανησυχεί για το απόρρητο, αλλά συχνά επιδεικνύει συμπεριφορά που θέτει τα δεδομένα του σε κίνδυνο. Αυτή η διαφορά μεταξύ της ανησυχίας και της γνωστοποίησης ονομάζεται παράδοξο της ιδιωτικής ζωής, το οποίο ορίζεται ως η ασυμφωνία μεταξύ της εκφρασμένης ανησυχίας και την πραγματικής συμπεριφοράς των χρηστών, και είναι μία κατάσταση που προέρχεται από την έλλειψη επίγνωσης. Αυτή η κατάσταση είναι ιδιαίτερα ανησυχητική σε ό,τι αφορά τα έξυπνα ρολόγια τα οποία είναι ακόμη καινούργια και όχι ιδιαίτερα γνωστά.

Τα έξυπνα ρολόγια προσφέρουν εντυπωσιακή λειτουργικότητα, παρέχουν διαδραστικές εφαρμογές και συνδέονται στο διαδίκτυο. Επιπλέον αποθηκεύουν πολλά και ποικίλα προσωπικά δεδομένα, όπως μηνύματα και στοιχεία επικοινωνίας. Είναι γεγονός όμως ότι οι χρήστες σπάνια χρησιμοποιούν τις διαθέσιμες ρυθμίσεις προστασίας απορρήτου. Γι᾽ αυτό και το παράδοξο της ιδιωτικότητας που αναφέρθηκε παραπάνω κυριαρχεί σε αυτή την τεχνολογία. Επειδή πολλές είναι οι μελέτες που έχουν προσπαθήσει να εκπαιδεύσουν τους χρήστες σε θέματα απορρήτου, και αυτό δεν έχει καταφέρει συχνά να αλλάξει την συμπεριφορά τους, τα παιχνίδια σοβαρού σκοπού μπορεί να το κάνουν καθώς ενσωματώνουν κίνητρα και διαδραστικότητα. Όμως τα παιχνίδια απορρήτου για smartwatches είναι σε έλλειψη. Οι παραπάνω πληροφορίες συλλέχθηκαν από την εργασία των Williams et al.(2019).

2.5.4.4.1 Το έξυπνο ρολόι “WearOS”

Την παραπάνω έλλειψη καλείται να καλύψει μία μελέτη, η οποία χωρίστηκε σε τρεις φάσεις, την προ-δοκιμή, το παιχνίδι και την μετά-δοκιμή (Williams et al, 2019). Στην πρώτη φάση, η οποία διήρκεσε 18 ημέρες παρακολουθήθηκαν οι βασικές ανησυχίες και συμπεριφορές των 10 συμμετεχόντων της έρευνας. Στη δεύτερη φάση η οποία διήρκεσε 16 ημέρες τα άτομα χωρίστηκαν σε δύο ομάδες, την treatment group και την control group, με τυχαίο τρόπο. Οι ομάδες έλαβαν ένα εξατομικευμένο παιχνίδι απορρήτου με προκλήσεις για την βελτίωση της συμπεριφοράς. Στην τρίτη και τελευταία φάση αυτή της μετά-δοκιμής, η οποία διήρκεσε 18 ημέρες, διερευνήθηκε εάν οι ενέργειες των συμμετεχόντων είχαν αλλάξει.

Συγκεκριμένα, την πρώτη ημέρα δόθηκε σε 10 άτομα ένα έξυπνο ρολόι “WearOS” (Android) στο οποίο εγκαταστάθηκε εφαρμογή παρακολούθησης. Μόλις

ολοκληρωθήκε η φάση παρακολούθησης, διάρκειας 18 ημερών, μοιράστηκε στους συμμετέχοντες ένα ερωτηματολόγιο ανησυχιών. Αυτή η αξιολόγηση πραγματοποιήθηκε στο στάδιο της προ-δοκιμής. Στην φάση του παιχνιδιού η ομάδα θεραπείας έλαβε ένα παιχνίδι με θέμα το απόρρητο και σκοπό την ενθάρρυνση της προστασία του. Παράλληλα, η ομάδα ελέγχου έλαβε το ίδιο παιχνίδι αλλά κλήθηκε να ασχοληθεί με την γενική χρήση του smartwatch, όπως την προσαρμογή της φωτεινότητας οθόνης.

Οι συμμετέχοντες είχαν την οδηγία να παίζουν το παιχνίδι τρεις φορές την ημέρα για 10 λεπτά κάθε φορά. Μετά την φάση του παιχνιδιού (16 ημέρες) ακολούθησε η φάση της μετά-δοκιμής. Σε αυτή τη φάση τα παιχνίδια απεγκαταστάθηκαν από τα ρολόγια και για 18 ημέρες παρακολουθήθηκε η συμπεριφορά απορρήτου των συμμετεχόντων. Έπειτα, στους συμμετέχοντες δόθηκαν παρόμοια ερωτηματολόγια με αυτά της προ-δοκιμασίας με στόχο να αναλυθεί εάν οι απόψεις των συμμετεχόντων άλλαξαν κατά τη διάρκεια της μελέτης. Έπειτα, έγιναν κάποιες συνεντεύξεις με σκοπό να διερευνηθεί το σκεπτικό της συμπεριφοράς των συμμετεχόντων και στη συνέχεια τα έξυπνα ρολόγια επιστράφηκαν και οι συμμετέχοντες αποζημιώθηκαν.

Αναφορικά με τα παιχνίδια, και τα δύο προκάλεσαν τους χρήστες να πλοηγηθούν σε ένα χάρτη ο οποίος μοιάζει με λαβύρινθο, βλέπε Εικόνα 13. Στο παιχνίδι ο παίκτης ξεκινάει από το σπίτι του και στη συνέχεια πρέπει να διασχίσει τέσσερα επίπεδα για να φτάσει τα καταστήματα. Στη διαδρομή συλλέγει νομίσματα για να αυξήσει την βαθμολογία του, ενώ όταν το παιχνίδι τελειώσει το σκορ κατατάσσεται σε ένα ανταγωνιστικό πίνακα κατάταξης. Κατά τη διάρκεια του ταξιδιού τους οι χρήστες συναντούν δύο τύπους χαρακτήρων (NPC) τους “χωρικούς” και τους “κλέφτες”. Οι πρώτοι κάνουν ερωτήσεις λειτουργικότητας και επιβραβεύουν σωστές απαντήσεις με πόντους. Οι “κλέφτες” μπλοκάρουν τη διαδρομή του χρήστη και προκαλούν προκλήσεις λειτουργικότητας στις οποίες οι χρήστες πρέπει να διαμορφώσουν ένα μενού ρυθμίσεων.

Εικόνα 13: Στιγμιότυπο από το παιχνίδι απορρήτου “WearOS”. Αριστερά ο χρήστης SAM παίζει το παιχνίδι σε λειτουργία “Morning” και δεξιά ο χρήστης BOB αντιμετωπίζει μία πρόκληση στην λειτουργία “Night”

Επιλογικά, η αξιολόγηση της μελέτης 52 ημερών του WearOs, και των παιχνιδιών του, έδειξε ότι η ομάδα θεραπείας άρχισε να λαμβάνει μεγαλύτερη δράση για την προστασία του απορρήτου της. Αντίθετα, η ομάδα ελέγχου δεν έδειξε τόση μεγάλη αλλαγή. Από την μελέτη διαπιστώθηκε ότι ένα άτομο δεν θα επενδύσει στο να προστατέψει τα δεδομένα του εκτός εάν αυτά θεωρηθούν πολύτιμα. Ακόμη όμως και αν επιθυμεί να τα προστατεύσει, το απόρρητο είναι κάτι που μπορεί εύκολα να παραβιαστεί. Επιπλέον, εντοπίστηκε ότι ενημερωμένοι χρήστες είναι πιθανό να θυσιάσουν τα δεδομένα τους για λόγους ευκολίας. Αν όμως κατανοήσουν τους κινδύνους μπορεί να κάνουν μία πιο προσεκτική επιλογή. Εν κατακλείδι, τα παιχνίδια smartwatch είναι ικανά να ενθαρρύνουν την προστασία του απορρήτου ως συμπλήρωμα σε μία γενικότερη προσπάθεια ευαισθητοποίησης (Williams et al.(2019); Hill Jr et al. (2020)).

2.5.5 Απόρρητο και γονείς

2.5.5.1 Εισαγωγή

Σύμφωνα με τους Manotipya et al. (2020), τα παιδιά που γεννιούνται στην σύγχρονη ψηφιακή εποχή έχουν ένα πλήρες ψηφιακό αποτύπωμα από την ηλικία των 2 ετών το οποίο συνεχίζεται καθ᾽ όλη τη διάρκεια της ζωής τους. Το προφίλ των παιδιών αυτών στο διαδίκτυο δημιουργείται από τους γονείς τους χωρίς τη συγκατάθεση των ίδιων, πράγμα που δεν τους δίνει τη δυνατότητα να προστατεύσουν το απόρρητό τους. Οι Manotipya et al. (2020) συμπληρώνουν ότι χρειάζεται να αναγνωριστεί το δικαίωμα

στα παιδιά να μην επιθυμούν να γνωστοποιηθούν τέτοιες πληροφορίες για αυτά ή ότι μπορεί να επιθυμούν να φτιάξουν το δικό τους ψηφιακό αποτύπωμα κατά την ενηλικίωση. Επίσης, σημαντικό πρόβλημα είναι το γεγονός ότι οι γονείς δεν γνωρίζουν ότι οι πληροφορίες που δημοσιοποιούν είναι ενδεχομένως επιβλαβείς για τα παιδιά τους.

2.5.5.2 Χρήσιμη ορολογία

Σε αυτή την υποενότητα θα αναφερθούν κάποιοι αξιοσημείωτοι όροι, σύμφωνα με τους Manotipya et al. (2020), όπως ο όρος "Sharenting" που χρησιμοποιείται για να απλοποιήσει τις ενέργειες των γονέων όταν δημοσιεύουν ή μοιράζονται τα προσωπικά στοιχεία των παιδιών τους στα κοινωνικά δίκτυα. Σε ότι αφορά αυτό εντοπίζεται μία σύγκρουση μεταξύ του ρόλου των γονέων ως φύλακες προσωπικών δεδομένων των παιδιών τους και ως αφηγητές των προσωπικών πληροφοριών τους.

Επίσης, ενδιαφέρουσα ορολογία είναι η "Digital Kidnapping" η οποία αποτυπώνει το γεγονός ότι οι γονείς δημοσιεύουν μερικές φωτογραφίες των χαριτωμένων παιδιών τους και οι άγνωστοι τις αποθηκεύουν για να τις χρησιμοποιούν στα δικά τους προφίλ σαν να είναι δικά τους παιδιά. Το "Digital Kidnapping" είναι μία μορφή ψηφιακής κλοπής η οποία εντοπίζεται δύσκολα, εκτός εάν κάποιος τυχαία βρεθεί στο προφίλ αυτού που έκλεψε τη φωτογραφία.

Επιπλέον, μία άλλη επικίνδυνη συμπεριφορά είναι αυτή κατά την οποία άγνωστοι αποθηκεύουν, αλλάζουν και δημοσιεύουν φωτογραφίες γυμνών παιδιών οι οποίες έχουν δημοσιευτεί από τους γονείς τους. Τέτοιες φωτογραφίες δεν είναι ενδεχόμενα ταπεινωτικές μόνο για τα παιδιά αλλά μπορεί να καταλήξουν σε ιστοτόπους παιδεραστών. Επομένως, μπορεί να συμπεράνει κανείς ότι τέτοιες αποκαλύψεις ενδέχεται να επηρεάσουν σε μεγάλο βαθμό αρνητικά το απόρρητο και την ασφάλεια των παιδιών.

2.5.5.3 Το παιχνίδι "Social Sim Parents" και οι γονείς

Το παιχνίδι "Social Sim Parents" έχει ως στόχο να εκπαιδεύσει τους γονείς μέσω της άμεσης εμπειρίας όταν επιλέγουν να μοιραστούν προσωπικά δεδομένα και φωτογραφίες που μπορεί να πλήξουν το απόρρητο (Manotipya et al., 2020). Το "Social Sim Parents" εξετάζει την ευαισθητοποίηση και τις γνώσεις των γονέων σχετικά με τις πληροφορίες που μοιράζονται στα κοινωνικά τους δίκτυα. Η διεπαφή του παιχνιδιού μοιάζει με μία διεπαφή ενός κοινωνικού δικτύου.

Το παιχνίδι περιλαμβάνει τη σελίδα καλωσορίσματος, τη σελίδα προφίλ, τα σενάρια, την αγαπημένη σελίδα, την κάρτα βαθμολογίας και την έρευνα. Το "SocialSimParents" ξεκινά ζητώντας από τον παίκτη να εγγραφεί. Έπειτα, κάνει "Sign-up" και βρίσκεται στο προφίλ του στο οποίο εισάγει πληροφορίες υποχρεωτικές και μη. Στη συνέχεια παρουσιάζονται στον παίκτη κάποια σενάρια που γίνονται πιο σοβαρά κατά τη διάρκεια του παιχνιδιού. Ενδεικτικά κάποια από τα διαβαθμισμένα σενάρια, το σενάριο 1 "Μόλις αγοράσατε ένα νέο σπίτι και θα θέλατε να πείτε στα κοινωνικά σας δίκτυα τα καλά σας νέα. Τα παιδιά σας επίσης μόλις ξεκινούν την πρώτη τους μέρα στο σχολείο ή στον παιδικό σταθμό.", το σενάριο 3 "Το παιδί σας επιτυγχάνει κάποια επιτεύγματα (απόκτηση άδειας οδήγησης) και θέλετε να μοιραστείτε τα νέα με άλλους. Είστε πολύ χαρούμενοι γι' αυτό και θέλετε να ανταμείψετε το παιδί και την οικογένειά σας κάνοντας όμορφες διακοπές." και το σενάριο 5 "Ανακαλύπτετε ότι το παιδί σας έχει διαγνωστεί με Μαθησιακές Δυσκολίες και ΔΕΠΥ. Πρέπει να φέρνετε το παιδί σας για θεραπεία μία φορά την εβδομάδα.". Μετά την ολοκλήρωση των 5 σεναρίων βλέπουν τη βαθμολογία τους και αφού κάνουν σχόλια για το παιχνίδι τότε αυτό ολοκληρώνεται.

Από τα αποτελέσματα του παιχνιδιού προέκυψε ότι οι περισσότεροι συμμετέχοντες αύξησαν με επιτυχία τα επίπεδα ευαισθητοποίησης τους σχετικά με το απόρρητο στο διαδίκτυο μετά τη συμμετοχή τους σε αυτή την προσομοίωση και οι περισσότεροι από αυτούς σκέφτηκαν να αλλάξουν τη διαδικτυακή τους συμπεριφορά.

2.5.6 Απόρρητο και κοινωνικά δίκτυα

2.5.6.1 Εισαγωγή

Τα κοινωνικά δίκτυα αποτελούν πλέον μέρος της ζωής των περισσοτέρων ανθρώπων. Κατά τους Pensa et al. (2019), περισσότεροι από δύο δισεκατομμύρια ενεργοί λογαριασμοί παράγουν petabytes δεδομένων συμπεριφοράς και αλληλεπίδρασης καθημερινά. Υπάρχει τεράστια διασύνδεση η οποία εκθέτει τους χρήστες στον κίνδυνο της διαρροής απορρήτου. Οι χρήστες χρειάζεται να ενημερωθούν για τους κινδύνους που συνδέονται με την αποκάλυψη των δεδομένων τους, ευαίσθητων και μη, αλλά και για την έκθεση της ιδιωτικής τους ζωής στα μέσα κοινωνικής δικτύωσης.

2.5.6.2 Εκτίμηση των κινδύνων απορρήτου στα κοινωνικά δίκτυα

Για να γίνει αντιληπτή η επικινδυνότητα της μη συνετής χρήσης του διαδικτύου αξίζει να αναφερθεί ένα παράδειγμα (Pensa et al., 2019). Η αποκάλυψη φωτογραφιών

κατά τη διάρκεια ενός ταξιδιού (από το ταξίδι) μπορεί να ειδοποιήσει πιθανούς διαρρήκτες και να αποτελέσει πηγή κάποιας αδικοπραξίας. Ένας, ακόμη, ανησυχητικός κίνδυνος είναι ότι η δραστηριότητα των χρηστών των κοινωνικών δικτύων μπορεί να αξιοποιηθεί για να προκύψουν ορισμένα χαρακτηριστικά της προσωπικότητας των χρηστών. Αυτή η δυνατότητα εξαγωγής συμπερασμάτων χρησιμοποιήθηκε για να βοηθήσει τον Ντόναλντ Τραμπ να νικήσει στις εκλογές των ΗΠΑ.

Αν και οι πλατφόρμες κοινωνικής δικτύωσης συχνά παρέχουν κάποιο είδος ειδοποίησης με σκοπό να ενημερώσουν τους χρήστες σχετικά με τους κινδύνους αποκάλυψης προσωπικών πληροφοριών, οι περισσότεροι απλώς τους παραβλέπουν (Pensa et al., 2019). Όμως στα μέτρα προστασίας της ιδιωτικής ζωής που έχουν προταθεί μέχρι στιγμής υπάρχει ένας ισχυρός περιορισμός. Αυτός αφορά τον κίνδυνο του απορρήτου ο όποιος δεν είναι θέμα μόνο των προτιμήσεων των χρηστών, αλλά επηρεάζεται και από τα χαρακτηριστικά του κοινωνικού δικτύου, δηλαδή τη θέση του χρήστη στο δίκτυο αλλά και τη στάση των φίλων του απέναντι στην ιδιωτικότητα. Όσες περιοριστικές ρυθμίσεις απορρήτου και αν έχει βάλει ο χρήστης εάν βρίσκεται σε ένα μη ασφαλές δίκτυο (δίκτυο που περιλαμβάνει κόμβους – φίλους οι οποίοι έχουν ελάχιστες ή καθόλου γνώσεις για την ιδιωτικότητα) τίθεται σε κίνδυνο και ο ίδιος. Επεξηγηματικά, όταν ένας χρήστης δημοσιεύει κάποια προσωπική του πληροφορία σε ένα υποδίκτυο όπου τα άτομα γνωρίζουν για το απόρρητο τους και των άλλων, ο κίνδυνος να διαδοθούν αυτές οι πληροφορίες, του πρώτου, είναι χαμηλός. Αντίθετα ένας χρήστης που δημοσιεύει κάτι σε ένα δίκτυο με άτομα τα οποία δε γνωρίζουν την ανάγκη ύπαρξης απορρήτου, ο κίνδυνος μεγαλώνει.

Με βάσει τα παραπάνω έχει προταθεί να υπάρχει μία βαθμολογία που ποσοτικοποιεί την διαρροή απορρήτου των χρηστών λαμβάνοντας υπόψιν τους κινδύνους που οφείλονται όχι μόνο στη στάση τους απέναντι στο απόρρητο αλλά και στην στάση του υποδικτύου τους (Pensa et al., 2019). Αυτό στηρίζεται στην υπόθεση ότι κάποιοι χρήστες είναι πιο επιρρεπείς να αποκαλύψουν τα προσωπικά τους δεδομένα από άλλους και αυτό είναι κάτι που αντικατοπτρίζεται στον τρόπο με τον οποίο διαμορφώνουν τις ρυθμίσεις απορρήτου τους. Έτσι λοιπόν εξάγεται το συμπέρασμα ότι αν δύο χρήστες έχουν την ίδια στάση απέναντι στην προστασία του απορρήτου δεν είναι απαραίτητο ότι υπόκειται στον ίδιο κίνδυνο. Εάν ο ένας περιβάλλεται από φίλους που δεν ενδιαφέρονται για το απόρρητο είναι περισσότερο εκτεθειμένος από τον άλλον που έχει φίλους που ενδιαφέρονται.

Συγκεκριμένα, σύμφωνα με τους Pensa et al. (2019), για την βαθμολογία οι συμμετέχοντες στην μελέτη έπρεπε να υποδείξουν σε ποιο βαθμό ήταν πρόθυμοι να αποκαλύψουν πέντε διαφορετικά θέματα της ζωής τους. Για κάθε ένα από αυτά έπρεπε να επιλέξουν να είναι ορατό (α) σε κανέναν, (β) μόνο σε στενούς φίλους, (γ) σε φίλους εκτός από γνωστούς, (δ) σε όλους τους φίλους, (ε) σε όλους τους φίλους των φίλων τους και (στ) σε όλους στο κοινωνικό δίκτυο. Από την βαθμολογία προέκυψε ότι είναι αναγκαία η ενσωμάτωση υπολογισμού μέτρησης απορρήτου σε οποιοδήποτε μέσο ή πλατφόρμα δικτύωσης.

2.5.6.3 Το παιχνίδι σοβαρού σκοπού "Friend Inspector" και το Facebook

Το "Friend Inspector" είναι ένα παιχνίδι κουίζ το οποίο συνδέεται με το προφίλ στο Facebook και χρησιμοποιεί δεδομένα από τον λογαριασμό του Facebook για να δημιουργήσει ερωτήσεις σχετικά με το απόρρητο στο διαδίκτυο και τα μέσα κοινωνικής δικτύωσης (Solberg (2018); Pape et al.(2021)). Στόχος του παιχνιδιού είναι ο παίκτης να μαντέψει την ορατότητα ενός στοιχείου που ο χρήστης έχει μοιραστεί μόνος του, σε συγκεκριμένο χρονικό διάστημα. Μετά την ολοκλήρωση του παιχνιδιού ο παίκτης παίρνει μία βαθμολογία με βάση το πόσο καλά απάντησε στις ερωτήσεις και πόσο χρόνο έκανε να τις απαντήσει. Δίνεται, επιπλέον, η δυνατότητα το σκορ να κοινοποιηθεί στο προφίλ του παίκτη.

2.5.7 Πολιτικές απορρήτου

2.5.7.1 Εισαγωγή

Σύμφωνα με τους Pape et al. (2021), μετά την ανάπτυξη και την εξέλιξη του "Internet of Things" οι πολιτικές απορρήτου δε χρησιμοποιούνται μόνο για την κάλυψη ιστοσελίδων αλλά και για κάθε υπηρεσία η οποία έχει σχέση με το διαδίκτυο. Όμως η εισαγωγή του GDPR έχει ως αποτέλεσμα οι περισσότερες πολιτικές απορρήτου να χρησιμοποιούνται ως νομικές συμφωνίες. Αυτό έχει ως αποτέλεσμα οι περισσότεροι χρήστες να τις αντιμετωπίζουν σε μεγάλο βαθμό ως δυσανάγνωστες. Οι Alhazmi και Arachchilage (2023) συμπληρώνουν ότι η πολιτική απορρήτου, σύμφωνα με τον GDPR, είναι χρήσιμη στους χρήστες διότι τους βοηθά να κατανοήσουν πως οι προγραμματιστές του λογισμικού που χρησιμοποιούν, πρόκειται να αξιοποιήσουν τα προσωπικά τους δεδομένα. Εάν οι χρήστες γνωρίζουν τη σημασία του GDPR και της προστασίας της

ιδιωτικότητας θα μπορούν να αναγνωρίζουν και να καταπολεμούν τις απειλές της ιδιωτικής ζωής.

2.5.7.2 Το παιχνίδι “think-aloud” και οι προγραμματιστές

Έχει αναπτυχθεί μία gamified εφαρμογή, η “think-aloud”, η οποία επιδιώκει την εκπαίδευση των προγραμματιστών στο πως να ενσωματώνουν νόμους περί απορρήτου και GDPR στις εφαρμογές που κατασκευάζουν (Alhazmi και Arachchilage, 2023). Η εφαρμογή αυτή επιθυμεί να διδάξει στους προγραμματιστές να χρησιμοποιούν στις εφαρμογές που φτιάχνουν τις έξι κατευθυντήριες αρχές του GDPR για την εφαρμογή του απορρήτου: νομιμότητα, δικαιοσύνη και διαφάνεια, περιορισμός του σκοπού, ελαχιστοποίηση δεδομένων, ακρίβεια, περιορισμός αποθήκευσης και ακεραιότητα και εμπιστευτικότητα,.

Το “think-aloud”, βασίζεται σε πρόγραμμα περιήγησης και έχει έξι επίπεδα και βίντεο. Ο παίκτης βλέπει σε κάθε επίπεδο το αντίστοιχο βίντεο το οποίο είναι μία συνομιλία μεταξύ ενός προγραμματιστή λογισμικού, ενός συμβούλου ασφαλείας, ενός γιατρού, ενός νοσοκόμου και ενός ασθενούς σχετικά με τις αρχές και τον τρόπο εφαρμογής τους και την υλοποίηση τους στην ανάπτυξη ενός Πληροφοριακού Συστήματος Υγείας το οποίο διατηρεί το απόρρητο του τελικού χρήστη. Έπειτα, ο παίκτης απαντά σε τρία ερωτήματα, κερδίζοντας ένα αστέρι για κάθε σωστή απάντηση και έτσι προχωρά στο επόμενο επίπεδο.

Το “think-aloud”, τέθηκε σε δοκιμή σε είκοσι συμμετέχοντες. Περίπου το 80% από αυτούς ανέφεραν ότι ικανοποιήθηκαν από το παιχνίδι. Οι βαθμολογίες των τεστ έδειξαν 88% επιτυχία οδηγώντας στο συμπέρασμα ότι το “think-aloud” ενθάρρυνε τη μάθηση σχετικά με το απόρρητο και την κατανόηση του GDPR και συνεπώς την αλλαγή της συμπεριφοράς των προγραμματιστών ως προς την ασφαλή κωδικοποίηση προγραμμάτων.

2.5.7.3 Το παιχνίδι σοβαρού σκοπού “Leech” και οι απλοί χρήστες

Έχει αναπτυχθεί ένα παιχνίδι σοβαρού σκοπού με στόχο την εκπαίδευση των απλών χρηστών σχετικά με την δομή και το περιεχόμενο των πολιτικών απορρήτου (Pape et al., 2021). Ανάγκη αυτού του παιχνιδιού αποτέλεσε το γεγονός ότι η άσκηση επιλογών απορρήτου απαιτεί υψηλό επίπεδο προσπάθειας από τους χρήστες. Στόχος του παιχνιδιού είναι να γίνουν καλύτερα κατανοητοί οι όροι απορρήτου και η δομή των

πολιτικών απορρήτου, να γίνουν αντιληπτές ποιες είναι οι πιθανές συνέπειες από την αποδοχή μίας πολιτικής απορρήτου και να συγκριθούν δύο πολιτικές απορρήτου.

Το παιχνίδι ονομάζεται “Leech” και σε αντίθεση με άλλα παιχνίδια που διδάσκουν τον χρήστη σχετικά με το απόρρητο στο διαδίκτυο, αυτό επικεντρώνεται στη δημιουργία καλύτερης κατανόησης των πολιτικών απορρήτου και του περιεχομένου τους (Pape et al., 2021). Οι πολιτικές απορρήτου αποτελούνται από πολύ μεγάλα κείμενα τα οποία στο παιχνίδι μεταφέρονται μέσω διαλόγων χαρακτήρων (non - player - characters NPCs). Στο παιχνίδι οι NPCs εξηγούν πως λειτουργούν οι πολιτικές απορρήτου και το αποτέλεσμα που μπορεί να έχει η παραμέληση τους. Επιπλέον, είναι ενσωματωμένα δύο mini games στην κυρία ιστορία τα οποία συμβάλλουν στην ύπαρξη διαδραστικότητας. Στο ένα ο παίκτης πρέπει να ταξινομήσει αποσπάσματα μίας πολιτικής απορρήτου με σκοπό να μάθει τη δομή της. Το άλλο είναι ένα κουίζ το οποίο καλύπτει διάφορα θέματα του GDPR.

Το παιχνίδι ξεκινάει με τον “Dave”, ο οποίος είναι ο κύριος χαρακτήρας και ανακαλύπτει μία νέα υπηρεσία το “Leech Cloud”. Ο πρωταγωνιστής χρησιμοποιεί αυτή την υπηρεσία χωρίς να διαβάσει την πολιτική απορρήτου και από τον ενθουσιασμό του θέλει να το μοιραστεί με όλους. Αρκετά νωρίς όμως, διαπιστώνει ότι αυτή η υπηρεσία δεν έχει μόνο πλεονεκτήματα. Μέσα από την υπηρεσία αλληλεπιδρά με πολλά και ενδιαφέροντα άτομα που του δείχνουν τα μειονεκτήματα της αγνόησης των όρων της πολιτικής απορρήτου. Ο “Dave” στον ύπνο του βλέπει την “Ευρώπη”, ως φιγούρα ήρωας, η οποία του εφιστά την προσοχή στο δικαίωμα στη διαγραφή που του παρέχει ο GDPR και τον ενθαρρύνει να ταξιδέψει στο κάστρο της “Leech” και να πάρει πίσω τα δεδομένα του. Ο “Dave” πρέπει να ολοκληρώσει τις εργασίες που προκύπτουν κατά τη διάρκεια του παιχνιδιού για να το ολοκληρώσει. Κατά την προσπάθεια αυτή συναντά το πρώτο mini game το οποίο είναι να συντάξει μία δήλωση προστασίας δεδομένων η οποία δεν έχει τη σωστή δομή. Τα αποτελέσματα της δήλωση προστασίας δεδομένων πρέπει να τοποθετηθούν στην σωστή σειρά χρησιμοποιώντας μεταφορά κι απόθεση. Μόνο εάν τα αποτελέσματα έχουν παραχθεί σωστά ο παίκτης μπορεί να προχωρήσει στο κύριο παιχνίδι, ενώ εάν η σειρά είναι λανθασμένη τότε θα του ζητηθεί να τα επεξεργαστεί ξανά. Αφού ο “Dave” ολοκληρώσει σωστά όλες τις εργασίες τότε θα οδηγηθεί στο κάστρο της “Leech” όπου εκεί θα έχει τη δυνατότητα αφού απαντήσει σε ένα κουίζ βασισμένο στον GDPR, να ανακτήσει τα προσωπικά του δεδομένα.

Το παιχνίδι έχει δοκιμαστεί δύο φορές σε λίγα άτομα και σε γενικές γραμμές αξιολογήθηκε θετικά από τους περισσότερους παίκτες (Pape et al., 2021). Αξίζει να σημειωθεί ότι όσοι γνώριζαν εκ των προτέρων πράγματα σχετικά με τις πολιτικές απορρήτου δήλωσαν ότι έμαθαν. Από την ποιοτική ανατροφοδότηση διαπιστώθηκε ότι αυτό το παιχνίδι είναι πολλά υποσχόμενο ως προς την προώθηση της καλύτερης κατανόησης των πολιτικών απορρήτου για τους απλούς χρήστες.

2.5.7.4 Το ψηφιακό δωμάτιο απόδρασης "Puzzle Policy" που αφορά τις συνέπειες των πολιτικών απορρήτου

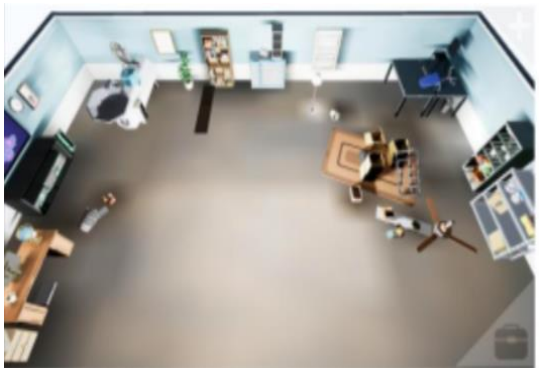
Το ψηφιακό δωμάτιο απόδρασης "Puzzle Policy" (Stellmacher et al, 2022) παρουσιάζει στους παίκτες πληροφορίες μίας πολιτικής απορρήτου μέσα από διάφορα puzzle. Το παιχνίδι είναι για κινητά και λαμβάνει χώρα σε ένα εργαστήριο όπου οι παίκτες πρέπει να αποδράσουν, βλέπε Εικόνα 14 και Εικόνα 15. Τα αντικείμενα που βρίσκονται στο ψηφιακό περιβάλλον προσφέρουν υποδείξεις και ενδείξεις που είναι απαραίτητες για τη συμπλήρωση ενός συνόλου δεδομένων το οποίο θα συμβάλλει στην απόδραση από το δωμάτιο. Με την επίλυση διαφορετικών παζλ και γρίφων, π.χ. συλλέγοντας και συναρμολογώντας πολλά κομμάτια ενός κειμένου χαρτιού ή αποκαλύπτοντας κρυμμένα γραπτά σε έναν τοίχο, ο χρήστης ανακαλύπτει χαμένα μέρη του συνόλου δεδομένων και μαθαίνει για διάφορες πρακτικές απορρήτου όπως συλλογή, επεξεργασία και μεταφορά δεδομένων.

Εικόνα 14: Στιγμιότυπα από το "Puzzle Policy"

Όπως αναφέρθηκε και παραπάνω, οι πολιτικές απορρήτου ενημερώνουν τους χρήστες σχετικά με τον τρόπο διαχείρισης των προσωπικών τους δεδομένων. Παράλληλα μελέτες έχουν δείξει ότι οι χρήστες δεν διαβάζουν τις πολιτικές απορρήτου τις περισσότερες φορές και δεν μπορούν συχνά να τις κατανοήσουν λόγω του όγκου και της πολυπλοκότητας. Έτσι καταλήγουν να παρέχουν τη συγκατάθεση τους χωρίς να γνωρίζουν. Μέσω του ψηφιακού δωματίου απόδρασης, "Puzzle Policy", πρόκειται να διερευνηθεί αν θα βελτιωθεί η κατανόηση των πολιτικών απορρήτου από τους χρήστες.

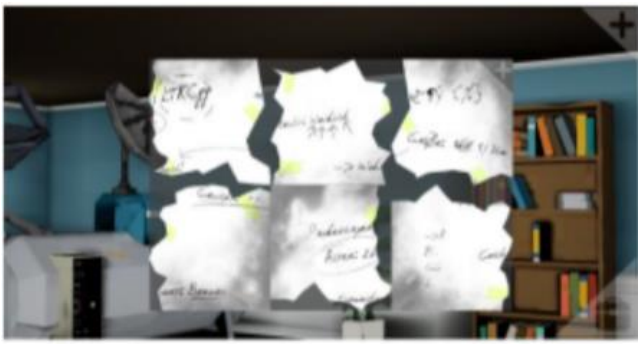
Χρησιμοποιώντας παιχνίδια οι χρήστες είναι πιο πιθανό να ασχοληθούν με το περιεχόμενο μίας πολιτικής απορρήτου και να βελτιώσουν την κατανόηση τους.

Το παιχνίδι χρησιμοποιεί μια πολιτική απορρήτου άλλης εφαρμογής ιστότοπου ψηφιακής υπηρεσίας με την οποία ο χρήστης χρειάζεται να εξοικειωθεί. Το παιχνίδι αποτελείται από μία σειρά με mini παζλ που πρέπει να λυθούν για να ολοκληρωθεί με επιτυχία. Τα παζλ αυτά έχουν σχεδιαστεί για να ενημερώσουν τον χρήστη σχετικά με τη χρήση των δεδομένων στην επιλεγμένη πολιτική απορρήτου. Η πολιτική απορρήτου που χρησιμοποιείται στο παρόν παιχνίδι είναι αυτή της "Corona-Datenspende-App", μία από τις πιο χρησιμοποιούμενες εφαρμογές στη Γερμανία το 2020. Στόχος του παιχνιδιού είναι να βγει ο παίκτης από το δωμάτιο λύνοντας διάφορους γρίφους. Οι χρήστες στην προσπάθεια τους να λύσουν τους γρίφους αλληλεπιδρούν με διάφορες πτυχές πολιτικών απορρήτου.



Εικόνα 15: Στιγμιότυπο από το "Puzzle Policy", επισκόπηση του δωματίου

Στο παιχνίδι οι παίκτες πιέζουν με τα δάχτυλα τους την οθόνη και μπορούν να κάνουν διάφορες κινήσεις στο παιχνίδι και αυτό τους προσφέρει τη δυνατότητα μίας πιο προσεκτικής εξέτασης του περιβάλλοντα χώρου και των αντικειμένων του παιχνιδιού. Οι παίκτες μπορούν να κάνουν "κλικ" στα αντικείμενα, να αλληλεπιδράσουν με αυτά και να τα συλλέξουν στο inventory τους. Επιπλέον, στους παίκτες κοινοποιούνται διάφορες συμβουλές ή πληροφορίες. Όταν το παιχνίδι ξεκινά οι παίκτες βρίσκονται στο δωμάτιο στο οποίο λαμβάνει χώρα ολόκληρο το παιχνίδι. Στους παίκτες εμφανίζεται το inventory τους το οποίο περιέχει ένα κομμάτι puzzle. Στη συνέχεια παροτρύνονται να ψάξουν και να βρουν τα υπόλοιπα κομμάτια μέσα στο δωμάτιο έτσι ώστε να συναρμολογήσουν το puzzle, βλέπε Εικόνα 16. Έτσι, λοιπόν, οι παίκτες εισάγονται στο παιχνίδι. Κάθε φορά που ο παίκτης εντοπίζει ένα στοιχείο εμφανίζεται ένα κείμενο περιγραφής το οποίο παρέχει πληροφορίες για το συγκεκριμένο αντικείμενο και τους επιτρέπεται να το χρησιμοποιήσουν.



Εικόνα 16: Στιγμιότυπο από το "Puzzle Policy", επισκόπηση των χαμένων κομματιών ενός παζλ

Στην έρευνα για το παιχνίδι συμμετείχαν 18 άτομα τα οποία χωρίστηκαν σε δύο ομάδες (Stellmacher et al, 2022). Στην πρώτη ομάδα διαβάστηκε η πολιτική απορρήτου στην αρχική της μορφή, αυτή του κειμένου, ενώ στην δεύτερη ομάδα δοκιμάστηκε το παιχνίδι που σχεδιάστηκε, δηλαδή το escape room. Μετά από αυτό αυτοί οι συμμετέχοντες απάντησαν σε ένα κουίζ με σκοπό να ελεγχθούν οι πληροφορίες που συνέλεξαν. Αποδείχτηκε ότι η ομάδα που συμμετείχε στο παιχνίδι σημείωσε σημαντικά υψηλότερη βαθμολογία σε όλους τους τομείς που αφορούσαν τις πληροφορίες. Παράλληλα, οι συμμετέχοντες στην ομάδα παιχνιδιού αφιέρωσαν περισσότερο χρόνο στο παιχνίδι από ότι οι συμμετέχοντες της ομάδας στην οποία χρησιμοποιήθηκε κείμενο, αν και θα έπρεπε να αφιερώσουν περίπου τον ίδιο. Αναφορικά με τις πολιτικές απορρήτου 72% των συμμετεχόντων απάντησε ότι δεν έχει διαβάσει ποτέ ή σπάνια την πολιτική απορρήτου σε έναν ιστότοπο τον οποίο επισκέπτεται πριν την χρήση του. Γενικά, οι συμμετέχοντες φάνηκε να ενδιαφέρονται να διαφυλάξουν τα προσωπικά τους δεδομένα, κάτι το οποίο από τις απαντήσεις προέκυψε ότι δεν έχουν την απαραίτητη συμπεριφορά για να το κάνουν. Τελικά, αποδείχτηκε ότι η κατανόηση των πολιτικών απορρήτου μέσω της χρήσης παιχνιδιών και συγκεκριμένα του δωματίου απόδρασης είναι χρήσιμη.

2.5.7.5 Παιχνίδια για νομοθεσίες

Οι περισσότεροι άνθρωποι, κατά τους Nahmias et al. (2020), παίζουν ηλεκτρονικά παιχνίδια, όμως λίγοι είναι αυτοί που θα ασχοληθούν με τα περίπλοκα νομικά έγγραφα που υπάρχουν για τον έλεγχο και τη ρύθμιση των δραστηριοτήτων. Οι περισσότεροι θα κάνουν κλικ στο «Συμφωνώ» καθώς δεν βρίσκουν κάποιο ενδιαφέρον στο να διαβάσουν αυτά τα νομικά έγγραφα. Έτσι, αυτά αντί να προωθούν ενημερωμένους χρήστες διαιωνίζουν το πρόβλημα της μη ανάγνωσης. Μέσω της

παιχνιδοποίησης υποστηρίζεται ότι μπορεί να μετριαστεί η αδυναμία των ατόμων να διαβάσουν αυτά τα πολλά και πολύπλοκα έγγραφα.

Στο παιχνίδι "PrivacyVille" (Nahmias et al.,2020), οι παίκτες ασχολούνται με διαφορετικά θέματα όπως η διαφήμιση, η κοινή χρήση και η αποθήκευση. Σε κάθε θέμα παρουσιάζεται στον παίκτη το αντίστοιχο μέρος της πολιτικής απορρήτου της εταιρεία Zynga. Στο "PrivacyVille" οι διαδικτυακές έννοιες απορρήτου γίνονται παιχνίδι. Το "PrivacyVille" αποτελείται από δύο μέρη, στο ένα οι χρήστες μπαίνοντας στην πόλη "PrivacyVille" διαβάζουν διάφορες έννοιες, όπως για παράδειγμα πώς η εταιρεία Zynga χρησιμοποιεί τα emails των παικτών, και στο άλλο μέρος οι παίκτες απαντούν σε ένα κουίζ ερωτήσεων με βάση το περιεχόμενο που διάβασαν.

Το παιχνίδι "Droit et EPN, le Jeul!", κατά τους Nahmias et al. (2020), μοιάζει με διαδραστικό κόμικ και επιδιώκει τη διδασκαλία βασικών νομικών εννοιών σχετικών με το διαδίκτυο και τα πολυμέσα. Έχει θεματικές όπως η ελευθερία έκφρασης, τα πνευματικά δικαιώματα, η επαναχρησιμοποίηση ψηφιακού περιεχομένου και το απόρρητο. Για κάθε ενότητα εξηγείται το θέμα, δίνεται ένα σενάριο κατασκευασμένο ως κόμικ και ένα κουίζ.

2.5.7.6 Τα cookies

Σύμφωνα με τους Diez και Melcer (2020), πολλά άτομα σήμερα, ιδιαίτερα παιδιά, εκτίθενται στο διαδίκτυο και αλληλεπιδρούν με έξυπνες συσκευές όπως τηλέφωνα και tablet σχεδόν από τη στιγμή της γέννησης τους. Όσο αυξάνεται η εξάρτηση των ατόμων νέων ηλικιών από την τεχνολογία τόσο αυξάνεται και η ανάγκη διδασκαλίας της τεχνολογίας και της απόκτησης ψηφιακής παιδείας, οι οποίες θα πρέπει να δίνουν ιδιαίτερη έμφαση στην απόκτηση γνώσεων σχετικών με τα cookies στο Διαδίκτυο.

Οι Diez και Melcer (2020) συμπληρώνουν, ότι πολλοί χρήστες του διαδικτύου δεν γνωρίζουν πλήρως πως λειτουργούν ή τι κάνουν τα cookies. Οι νεαροί είναι σημαντικό να γνωρίζουν για τα cookies, καθώς εκθέτουν συχνά πληροφορίες για την ζωή τους στα μέσα κοινωνικής δικτύωσης και στις μηχανές αναζήτησης. Τα cookies είναι εργαλεία αποθήκευσης δεδομένων τα οποία συλλέγουν πληροφορίες από τους χρήστες μίας ιστοσελίδας για να ενημερώσουν διάφορες πτυχές της, όπως συστήματα μάρκετινγκ κ.α.. Τα cookies μπορεί να χρησιμοποιηθούν, επίσης, για την παροχή πλεονεκτήματος ευκολίας αποθήκευσης σημαντικών πληροφοριών όπως κωδικοί

πρόσβασης, προτιμώμενες ρυθμίσεις ιστοτόπου κ.α.. Όμως, παρουσιάζουν προβλήματα σχετικά με το απόρρητο και τη συναίνεση, διότι έχουν την ικανότητα να αποθηκεύουν ευαίσθητες πληροφορίες για μεγάλο χρονικό διάστημα χωρίς την ύπαρξη ασφαλών διακομιστών ή κατάλληλης προστασίας. Ο κίνδυνος πίσω από τα cookies εντοπίζεται στον τρόπο με τον οποίο οι εταιρείες χρησιμοποιούν τις διαφορετικές μορφές cookies. Είναι σημαντικό τα cookies να χρησιμοποιούνται από τις εταιρείες με καλές προθέσεις και να μην γίνεται κατάχρηση.

Συγκεκριμένα, κατά τους Gey και Varvne (2023), οι εταιρείες διαφήμισης χρησιμοποιούν τα cookies για να συλλέξουν πληροφορίες σχετικά με τη συμπεριφορά των χρηστών και να εξατομικεύσουν το περιεχόμενο για τον χρήστη με στόχο την αύξηση των πωλήσεων και τα έσοδα. Επίσης, άλλο πλεονέκτημα των cookies είναι ότι μπορούν να δημιουργήσουν αξία για τους χρήστες καθώς παρέχοντας εξατομικευμένες διαφημίσεις και αναζητήσεις στην Google είναι ικανά να εξοικονομήσουν χρόνο για τον χρήστη. Επιπλέον, χρόνος εξοικονομείται και από τις πληροφορίες που αποθηκεύουν τα cookies όπως αναφέρθηκε και στην προηγούμενη παράγραφο.

Οι Gey και Varvne (2023) συμπληρώνουν ότι, αν και σκοπός των cookies ήταν αρχικά η διατήρηση πληροφοριών σε ιστοτόπους για τη βελτίωση της εμπειρίας του χρήστη, τα cookies σήμερα συλλέγουν και δεδομένα τα οποία όπως αναφέρθηκε πιο πάνω μπορεί να αποτελέσουν απειλή για το απόρρητο των χρηστών. Αναφορικά με αυτό προβληματισμοί δημιουργούνται γύρω από το γεγονός ότι ενώ οι χρήστες δηλώνουν ότι έχουν ενδιαφέρον για το απόρρητο τους δεν κάνουν ιδιαίτερες ενέργειες για να το προστατεύσουν. Επιπρόσθετα, η λήψη πάρα πολλών πληροφοριών σε συνδυασμό με σκοτεινά μοτίβα, που σημαίνει χειραγώγηση των χρηστών μέσω του σχεδιασμού, καθοδηγεί τους χρήστες να δώσουν τη συγκατάθεση τους όταν οι ίδιοι δεν αναγνωρίζουν γιατί συλλέγονται και πώς χρησιμοποιούνται αυτές οι πληροφορίες. Οι ιστότοποι έχουν την υποχρέωση μόνο να παρέχουν γραπτή πολιτική σχετικά με τη χρήση των δεδομένων των καταναλωτών, με σεβασμό στο απόρρητο τους, ενώ δεν έχουν καμία υποχρέωση που αφορά τη διαμόρφωση της πολιτικής ούτε ότι η πολιτική πρέπει να είναι κατανοητή από τον χρήστη.

Αξίζει να αναφερθεί, σημειώνουν οι Gey και Varvne (2023), ότι οι άνθρωποι αντιλαμβάνονται την ιδιωτικότητα τους παράδοξα. Έχει παρατηρηθεί ένα φαινόμενο το οποίο ονομάζεται παράδοξο της ιδιωτικής ζωής. Υπάρχει άγνοια σχετικά με το πώς οι άνθρωποι αφήνουν τον εαυτό τους ευάλωτο στο διαδίκτυο λόγω της άγνοιάς για το πως

να προστατευτούν, της αντιληπτής προσπάθειας που απαιτείται για να προστατευτούν στο διαδίκτυο ή της προθυμίας να θυσιάσουν το απόρρητο τους προκειμένου να κερδίσουν κάτι άλλο σε αντάλλαγμα, όπως ένα προϊόν ή μία εξατομικευμένη υπηρεσία. Οι Gey και Varvne (2023) αναφέρουν, επίσης, ότι για την προστασία των χρηστών το Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο έχει εκδώσει την οδηγία 2009/136/ΕΚ η οποία εναποθέτει βέβαια στα κράτη να θεσπίσουν νόμους που την εφαρμόζουν. Σύμφωνα με αυτή οι πάροχοι ιστοτόπων πρέπει να ζητούν από τους χρήστες την συγκατάθεση τους κατά την τοποθέτηση των cookies, οπότε έτσι προέκυψαν και οι ειδοποιήσεις cookies. Αν και η συγκατάθεση του χρήστη πρέπει να έρχεται μετά από ενημέρωση και να του παρέχονται πληροφορίες προτού συναινέσει προκειμένου η συγκατάθεση να θεωρείται έγκυρη, ο GDPR δεν διευκρινίζει σε ποια μορφή θα πρέπει να παρέχονται οι πληροφορίες.

Αυτή η πληθώρα πληροφοριών που χρειάζεται να γνωρίσει ο χρήστης για να προστατεύσει το απόρρητο του και να διαχειριστεί αποτελεσματικά τις προσωπικές του πληροφορίες, σύμφωνα με τους Gey και Varvne (2023), δημιουργεί αυτό που ορίζεται ως κόπωση απορρήτου. Παρατηρήθηκε ότι όταν παρουσιάζονται στον χρήστη οι ρυθμίσεις απορρήτου και καλούνται να επιλέξουν τις προτιμήσεις τους, αυτοί κατακλύζονται από το πλήθος των επιλογών και αυτό τους δημιουργεί κόπωση με αποτέλεσμα να μην μπορούν να λάβουν σωστές αποφάσεις και να επιλέγουν την επιλογή που απαιτεί την μικρότερη προσπάθεια, συνήθως αυτή της προεπιλογής.

Στην ΕΕ, κατά τους Diez και Melcer (2020), ο GDPR προστατεύει τους χρήστες από τη σύγχυση που προκαλούν τα cookies σχετικά με το απόρρητο. Παρά το γεγονός ότι έχουν γίνει σημαντικά βήματα για την σωστή ενημέρωση και προστασία των χρηστών, εξακολουθούν να υπάρχουν άτομα που δεν έχουν επαρκείς γνώσεις για τα cookies. Αυτό οδήγησε στην ανάπτυξη ενός παιχνιδιού σοβαρού σκοπού με θέμα τα cookies.

2.5.7.6.1 Το παιχνίδι σοβαρού σκοπού “Cookie Mania”

Το παιχνίδι σοβαρού σκοπού με θέμα τα cookies είναι το “Cookie Mania”, το οποίο επικεντρώνεται τόσο στη διδασκαλία των παικτών σχετικά με τα cookies στο διαδίκτυο όσο και στο πως αυτά μπορεί να επηρεάσουν τη ζωή τους (Diez και Melcer, 2020). Για την κατασκευή του “Cookie Mania” αναπτύχθηκαν τρεις τύποι cookies οι οποίοι αντιπροσωπεύουν οπτικά τους τύπους διαδικτυακών cookies. Στο “Cookie

Mania" τα γεγονότα του παιχνιδιού αντικατοπτρίζουν συμβάντα της πραγματικής ζωής και εστιάζουν σε διαφορετικά σκάνδαλα μεγάλων εταιρειών τεχνολογίας cookies. Το "Cookie Mania" λαμβάνοντας υπόψιν το συμβάν της "Cambridge Analytica" και του "Facebook" εφήρμοσε μία ιστορία μέσα στο παιχνίδι η οποία μιμείται τα γεγονότα αυτά με ηθική λήψη αποφάσεων και επιπτώσεις για το αν θα συμπεριληφθεί η συναίνεση στην εταιρεία του παίκτη.

Το "Cookie Mania" έχει δύο κύριες οθόνες κατά τη διάρκεια του, τα γραφεία, βλέπε Εικόνα 17, και την επιφάνεια εργασίας. Επιπλέον, το "Cookie Mania" αποτελείται από mini games τα οποία με τη σειρά τους κεντρίζουν το ενδιαφέρον των παικτών. Στο mini game marketing οι παίκτες λαμβάνουν οδηγίες να μεταβούν σε διάφορες πλατφόρμες για να αποφύγουν κακόβουλα cookies και να συλλέξουν μόνο όσα θα τους επιτρέψουν να αποκτήσουν αναβαθμίσεις και να βελτιώσουν τη συλλογή των δεδομένων του ιστοτόπου τους. Στο mini game security οι παίκτες λαμβάνουν οδηγίες να προστατεύουν τα δεδομένα των πελατών τους καταστρέφοντας ιούς και cookies ζόμπι ώστε να μην φτάσουν στα δεδομένα τα οποία με τη σειρά τους κεντρίζουν το ενδιαφέρον των παικτών. Μόλις οι παίκτες ολοκληρώσουν τα mini games θα έχουν συγκεντρώσει πόντους για να πραγματοποιήσουν αναβαθμίσεις στο παιχνίδι οι οποίες το βελτιώνουν και προσθέτουν στοιχεία στη σελίδα "Analytics". Η σελίδα "Analytics" που παρέχει στους παίκτες ένα αυξανόμενο σύνολο γνώσεων για το πως λειτουργούν τα cookies και τι πληροφορίες παρέχουν στον διαχειριστή ιστοτόπου. Τέλος, υπάρχει και η καρτέλα email στην οποία υπάρχουν πληροφορίες σχετικές με την ιστορία και τη λήψη ηθικών αποφάσεων.

Επιλογικά, το "Cookie Mania" είναι ένα παιχνίδι σοβαρού σκοπού το οποίο στοχεύει στην ανάπτυξη γνώσεων σχετικών με τα cookies στο Διαδίκτυο.

Εικόνα 17: Στιγμιότυπο από το παιχνίδι "Cookie Mania". Αριστερά το γραφείο του αφεντικού και δεξιά το κεντρικό γραφείο

2.5.8 Απόρρητο και γεωγραφική τοποθεσία

2.5.8.1 Εισαγωγή

Ο Thieu (2019) υποστηρίζει ότι αρκετές εφαρμογές και κινητά και μέσα κοινωνικής δικτύωσης χρησιμοποιούν την γεωγραφική τοποθεσία. Αυτή η τεχνολογία και τα γεωγραφικά δεδομένα πυροδοτούν καινοτόμες ιδέες και συμβάλλουν στην ύπαρξη χρήσιμων λειτουργιών αυτών των εφαρμογών. Όμως όσο αυξάνονται οι δυνατότητες αυξάνεται και ο κίνδυνος για επιβλαβείς διαρροές δεδομένων απορρήτου. Όπως έχει αναφερθεί πολλές φορές πιο επιρρεπή άτομα για να εκτεθούν σε κινδύνους παραβίασης της ιδιωτικής ζωής στα μέσα κοινωνικής δικτύωσης είναι οι έφηβοι και οι νεαροί ενήλικες. Αποτελούν λοιπόν μία ηλικιακή ομάδα η οποία έχει γενικά λιγότερη εκπαίδευση σχετική με ζητήματα επίγνωσης του απορρήτου της τοποθεσίας. Τίθεται λοιπόν το ερώτημα αν θα μπορούσε να σχεδιαστεί ένα παιχνίδι σοβαρού σκοπού για κινητά το οποίο να επιδιώκει να αυξηθεί η ευαισθητοποίηση σχετικά με ζητήματα απορρήτου τοποθεσίας.

Σύμφωνα με τον Thieu (2019), το πρόβλημα του απορρήτου της τοποθεσίας εντάσσεται στο γενικότερο φαινόμενο ότι η τεχνολογία είναι ενεργά ενσωματωμένη στην καθημερινή ζωή των νεαρών ανθρώπων, γι' αυτό και είναι σημαντικό να υπάρχουν γνώσεις σχετικές με τους κινδύνους που ελλοχεύουν. Αρχικά, αξίζει να αναφερθούν κάποιοι χρήσιμοι ορισμοί. Πρώτον, η ιδιωτική ζωή είναι το δικαίωμα να είσαι μόνος, αν και η αντίληψη ενός ατόμου για την ιδιωτικότητα μπορεί να ποικίλει. Δεύτερον, ως ιδιωτικό απόρρητο ορίζεται το δικαίωμα να είσαι μόνος ή ελεύθερος από παρέμβαση ή εισβολή. Τρίτον, το απόρρητο των πληροφοριών είναι το δικαίωμα που έχει κανείς να ελέγχει τα προσωπικά του δεδομένα και τον τρόπο συλλογής και χρήσης τους.

2.5.8.2 Απόρρητο τοποθεσίας και κοινωνικά δίκτυα

Ο Thieu (2019) υποστηρίζει ότι οι χρήστες των μέσων κοινωνικής δικτύωσης είναι ευάλωτοι στο να αποκαλύπτουν προσωπικές τους πληροφορίες. Γνωστοποιώντας συγκεκριμένες πληροφορίες τοποθεσίας κινδυνεύουν να αποκαλύψουν άλλες ευαίσθητες προσωπικές πληροφορίες, για παράδειγμα προβλήματα υγείας ή τις συνήθειες κάποιου. Αξίζει βέβαια να σημειωθεί ότι αν και η χρήση δεδομένων τοποθεσίας δημιουργεί διάφορες ανησυχίες δεν έχει μόνο αρνητικές συνέπειες. Είναι χρήσιμη στους προγραμματιστές με σκοπό να δημιουργήσουν καινοτομίες, όπως η εύρεση κοντινών αξιοθέατων ή τα πλησιέστερα εστιατόρια κ.α.. Επιπλέον, θα ήταν χρήσιμο να γίνει

γνωστό ότι ένα γεωκοινωνικό δίκτυο είναι ένα κοινωνικό δίκτυο που παρέχει μία υπηρεσία που χρησιμοποιεί πληροφορίες τοποθεσίας που σχετίζονται με τις ρίζες και το περιεχόμενο τους. Τέτοια κοινωνικά δίκτυα είναι το Facebook, το Twitter κ.α.. Οι απειλές απορρήτου τοποθεσίας ανήκουν σε τρεις κατηγορίες: το απόρρητο τοποθεσίας, το απόρρητο απουσίας και το απόρρητο συντοποθεσίας. Απόρρητο τοποθεσίας σημαίνει να αποκαλύπτει την τοποθεσία του χρήστη σε άλλους στο γεωκοινωνικό δίκτυο. Στο απόρρητο απουσίας εντάσσεται η περίπτωση ενός διαρρήκτη που σχεδιάζει να ληστέψει το σπίτι του χρήστη όσο αυτός λείπει. Στην κατηγορία απειλής απορρήτου συντοποθεσίας περιλαμβάνεται το Co-Location Privacy, σύμφωνα με το οποίο θεωρείται ότι ένας χρήστης μπορεί να παρατηρήσει την ταυτόχρονη παρουσία άλλων χρηστών. Οι πληροφορίες τοποθεσίας που θα ανακτηθούν από τους χρήστες θα προέρχονται από έναν χρήστη στο δίκτυο ο οποίος παρατηρεί τους άλλους.

Υπάρχουν διάφορα παιχνίδια που βασίζονται στην τοποθεσία διαθέσιμα αυτή τη στιγμή τόσο για εκπαιδευτικούς όσο και για ψυχαγωγικούς σκοπούς (Thieu, 2019). Ένα πολύ δημοφιλές σε παγκόσμιο επίπεδο είναι το Pokemon GO. Πρόκειται για ένα παιχνίδι για ψυχαγωγικούς σκοπούς, το οποίο συνδυάζει τεχνολογίες που βασίζονται στην τοποθεσία με επαυξημένη πραγματικότητα.

2.5.8.3 Το παιχνίδι “PrivaCity” και το απόρρητο τοποθεσίας

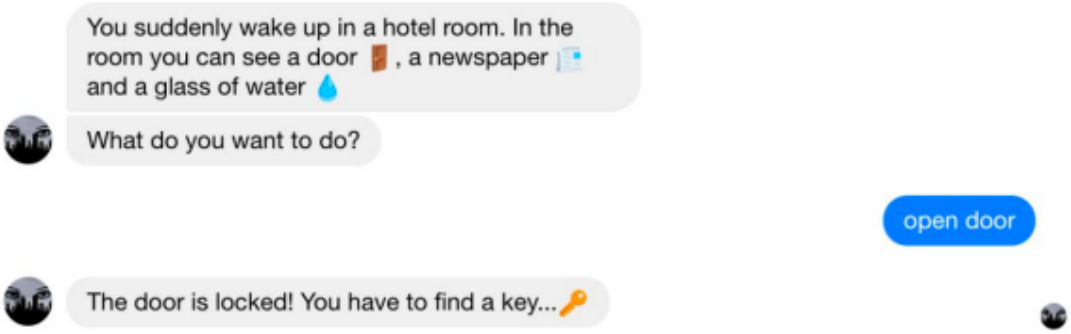
Στην προσπάθεια οι νεαροί να γνωρίσουν περισσότερες πληροφορίες σχετικά με το απόρρητο της γεωγραφικής τοποθεσίας δημιουργήθηκε το παιχνίδι “PrivaCity”. Το παιχνίδι είναι ένα σοβαρό παιχνίδι chatbot στην πλατφόρμα του Facebook Messenger, βλέπε Εικόνα 18, και στο πρόγραμμα περιήγησης ιστού. Είναι ένα παιχνίδι περιπέτειας στο οποίο ο παίκτης προχωρά στην ιστορία συμπληρώνοντας επίπεδα. Κάθε επίπεδο σχετίζεται με την αύξηση της επίγνωσης του απορρήτου του παίκτη. Στο “PrivaCity” αναφέρονται οι Thieu (2019) και Berger και Sæthre (2018).

Εικόνα 18: Στιγμιότυπο από το "PrivaCity"

Σύμφωνα με τους Berger και Sæthre (2018), η κύρια ιστορία του παιχνιδιού είναι ότι η φανταστική πόλη "Metropolis" είναι μία έξυπνη πόλη εδώ και μερικά χρόνια. Το δημοτικό συμβούλιο χρησιμοποιεί αισθητήρες IoT για τη συλλογή πολλών πληροφοριών σε όλη την πόλη και τις χρησιμοποιεί για να βελτιώσει την αποτελεσματικότητα, το περιβάλλον, την ασφάλεια και την οικονομία της πόλης. Ωστόσο, κατά τη διάρκεια του παιχνιδιού ένα νέο κόμμα το "Electoral Norwegian Democracy Privacy – E.N.D. Privacy", αναλαμβάνει τον έλεγχο του δημοτικού συμβουλίου. Αυτό προσπαθεί να κάνει κατάχρηση πληροφοριών που συλλέγονται στο δίκτυο έξυπνων πόλεων για δικό του όφελος, μη σεβόμενο το απόρρητο των πολιτών της πόλης.

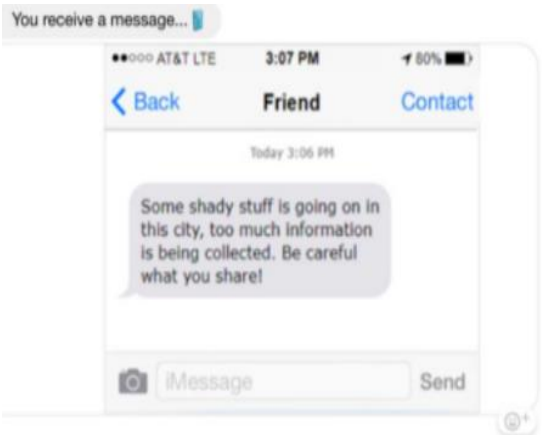
Οι Berger και Sæthre (2018) συμπληρώνουν ότι, κύριος μαθησιακός στόχος του παιχνιδιού είναι να αυξηθεί η επίγνωση του απορρήτου του παίκτη και να είναι επικεντρωμένη σε όλες τις πτυχές της ζωής και κυρίως στη ζωή στις έξυπνες πόλεις. Αυτό είναι σημαντικό για να μπορέσει ο παίκτης να αναγνωρίσει ότι μία έξυπνη πόλη έχει πολλά πλεονεκτήματα αλλά και αρκετά ζητήματα απορρήτου. Καθώς το παιχνίδι εξελίσσεται ολοένα και περισσότερα ζητήματα απορρήτου έρχονται στην επιφάνεια και δημιουργούν ανησυχία στον παίκτη. Ουσιαστικά επιδιώκεται ο παίκτης να δει τις αρνητικές και θετικές πτυχές της έξυπνης πόλης. Το παιχνίδι μπορεί να λήξει είτε έχοντας ως αποτέλεσμα την καταστροφή όλων των δεδομένων που συλλέγονται στην έξυπνη πόλη, αυτήν την απόφαση την παίρνει ο παίκτης όταν τελικά φτάσει στον διακομιστή, ή όχι.

Το παιχνίδι αποτελείται από διάφορα επίπεδα (Berger καιSæthre, 2018). Ξεκινάει από το μηδενικό "δωμάτιο ξενοδοχείου", βλέπε Εικόνα 19, στο οποίο ο παίκτης τοποθετείται σε ένα δωμάτιο ξενοδοχείου και το bot του παρουσιάζει τα αντικείμενα στο δωμάτιο. Ο παίκτης πρέπει να βρει το κλειδί, να ανοίξει την πόρτα και να βρεθεί στον διάδρομο.



Εικόνα 19: Στιγμιότυπο από το μηδενικό επίπεδο του "PrivaCity"

Στο πρώτο επίπεδο, το επίπεδο "διάδρομος", ο παίκτης τοποθετείται σε έναν διάδρομο με πολλές κλειδωμένες πόρτες, έναν ανελκυστήρα και μία μηχανή παγοκύβων. Πριν μπει στο διάδρομο ο παίκτης λαμβάνει ένα μήνυμα κειμένου από ένα φίλο του, βλέπε Εικόνα 20, στο δημοτικό συμβούλιο που τον προειδοποιεί να είναι προσεκτικός σχετικά με την κοινή χρήση πολλών προσωπικών του πληροφοριών. Πριν ο παίκτης φύγει από το διάδρομο και προχωρήσει στο παιχνίδι λαμβάνει μια ειδοποίηση που του ζητάει αν θέλει να μοιραστεί την τοποθεσία του στο "Snapchat" και να κερδίσει πόντους στο παιχνίδι. Το συγκεκριμένο επίπεδο επιδιώκει να δείξει στον παίκτη ότι συχνά κανείς συμβιβάζεται με το να δώσει προσωπικές πληροφορίες για να πάρει μία αμοιβή.



Εικόνα 20: Στιγμιότυπο από το προειδοποιητικό μήνυμα του φίλου

Επόμενο επίπεδο είναι το "λόμπι ξενοδοχείου" το οποίο επιδιώκει να μάθει περισσότερα στους παίκτες για τις έξυπνες πόλεις και την ιδιωτικότητα μέσα από ένα κουίζ. Έπειτα υπάρχει το επίπεδο του "καφέ" στο οποίο οι παίκτες ασχολούνται με τους τρόπους κατάχρησης των πληροφοριών σε μία έξυπνη πόλη από τα άτομα που έχουν πρόσβαση στις πληροφορίες. Μαθαίνουν επίσης και για το γεγονός ότι πληροφορίες μπορεί να συλλέγονται για ένα σκοπό αλλά αργότερα να χρησιμοποιηθούν για άλλο. Επιπλέον, τους γνωστοποιούνται σκάνδαλα όπως αυτό της "Facebook" και της "Cambridge Analytica". Έπειτα, υπάρχει το επίπεδο "ταξινόμησης" απορρήτου το οποίο στοχεύει στην γνωστοποίηση της επικίνδυνης κακής χρήσης των προσωπικών δεδομένων. Σε αυτό το επίπεδο ο παίκτης καλείται να σκεφτεί τι είδους προσωπικά δεδομένα δεν έχει πρόβλημα να κάνει κοινή χρήση και πιθανά να διαβαστούν από τρίτο μέρος. Μετά το επίπεδο αυτό ακολουθεί το επίπεδο "εισόδου στην αίθουσα διακομιστή". Αυτό το επίπεδο εστιάζει περισσότερο στο κομμάτι της διασκέδασης σε αντίθεση με τα προηγούμενα που επικεντρώνονται στην επίτευξη των εκπαιδευτικών στόχων. Στο επόμενο επίπεδο με όνομα "συνέντευξη για εργασία" ο παίκτης καλείται να χρησιμοποιήσει αυτά που ήδη γνωρίζει σχετικά με το απόρρητο στις έξυπνες πόλεις. Μέχρι τώρα έχει εστιάσει στον εντοπισμό ζητημάτων απορρήτου αλλά εδώ πρέπει να δει τα πράγματα από την πλευρά του εισβολέα και να φανταστεί τους τρόπους με τους οποίους μπορεί να χρησιμοποιηθούν οι πληροφορίες του από μία έξυπνη πόλη. Μετά ακολουθεί το επίπεδο "υποκλοπή" όπου ο παίκτης βλέπει τους πιθανούς κινδύνους του IoT.

Τέλος, ακολουθεί το επίπεδο "αίθουσα του διακομιστή". Αυτό το επίπεδο καλύπτει τον τελικό στόχο του παιχνιδιού που είναι να διδάξει τον παίκτη ότι οι αποφάσεις απορρήτου δεν είναι άσπρες ή μαύρες. Στο μεγαλύτερο μέρος του παιχνιδιού στόχος ήταν η καταστροφή του διακομιστή δεδομένων όταν όμως ο παίκτης φτάσει στο στόχο του θα του παρουσιαστούν για ακόμη μία φορά τα πλεονεκτήματα μίας έξυπνης πόλης και όλα τα θετικά από την συλλογή πληροφοριών, όπως για παράδειγμα η βελτίωση της κυκλοφορίας. Έτσι λοιπόν ο παίκτης καλείται να πάρει μία απόφαση απορρήτου με συμβιβασμούς. Με την απόφαση καταστροφής ή όχι του διακομιστή το παιχνίδι τελειώνει. Ο παίκτης ενημερώνεται ότι το απόρρητο είναι ένα ευαίσθητο θέμα και ότι δεν υπάρχει μόνο μία σωστή απόφαση αν πρέπει να καταστραφεί ή όχι ο διακομιστής. Εάν ο παίκτης καταστρέψει τον διακομιστή η πόλη "Metropolis" από έξυπνη πόλη θα μετατραπεί σε μία συνηθισμένη πόλη, αλλά το απόρρητο των πολιτών

θα παραμείνει ακέραιο. Αν ο παίκτης δεν καταστρέψει το διακομιστή η πόλη "Metropolis" θα συνεχίσει να είναι μία έξυπνη πόλη αλλά αυτό θα γίνεται σε βάρος της ιδιωτικής ζωής των πολιτών. Η τελική απόφαση είναι στο χέρι του παίκτη. Με τη λήξη του παιχνιδιού παρουσιάζεται στον παίκτη η βαθμολογία του από τα κουίζ και τις ερωτήσεις, η βαθμολογία από τις ταξινομήσεις και ο χρόνος που έκανε. Επιπλέον, του δίνει τη δυνατότητα να επαναλάβει το παιχνίδι και ενδεχομένως να απαντήσει σωστά σε λάθη που έκανε την πρώτη φορά. Το επίπεδο αυτό αποτελεί μία ανασκόπηση.

Το παιχνίδι δοκιμάστηκε πιλοτικά και για να αξιολογηθεί εάν αύξησε την επίγνωση για το απόρρητο των παικτών χρησιμοποιήθηκε ένα ερωτηματολόγιο. Παρατηρήθηκε ότι οι ερωτηθέντες σημείωσαν υψηλότερες βαθμολογίες στις ερωτήσεις σχετικά με το μαθησιακό αποτέλεσμα και σημείωσαν ότι η ευαισθητοποίηση σχετικά με το αν θα άλλαζαν τη συμπεριφορά τους αυξήθηκε (Berger καιSæthre, 2018).

2.5.8.4 Το παιχνίδι "Location Stalker" για το απόρρητο τοποθεσίας

Μία προσέγγιση η οποία θα μπορούσε να συμβάλλει σημαντικά στην εκμάθηση του απορρήτου τοποθεσίας, σύμφωνα με τον Thieu (2019), είναι η χρήση ενός παιχνιδιού σοβαρού σκοπού με αυτή τη θεματική. Το απόρρητο της τοποθεσίας παρουσιάζει ενδιαφέρον όταν η εφαρμογή που κάνει χρήση της τοποθεσίας είναι εγκατεστημένη σε κινητές συσκευές. Αξίζει να σημειωθεί ότι εκτός από τα social media, όπως το Snapchat, το Tinder, που αναφέραμε παραπάνω, κ.α., έχουν αναπτυχθεί και διάφορα παιχνίδια, ενδεικτικά "Pokemon GO", τα οποία κάνουν χρήση της τοποθεσίας. Ένα παιχνίδι σοβαρού σκοπού το οποίο έχει σχεδιαστεί και άπτεται της θεματικής του απορρήτου τοποθεσίας είναι το "Location Stalker".

Το "Location Stalker" είναι ένα παιχνίδι σοβαρού σκοπού κατασκευασμένο να παίζεται σε φορητές συσκευές από πολλούς παίκτες. Στο "Location Stalker" χρειάζονται δύο ή περισσότεροι χρήστες να παίξουν τον μυστικό ρόλο του χάκερ και οι υπόλοιποι να είναι ντετέκτιβ ή αθώοι, συνολικά χρειάζονται τουλάχιστον 8 άτομα. Η ιστορία του παιχνιδιού εκτυλίσσεται ως εξής: οι παίκτες του παιχνιδιού έχουν την αίσθηση ότι όσο παίζουν το παιχνίδι κάποιος παρακολουθεί την τοποθεσία τους. Στόχος των παικτών είναι ο εντοπισμός και η εκδίωξη των χάκερ μέσω αλληλοκατηγορίας. Συγκεκριμένα, το παιχνίδι για να ξεκινήσει χρειάζονται τουλάχιστον 8 παίκτες και εξελίσσεται σε δύο φάσεις, της νύχτας και της ημέρας. Στην φάση της νύχτας, βλέπε Εικόνα 21, οι χάκερ συνεργάζονται μεταξύ τους για να επιτεθούν σε έναν παίκτη κάθε βράδυ. Παράλληλα, οι

ντετέκτιβ, παίκτες της ομάδας αθώοι, συνεργάζονται μεταξύ τους και μπορούν να αποκαλύπτουν την ταυτότητα κάποιου άλλου παίκτη, έτσι γνωρίζουν αν είναι χάκερ και πρέπει να ψηφιστεί ή αν είναι αθώος. Ταυτόχρονα, στόχος των χάκερ και των ντετέκτιβ είναι να μην γίνει αντιληπτή η ταυτότητα τους. Την ημέρα, βλέπε Εικόνα 22, ανακοινώνεται ο παίκτης που δέχτηκε επίθεση από τους χάκερ, ο παίκτης αυτός είναι πλέον εκτός παιχνιδιού, και οι εναπομείναντες παίκτες, χάκερ και αθώοι, αλληλοκατηγορούνται και απομακρύνουν έναν παίκτη από το παιχνίδι. Η διαδικασία συνεχίζεται μέχρι να απομακρυνθούν όλοι οι χάκερ ή να υπάρχουν τόσοι σε αριθμό όσοι και οι αθώοι. Στην πρώτη περίπτωση νικητές είναι οι αθώοι ενώ στη δεύτερη οι χάκερ.

Εικόνα 21: Στιγμιότυπο του παιχνιδιού “Location Stalker” από τη φάση της νύχτας

Εικόνα 22: Στιγμιότυπο του παιχνιδιού “Location Stalker” από τη φάση της ημέρας

Ο γενικότερος στόχος του παιχνιδιού είναι η αύξηση της ευαισθητοποίησης των παικτών, σχετικά με το απόρρητο της τοποθεσίας, στην πραγματική ζωή. Το “Location

Stalker" συνδέει την ιστορία του με την πραγματική ζωή. Επιδιώκει να αφυπνίσει τους παίκτες να κατανοήσουν τι είναι το απόρρητο της τοποθεσίας, ποιες είναι οι απειλές που μπορεί να δεχτεί, γιατί αυτό είναι επικίνδυνο και πως μπορούν να προφυλαχτούν από αυτές τις απειλές. Επίσης, το παιχνίδι απευθύνεται κυρίως σε έφηβους χρήστες καθώς εντοπίστηκε ότι αποτελούν ομάδα με ελλιπείς γνώσεις των κινδύνων της προστασίας της τοποθεσίας.

Για την επίτευξη των παραπάνω, εκτός από το ίδιο το παιχνίδι, μετά την εφαρμογή του, παρέχεται επιπλέον στους παίκτες ένα σύνολο από πληροφορίες σχετικές με το απόρρητο της τοποθεσίας, την προστασία των προσωπικών τους πληροφοριών και διάφορα παραδείγματα από το παιχνίδι. Έτσι υπογραμμίζεται στους παίκτες ότι είναι πιθανό ο καθένας να επιθυμεί να τους βλάψει χρησιμοποιώντας κακόβουλα τις πληροφορίες της τοποθεσίας του.

Τέλος, το "Location Stalker" τέθηκε σε πιλοτική δοκιμή, 2 φορές, σε οκτώ μαθητές 16 έως 25 ετών, κάθε φορά. Οι συμμετέχοντες παρατήρησαν ότι οι πληροφορίες που τους αποτυπώθηκαν σχετικά με το απόρρητο της τοποθεσίας ήταν λίγες, αλλά αρκετές ώστε να συνειδητοποιήσουν την κατάσταση απειλής που μπορεί αυτό να δεχτεί και να ευαισθητοποιηθούν.

Επιλογικά, το "Location Stalker" είναι μία εφαρμογή με στόχο την ευαισθητοποίηση των παικτών σχετικά με το απόρρητο της τοποθεσίας. Μέσα από αυτό το παιχνίδι οι παίκτες λαμβάνουν πληροφορίες για τις απειλές που μπορεί να δεχτεί το απόρρητο της τοποθεσίας και πως να τις χειριστούν. Το παιχνίδι πέτυχε ικανοποιητικά σε πιλοτικό επίπεδο τον στόχο του καθώς οι χρήστες διασκέδασαν παίζοντας το αλλά και ευαισθητοποιήθηκαν σημαντικά. Όλες οι πληροφορίες για το "Location Stalker" εντοπίστηκαν στην εργασία του Thieu (2019).

2.5.9 Συμπεράσματα

Η προστασία του απορρήτου είναι ιδιαίτερα σημαντική. Τα παιχνίδια σοβαρού σκοπού με επίκεντρο το απόρρητο μπορούν να βοηθήσουν στην ευαισθητοποίηση σχετικά με την προστασία του αλλά και στην αλλαγή της συμπεριφοράς των ατόμων απέναντι σε αυτό.

Υπάρχουν διάφορα παιχνίδια απορρήτου τα οποία απευθύνονται σε διαφορετικές ηλικιακές ομάδες. Κάποια αφορούν την προστασία του απορρήτου και τις συσκευές (κινητό τηλέφωνο, έξυπνο ρολόι κ.α.). Άλλα, αφορούν το απόρρητο και τα μέσα

κοινωνικής δικτύωσης. Παράλληλα, έχουν αναπτυχθεί πολλά παιχνίδια με επίκεντρο τις πολιτικές απορρήτου αλλά και αρκετά αναφορικά με το απόρρητο της τοποθεσίας.

Γενικά, διαπιστώθηκε ότι όσα παιχνίδια αυτής της ενότητας δοκιμάστηκαν αξιολογήθηκαν θετικά ως προς την ευαισθητοποίηση των παικτών σχετικά με το απόρρητο. Ταυτόχρονα, κυρίως οι ενήλικες και οι έφηβοι που έπαιξαν ορισμένα από αυτά τα παιχνίδια υπογράμμισαν ότι θα αλλάξουν την συμπεριφορά τους και θα προστατεύουν το απόρρητο τους μετά από την επαφή τους με το παιχνίδι.

2.6 Προσωπικά δεδομένα και παιχνίδια σοβαρού σκοπού

2.6.1 Εισαγωγή

Στο προηγούμενο κεφάλαιο συζητήθηκαν εκτενώς ζητήματα τα οποία αφορούν το απόρρητο. Επιπλέον, αναφέρθηκαν και παιχνίδια τα οποία έχουν δημιουργηθεί με σκοπό την εκπαίδευση των παιδιών στο απόρρητο. Παράλληλα, αξίζει να σημειωθεί ότι κάθε άνθρωπος, ανεξάρτητα από την ηλικία του έχει το δικαίωμα στην προστασία των προσωπικών του δεδομένων. Όμως, δεν είναι λίγοι οι νέοι οι οποίοι κοινολογούν πληθώρα προσωπικών τους πληροφοριών στα μέσα κοινωνικής δικτύωσης χωρίς να κατανοούν τους κινδύνους του περιβάλλοντος του διαδικτύου. Αυτό συμβαίνει διότι σημαντικός αριθμός χρηστών του διαδικτύου αγνοεί τους κινδύνους της κοινολόγησης των προσωπικών πληροφοριών ή δεν έχει τις επαρκείς γνώσεις και μέσα για την προστασίας τους. Στις περιπτώσεις όμως στις οποίες πρόκειται για παιδιά οι ανησυχίες είναι ακόμη μεγαλύτερες. Άρα, το πρόβλημα που υπάρχει σχετικά με το απόρρητο στο διαδίκτυο αφορά την προστασία των προσωπικών δεδομένων και την συναίνεση των χρηστών. Το πρόβλημα της προστασίας των προσωπικών δεδομένων βρίσκει έδαφος στην έλλειψη του ψηφιακού γραμματισμού. Η σχετική βιβλιογραφία έχει αναπτυχθεί εξαιρετικά τα τελευταία χρόνια (Jaccheri et al.(2017); Manotipya και Ghazinour (2020); Barnard-Wills και Ashenden (2015)).

Η έλλειψη γνώσεων σχετικών με το απόρρητο έχει ως αποτέλεσμα την παθητική στάση των χρηστών, ειδικά των εφήβων, σχετικά με την διαδικτυακή τους κοινωνικότητα. Οι χρήστες των μέσων κοινωνικής δικτύωσης δημιουργούν προφίλ και κοινολογούν προσωπικές τους πληροφορίες, οι οποίες δεν πληρούν συνθήκες μυστικότητας. Η απουσία μυστικότητας των πληροφοριών και η έλλειψη σημαντικών γνώσεων των χρηστών προκαλεί παρανόηση των κινδύνων. Δεν μπορεί να γίνει αντιληπτό ότι οι προσωπικές πληροφορίες οι οποίες δημοσιοποιούνται στα μέσα

κοινωνικής δικτύωσης γίνονται μέρος της οικονομίας των προσωπικών δεδομένων στην οποία οι χρήστες γίνονται ορατοί σε εταιρικές και κυβερνητικές οντότητες και μέρη μίας τεράστιας και αυξανόμενης αγοράς προσωπικών πληροφοριών. Επιπρόσθετα, αξίζει να υπογραμμιστεί ότι μέσα σε αυτή την αγορά γίνονται διακρίσεις των χρηστών βασισμένες στις πληροφορίες που έχουν συλλεχθεί οι οποίες οδηγούν σε μία κοινωνική ταξινόμηση που με τη σειρά της έχει ουσιαστικές επιπτώσεις στη ζωή των ατόμων και των κοινοτήτων. Εφόσον λοιπόν οι χρήστες δε γνωρίζουν πόσα μοιράζονται, με ποιον και πώς μπορούν οι επιχειρήσεις να αξιοποιήσουν τα δεδομένα που συλλέγουν, ο GDPR έρχεται να βελτιώσει την κατάσταση συλλογής και χρήσης των δεδομένων. Ο GDPR διευκολύνει τους καταναλωτές να κατανοήσουν ποιες πληροφορίες χρειάζονται και εναποθέτει σε αυτούς να αποφασίσουν τι θα μοιραστούν (Barnard-Wills και Ashenden (2015); Solberg (2018)).

Γίνεται, λοιπόν αντιληπτό, σύμφωνα με τους Bioglio et al (2018), ότι οι ίδιοι οι χρήστες είναι οι προστάτες των προσωπικών τους δεδομένων. Τα κοινωνικά δίκτυα (Facebook, Instagram, Twitter κ.α.) είναι στην πραγματικότητα αρχεία καταγραφής που δημιουργούνται από τον άνθρωπο. Οι χρήστες τους είναι τόσο ενήλικες όσο και ανήλικοι («ψηφιακοί ιθαγενείς») οι οποίοι έχουν λανθασμένη αντίληψη για το διαδικτυακό τους απόρρητο. Επίσης, έρευνες έχουν δείξει ότι η δραστηριότητα των χρηστών του Facebook, για παράδειγμα η επιλογή “Μου αρέσει” σε μία ανάρτηση, δίνει τη δυνατότητα να εντοπισθούν συγκεκριμένα ιδιωτικά χαρακτηριστικά του χρήστη. Επιπλέον, χαρακτηριστικά του χρήστη μπορεί να προκύψουν από χαρακτηριστικά χρηστών που ανήκουν στις ίδιες κοινότητες. Γενικότερα, προκύπτει ότι η αποκάλυψη πληροφοριών στο διαδίκτυο είναι μία εθελοντική δραστηριότητα από τους χρήστες. Βέβαια αξίζει να σημειωθεί ότι σημασία έχει και οι έλεγχοι απορρήτου να είναι πλήρως ενημερωμένοι και το δίκτυο να είναι ασφαλές.

Συμπεραίνεται, λοιπόν, από τους Barnard-Wills και Ashenden (2015), ότι είναι σημαντικό ο χρήστες του διαδικτύου να αποκτήσουν γνώσεις και δεξιότητες σχετικές με την κατανόηση των κανόνων και των πρακτικών διατήρησης διαδικτυακής ιδιωτικότητας. Ένας τρόπος να αποκτηθούν αυτές οι γνώσεις είναι μέσω της εκπαίδευσης μέσω παιχνιδιών σοβαρού σκοπού. Σε αυτό το σημείο αξίζει να επαναδιατυπωθεί ότι είναι σημαντικό ένα τέτοιο παιχνίδι να είναι σχεδιασμένο έτσι ώστε η εξέλιξη του να δεσμεύεται με τους επιδιωκόμενους στόχους μάθησης ώστε να πετύχει τα εκπαιδευτικά επιδιωκόμενα αποτελέσματα.

2.6.2 Παιχνίδι καρτών για την ορθολογική κοινή χρήση πληροφοριών στο Διαδίκτυο

Οι Fatima et al. (2019) σημειώνουν ότι, υπάρχει μία αντίληψη ότι το διαδίκτυο είναι σε γενικές γραμμές ασφαλές. Όμως εάν λάβει κανείς υπόψιν ότι ένα άτομο συνδεδεμένο στο διαδίκτυο παρακολουθείται από διάφορους ιστοτόπους αυτή η άποψη φαίνεται να μην αληθεύει. Δεν αληθεύει διότι για οποιαδήποτε δραστηριότητα πραγματοποιεί κανείς στο διαδίκτυο αφήνει και ένα ψηφιακό αποτύπωμα. Επίσης, τα κοινωνικά δίκτυα πλέον αποτελούν ένα από τα κυριότερα εργαλεία επικοινωνίας, και έχουν πολλά πλεονεκτήματα αλλά και προκλήσεις που πρέπει να αντιμετωπίσουν οι χρήστες όπως ζητήματα απορρήτου, απειλές για την ασφάλεια και κλοπές ταυτότητας. Γι᾽ αυτό και κατά τη σχεδίαση του λογισμικού το απόρρητο και η ασφάλεια πρέπει να λαμβάνονται σοβαρά υπόψιν από τους σχεδιαστές.

Οι Fatima et al. (2019) προσθέτουν ότι, στόχος του παιχνιδιού καρτών είναι να εκπαιδευτούν οι παίκτες σχετικά με του κινδύνους από την υπερβολική διαδικτυακή αποκάλυψη προσωπικών πληροφοριών. Νικητής του παιχνιδιού είναι αυτός που στο τέλος έχει τα μέγιστα προσωπικά του περιουσιακά στοιχεία διαθέσιμα (χωρίς δάνεια). Στο παιχνίδι οι παίκτες αλληλεπιδρούν με στόχο την πώληση και την αγορά περιουσιακών στοιχείων και προσωπικών πληροφοριών. Ουσιαστικά κάποιος πρέπει να αγοράσει τα μέγιστα περιουσιακά στοιχεία και να γίνει πλούσιος και έτσι να κερδίσει το παιχνίδι.

Οι Fatima et al.(2019) αναφέρουν ότι, το παιχνίδι επιδιώκει οι παίκτες να ενημερωθούν για το ψηφιακό τους αποτύπωμα, το ποιες πληροφορίες αποκαλύπτουν και τον έλεγχο των πληροφοριών τους. Δηλαδή κατά τη διάρκεια του παιχνιδιού πραγματοποιείται αγοραπωλησία προσωπικών πληροφοριών και το κίνητρο του παίκτη είναι να διατηρήσει το απόρρητο των προσωπικών δεδομένων κάποιου και το δικό του. Το παιχνίδι επιδιώκει να τονίσει τους κινδύνους που συνδέονται με την υπερβολική αποκάλυψη πληροφοριών. Επίσης, καλείται να διευθετήσει την έννοια της μάθησης μέσω παιχνιδιού.

Επιλογικά, διαπιστώθηκε από τους Fatima et al.(2019) ότι στην πραγματική ζωή οι άνθρωποι δεν είναι ιδιαίτερα προσεκτικοί σχετικά με τα προσωπικά τους στοιχεία και την κοινοποίηση τους στα μέσα κοινωνικής δικτύωσης. Οι πληροφορίες που εκθέτουν μπορεί να χρησιμοποιηθούν από εταιρείες και άλλους. Αυτή την κατάσταση προσπαθεί να προσομοιώσει το φυσικό αυτό παιχνίδι καρτών, την κατάσταση στην οποία η

απώλεια δεδομένων δημιουργεί ανασφάλεια στους παίκτες, και έτσι οι παίκτες ωθούνται στο να ανακτήσουν τις προσωπικές τους πληροφορίες. Μέσω του παιχνιδιού οι παίκτες μπορούν να αναλογιστούν ότι οι εταιρείες χρησιμοποιούν ηλεκτρονικά δεδομένα χωρίς καν να ενημερώνουν τον ιδιοκτήτη τους. Το παιχνίδι έδειξε θετικά αποτελέσματα στην ευαισθητοποίηση των συμμετεχόντων σχετικά με τους κινδύνους που συνδέονται με την υπερβολική διαδικτυακή αποκάλυψη πληροφοριών και σχετικά με την αναγνώριση των κινδύνων.

2.6.3 Το παιχνίδι καρτών “Privacy”

Το “Privacy” είναι ένα παιχνίδι καρτών, βλέπε Εικόνα 23, για δύο έως πέντε παίκτες και έχει ως στόχο να μάθουν οι παίκτες να εξισορροπούν τις δημόσιες και τις ιδιωτικές του πληροφορίες (Berger και Sæthre, 2018). Οι πληροφορίες αυτές στο παιχνίδι αντιπροσωπεύονται ως κάρτες και έτσι οι παίκτες επιλέγουν ποιες πληροφορίες θα κρατήσουν, θα ανταλλάξουν με άλλους ή θα παίξουν στο παιχνίδι.

Συγκεκριμένα, κάθε παίκτης είναι ένας χαρακτήρας που παραμένει κρυφός μέχρι το τέλος του παιχνιδιού. Οι παίκτες κρατούν στα χέρια τους τις κάρτες προσωπικών πληροφοριών. Αυτές τις διαχειρίζονται είτε παίζοντας ’τες προσπαθώντας να τις ταιριάξουν σε διάφορες στήλες κατηγοριών στο τραπέζι είτε ανταλλάσσοντας ’τες με συμπαίκτες και μετά παίρνουν μία κάρτα από τη τράπουλα Προσωπικών Πληροφοριών. Το παιχνίδι τελειώνει όταν εξαντληθούν οι κάρτες από την τράπουλα Προσωπικών Πληροφοριών. Τότε οι παίκτες αποκαλύπτουν τον χαρακτήρα τους και υπολογίζουν το σκορ τους με βάση τις κάρτες που έχουν κρατημένες στο χέρι.

Συμπερασματικά, νικητής του παιχνιδιού είναι αυτός ο οποίος έχει κάνει την καλύτερη διαχείριση των πληροφοριών - καρτών. Η διαχείριση γίνεται με τρεις τρόπους. Πρώτος, είναι το να κρατήσει ο παίκτης την κάρτα στο χέρι, δηλαδή την πληροφορία ιδιωτική. Δεύτερος τρόπος είναι να την παίξει στο τραπέζι, δηλαδή να κοινοποιήσει την πληροφορία δημόσια. Τρίτος και τελευταίος τρόπος είναι να την ανταλλάξει με άλλο παίκτη.

Επιλογικά, το παιχνίδι αξιολογήθηκε σε τρία επίπεδα, ως παιχνίδι, ως εκπαιδευτική και κοινωνική παρέμβαση και ως εργαλείο έρευνας, από διαφορετικούς ανθρώπους, αν και διαπιστώθηκε ότι ήταν περίπλοκο για νεαρούς μαθητές. Το παιχνίδι έγινε αποδεκτό από πολλούς οι οποίοι το βρήκαν ενδιαφέρον. Θετική ήταν και η στάση των παικτών απέναντι στον βαθμό στον οποίο το παιχνίδι βοήθησε στην κατανόηση και

τη σκέψη σχετικά με το απόρρητο στο διαδίκτυο. Προκύπτει ότι το παιχνίδι μπορεί να λειτουργήσει ως χρήσιμο κίνητρο για θέματα σχετικά με την ιδιωτικότητα και το απόρρητο (Barnard-Wills και Ashenden,2015).

Εικόνα 23: Στιγμιότυπο από το παιχνίδι "Privacy"

2.6.4 Το παιχνίδι "Social4School"

Το "Social4School" έχει ως στόχο τα παιδιά και οι έφηβοι να βιώσουν την τυπική δυναμική ενός διαδικτυακού κοινωνικού δικτύου σε ένα προσομοιωμένο και ελεγχόμενο περιβάλλον (Bioglio et al. 2018). Η προσομοίωση γίνεται υπό την επίβλεψη του δασκάλου/ας ο οποίος παρακολουθεί και την δραστηριότητα κάθε συμμετέχοντα. Οι παίκτες ανακαλύπτουν το φαινόμενο της διάδοσης πληροφοριών και ενισχύουν την αντίληψη τους για ζητήματα απορρήτου σχετικά με τα κοινωνικά δίκτυα. Επιπλέον, μέσα από το παιχνίδι επιδιώκεται να βελτιωθεί η ευαισθητοποίηση των παικτών σχετικά με την προστασία των προσωπικών τους δεδομένων. Στο τέλος της προσομοίωσης παρέχεται ένα σύνολο βαθμολογιών συμπεριφοράς.

Το παιχνίδι έχει τρεις φάσεις. Επίσης, το κοινωνικό δίκτυο που αναπαριστάται στο παιχνίδι είναι συνδεδεμένο. Στην πρώτη φάση ο παίκτης δημοσιεύει στο προφίλ του μια από τις προκαθορισμένες αναρτήσεις της ομάδας του και επιλέγει τη λίστα με τους φίλους του. Στην δεύτερη φάση, το παιχνίδι δείχνει σε κάθε παίκτη τα στοιχεία της προηγούμενης φάσης τα οποία δημοσίευσαν οι φίλοι του και ο παίκτης μπορεί να αντιδράσει σε αυτά είτε με like είτε μοιράζοντας 'τα με άλλους φίλους στο επόμενο βήμα του παιχνιδιού. Στην τελευταία φάση, το παιχνίδι δείχνει σε κάθε χρήστη στοιχεία που άρεσαν ή μοίρασαν οι φίλοι του, συμπεριλαμβανομένων αναρτήσεων χρηστών που δεν είναι φίλοι. Έτσι γίνεται αντιληπτός ο τρόπος διάδοσης των αναρτήσεων στα μέσα κοινωνικής δικτύωσης.

Τέλος, η βαθμολογία των παικτών παρέχεται από τον δάσκαλο όταν αυτοί ολοκληρώσουν το παιχνίδι και περιγράφει πόσο σεβάστηκαν ή όχι το απόρρητο τους και των άλλων. Τα αποτελέσματα του παιχνιδιού έδειξαν την αποτελεσματικότητα της διαδραστικής αυτής προσέγγισης μέσω του παιχνιδιού για την τόνωση της ευαισθητοποίησης των μαθητών σχετικά με τη διάδοση ιδιωτικών πληροφοριών στα διαδικτυακά κοινωνικά δίκτυα.

2.6.5 Το παιχνίδι "Kahooth"

Το "Kahooth" είναι ένα παιχνίδι ερωτήσεων πολλαπλής επιλογής που απευθύνεται σε μαθητές δευτεροβάθμιας εκπαίδευσης το οποίο συνοδευόμενο από ένα ερωτηματολόγιο επιθυμεί να μελετήσει τι γνωρίζουν οι μαθητές για την ιδιωτικότητα και την στάση τους απέναντι σε αυτή (Solberg 2018). Οι συμμετέχοντες για να παίξουν το παιχνίδι χρησιμοποιούν υπολογιστή ή φορητή συσκευή, ενώ οι ερωτήσεις εμφανίζονται στην οθόνη και συνοδεύονται από τέσσερις επιλογές/απαντήσεις. Σημασία στο παιχνίδι έχει και ο χρόνος απάντησης των ερωτήσεων, καθώς όσο αργούν οι παίκτες τόσο λιγότερους πόντους παίρνουν. Αφού τελειώσει ο χρόνος και όλοι οι μαθητές έχουν απαντήσει εμφανίζεται η σωστή απάντηση και πόσοι απάντησαν λάθος. Σε αυτόν που τρέχει το παιχνίδι δίνεται η δυνατότητα να εξηγήσει γιατί η απάντηση αυτή είναι σωστή. Τέλος, μετά την απάντηση εμφανίζονται και οι κορυφαίοι συμμετέχοντες.

Τα αποτελέσματα του "Kahooth" έδειξαν ότι το 42% των ερωτήσεων απαντήθηκαν λανθασμένα (Solberg 2018). Η ερώτηση με τις λιγότερες σωστές απαντήσεις ήταν η «Μπορεί το Snapchat να πουλήσει τις φωτογραφίες και την τοποθεσία σας;», με το ένα τέταρτο μόνο των συμμετεχόντων να απαντούν σωστά. Σύμφωνα με την πολιτική απορρήτου της συγκεκριμένης πλατφόρμας, "Snapchat", οποιοδήποτε περιεχόμενο που παρέχεται στην υπηρεσία μπορεί να διανεμηθεί σε τρίτους χωρίς να υπάρχει ευθύνη για τον τρόπο με τον οποίο το τρίτο μέρος θα χρησιμοποιεί τα δεδομένα. Μία ακόμα ερώτηση στην οποία σωστές απαντήσεις είχαν μόνο το 36% των συμμετεχόντων ήταν «Το Facebook ξέρει ποιους άλλους ιστότοπους επισκέπτεστε;» - οι απαντήσεις εδώ ήταν λανθασμένες κυρίως γιατί η πλειοψηφία πιστεύει ότι το Facebook γνωρίζει όλες τις ιστοσελίδες που επισκέπτονται οι χρήστες στο διαδίκτυο.

Γενικά, οι συμμετέχοντες έδειξαν να κατανοούν το είδος των πληροφοριών που δεν πρέπει να δημοσιεύονται στα μέσα κοινωνικής δικτύωσης. Επίσης, έδειξαν να γνωρίζουν ότι οι όροι και οι προϋποθέσεις μίας υπηρεσίας είναι δεσμευτικοί και πως οι

εφαρμογές για κινητές συσκευές έχουν πρόσβαση σε πληροφορίες τοποθεσίας σύζευξης. Κατά τη διάρκεια του "Kahooth" παρατηρήθηκε ότι οι μαθητές ήταν πολύ αφοσιωμένοι και έδειξαν να καταλαβαίνουν το παιχνίδι. Οι απαντήσεις στο ερωτηματολόγιο που ακολουθεί το "Kahooth" έδειξαν ότι το 61% των συμμετεχόντων πιστεύει ότι γνωρίζει αρκετά για το απόρρητο και το 62% δεν ενδιαφέρεται να μάθει περισσότερα γι' αυτό. Εντύπωση έκανε το γεγονός ότι το 34% απαντά ότι δεν μοιράζεται προσωπικά δεδομένα στο διαδίκτυο (όταν ακόμη και η διεύθυνση IP ενός ατόμου μπορεί να θεωρηθεί προσωπικό δεδομένο). Τέλος, το 46% των συμμετεχόντων απαντά ότι έχει μάθει κάτι παίζοντας το "Kahooth" και το 40% απαντά θετικά στο γεγονός ότι θα είναι περισσότερο ενήμερο για το απόρρητο στο μέλλον.

2.6.6 Το "Data Dealer", το "DataK" και το "Data Defenders"

Το "Data Dealer", κατά τους Nahmias et al. (2020), είναι ένα διαδικτυακό παιχνίδι για τη συλλογή και την πώληση προσωπικών δεδομένων. Στο παιχνίδι ο χρήστης αποθηκεύει μία κρυφή μνήμη φανταστικών προσωπικών δεδομένων και στη συνέχεια τα πουλάει σε εταιρείες, ασφαλιστικές εταιρείες, τμήματα ανθρώπινων πόρων ή κυβερνητικές υπηρεσίες. Στόχος του παιχνιδιού είναι να εκπαιδεύσει τους χρήστες σχετικά με την ποσότητα και την αξία των διαφορετικών τύπων προσωπικών πληροφοριών που συλλέγονται σήμερα και την πιθανή εμπορική χρήση τέτοιων δεδομένων.

Επίσης το παιχνίδι "DataK", κατά τους Nahmias et al. (2020), είναι ένα διαδικτυακό παιχνίδι που στοχεύει να ευαισθητοποιηθούν περισσότερο οι παίκτες σχετικά με την προστασία των δεδομένων. Οι παίκτες καλούνται να αντιμετωπίσουν καθημερινά διλήμματα και κάθε απόφαση τους έχει αντίκτυπο στην πρόοδο τους σε διάφορα επίπεδα.

Επιπρόσθετα, το "Data Defenders", κατά τους Nahmias et al. (2020), απευθύνεται σε παιδιά και προέφηβους και τους δείχνει πως μέσα από τις διαφημίσεις μπορούν να συλλεχθούν τα προσωπικά τους στοιχεία. Μέσα από το παιχνίδι οι έφηβοι διδάσκονται τις έννοιες των προσωπικών δεδομένων και την οικονομική τους αξία και αποκτούν στρατηγικές για να διατηρήσουν τις πληροφορίες τους ιδιωτικές. Το παιχνίδι έχει δύο γύρους και μαθαίνει στους παίκτες έννοιες της οικονομίας της πληροφορίας. Οι χρήστες μπορούν να αυξήσουν τη βαθμολογία τους στο παιχνίδι αποκαλύπτοντας πράγματα σχετικά με τον εαυτό τους, πράγμα που κάνουν πολλά δωρεάν παιχνίδια που

κερδίζουν χρήματα συλλέγοντας και πουλώντας δεδομένα χρηστών. Όμως σε αυτό το παιχνίδι οι παίκτες αποκαλύπτοντας αυτές τις πληροφορίες μειώνουν τις κρυφές βαθμολογίες απορρήτου τους.

2.6.7 Παιχνίδι για την ασφάλεια των πληροφοριών του προσωπικού υγειονομικής περίθαλψης

Έχει παρατηρηθεί, από τους Pulido et al. (2021), ότι το έγκλημα στον κυβερνοχώρο στοχεύει σε μεγάλο βαθμό στο κλάδο της υγειονομικής περίθαλψης. Αυτό συμβαίνει διότι οι ιατρικές πληροφορίες είναι πολυτιμότερες συγκριτικά με τα προσωπικά οικονομικά δεδομένα ή τα στοιχεία των πιστωτικών καρτών. Επομένως, οι εγκληματίες του κυβερνοχώρου έχουν υψηλότερα κίνητρα να στοχεύουν σε ιατρικά δεδομένα για σκοπούς οικονομικής εκμετάλλευσης ή εκμετάλλευσης για προσωπικό όφελος.

Παράλληλα, έχει διαπιστωθεί,από τους Pulido et al. (2021), ότι οι παραβιάσεις της ασφάλειας των πληροφοριών προέρχονται από το προσωπικό. Συνεπώς, αποτελεί ενδιαφέρον να αξιολογηθεί το επίπεδο ευαισθητοποίησης της ασφάλειας των μελών του υγειονομικού προσωπικού. Για τον σκοπό αυτό έχει προταθεί ένα εκπαιδευτικό επιτραπέζιο παιχνίδι που αποτελείται από μία εκπαιδευτική πλατφόρμα που είναι ένα περιβάλλον προσομοίωσης υγειονομικής περίθαλψης και επιδιώκει να ενημερώσει τους παίκτες για ενδεχόμενα συμβάντα ασφάλειας τα οποία μπορεί να θέσουν σε κίνδυνο πληροφορίες σχετικές με την υγεία. Οι παίκτες πρέπει να εντοπίσουν τις ενέργειες που διατηρούν ασφαλή τα ιατρικά δεδομένα και να διαμορφώσουν πιθανές λύσεις σε συμβάντα ασφάλειας.

Οι Pulido et al. (2021) υπογραμμίζουν ότι, στόχος του πειράματος εφαρμογής αυτού του επιτραπέζιου παιχνιδιού ήταν να συγκριθεί το επίπεδο ευαισθητοποίησης για την ασφάλεια των πληροφοριών των παικτών πριν και μετά το παιχνίδι. Οι παίκτες αρχικά απάντησαν σε ένα ερωτηματολόγιο με δημογραφικές ερωτήσεις, στη συνέχεια απάντησαν σε ερωτήσεις σχετικές με την ασφάλεια των πληροφοριών, την ευαισθητοποίηση για την ασφάλεια και τα συστήματα υγειονομικής περίθαλψης για να γίνει γνωστό το υπόβαθρό τους σε αυτά τα θέματα. Έπειτα απάντησαν σε ένα ερωτηματολόγιο προ-αξιολόγησης. Στη συνέχεια, έπαιξαν το παιχνίδι και μετά απάντησαν σε ερωτήσεις με περιεχόμενα παρόμοια με τις αρχικές. Αφού ολοκληρώθηκε η συμμετοχή των παικτών τα ευρήματα συγκεντρώθηκαν και αξιολογήθηκαν με σκοπό

να εντοπισθεί αν υπήρξε αλλαγή στο επίπεδο ευαισθητοποίησης τους μετά την επαφή με το παιχνίδι. Από την αξιολόγηση προέκυψε ότι οι συμμετέχοντες είχαν μικρή σαφήνεια σχετικά με το περιεχόμενο του παιχνιδιού. Οι έλεγχοι ασφαλείας είναι περίπλοκοι και γι' αυτό είναι σημαντική η εκπαίδευση ευαισθητοποίησης να γίνεται με τέτοιο τρόπο που το προσωπικό να κατανοεί ποιες διαδικασίες χρειάζεται να ακολουθούνται για ένα περιστατικό ασφαλείας και ποιος μπορεί να είναι ο αντίκτυπος ενός περιστατικού ασφαλείας.

2.6.8 Το παιχνίδι "Cybersmart Detective" του Cybersmart

Το "Cybersmart Detective", σύμφωνα με τους Chadwick και Knight (2010), ανήκει στο Cybersmart το οποίο αναπτύχθηκε από την Αυστραλιανή Αρχή Επικοινωνιών και Μέσων (ACMA) στα πλαίσια του προγράμματος ασφάλειας στον κυβερνοχώρο της Αυστραλιανής Κυβέρνησης. Έχοντας ως δεδομένο ότι οι σημερινοί μαθητές δεν γνώρισαν ποτέ τον κόσμο χωρίς την ύπαρξη του διαδικτύου αλλά και την ολοένα και αυξανόμενη χρήση του από τους νεαρούς η ACMA δημιούργησε το Cybersmart (Britnell(2012); Chadwick και Knight (2010)).

Το Cybersmart περιλαμβάνει το παιχνίδι "Cybersmart Detectives" το οποίο απευθύνεται σε μαθητές ηλικίας 10 έως 12 ετών και ασχολείται με την αντιμετώπιση της διαδικτυακής αποπλάνησης και την προστασία των προσωπικών δεδομένων. Στο "Cybersmart Detectives" τα παιδιά εργάζονται σε ομάδες για να διερευνήσουν και να λύσουν ένα πρόβλημα σχετικά με το διαδίκτυο. Διδάσκει στα παιδιά το πόσο αναγκαία είναι η προστασία των προσωπικών πληροφοριών στο διαδίκτυο (Britnell(2012); Chadwick και Knight (2010)).

Το "Cybersmart Detectives", όπως αναφέρουν οι Zhang-Kennedy και Chiasson (2021), αποτελεί μέρος της σειρά βίντεο κινουμένων σχεδίων Cybersmart Challenge. Συγκεκριμένα, οι χαρακτήρες βρίσκουν ένα χαμένο κινητό τηλέφωνο το οποίο λαμβάνει ένα μήνυμα κειμένου στο ¨Rollergirl13¨. Έπειτα οι πρωταγωνιστές βρίσκουν τα προσωπικά στοιχεία του ¨Rollergirl13¨ στο διαδίκτυο αλλά αργότερα μία συζήτηση διακόπτει την ιστορία.

Το παιχνίδι, αναφέρουν οι Nicolaidou και Venizelou (2020), δοκιμάστηκε σε 292 μαθητές με σκοπό τη διδασκαλία της ηλεκτρονικής ασφάλειας. Αξιολογήθηκε από ένα δείγμα των μαθητών με ένα ερωτηματολόγιο σχετικό με τις συνήθειες τους στο διαδίκτυο και τη χρήση φορητών συσκευών. Αυτό το ερωτηματολόγιο δόθηκε στα

παιδιά πριν και μετά την ενασχόληση τους με το παιχνίδι. Προέκυψε ότι το παιχνίδι ωφέλησε τα παιδιά.

2.6.9 Συμπεράσματα

Συμπερασματικά, όλοι οι άνθρωποι έχουν το δικαίωμα να επιθυμούν την προστασία των προσωπικών τους δεδομένων. Όμως, δεν έχουν όλοι οι χρήστες του διαδικτύου τις γνώσεις ή τα μέσα να αντιληφθούν τις επιπτώσεις της υπερβολικής αποκάλυψης πληροφοριών σε αυτό. Για τον σκοπό αυτό έχουν δημιουργηθεί πληθώρα παιχνιδιών που στοχεύουν στην ευαισθητοποίηση σχετικά με την προστασία των προσωπικών πληροφοριών των χρηστών του διαδικτύου.

Τα παιχνίδια αυτά απευθύνονται σε διάφορες ηλικίες, άλλα σε μαθητές και σπουδαστές και άλλα σε ενήλικες. Σε γενικές γραμμές όλα φάνηκαν χρήσιμα στους χρήστες στους οποίους δοκιμάστηκαν. Επιπλέον, κατάφεραν να επηρεάσουν θετικά τους παίκτες και να τους κάνουν να ευαισθητοποιηθούν απέναντι στα ζητήματα που αφορούν την προστασία των προσωπικών δεδομένων.

2.7 Απαντήσεις στα ερωτήματα της βιβλιογραφικής μελέτης

2.7.1 Εισαγωγή

Στην παρούσα ενότητα πραγματοποιείται μία σύνθεση ευρημάτων, που αφορούν τα παιχνίδια τα οποία αναλύθηκαν στα πλαίσια της βιβλιογραφικής επισκόπησης. Επιπλέον, μέσα από αυτή την ενότητα θα απαντηθούν συλλογικά όλα τα ερωτήματα τα οποία αφορούν την βιβλιογραφική μελέτη.

Τα ερωτήματα τα οποία κλήθηκε να απαντήσει η βιβλιογραφική επισκόπηση είναι τα ακόλουθα:

(Ε.Β.Ε.1) Ποια παιχνίδια σοβαρού σκοπού είναι σχετικά με την ασφάλεια και το απόρρητο στο διαδίκτυο;

(Ε.Β.Ε.2) Σε ποιους απευθύνονται;

(Ε.Β.Ε.3) Ποια είναι η εμπειρία του χρήστη από αυτά;

(Ε.Β.Ε.4) Ποια είναι τα μαθησιακά αποτελέσματα;

2.7.2 Ερωτήματα

2.7.2.1 Ποια παιχνίδια σοβαρού σκοπού έχουν αναπτυχθεί σχετικά με την ασφάλεια και το απόρρητο στο διαδίκτυο; Σε ποιους απευθύνονται;

Στην παρούσα ενότητα παρουσιάζονται τα παιχνίδια που εντοπίστηκαν στην βιβλιογραφία σε πίνακες. Κάθε στήλη του πίνακα, εκτός από την πρώτη, αφορά και διαφορετικά χαρακτηριστικά του εκάστοτε παιχνιδιού. Στην πρώτη στήλη με έντονη γραφή αναφέρεται το όνομα του παιχνιδιού, στην δεύτερη η μορφή του (αναλογική ή ψηφιακή) και στην τρίτη το είδους συσκευής για την οποία προορίζεται. Στις επόμενες δύο στήλες αναγράφεται η ηλικία στην οποία απευθύνεται η χρήση του και το βασικό θέμα του παιχνιδιού, αντίστοιχα. Τέλος, τα κελιά του πίνακα με περιεχόμενο "Δεν εντοπίστηκε" ξεκαθαρίζουν ότι για το συγκεκριμένο παιχνίδι στην παρούσα βιβλιογραφία δεν εντοπίστηκε το περιεχόμενο της στήλης του πίνακα. Επεξηγηματικά, για το παιχνίδι "**CySecEscape"** δεν εντοπίστηκε στη βιβλιογραφία οι ηλικίες στις οποίες απευθύνεται.

Στην πρώτη κατηγορία παιχνιδιών, "Ασφάλεια στον Κυβερνοχώρο", εντοπίστηκαν δώδεκα παιχνίδια, το οποία παρουσιάζονται στον Πίνακα 1.

Πίνακας 1: Παιχνίδια σχετικά με την Ασφάλεια στον Κυβερνοχώρο

Παιχνίδια	Αναλογικά/ Ψηφιακά	Συσκευή	Ηλικία	Θέμα
Happy Hippo	Ψηφιακό	Κινητές συσκευές	Παιδιά προσχολικής ηλικίας	Ψηφιακή ευεξία
Be smart when online!	Ψηφιακό	Φορητές συσκευές	Παιδιά ηλικίας 11-12	Δεξιότητες ηλεκτρονικής ασφάλειας
Internet Safety Game	Ψηφιακό Διαδικτυακό	*Δεν εντοπίστηκε*	Μικρά ηλικιακά παιδιά	Ασφάλεια στο διαδίκτυο
Cyber Smart	Ψηφιακό	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	e-Safety
CySecEscape	Η δεύτερη έκδοση είναι ψηφιακή	Φορητή συσκευή	*Δεν εντοπίστηκε*	Ασφάλεια των μικρομεσαίων επιχειρήσεων στον κυβερνοχώρο
PASDJO	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Κωδικοί πρόσβασης
SREG	Αναλογικό	Παιχνίδι καρτών	*Δεν εντοπίστηκε*	Ασφάλεια στον κυβερνοχώρο
Internet Hero	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Παιδιά ηλικίας 9-12 ετών	Τρόπος χρήσης του διαδικτύου
Pomega	Ψηφιακό	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Phishing, κωδικοί πρόσβασης, κοινωνικά δίκτυα, ασφάλεια κινητών τηλεφώνων και φυσική ασφάλεια
Cyber Air-Strike	Ψηφιακό Διαδικτυακό	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Κυβερνοασφάλεια
Cyber Detective	Ψηφιακό	Κινητές συσκευές	*Δεν εντοπίστηκε*	Κοινωνικά δίκτυα, phishing και κωδικοί πρόσβασης
Gamified Approach	Ψηφιακό	*Δεν εντοπίστηκε*	Ενήλικες	Δεξιότητες κυβερνοασφάλειας

Συνοπτικά, από τα στοιχεία του παραπάνω πίνακα προέκυψε ότι μόνο ένα παιχνίδι αυτής της κατηγορίας είναι αναλογικό ενώ εννέα είναι σε ψηφιακή μορφή. Επιπλέον, όσα παιχνίδια εντοπίστηκαν είναι κατάλληλα για φορητές συσκευές. Παράλληλα, τέσσερα παιχνίδια απευθύνονται σε παιδιά ενώ ένα σε ενήλικες.

Στην δεύτερη κατηγορία παιχνιδιών, “Phishing” και “Hacking”, εντοπίστηκαν οκτώ παιχνίδια, τα οποία φαίνονται στον Πίνακα 2.

Πίνακας 2: Παιχνίδια σχετικά με το Phishing και το Hacking

Παιχνίδια	Αναλογικά/ Ψηφιακά	Συσκευή	Ηλικία	Θέμα
Anti-Phishing Educational Game	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Σχετικό με URL διευθύνσεις
Anti-Phishing Phill	Ψηφιακό	Κινητές συσκευές	*Δεν εντοπίστηκε*	Σχετικό με URL διευθύνσεις
What.Hack	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Λήψη αποφάσεων
Hacknet	Ψηφιακό	Η/Υ	*Δεν εντοπίστηκε*	Προσομοίωση Hacking
Uplink	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Εντολές δικτύου
CyberCIEGE	Ψηφιακό	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Ασφάλεια υπολογιστή και δικτύου
NITE TEAM 4	Ψηφιακό	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Προσομοίωση υπολογιστή σε θέματα κυβερνοασφάλειας
HackLearn	Ψηφιακό	Αρχικά αυτόνομη εφαρμογή Η/Υ Τελικά εφαρμογή για όλες τις συσκευές	*Δεν εντοπίστηκε*	Προσομοίωση Hacking

Συνοψίζοντας, από τα στοιχεία του παραπάνω πίνακα προέκυψε ότι πέντε παιχνίδια είναι σε ψηφιακή μορφή. Επιπλέον, ένα είναι κατασκευασμένο για κινητές συσκευές, ένα για Ηλεκτρονικό Υπολογιστή και ένα ενδείκνυται για όλες τις συσκευές.

Στην τρίτη κατηγορία, “Ζητήματα Απορρήτου”, εντοπίστηκαν δεκαεπτά παιχνίδια, τα οποία παρουσιάζονται στον Πίνακα 3.

Πίνακας 3: Παιχνίδια σχετικά με Ζητήματα Απορρήτου

Παιχνίδια	Αναλογικά/ Ψηφιακά	Συσκευή	Κατάλληλη Ηλικία	Θέμα
Δωμάτιο Απόδρασης για Ζητήματα Απορρήτου	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Δεξιότητες απορρήτου
Privacy and Security Awareness Training Game	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Μεγαλύτερα ηλικιακά άτομα	Εντοπισμός ζητημάτων απορρήτου
Interland-Be Internet Awesome	Ψηφιακό	*Δεν εντοπίστηκε*	Παιδιά δευτέρας έως έκτης δημοτικού	Απόρρητο, κοινή χρήση πληροφοριών, πλαστά προφίλ και phishing
Privacy Pirates	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Παιδιά ηλικίας 7- 9 ετών	Έννοιες σχετικές με το διαδίκτυο
What Can Go Wrong?	Ψηφιακό	Η/Υ	*Δεν εντοπίστηκε*	Ασφάλεια και απόρρητο κινητών συσκευών
Make My Phone Secure!	Ψηφιακό	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Απόρρητο κινητού τηλεφώνου
Be Aware!	Ψηφιακό	Android	*Δεν εντοπίστηκε*	Παραβίαση ΑΤΜ
Wear OS	Ψηφιακό	Έξυπνο Android ρολόι	*Δεν εντοπίστηκε*	Απόρρητο και έξυπνο ρολόι
Social Sim Parents	Ψηφιακό	*Δεν εντοπίστηκε*	Ενήλικες	Γονείς και απόρρητο
Friend Inspector	Ψηφιακό, συνδέεται με το προφίλ στο Facebook	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Απόρρητο στο Facebook
Think aloud	Ψηφιακό	Κινητές συσκευές	Ενήλικες, προγραμματιστές	Πολιτικές απορρήτου
Leech	Ψηφιακό	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Πολιτικές απορρήτου
Puzzle Policy	Ψηφιακό	Κινητές συσκευές	*Δεν εντοπίστηκε*	Πολιτικές απορρήτου
Cookie Mania	Ψηφιακό	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Cookies
PrivaCity	Ψηφιακό Διαδικτυακό, chatbot στην πλατφόρμα του Facebook Messenger	*Δεν εντοπίστηκε*	Για μαθητές ηλικίας 16-18	Απόρρητο γεωγραφικής τοποθεσίας
Location Stalker	Ψηφιακό	Φορητές συσκευές	*Δεν εντοπίστηκε*	Απόρρητο γεωγραφικής τοποθεσίας

Περιληπτικά, από τα στοιχεία του παραπάνω πίνακα προέκυψε ότι δεκατρία παιχνίδια είναι σε ψηφιακή μορφή. Επιπλέον, τέσσερα είναι κατασκευασμένα για κινητές συσκευές, ένα για Ηλεκτρονικό Υπολογιστή και ένα για έξυπνο ρολόι. Επίσης, τρία απευθύνονται σε μαθητές διαφόρων ηλικιών και τρία σε ενήλικες.

Στην τέταρτη κατηγορία, "Προσωπικά Δεδομένα", εντοπίστηκαν εννέα παιχνίδια, τα οποία αποτυπώνονται στον Πίνακα 4.

Πίνακας 4: Παιχνίδια σχετικά με τα Προσωπικά Δεδομένα

Παιχνίδια	Αναλογικά/ Ψηφιακά	Συσκευή	Ηλικία	Θέμα
Παιχνίδι Καρτών για ορθολογική κοινή χρήση πληροφοριών στο Διαδίκτυο	Αναλογικό	Παιχνίδι καρτών	*Δεν εντοπίστηκε*	Ψηφιακό αποτύπωμα και αποκάλυψη προσωπικών πληροφοριών
Privacy	Αναλογικό	Παιχνίδι καρτών	*Δεν εντοπίστηκε*	Εξισορρόπηση δημόσιων και ιδιωτικών πληροφοριών
Social4School	Ψηφιακό	*Δεν εντοπίστηκε*	Παιδιά και έφηβοι	Προσομοίωση κοινωνικού δικτύου
Kahooth	Ψηφιακό, πλατφόρμα παιχνιδιού	Η/Υ και φορητή συσκευή	Μαθητές δευτεροβάθμιας εκπαίδευσης	Ιδιωτικότητα
Data Dealer	Διαδικτυακό-Ψηφιακό	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Συλλογή και πώληση προσωπικών δεδομένων
DataK	Διαδικτυακό	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Αντιμετώπιση καθημερινών διλημμάτων σχετικών με τα προσωπικά δεδομένα
DataDefenders	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Παιδια και προέφηβοι	Συλλογή προσωπικών δεδομένων
Ασφάλεια πληροφοριών προσωπικού υγειονομικής περίθαλψης	Αναλογικό	Επιτραπέζιο παιχνίδι	Ενήλικες	Ασφάλεια πληροφοριών προσωπικού υγειονομικής περίθαλψης
Cybersmart Detective	Ψηφιακό	*Δεν εντοπίστηκε*	Παιδιά ηλικίας 10 έως 12 ετών	Αντιμετώπιση διαδικτυακής αποπλάνησης

Περιληπτικά, από τα στοιχεία του παραπάνω πίνακα προέκυψε ότι τρία παιχνίδια είναι σε αναλογική μορφή και τέσσερα σε ψηφιακή. Επιπρόσθετα, τέσσερα απευθύνονται σε ανήλικους και ένα σε ενήλικες.

2.7.2.2 Ποια είναι η εμπειρία του χρήστη από τα παιχνίδια που εντοπίστηκαν;

Στην παρούσα ενότητα παρουσιάζεται η εμπειρία του χρήστη από τα παιχνίδια που εντοπίστηκαν. Κάθε στήλη του πίνακα, εκτός από την πρώτη, αφορά την αξιολόγηση του εκάστοτε παιχνιδιού σχετικά με την εμπειρία των χρηστών που το δοκίμασαν. Στην πρώτη στήλη με έντονη γραφή αναφέρεται το όνομα του παιχνιδιού και στην δεύτερη αν αξιολογήθηκε, στην Εικόνα 24 παρουσιάζεται σε ποσοστά το σύνολο των παιχνιδιών, όλων των κατηγοριών, που έχουν ή δεν έχουν αξιολογηθεί ή δεν έχει εντοπιστεί η αξιολόγηση τους στην παρούσα βιβλιογραφική επισκόπηση. Εάν από την παρούσα βιβλιογραφική επισκόπηση εντοπίστηκε ότι το παιχνίδι αξιολογήθηκε στις υπόλοιπες στήλες του πίνακα αναγράφεται η αξιολόγηση του ως προς τη διεπαφή, το υλικό και το περιβάλλον, τους στόχους, τα σχόλια, την πρόκληση και το αν οι παίκτες χρειάστηκαν βοήθεια. Τέλος, τα κελιά του πίνακα με περιεχόμενο "Δεν εντοπίστηκε" ξεκαθαρίζουν ότι για το συγκεκριμένο παιχνίδι στην παρούσα βιβλιογραφία δεν εντοπίστηκε το περιεχόμενο της στήλης του πίνακα. Επεξηγηματικά, για το παιχνίδι "**Happy Hippo"** δεν εντοπίστηκε στη βιβλιογραφία αν οι παίκτες που το αξιολόγησαν χρειάστηκαν βοήθεια.

Στον παρακάτω πίνακα παρουσιάζονται στοιχεία για την εμπειρία των χρηστών στα παιχνίδια της κατηγορίας "Ασφάλεια στον Κυβερνοχώρο". Οι πληροφορίες συλλέχθηκαν από την βιβλιογραφία. Για όσα παιχνίδια του Πίνακα 1 δεν βρέθηκαν, από την παρούσα βιβλιογραφική επισκόπηση, στοιχεία αξιολόγησης, δεν γίνεται αναφορά τους στον Πίνακα 5.

Πίνακας 5: Εμπειρία των χρηστών στα παιχνίδια της κατηγορίας Ασφάλεια στον Κυβερνοχώρο

Παιχνίδια	Αξιολόγηση	Διεπαφή Επιλογή υλικού Περιβάλλον	Στόχοι Σαφείς και απλοί	Σχόλια και ανταμοιβές	Πρόκληση	Βοήθεια
Happy Hippo	Ναι , από 6 ειδικούς του χώρου της προσχολικής εκπαίδευσης	Πολύ καλή διεπαφή (4,3/5) Πολύ καλή η επιλογή υλικού και το περιβάλλον, τα θέμα των ζώων, οι εικόνες, οι ήχοι κτλ (4,5/5)	Καλοί στόχοι (4/5) Ζητήθηκε οι οδηγίες να ήταν πιο ξεκάθαρες	Καλά (4/5)	Καλή (4/5)	*Δεν εντοπίστηκε*
Be smart when online!	Ναι, από μαθητές σχολείου	Πολύ καλή διεπαφή 4,39/5 Το 93,7% των μαθητών βρήκε ενδιαφέρον το περιβάλλον, το 83,4% τις εικόνες και το 93,8% τα βίντεο	Το 87,6% απάντησε ότι βρήκε το περιεχόμενο κατανοητό	Το 97,9% σχολίασε θετικά την ανατροφοδότηση	*Δεν εντοπίστηκε*	Δεν χρειάστηκαν βοήθεια
CySecEscape	Ναι, από 4 συμμετέχοντες	Η διεπαφή μπέρδεψε τους συμμετέχοντες	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Ικανοποιητική	*Δεν εντοπίστηκε*
PASDJO	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Σύντομο και απλό	Υπάρχει ανατροφοδότηση	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Pomega	Ναι, από 3 ομάδες χρηστών	Ικανοποιητική	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Cyber Detective	Ναι , από έφηβους	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Gamified Approach	Δεν έχει δοκιμαστεί					

Στον παρακάτω πίνακα παρουσιάζονται στοιχεία για την εμπειρία των χρηστών στα παιχνίδια της κατηγορίας "Phishing" και "Hacking". Οι πληροφορίες συλλέχθηκαν από τη βιβλιογραφία. Για όσα παιχνίδια του Πίνακα 2 δεν εντοπίστηκε από την παρούσα βιβλιογραφική επισκόπηση αξιολόγηση, δεν γίνεται αναφορά τους στον Πίνακα 6.

Πίνακας 6: Εμπειρία των χρηστών στα παιχνίδια της κατηγορίας Phishing και Hacking

Παιχνίδια	Αξιολόγηση	Διεπαφή Επιλογή υλικού Περιβάλλον	Στόχοι Σαφείς και απλοί	Σχόλια και ανταμοιβές	Πρόκληση	Βοήθεια
Anti-Phishing Educational Game	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Άμεση ανατροφοδότηση	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Anti-Phishing Phill	Ναι	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Άμεση ανατροφοδότηση	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
CyberCIEGE	Ναι , από διάφορες μελέτες ως προς την αποτελεσματικότητα του	Πολύπλοκο περιβάλλον	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Πάντα με βοήθεια από δάσκαλο-εκπαιδευτή
NITE TEAM 4	Ναι, από μαθητές	Υψηλή διαδραστικότητα Παροχή υποστηρικτικού υλικού	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Υψηλή πρόκληση	Αυτομάθηση και αυτοαξιολόγηση
HackLearn	Ναι, από μαθητές	Ωραία χρώματα, φόντο και εικονίδια Εύκολα κατανοητή η χρήση της διεπαφής	Τα διδακτικά περιεχόμενα βοηθούν τον παίκτη να θυμηθεί-κατανοήσει πτυχές του παιχνιδιού	Οι συμβουλές βοηθούν τον παίκτη να ολοκληρώσει την αποστολή	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*

Στον παρακάτω πίνακα παρουσιάζονται στοιχεία για την εμπειρία των χρηστών στα παιχνίδια της κατηγορίας “Ζητήματα Απορρήτου”. Οι πληροφορίες συλλέχθηκαν από τη βιβλιογραφία της παρούσας διπλωματικής. Για όσα παιχνίδια του Πίνακα 3 δεν εντοπίστηκε από την παρούσα βιβλιογραφική επισκόπηση αξιολόγηση, δεν γίνεται αναφορά τους στον Πίνακα 7.

Πίνακας 7: Εμπειρία των χρηστών στα παιχνίδια της κατηγορίας Ζητήματα Απορρήτου

Παιχνίδια	Αξιολόγηση	Διεπαφή Επιλογή υλικού Περιβάλλον	Στόχοι Σαφείς και απλοί	Σχόλια και ανταμοιβές	Πρόκληση και δέσμευση	Βοήθεια
Privacy and Security Awareness Training Game	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Ο παίκτης λαμβάνει σχόλια για κάθε κίνδυνο μαθαίνοντας έτσι περισσότερα για κάθε ζήτημα	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Interland-Be Internet Awesome	Ναι	Περιλαμβάνει πρόγραμμα σπουδών για δασκάλους, πόρους για γονείς και ένα διαδικτυακό παιχνίδι	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
What Can Go Wrong?	Ναι, από 21 συμμετέχοντες	Δεν εντοπίστηκε	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Make My Phone Secure!	Ναι, από 20 συμμετέχοντες	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Be Aware!	Δεν έχει δοκιμαστεί					
Wear OS	Ναι, από 10 ενήλικες φοιτητές 5 ήταν στην ομάδα (1) θεραπείας, και 5 στην ομάδα (2) ελέγχου	Χρηστικό, ευκολία αλληλεπίδρασης. Επαναλαμβανόμενο. Για Android πράγμα που αποκλείει το AppleWatch	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Οι χρήστες ήθελαν επιπλέον προκλήσεις	*Δεν εντοπίστηκε*
SocialSimParents	Ναι, από ενήλικες γονείς	Μία διεπαφή ιστού κοινωνικού δικτύου	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Λίγοι ήταν αυτοί που χρειάστηκαν περισσότερες οδηγίες
Think aloud	Ναι, από 20 συμμετέχοντες	Πολλοί το βρήκαν εύχρηστο, δήλωσαν ότι οι περισσότεροι θα μπορούσαν να μάθουν να το παίζουν Λίγοι το βρήκαν περίπλοκο και άβολο στη χρήση	Οι λειτουργίες του παιχνιδιού σε πολλούς φάνηκαν καλά ενσωματωμένες	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Λίγοι χρειάστηκαν υποστήριξη από τεχνικό
Leech	Έγιναν δύο αξιολογήσεις: η πρώτη με 12 ερευνητές από το Πανεπιστήμιο Goethe και η δεύτερη από 6 άτομα μικτού υποβάθρου	Από την αξιολόγηση προέκυψε ανάγκη βελτιστοποίησης της χρηστικότητας, το οποίο έγινε, αργότερα με την προσθήκη επεξηγήσεων και οδηγιών	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*

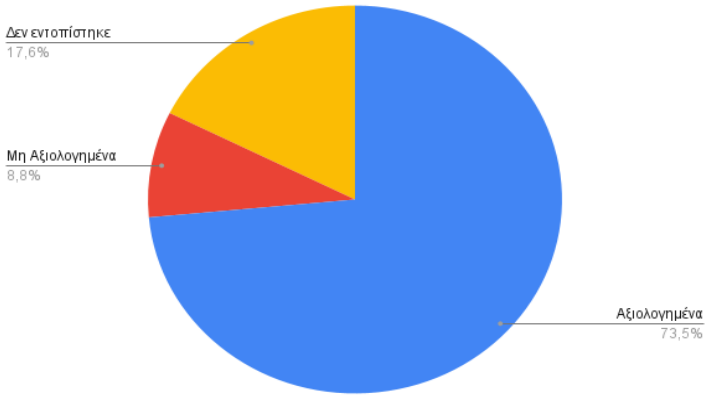
Puzzle Policy	Ναι, από 18 συμμετέχοντες	8 βρήκαν το παιχνίδι διασκεδαστικό, καλό και ενδιαφέρον, ένας το βρήκε απογοητευτικό, όσοι ήταν στην ομάδα που ασχολήθηκε με το κείμενο βρήκαν το παιχνίδι μονότονο και επαναλαμβανόμενο. Τα εφέ του παιχνιδιού ήταν πολύ μικρά, κάποια αντικείμενα ήταν δύσκολο να βρεθούν	Οι περισσότεροι συμμετέχοντες στην ομάδα κειμένου δυσκολεύτηκαν να συγκεντρωθούν σε αντίθεση με αυτούς της ομάδας παιχνιδιού, 6 στους 9 συμμετέχοντες βρήκαν εύκολη την επίλυση του παιχνιδιού	*Δεν εντοπίστηκε*	Οι παίκτες ηθελαν περισσότερα παζλ	*Δεν εντοπίστηκε*
Cookie Mania	Δεν έχει δοκιμαστεί					
PrivaCity	Ναι, από 7 μεταπτυχιακούς φοιτητές πληροφορικής	Διεπαφή Facebook Messenger Η χρήση των emojis είχε ως αποτέλεσμα η χρηστικότητα του παιχνιδιού να είναι πολύ καλή	Οι παίκτες κατάλαβαν γρήγορα πώς να παίξουν το παιχνίδι και χρειάστηκαν 15-35 λεπτά για να το ολοκληρώσουν. Αρκετά χαμηλής δυσκολίας. Η γλώσσα του παιχνιδιού απλή και κατανοητή με εξαίρεση κάποιες λέξεις που δυσκόλεψαν κάποιους παίκτες	Τα σχόλια feedback μετά τις λανθασμένες απαντήσεις στο κουίζ ήταν πολύ διδακτικά, οι παίκτες ήθελαν να μάθουν γιατί έκαναν λάθος	Τα κύρια στοιχεία δέσμευσης ήταν το παιχνίδι ρόλων και ο χαρακτήρας του chatbot	*Δεν εντοπίστηκε*
Location Stalker	Ναι, από 8 μαθητές/φοιτητές 16-25 ετών που έπαιξαν και αξιολόγησαν την έκδοση σε φυσική μορφή και όχι στην ψηφιακή που είναι η επιθυμητή, στην οποία οι παίκτες δεν θα μπορούν να κοιτάζονται	Διασκεδαστικό Ευκολότερο σε όσους είχαν παίξει το παιχνίδι Mafia Το γεγονός ότι είχαν περισσότερη επαφή μεταξύ τους οι παίκτες έκανε το παιχνίδι πιο ενδιαφέρον από το να μη βλέπουν τις σωματικές κινήσεις το παικτών (ψηφιακή έκδοση)	Οι κανόνες του παιχνιδιού ήταν μπερδεμένοι στην κατανόηση στην αρχή αλλά μετά από μία δοκιμή ξεκαθαρίστηκαν πλήρως	*Δεν εντοπίστηκε*	Αν το παιχνίδι είχε νέους κανόνες διαφορετικούς από το παιχνίδι Mafia θα βοηθούσε στο να δοθεί μία αίσθηση ατομικότητας	*Δεν εντοπίστηκε*

Στον Πίνακα 8 παρουσιάζονται στοιχεία για την εμπειρία των χρηστών στα παιχνίδια της κατηγορίας “Προσωπικά Δεδομένα”. Οι πληροφορίες συλλέχθηκαν από τη βιβλιογραφία της παρούσας διπλωματικής. Για όσα παιχνίδια του Πίνακα 4 δεν εντοπίστηκε από την παρούσα βιβλιογραφική επισκόπηση αξιολόγηση, δεν γίνεται αναφορά τους στον Πίνακα 8.

Πίνακας 8: Εμπειρία των χρηστών στα παιχνίδια της κατηγορίας Προσωπικά Δεδομένα

Παιχνίδια	Αξιολόγηση	Διεπαφή Επιλογή υλικού Περιβάλλον	Στόχοι Σαφείς και απλοί	Σχόλια και ανταμοιβές	Πρόκληση και δέσμευση	Βοήθεια
Παιχνίδι Καρτών για ορθολογική κοινή χρήση πληροφοριών στο Διαδίκτυο	Ναι, πιλοτικής εφαρμογής από 37 φοιτητές	Προτάθηκε βελτίωση των καρτών και των κανόνων	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Privacy	Ναι, από 130 παίκτες	Μερικοί παίκτες απογοητεύτηκαν από την πολυπλοκότητα αλλά γενικά έγινε αποδεκτό και σχολιάστηκε ως διασκεδαστικό. Γενικά υποστήριξαν ότι θα ήθελαν μεγαλύτερη πολυπλοκότητα. Η γραφική σχεδίαση αξιολογήθηκε ως καλή και ενδιαφέρουσα. Τα προτεινόμενα από τους συμμετέχοντες σχέδια ενσωματώθηκαν σε άλλες εκδόσεις. Οι παίκτες εστίασαν στην εμφάνιση των καρτών και όχι τόσο στην ιστορία.	Το παιχνίδι χαρακτηρίστηκε περίπλοκο από ορισμένους παίκτες και ότι αυτό αποσπά την προσοχή από ορισμένους επιδιωκόμενους στόχους	Δυσκολία στον τελικό υπολογισμό της βαθμολογίας	Κάποιοι υποστήριξαν ότι το παιχνίδι δεν είχε ανταγωνιστικό πλεονέκτημα. Κάποιος πρότεινε την προσθήκη περισσότερων καρτών για χειρισμό, αποκλεισμό ή παραπληροφόρηση αντιπάλων	*Δεν εντοπίστηκε*
Social4School	Ναι, από μαθητές 7 δημοτικών σχολίων στην Ιταλία. (14 τάξεις παιδιών 9-10, 8 τάξεις παιδιών 10-11) Συνολικά 450 παιδιά και 22 δάσκαλοι	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Kahooth	Ναι, από μαθητές δευτεροβάθμιας εκπαίδευσης	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	Σχολιάστηκε ως θετικό ότι εξηγήθηκαν οι ερωτήσεις μετά και έτσι το παιχνίδι ήταν πιο εκπαιδευτικό	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Ασφάλεια πληροφοριών προσωπικού υγειονομικής περίθαλψης	Ναι, η πρώτη αξιολόγηση έγινε από 16 συμμετέχοντες. Η δεύτερη αξιολόγηση έγινε, μετά από κάποιες αλλαγές, από	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*

	διδακτορικούς φοιτητές					
Cybersmart Detective	Ναι, αξιολογήθηκε από ένα δείγμα των 292 μαθητών 9 σχολείων στους οποίους δοκιμάστηκε	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*



Εικόνα 24: Ποσοστά των παιχνιδιών σοβαρού σκοπού όλων των κατηγοριών που αξιολογήθηκαν ή δεν αξιολογήθηκαν ή δεν εντοπίστηκαν οι αξιολογήσεις τους

Συνολικά, προκύπτει ότι τα περισσότερα παιχνίδια, για τα οποία εντοπίστηκαν πληροφορίες, αξιολογήθηκαν θετικά ως προς την ευχρηστία τους, βλέπε Εικόνα 25.

Εικόνα 25: Αποτελέσματα αξιολόγησης

2.7.2.3 Ποια είναι τα μαθησιακά αποτελέσματα για τον χρήστη από τα παιχνίδια που εντοπίστηκαν;

Στην παρούσα ενότητα παρουσιάζονται τα μαθησιακά αποτελέσματα που προέκυψαν από την αξιολόγηση των παιχνιδιών που εντοπίστηκαν. Στην πρώτη στήλη με έντονη γραφή αναφέρεται το όνομα του παιχνιδιού, στην δεύτερη η καταλληλότητα και η αποτελεσματικότητα του, στις Εικόνες 26 και 27 παρουσιάζονται συνολικά τα ποσοστά της καταλληλότητας και της αποτελεσματικότητας των παιχνιδιών όλων των

κατηγοριών. Επιπλέον, στην τρίτη στήλη αναγράφεται η εκπαιδευτική αξία του κάθε παιχνιδιού, στην τέταρτη αν δημιουργεί κίνητρα και στην τελευταία αν υπήρχε ενεργή συμμετοχή. Εάν από την παρούσα βιβλιογραφική επισκόπηση εντοπίστηκε ότι το παιχνίδι δεν αξιολογήθηκε τότε αυτό έχει αφαιρεθεί από τον πίνακα. Επιπλέον, στον πίνακα δεν υπάρχουν και τα παιχνίδια των οποίων η αξιολόγηση δεν εντοπίστηκε στην παρούσα βιβλιογραφική επισκόπηση. Τέλος, τα κελιά του πίνακα με περιεχόμενο "Δεν εντοπίστηκε" ξεκαθαρίζουν ότι για το συγκεκριμένο παιχνίδι στην παρούσα βιβλιογραφία δεν εντοπίστηκε το περιεχόμενο της στήλης του πίνακα. Επεξηγηματικά, για το παιχνίδι "**Happy Hippo"** δεν εντοπίστηκε στη βιβλιογραφία αν οι παίκτες είχαν ενεργή συμμετοχή.

Στον Πίνακα 9 παρουσιάζονται στοιχεία για τα μαθησιακά αποτελέσματα των παιχνιδιών της κατηγορίας "Ασφάλεια στον Κυβερνοχώρο". Οι πληροφορίες συλλέχθηκαν από την βιβλιογραφία.

Πίνακας 9: Μαθησιακά αποτελέσματα των παιχνιδιών της κατηγορίας Ασφάλεια στον Κυβερνοχώρο

Παιχνίδια	Καταλληλότητα και Αποτελεσματικότητα	Εκπαιδευτική αξία	Κίνητρο	Ενεργή συμμετοχή
Happy Hippo	Η καταλληλότητα βαθμολογήθηκε με 4,5/5 Για παιδιά προσχολικής ηλικίας η αποτελεσματικότητα βαθμολογήθηκε με 4,5/5	Σχολιάστηκε πως το παιχνίδι θα διαδώσει την ευαισθητοποίηση για την ψηφιακή ευεξία	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Be smart when online!	Η σύγκριση των αποτελεσμάτων της αξιολόγησης των μαθητών πριν και μετά την εφαρμογή του παιχνιδιού έδειξαν ότι η απόδοση τους στην ηλεκτρονική ασφάλεια αυξήθηκε	Η εκπαιδευτική αξία του παιχνιδιού βαθμολογήθηκε με 4,89/5	Ο βαθμός των κινήτρων που δημιουργεί το παιχνίδι βαθμολογήθηκε με 4,54/5	Η ενεργή συμμετοχή του παιχνιδιού βαθμολογήθηκε με 4/5
CySecEscape	Μετά το παιχνίδι οι συμμετέχοντες συνομίλησαν για την κυβερνοασφάλεια και φάνηκε ότι όσοι έπαιξαν το παιχνίδι θα μπορούσαν να μεταδώσουν τις γνώσεις τους μέσω της αφήγησης	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
PASDJO	Σε ότι αφορά την καταλληλότητα διαπιστώθηκε ότι το θέμα της ισχύος των κωδικών πρόσβασης δεν αντιμετωπίζεται πολύ διεξοδικά. Σε ότι αφορά την αποτελεσματικότητα διαπιστώθηκε ότι δεν διδάσκει βιώσιμες δεξιότητες και γνώσεις σχετικές με το Cyber Security	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
SREG	Θετική αξιολόγηση ως προς το ότι βοηθά τους παίκτες να κατανοήσουν τις επιθέσεις ασφαλείας	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Pomega	Οι χρήστες στην αξιολόγηση μετά το παιχνίδι σημείωσαν υψηλότερες βαθμολογίες από αυτές που συμπλήρωσαν πριν τη δοκιμή του	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Cyber Detective	Βοηθά σημαντικά στην βελτίωση της επάρκειας στην κυβερνοασφάλεια	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*

Στον Πίνακα 10 παρουσιάζονται στοιχεία για την εμπειρία των χρηστών στα παιχνίδια της κατηγορίας “Phishing” και “Hacking”. Οι πληροφορίες συλλέχθηκαν από την βιβλιογραφία.

Πίνακας 10: Μαθησιακά αποτελέσματα των παιχνιδιών της κατηγορίας Phishing και Hacking

Παιχνίδια	Καταλληλότητα Αποτελεσματικότητα	Εκπαιδευτική αξία	Κίνητρο	Ενεργή συμμετοχή
Anti-PhishingEducationalGame	Θα πρέπει να βελτιωθεί η συμπεριφορά απειλών phishing του ατόμου	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Anti-Phishing Phill	Θετικός αντίκτυπος ως προς την μάθηση και την ευαισθητοποίηση σχετικά με το phishing	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
What.Hack	Κατάλληλο για να βελτιώσει την ακρίβεια των παικτών στον εντοπισμό επερχόμενων απειλών κατά 36,7%	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Hacknet	Αποτελεσματική διδασκαλία των εντολών και εξοικείωση με συστήματα UNIX και θέματα κυβερνοασφάλειας	Η αποτελεσματικότητα του στα συγκεκριμένα θέματα οδηγεί και σε ένα ευρύ φάσμα θετικών μαθησιακών αποτελεσμάτων	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
CyberCIEGE	Δύσκολο παιχνίδι με σημεία εισόδου που μπορεί να ταλαιπωρήσουν τον χρήστη. Κατάλληλη προσέγγιση ως προς το περιεχόμενο.	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
NITE TEAM 4	Οι μαθητές κατανόησαν τη συνάφεια προϋπαρχουσών γνώσεων. Οι μαθητές εξοικειώθηκαν με τις θεμελιώδεις έννοιες.	*Δεν εντοπίστηκε*	Οι μαθητές που δοκίμασαν το παιχνίδι είχαν κίνητρο γιατί εντόπισαν μεγάλη συσχέτιση του με τα ενδιαφέροντα τους	73,46% Σημαντική και η συνεργατική μάθηση
HackLearn	Βοηθητικό ως προς την κατανόηση μοντέλων και μοτίβων επιθέσεων. Οι μαθητές εκτίμησαν τη χρησιμότητα του στη κατανόηση του μοντέλου CKC. Ενισχύθηκε η διδακτική διαδικασία μέσω του παιχνιδιού. Αποτελεσματικό ως προς την κατανόηση των θεμάτων που άπτεται.	*Δεν εντοπίστηκε*	Οι μαθητές ήθελαν περισσότερες αποστολές. Θα ήθελαν να βλέπουν και τις βαθμολογίες των άλλων παικτών.	*Δεν εντοπίστηκε*

Στον Πίνακα 11 παρουσιάζονται στοιχεία για την εμπειρία των χρηστών στα παιχνίδια της κατηγορίας “Ζητήματα Απορρήτου”. Οι πληροφορίες συλλέχθηκαν από την βιβλιογραφία της παρούσας διπλωματικής.

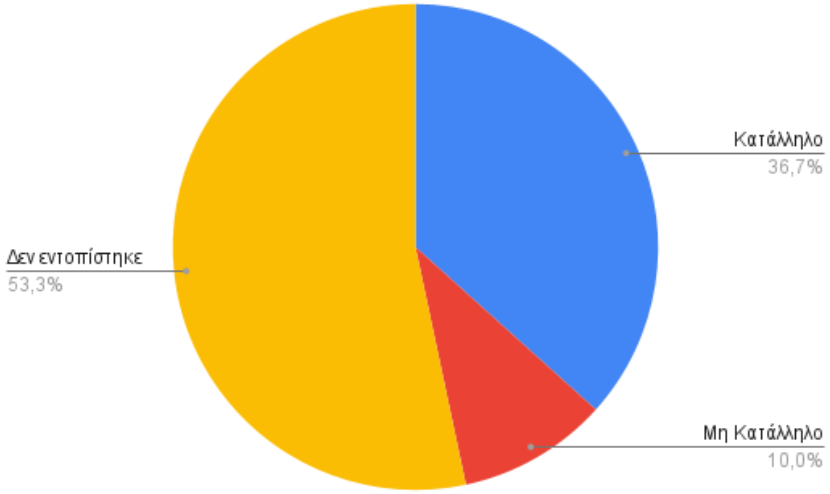
Πίνακας 11: Μαθησιακά αποτελέσματα των παιχνιδιών της κατηγορίας Ζητήματα Απορρήτου

Παιχνίδια	Καταλληλότητα Αποτελεσματικότητα	Εκπαιδευτική αξία	Κίνητρο	Ενεργή συμμετοχή
Interland-Be Internet Awesome	Προέκυψε ότι παραλείπει βασικά ζητήματα ασφάλειας στο διαδίκτυο	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
What Can Go Wrong?	Επιτυχής προσέγγιση ως προς την αύξηση της ευαισθητοποίησης	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Make My Phone Secure!	Διασκεδαστικό	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Wear OS	Οι παίκτες της ομάδας (1) θεραπείας έδειξαν να ενδιαφέρονται και να αλλάζουν περισσότερο/θεαματικά τη στάση τους απέναντι στην προστασία του απορρήτου σε αντίθεση με τους παίκτες της ομάδας (2) ελέγχου	Οι παίκτες χαρακτήρισαν το παιχνίδι ως εκπαιδευτικό	6 στους 10 το απήλαυσαν	Πλήρης ενεργή συμμετοχή των 10 ατόμων
Social Sim Parents	Οι παίκτες δήλωσαν ότι μετά τη δοκιμή απέκτησαν γνώσεις σχετικές με το απόρρητο	Το 43% των παικτών έμεινε ικανοποιημένο από τα μαθησιακά αποτελέσματα, ενώ το 22% πολύ ικανοποιημένο. Οι γονείς δεν επέδειξαν σημαντική αλλαγή στις γνώσεις τους σχετικά με την υπερβολική κοινή χρήση	*Δεν εντοπίστηκε*	Ναι
Think aloud	Οι περισσότεροι ένιωσαν μεγάλη αυτοπεποίθηση με τη χρήση του παιχνιδιού. Λίγοι ένιωσαν να χρειάζονται να μάθουν πολλά πράγματα για να παίξουν το παιχνίδι. Γενικά το 81% έμεινε ικανοποιημένο από το παιχνίδι. Το παιχνίδι συνέβαλε στην αύξηση της ευαισθητοποίησης της εκπαίδευσης για την διατήρηση της ιδιωτικής ζωής.	Οι προγραμματιστές μέσα από το παιχνίδι βοηθήθηκαν στο να αποτρέπουν τις απειλές απορρήτου. Δίδαξε στους προγραμματιστές τις αρχές του GDPR.	Από το παιχνίδι προέκυψε ότι υπάρχει ιδιαίτερο ενδιαφέρον για την ανάπτυξη εφαρμογών με δυνατότητα ιδιωτικής ζωής που να μειώνουν την υπερβολική επιτήρηση	*Δεν εντοπίστηκε*
Leech	Γενικά το παιχνίδι αξιολογήθηκε θετικά και άρεσε στους συμμετέχοντες	Όσοι δεν γνώριζαν για τις πολιτικές απορρήτου επιβεβαίωσαν ότι έμαθαν	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Puzzle Policy	Όλοι οι συμμετέχοντες ολοκλήρωσαν το πείραμα. Δύο ομάδες συμμετεχόντων, η ομάδα κειμένου είχε μικρότερη επιτυχία σε σχέση με την ομάδα παιχνιδιού	Οι περισσότεροι συμμετέχοντες άλλαξαν την στάση τους απέναντι στις πολιτικές απορρήτου και την ανάγνωσή τους. Άλλοι το βρήκαν δύσκολο και άλλοι πληροφοριακό και εκπαιδευτικό.	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
PrivaCity	Οι συμμετέχοντες πιστεύουν ότι έμαθαν κάτι για το απόρρητο. Το παιχνίδι αναγνωρίστηκε ως σχετικά διασκεδαστικό. Ο βαθμός που έδωσαν οι παίκτες για την διασκέδαση τους από το παιχνίδι ήταν 3,5/5	Όσοι είχαν γνώσεις σχετικές με το απόρρητο τα πήγαν καλύτερα. Τα κουιζ ήταν πολύ διδακτικά. Οι συμμετέχοντες αύξησαν την ευαισθητοποίηση κυρίως μέσα από το κουίζ.	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Location Stalker	Οι αρχικές πληροφορίες ήταν χρήσιμες ως προς την ευαισθητοποίηση αλλά μετά δεν ήταν πια ενδιαφέρουσες .	Ενδιαφέρον, διασκεδαστικό, αρκετές σε αριθμό πληροφορίες σχετικές με το απόρρητο της τοποθεσίας	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*

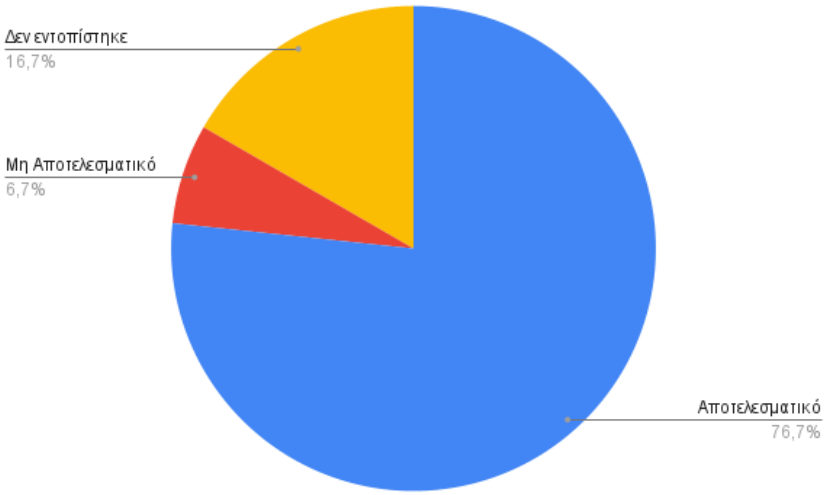
Στον Πίνακα 12 παρουσιάζονται στοιχεία για την εμπειρία των χρηστών στα παιχνίδια της κατηγορίας "Προσωπικά Δεδομένα". Οι πληροφορίες συλλέχθηκαν από την βιβλιογραφία της παρούσας διπλωματικής.

Πίνακας 12: Μαθησιακά αποτελέσματα των παιχνιδιών της κατηγορίας Προσωπικά Δεδομένα

Παιχνίδια	Καταλληλότητα Αποτελεσματικότητα	Εκπαιδευτική αξία	Κίνητρο	Ενεργή συμμετοχή
Παιχνίδι Καρτών για ορθολογική κοινή χρήση πληροφοριών στο Διαδίκτυο	Το παιχνίδι αξιολογήθηκε από τους συμμετέχοντες ως καλό	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Privacy	Το παιχνίδι βοήθησε στην κατανόηση σχετικά με το απόρρητο στο διαδίκτυο. Από την αξιολόγηση προέκυψε ότι το παιχνίδι λειτουργεί ως ερέθισμα και πηγή έμπνευσης για συζητήσεις σχετικές με το απόρρητο. Οι ίδιες οι κάρτες χρησιμεύουν και ως έναυσμα για συζητήσεις σχετικές με το θέμα.	Το παιχνίδι αξιολογήθηκε θετικά ως προς την εκπαιδευτική του αξία καθώς συμβάλει στην ανάπτυξη συζητήσεων και στην υποστήριξη, μέσω πόρων και πληροφοριών	Το παιχνίδι φαίνεται να λειτουργεί ως χρήσιμο κίνητρο για συλλογικές συζητήσεις σχετικά με το απόρρητο στο διαδίκτυο	Οι παίκτες συζήτησαν μεταξύ τους ζητήματα απορρήτου, μοιράστηκαν εμπειρίες και στρατηγικές
Social4School	Οι μαθητές μετά την εφαρμογή είχαν πιο προσεκτική συμπεριφορά	Από την αξιολόγηση του παιχνιδιού εντοπίστηκε έντονη έλλειψη εκπαίδευσης σχετικά με το απόρρητο τόσο στους δασκάλους όσο και στους μαθητές. Όλοι οι δάσκαλοι θεωρούν ότι είναι πολύ σημαντικό οι μαθητές να γνωρίζουν για το απόρρητο.	Οι δάσκαλοι δήλωσαν ότι το 27% των παιδιών είχαν μέτριο κίνητρο, ενώ το 63% υψηλό, Το ενδιαφέρον των μαθητών ήταν 20% εξαιρετικό και 80% πολύ καλό	Προσομοίωση κοινωνικού δικτύου
Kahooth	Οι παίκτες ήταν αφοσιωμένοι και απολάμβαναν το παιχνίδι. Θεωρήθηκε καλύτερο το παιχνίδι να ακολουθεί μετά από μία σύντομη διάλεξη.	Οι μαθητές έμοιαζαν να μαθαίνουν κάτι αλλά κυρίως σχετικά με την ασφάλεια πάρα με το απόρρητο	*Δεν εντοπίστηκε*	Ενεργή εμπλοκή των μαθητών
Ασφάλεια πληροφοριών προσωπικού υγειονομικής περίθαλψης	Οι συμμετέχοντες δήλωσαν ότι έμαθαν πολλά πράγματα σχετικά με την ασφάλεια των πληροφοριών, την ευαισθητοποίηση για θέματα ασφάλειας ενώ όχι τόσα για τα συστήματα υγειονομικής περίθαλψης (από πρώτη αξιολόγηση)	Από την δεύτερη αξιολόγηση προέκυψε ότι το επίπεδο μέγιστης δυνητικής ανάπτυξης των συμμετεχόντων μπορεί να επιτευχθεί μέσω της κοινωνικοποίησης μεταξύ τους	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*
Cybersmart Detective	Ωφέλιμο για μαθητές	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*	*Δεν εντοπίστηκε*



Εικόνα 26: Ποσοστό των παιχνιδιών σοβαρού σκοπού όλων των κατηγοριών τα οποία αξιολογήθηκαν ως κατάλληλα για τον σκοπό για τον οποίο δημιουργήθηκαν



Εικόνα 27: Ποσοστό των παιχνιδιών σοβαρού σκοπού όλων των κατηγοριών τα οποία αξιολογήθηκαν ως αποτελεσματικά για τον σκοπό για τον οποίο δημιουργήθηκαν

3 Εμπειρική μελέτη

3.1 Μεθοδολογία εμπειρικής μελέτης

3.1.1 Εισαγωγή

Αυτό το μέρος της διπλωματικής ασχολείται με το ερευνητικό κομμάτι της εργασίας. Η εμπειρική μελέτη καλείται να απαντήσει στα ακόλουθα ερωτήματα:

(Ε.Ε.Μ.1.) Ποια είναι η στάση των μαθητών απέναντι στη μάθηση μέσω παιχνιδιών σοβαρού σκοπού;

(Ε.Ε.Μ.2.) Ποια είναι η στάση των μαθητών απέναντι στην προστασία των προσωπικών τους δεδομένων και γενικότερα την προστασία τους στον κυβερνοχώρο;

(Ε.Ε.Μ.3.) Οι μαθητές προτιμούν να μαθαίνουν για την προστασία της ιδιωτικότητας τους μόνο μέσα από παραδοσιακούς τρόπους εκπαίδευσης και το σχολικό βιβλίο, ή συνδυαστικά με παιχνίδια σοβαρού σκοπού;

(Ε.Ε.Μ.4.) Οι μαθητές χρειάζονται βοήθεια για να ασχοληθούν με το διαδικτυακό περιβάλλον (παιχνίδι σοβαρού σκοπού) ή μπορούν να χρησιμοποιήσουν αυτά τα παιχνίδια μόνοι τους εκτός του σχολικού ωραρίου ως συμπληρωματική μάθηση;

(Ε.Ε.Μ.5.) Είναι αποτελεσματική τελικά η εκπαίδευση των μαθητών μέσω της χρήσης παιχνιδιών σοβαρού σκοπού (Digital Game-Based Learning - DGBL) στην ανάπτυξη δεξιοτήτων προστασίας στον κυβερνοχώρο;

(Ε.Ε.Μ.6.) Η εφαρμογή παιχνιδιών συμβάλλει στην ευαισθητοποίηση σχετικά με το απόρρητο και στην αλλαγή της συμπεριφοράς των μαθητών;

(Ε.Ε.Μ.7.) Ποια είναι η στάση των μαθητών απέναντι στην ασφάλεια και το απόρρητο στο διαδίκτυο, πριν και ποια μετά την εφαρμογή των παιχνιδιών;

Για να απαντηθούν αυτά τα ερωτήματα πραγματοποιήθηκε μία σειρά από διαδικασίες. Αρχικά επιλέχθηκαν δωρεάν διαδικτυακά παιχνίδια με περιεχόμενο σχετικό με την ασφάλεια και το απόρρητο στο διαδίκτυο. Έπειτα, κατασκευάστηκε ένα ερωτηματολόγιο προ-ερωτήσεων και ένα ερωτηματολόγιο μετά-ερωτήσεων. Τέλος, επιλέχθηκε ένα δείγμα μαθητών στο οποίο τέθηκαν σε εφαρμογή τα ερωτηματολόγια και δύο παιχνίδια. Ουσιαστικά, το δείγμα μαθητών κλήθηκε να απαντήσει στο

ερωτηματολόγιο προ-ερωτήσεων, στη συνέχεια να παίξει αυτά τα παιχνίδια και τέλος να απαντήσει στο ερωτηματολόγιο μετά-ερωτήσεων.

3.1.2 Εντοπισμός παιχνιδιών και επιλογή

Για την εφαρμογή της εμπειρικής μελέτης ήταν απαραίτητη η αξιοποίηση και η χρήση παιχνιδιών με περιεχόμενο σχετικό με την ασφάλεια και το απόρρητο στο διαδίκτυο. Για την επιλογή κατάλληλων παιχνιδιών υπήρχαν και άλλα κριτήρια εκτός από το να έχουν περιεχόμενο σχετικό με την ασφάλεια και το απόρρητο στο διαδίκτυο. Τα παιχνίδια έπρεπε να είναι διαθέσιμα δωρεάν, ψηφιακά και διαδικτυακά. Επιπλέον, να μην απαιτούν πολύ χρόνο για την ολοκλήρωση τους. Παράλληλα, χρήσιμα θεωρήθηκαν μόνο παιχνίδια τα οποία απευθύνονται σε ανηλίκους. Τέλος, απορρίφθηκαν παιχνίδια τα οποία απευθύνονταν σε άτομα με υπάρχουσες γνώσεις στον τομέα της Πληροφορικής. Στον Πίνακα 13 περιλαμβάνονται παιχνίδια που εντοπίστηκαν στο διαδίκτυο με θεματική σχετική με την ασφάλεια και το απόρρητο στο διαδίκτυο, τα κριτήρια τα οποία πληρούνται είναι σημειωμένα με Χ.

Πίνακας 13: Παιχνίδια

Παιχνίδια	Κριτήρια επιλογής-απόρριψης	Ικανοποίηση κριτηρίου	Επιλογή
Safe Online Surfing	Περιεχόμενο Δωρεάν Ψηφιακό Διαδικτυακό Χαμηλός χρόνος ολοκλήρωσης Απευθύνεται σε ανήλικους Δεν απαιτεί γνώσεις	X X X X X X X	Ναι
NetSmartzKids	Περιεχόμενο Δωρεάν Ψηφιακό Διαδικτυακό Χαμηλός χρόνος ολοκλήρωσης Απευθύνεται σε ανήλικους Δεν απαιτεί γνώσεις	- X X X - Ναι αλλά σε αρκετά μικρότερες ηλικίες X	Όχι
Space Shelter	Περιεχόμενο Δωρεάν Ψηφιακό Διαδικτυακό Χαμηλός χρόνος ολοκλήρωσης Απευθύνεται σε ανήλικους Δεν απαιτεί γνώσεις	X X X X X X X	Ναι
Be Internet Awesome-Reality River	Περιεχόμενο Δωρεάν Ψηφιακό Διαδικτυακό Χαμηλός χρόνος ολοκλήρωσης Απευθύνεται σε ανήλικους Δεν απαιτεί γνώσεις	X X X X X X X	Ναι
vulnhub	Περιεχόμενο Δωρεάν Ψηφιακό Διαδικτυακό Χαμηλός χρόνος ολοκλήρωσης Απευθύνεται σε ανήλικους Δεν απαιτεί γνώσεις	X X X Διαθέσιμα μόνο για λήψη - - -	Όχι
CyberCIEGE	Περιεχόμενο Δωρεάν Ψηφιακό Διαδικτυακό Χαμηλός χρόνος ολοκλήρωσης Απευθύνεται σε ανήλικους Δεν απαιτεί γνώσεις	X X X Διαθέσιμο μόνο για λήψη - - -	Όχι
Data Dealer	Περιεχόμενο Δωρεάν Ψηφιακό Διαδικτυακό Χαμηλός χρόνος ολοκλήρωσης Απευθύνεται σε ανήλικους Δεν απαιτεί γνώσεις	X X X Χρήση μετά από δημιουργία λογαριασμού - - X	Όχι
Datak	Περιεχόμενο Δωρεάν Ψηφιακό Διαδικτυακό Χαμηλός χρόνος ολοκλήρωσης Απευθύνεται σε ανήλικους Δεν απαιτεί γνώσεις	X X X X Απαιτεί πολύ χρόνο X X	Όχι

Τα παιχνίδια τα οποία αξιοποιήθηκαν ήταν τρία, το Safe Online Surfing, το Space Shelter και το Be Internet Awesome-Reality River . Τα παιχνίδια αυτά αποτέλεσαν έμπνευση για τη δημιουργία ορισμένων ερωτήσεων του ερωτηματολογίου προ-ερωτήσεων. Συγκεκριμένα, το Safe Online Surfing είναι ένα παιχνίδι διαθέσιμο στην

ιστοσελίδα fbi.gov, η οποία είναι μία επίσημη ιστοσελίδα της Αμερικανικής Κυβέρνησης. Μέσα από αυτό το παιχνίδι οι μαθητές μπορούν να μάθουν για τη διαδικτυακή ασφάλεια και την ψηφιακή ιθαγένεια. Το παιχνίδι αυτό απευθύνεται κυρίως σε μαθητές από την τρίτη έως την όγδοη τάξη (δηλαδή δευτέρα γυμνασίου). Το Safe Online Surfing, της όγδοης τάξης, αξιοποιήθηκε μόνο ως εργαλείο έμπνευσης ορισμένων ερωτήσεων του ερωτηματολογίου προ-ερωτήσεων. Δεν εφαρμόστηκε ως παιχνίδι στα πλαίσια της έρευνας, διότι, διαπιστώθηκε ότι απαιτούσε περισσότερο χρόνο από τα υπόλοιπα δύο η ολοκλήρωση του.

Το Space Shelter είναι ένα παιχνίδι της Google το οποίο είναι διαθέσιμο σε επτά γλώσσες. Στην παρούσα διπλωματική αξιοποιήθηκε η έκδοση του στην αγγλική γλώσσα. Σκοπός του παιχνιδιού είναι να διδάξει στους παίκτες πώς να παραμείνουν ασφαλείς στον κυβερνοχώρο. Το περιβάλλον του παιχνιδιού καλεί τον παίκτη να επιλέξει έναν αστροναύτη και να ξεκινήσει την αποστολή. Η αποστολή είναι ο παίκτης να οδηγήσει το διαστημόπλοιο με ασφάλεια μέσα στο διάστημα και να το ελλιμενίσει με ασφάλεια στον διαστημικό σταθμό. Αρχικά, ο παίκτης καλείται να απαντήσει σε μία σειρά ερωτήσεων με σκοπό να επιβεβαιωθεί η ικανότητα του να πλοηγήσει το διαστημόπλοιο. Όσο ο παίκτης απαντά ορθά σε ερωτήσεις η μπάρα γνώσεων που βρίσκεται στην οθόνη γεμίζει με πράσινο χρώμα. Οι πρώτες αναγνωριστικές ερωτήσεις αφορούν κωδικούς πρόσβασης, ασφάλεια υπολογιστών και ηλεκτρονικό ψάρεμα. Η πρώτη δοκιμασία της αποστολής μαθαίνει στον παίκτη να δημιουργεί ισχυρούς κωδικούς πρόσβασης. Στην δεύτερη δοκιμασία της αποστολής ο παίκτης καλείται να μάθει για τον έλεγχο ταυτότητας δύο παραγόντων ο οποίος μαζί με τον ισχυρό κωδικό προσφέρουν δύο επίπεδα προστασίας. Έπειτα από αυτές τις δοκιμασίες ο παίκτης καλείται να πλοηγήσει το διαστημόπλοιο. Στην προσπάθεια του αυτή πέφτει πάνω σε διάφορα εμπόδια-κομήτες που ουσιαστικά αποτελούν περιπτώσεις ή μη scam. Ο παίκτης καλείται να αναγνωρίσει ποια από τα μηνύματα είναι περιπτώσεις ηλεκτρονικού “ψαρέματος”. Τελικά, όταν ο παίκτης καταφέρει να φτάσει στον διαστημικό σταθμό καλείται να απαντήσει σε κάποιες ερωτήσεις με σκοπό να διαπιστωθεί εάν εμπέδωσε τις πληροφορίες που του προσέφερε το παιχνίδι. Αφού απαντήσει ο παίκτης σε αυτές τις ερωτήσεις η αποστολή ολοκληρώνεται. Αξίζει να υπογραμμισθεί ότι κατά τη διάρκεια του παιχνιδιού αν ο παίκτης κάνει λάθος σε κάποια ερώτηση του γίνεται γνωστή η ορθή απάντηση. Το παιχνίδι αυτό αποτέλεσε επίσης έμπνευση για κάποιες από της ερωτήσεις του ερωτηματολογίου προ-ερωτήσεων. Παράλληλα αξιοποιήθηκε αυτούσιο στα πλαίσια της

έρευνας καθώς αποτέλεσε ένα από τα δύο παιχνίδια με τα οποία ασχολήθηκαν οι μαθητές στην σχολική τάξη.

Το Be Internet Awesome είναι και αυτό ένα παιχνίδι της Google μέσα από το οποίο επιδιώκεται τα παιδιά να είναι ασφαλείς και σίγουροι εξερευνητές του διαδικτυακού κόσμου. Απαρτίζεται από τέσσερα mini-games, το Kind Kingdom το οποίο επιδιώκει οι παίκτες να μάθουν να είναι καλοί και ευγενικοί στον κυβερνοχώρο, το Tower of Treasure που επιθυμεί οι παίκτες να μάθουν να προστατεύουν καλύτερα τα μυστικά τους, το Mindful Mountain το οποίο εξηγεί στους παίκτες ότι πρέπει να μοιράζονται πληροφορίες για αυτούς στο διαδίκτυο με προσοχή και το Reality River το οποίο αξιοποίησε η παρούσα διπλωματική μελέτη και θα εξηγηθεί εκτενώς.

Συγκεκριμένα, στο Reality River ο παίκτης αρχικά καλείται να απαντήσει σε 10 ερωτήσεις που αφορούν περιπτώσεις scam, phishing, hacking και ασφάλειας λογαριασμού. Αφού ο παίκτης απαντήσει και στις 10 ερωτήσεις με επιτυχία καλείται να απαντήσει και σε ένα ακόμη σύνολο ερωτήσεων. Αυτές του προσφέρουν περισσότερες γνώσεις. Μετά την ολοκλήρωση και αυτών των ερωτήσεων με επιτυχία ο παίκτης έχει ολοκληρώσει το παιχνίδι. Αξίζει να σημειωθεί ότι το παιχνίδι αυτό υποχρεώνει τον παίκτη να επιλέξει την σωστή απάντηση δίνοντας του την ευκαιρία μετά από επιλογή λανθασμένης απάντησης να διαβάσει συμβουλές μέχρι να επιλέξει την σωστή απάντηση. Ενδιαφέρον είναι ακόμη το γεγονός ότι οι ερωτήσεις δεν είναι οι ίδιες κάθε φορά όποτε ο παίκτης μπορεί να επιστρέψει στο παιχνίδι μετά από ένα χρονικό διάστημα και να ελέγξει τις γνώσεις του σε μία διαφορετική ποικιλία ερωτήσεων. Το Reality River εκτός από έμπνευση στις ερωτήσεις του ερωτηματολογίου προ-ερωτήσεων χρησιμοποιήθηκε αυτούσιο και από τους μαθητές με σκοπό να απαντηθεί το ερωτηματολόγιο μετά-ερωτήσεων.

3.1.3 Ερωτηματολόγιο προ-ερωτήσεων

Το ερωτηματολόγιο προ-ερωτήσεων δημιουργήθηκε στο Google Forms και ήταν διαθέσιμο προς απάντηση σε ψηφιακή μορφή και διαδικτυακά. Το ερωτηματολόγιο προ-ερωτήσεων αποτελούνταν από πέντε ενότητες. Η πρώτη ενότητα περιελάμβανε το εισαγωγικό σημείωμα το οποίο ενημέρωνε τους μαθητές ότι χρησιμοποιείται ως ερευνητικό εργαλείο στα πλαίσια εκπόνησης της παρούσας διπλωματικής εργασίας. Παράλληλα, ενημέρωνε τους μαθητές ότι η αποχώρηση τους από τη συμπλήρωση του ερωτηματολογίου είναι δυνατόν να πραγματοποιηθεί ανά πάσα στιγμή χωρίς καμία

επίπτωση. Επιπρόσθετα, καθιστούσε στους μαθητές γνωστό τον σκοπό του, ο οποίος ήταν η εξέταση της στάσης των νεαρών απέναντι στην διαφύλαξη της ασφάλειας και του απορρήτου τους στον κυβερνοχώρο. Τέλος, ανέφερε ρητά ότι η σύνθεση του ερωτηματολογίου είναι τέτοια ώστε να διαφυλάσσεται η ανωνυμία των ερωτώμενων.

Η δεύτερη ενότητα ζητούσε τη συγκατάθεση των μαθητών. Η τρίτη ενότητα περιελάμβανε τα δημογραφικά στοιχεία, ηλικία και φύλο συμμετέχοντα. Η τέταρτη ενότητα απαρτίζονταν από ερωτήσεις πολλαπλής επιλογής κάποιες από τις οποίες ήταν εμπνευσμένες από τα 3 παιχνίδια που αναλύονται στην ενότητα 3.1.2.. Η πέμπτη και τελευταία ενότητα αποτελούνταν από τέσσερις ερωτήσεις σύντομης ανάπτυξης.

Οι ερωτήσεις του ερωτηματολογίου προ-ερωτήσεων βρίσκονται στο Παράρτημα Α.

3.1.4 Ερωτηματολόγιο μετά-ερωτήσεων

Το ερωτηματολόγιο μετά-ερωτήσεων δημιουργήθηκε στο Google Forms και ήταν διαθέσιμο προς απάντηση σε ψηφιακή μορφή και διαδικτυακά. Το ερωτηματολόγιο μετά-ερωτήσεων αποτελούνταν από έξι ενότητες. Η πρώτη ενότητα περιελάμβανε το εισαγωγικό σημείωμα το οποίο ενημέρωνε τους μαθητές ότι χρησιμοποιείται ως ερευνητικό εργαλείο στα πλαίσια εκπόνησης της παρούσας διπλωματικής εργασίας. Παράλληλα, ενημέρωνε τους μαθητές ότι η αποχώρηση τους από τη συμπλήρωση του ερωτηματολογίου είναι δυνατόν να πραγματοποιηθεί ανά πάσα στιγμή χωρίς καμία επίπτωση. Επιπρόσθετα, καθιστούσε στους μαθητές γνωστό τον σκοπό του, ο οποίος ήταν η εξέταση της στάσης των νεαρών απέναντι στη διαφύλαξη της ασφάλειας και του απορρήτου τους στον κυβερνοχώρο. Ταυτόχρονα, ενημέρωνε τους συμμετέχοντες ότι για να απαντήσουν στο ερωτηματολόγιο θα πρέπει πρωτίστως να έχουν συμπληρώσει το ερωτηματολόγιο προ-ερωτήσεων και να έχουν παίξει τα παιχνίδια Space Shelter και το Be Internet Awesome-Reality River, τα οποία αναφέρονται στην ενότητα 3.1.2. Τέλος, ανέφερε ρητά ότι η σύνθεση του ερωτηματολογίου είναι τέτοια ώστε να διαφυλάσσεται η ανωνυμία των ερωτώμενων.

Η δεύτερη ενότητα ζητούσε την συγκατάθεση των μαθητών. Η τρίτη ενότητα περιελάμβανε τα δημογραφικά στοιχεία, ηλικία και φύλο συμμετέχοντα. Η τέταρτη ενότητα απαρτίζονταν από ερωτήσεις που αφορούσαν την εμπειρία των συμμετεχόντων σε κάθε παιχνίδι. Η πέμπτη αποτελούνταν από δύο ερωτήσεις σχετικές με την ευχρηστία των παιχνιδιών. Οι ερωτήσεις της τέταρτης και της πέμπτης ενότητας δέχονται

απαντήσεις σύμφωνα με την κλίμακα Liker. Η τελευταία ενότητα, η έκτη, περιελάμβανε ερωτήσεις με περιεχόμενο σχετικό με τον εντοπισμό των μαθησιακών αποτελεσμάτων. Οι απαντήσεις στις ερωτήσεις αυτής της ενότητας ήταν είτε πολλαπλής επιλογής είτε επιλογής με βάση την κλίμακα Likert.

Οι ερωτήσεις του ερωτηματολογίου μετά-ερωτήσεων βρίσκονται στο Παράρτημα Α.

3.1.5 Εφαρμογή της μελέτης

Η παρούσα εμπειρική μελέτη εφαρμόστηκε σε μαθητές Γενικού Λυκείου. Το σχολείο το οποίο επιλέχθηκε για τον σκοπό της έρευνας ήταν το Γενικό Λύκειο Νέων Μουδανιών. Η εφαρμογή της μελέτης πραγματοποιήθηκε στις 14/12/2023 και έλαβε χώρα στο μάθημα της πληροφορικής με μαθητές και μαθήτριες δύο τμημάτων της Β' τάξης μετά από άδεια η οποία ζητήθηκε από τη διευθύντρια του σχολείου και τον καθηγητή Πληροφορικής. Επιπλέον, στο τέλος της έρευνας παραχωρήθηκε βεβαίωση από τη διευθύντρια του σχολείου.

Η έρευνα πραγματοποιήθηκε χωριστά για κάθε τμήμα. Το πρώτο τμήμα πραγματοποίησε την έρευνα σε μία διδακτική ώρα 45 λεπτών και ενός διαλείμματος 10 λεπτών. Το δεύτερο τμήμα πραγματοποίησε την έρευνα σε μία διδακτική ώρα 40 λεπτών και ενός διαλείμματος 15 λεπτών. Συνολικά στην έρευνα συμμετείχαν 41 μαθητές, 22 από το ένα τμήμα και 19 από το άλλο.

Οι μαθητές έπρεπε να απαντήσουν στο ερωτηματολόγιο προ-ερωτήσεων, έπειτα να παίξουν τα παιχνίδια,το Space Shelter και το Be Internet Awesome-Reality River, και στη συνέχεια να απαντήσουν στο ερωτηματολόγιο μετά-ερωτήσεων. Στην όλη διαδικασία υπήρξε ένα πρόβλημα και αυτό ήταν το γεγονός ότι η αίθουσα πληροφορικής είχε 16 ηλεκτρονικούς υπολογιστές. Αυτό είχε ως άμεση επίπτωση κάποιοι από τους μαθητές να κάθονται ανά δύο στους υπολογιστές. Σε αυτές τις περιπτώσεις απαντούσε αρχικά ο ένας μαθητής στο ερωτηματολόγιο και όταν το ολοκλήρωνε απαντούσε και ο άλλος. Αυτό έγινε και για τα δύο ερωτηματολόγια. Τα παιχνίδια στις περιπτώσεις δύο μαθητών ανά ηλεκτρονικό υπολογιστή παίχτηκαν συνεργατικά από τους μαθητές.

Τέλος, αξίζει να σημειωθεί ότι τα αποτελέσματα των ερωτηματολογίων πριν και μετά την εφαρμογή των παιχνιδιών είναι συγκεντρωτικά και για τα δύο τμήματα της Β' τάξης.

3.2 Αποτελέσματα ερωτηματολογίου προ-ερωτήσεων

3.2.1 Εισαγωγή και δημογραφικά στοιχεία

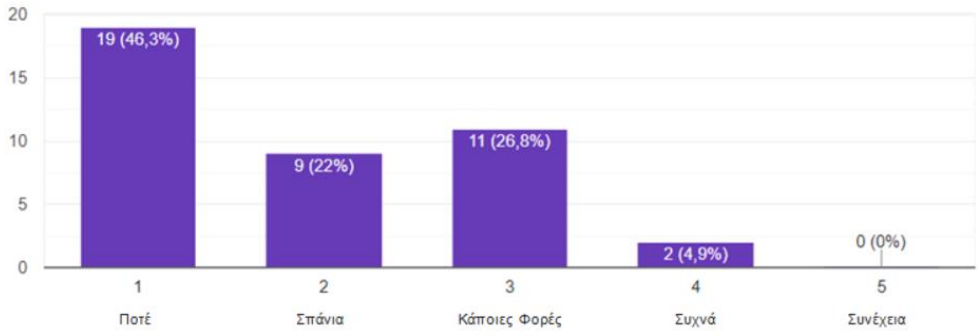
Το ερωτηματολόγιο προ-ερωτήσεων τέθηκε πρώτο σε εφαρμογή. Όλοι οι μαθητές αφού διάβασαν το εισαγωγικό σημείωμα έδωσαν τη συγκατάθεση τους για την επεξεργασία των απαντήσεων για τις ανάγκες της έρευνας. Επομένως, δέχτηκαν να συμμετέχουν στο ερωτηματολόγιο 41 μαθητές. Από αυτούς οι 24 συμπλήρωσαν στην φόρμα το φύλο άντρας και 17 το φύλο γυναίκα. Τέλος, όλοι οι συμμετέχοντες είχαν την ίδια ηλικία αυτή των 16 ετών.

Μετά τις ερωτήσεις συλλογής δημογραφικών στοιχείων ακολούθησαν 32 ερωτήσεις πολλαπλών επιλογών και τέσσερις ερωτήσεις σύντομης ανάπτυξης. Οι συμμετέχοντες έπρεπε να απαντήσουν σε κάθε ερώτηση του ερωτηματολογίου, καθώς όλες ήταν υποχρεωτικές. Επίσης, έγινε σαφές μέσα από διευκρίνηση του ερωτηματολογίου ότι όποιος δεν γνώριζε τι να απαντήσει στις ερωτήσεις ανάπτυξης μπορούσε να εκχωρήσει ότι δεν γνωρίζει.

3.2.2 Ερωτήσεις πολλαπλής επιλογής

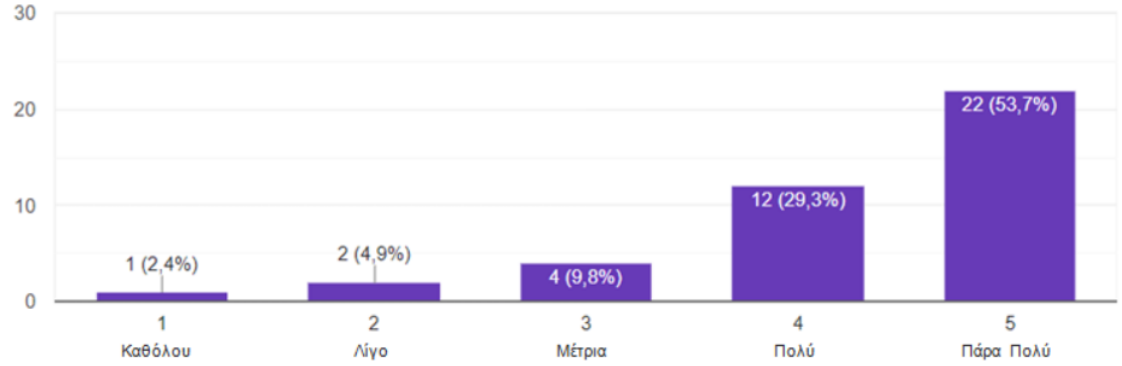
3.2.2.1 Εκπαιδευτικά παιχνίδια και προσωπικά δεδομένα

Η πρώτη ερώτηση του ερωτηματολογίου ρωτούσε τους συμμετέχοντες εάν έχουν παίξει εκπαιδευτικά παιχνίδια στα πλαίσια του μαθήματος της πληροφορικής. Οι απαντήσεις στην ερώτηση αυτή είχαν την μορφή της κλίμακας Likert και θα ήταν σημαντικό να υπογραμμιστεί ότι 19 στους 41 μαθητές δήλωσαν ότι δεν έχουν παίξει ποτέ εκπαιδευτικά παιχνίδια στο μάθημα της πληροφορικής. Τα αποτελέσματα αυτή της ερώτησης φαίνονται συγκεντρωτικά στην Εικόνα 28.



Εικόνα 28: Απαντήσεις στην ερώτηση "Έχεις παίξει εκπαιδευτικά παιχνίδια στα πλαίσια του μαθήματος της πληροφορικής;"

Η επόμενη ερώτηση του ερωτηματολογίου αφορούσε τα προσωπικά δεδομένα. Σε αυτή την ερώτηση οι συμμετέχοντες χρειαζόταν να εκφράσουν πόσο σημαντική νιώθουν ότι είναι η ανάγκη για την προστασία του απορρήτου τους και των προσωπικών τους δεδομένων. Εδώ οι πλειοψηφία των συμμετεχόντων απάντησε πάρα πολύ ή πολύ. Μόνο ένας μαθητής/τρια απάντησε καθόλου, βλέπε Εικόνα 29.



Εικόνα 29: Απαντήσεις στην ερώτηση "Αισθάνεσαι σημαντική την ανάγκη προστασίας του απορρήτου σου και των προσωπικών σου δεδομένων;"

3.2.2.2 Μέσα κοινωνικής δικτύωσης και δραστηριότητα μαθητών

Όλοι οι συμμετέχοντες είχαν λογαριασμό σε τουλάχιστον ένα μέσο κοινωνικής δικτύωσης. Η ερώτηση αν έχουν λογαριασμό σε κάποιο μέσο κοινωνικής δικτύωσης έδινε τη δυνατότητα επιλογής ενός ή περισσοτέρων απαντήσεων από τις: "Instagram", "Facebook", "Youtube", "Tik Tok", "Άλλο" και την προαιρετικής συμπλήρωσης της με κάποιο/α μέσο κοινωνικής δικτύωσης το οποίο δεν αναφέρονταν και την επιλογή "δεν έχω social media". Στον Πίνακα 14 παρουσιάζονται οι απαντήσεις των μαθητών.

Πίνακας 14: Τα μέσα κοινωνικής δικτύωσης στα οποία οι μαθητές έχουν λογαριασμό

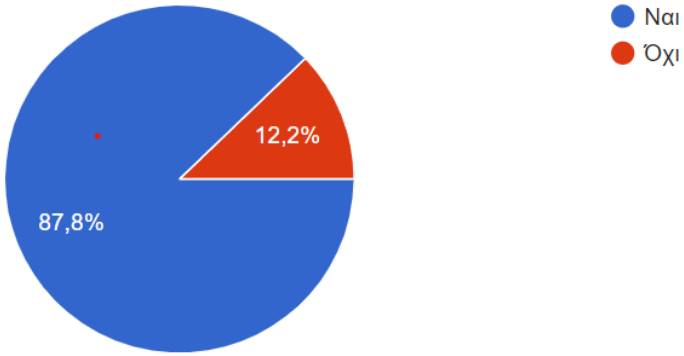
Μέσο Κοινωνικής Δικτύωσης	Πλήθος μαθητών που έχουν λογαριασμό	Ποσοστό Επιλογής
Instagram	40	97,6%
Tik Tok	39	95,1%
Youtube	38	92,7%
Facebook	17	41,5%
Bereal	7	17%
Snapchat	5	12,5%
Messenger	1	2,4%
Επιλογή "Άλλο" χωρίς συμπλήρωση	5	12,2%
Δεν έχω social media	0	0%

Μία ακόμη ερώτηση που αφορούσε τα μέσα κοινωνική δικτύωσης ήταν "Ποιος μπορεί να σε ακολουθήσει στα social media;". Η ερώτηση ήταν πολλαπλής επιλογής. Οι προτεινόμενες απαντήσεις και οι επιλογές των μαθητών φαίνονται στον Πίνακα 15.

Πίνακας 15: Απαντήσεις στην ερώτηση πολλαπλής επιλογής "Ποιος μπορεί να σε ακολουθήσει στα social media;"

Προτεινόμενες Επιλογές	Πλήθος μαθητών που επέλεξαν την απάντηση	Ποσοστό Επιλογής
Όποιος θέλει. Έχω ανοιχτό προφίλ και μπορεί να με ακολουθήσει ο καθένας	5	12,2%
Όποιος θέλει. Έχω κλειστό προφίλ, για να δει κάποιος το περιεχόμενο μου χρειάζεται πρώτα με ακολουθήσει, αλλά πολλούς από τους ακολούθους μου δεν τους γνωρίζω και συνήθως αποδέχομαι όλα τα αιτήματα	5	12,2%
Μόνο κάποιος που γνωρίζω εγώ ή που έχουμε κοινούς γνωστούς στα social. Έχω κλειστό προφίλ, πολλούς από τους ακολούθους τους γνωρίζω και με άλλους έχουμε κοινούς γνωστούς στα social	19	46,3%
Μόνο κάποιος που γνωρίζω πολύ καλά. Ακολουθώ και με ακολουθούν άτομα που γνωρίζω πολύ καλά	12	29,3%
Ακολουθώ και με ακολουθούν άτομα που γνωρίζω πολύ καλά και ενδιαφερόμαστε όλοι για την προστασία των προσωπικών μας δεδομένων	0	0%

Μία ακόμη ενδιαφέρουσα ερώτηση για τα μέσα κοινωνικής δικτύωσης αφορούσε το αν έχουν μοιραστεί σε αυτά τα μέρη που τους αρέσει να συχνάζουν. Οι απαντήσεις σε αυτή την ερώτηση παρουσιάζονται στην Εικόνα 30.



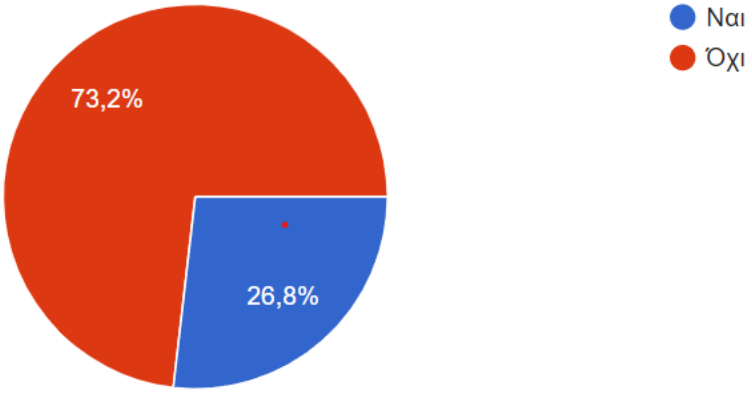
Εικόνα 30: Απάντηση με Ναι ή Όχι στην ερώτηση "Έχεις μοιραστεί στα social media τα μέρη που σου αρέσει να συχνάζεις;"

Επίσης, στους συμμετέχοντες τέθηκε η εξής ερώτηση σχετικά με το "TikTok": "Το "tiktok" σου δίνει την ευκαιρία να μιλάς με αγνώστους, να κάνεις ή να συμμετέχεις σε livestream και να βλέπεις αστεία αλλά και χρήσιμα βίντεο. Ποιοι είναι οι κίνδυνοι;". Σε αυτή την ερώτηση οι επιλογές φαίνονται στον Πίνακα 16.

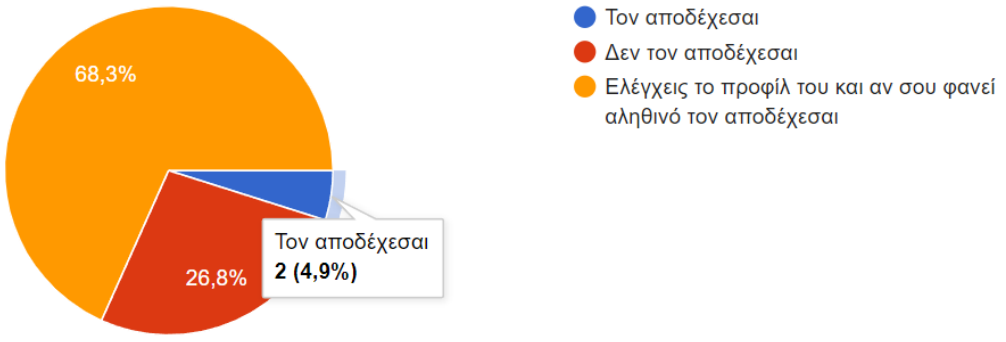
Πίνακας 16: Απαντήσεις στην ερώτηση "Το "Tik Tok" σου δίνει την ευκαιρία να μιλάς με αγνώστους, να κάνεις ή να συμμετέχεις σε livestream και να βλέπεις αστεία αλλά και χρήσιμα βίντεο. Ποιοι είναι οι κίνδυνοι;"

Προτεινόμενες Επιλογές	Πλήθος μαθητών που επέλεξαν την απάντηση	Ποσοστό Επιλογής
Η τοποθεσία σου μπορεί να παρακολουθηθεί	0	0%
Άγνωστοι μπορούν να επικοινωνήσουν μαζί σου	5	12,2%
Μπορεί να πέσεις θύμα bulling	1	2,4%
Μπορεί να συναντήσεις κακή φρασεολογία και εξτρεμιστικές απόψεις	1	2,4%
Μπορεί να δεις ακατάλληλο περιεχόμενο	2	4,9%
Όλα τα παραπάνω	30	73,2%
Τίποτα από τα παραπάνω	2	4,9%

Παράλληλα, οι συμμετέχοντες/ουσες ρωτήθηκαν αν έχουν συναντήσει κάποιον άγνωστο τον οποίο γνώρισαν online. Οι απαντήσεις φαίνονται στην Εικόνα 31. Επιπλέον, ρωτήθηκαν πως διαχειρίζονται τα αιτήματα ακολούθησης από αγνώστους στα μέσα κοινωνικής δικτύωσης, με τις απαντήσεις να παρουσιάζονται στην Εικόνα 32.



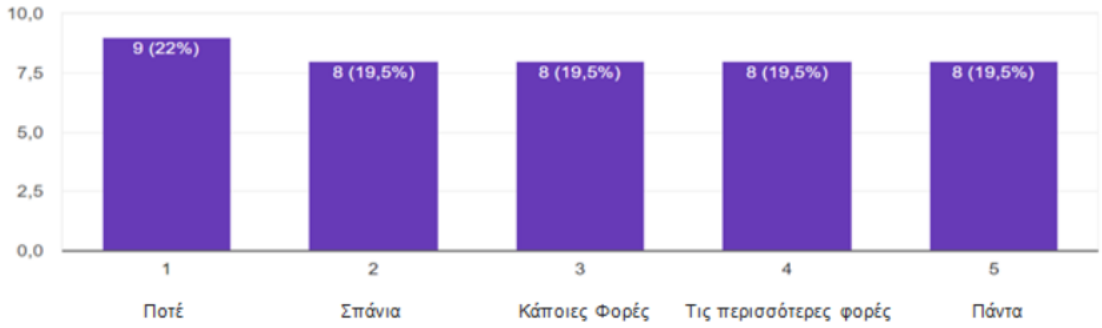
Εικόνα 31: Απάντηση με Ναι ή Όχι στην ερώτηση "Έχεις συναντήσει ποτέ κάποιον άγνωστο που γνώρισες online;"



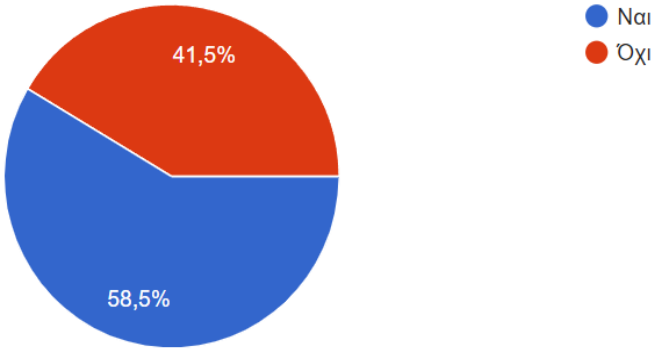
Εικόνα 32: Απαντήσεις στην ερώτηση "Δέχεσαι follow στο Instagram από άγνωστο. Τι κάνεις;"

Επίσης, οι μαθητές ερωτήθηκαν αν μπλοκάρουν αριθμούς τηλεφώνου ή αιτήματα φιλία τα οποία τους φαίνονται ύποπτα. Σε αυτή την ερώτηση οι απαντήσεις στην

κλίμακα Likert ήταν ισορροπημένες με πρώτη αυτή η οποία δήλωνε ότι ποτέ δεν μπλοκάρουν ύποπτους αριθμούς ή αιτήματα, βλέπε Εικόνα 33. Μία ακόμη ερώτηση που παρουσιάζει ενδιαφέρον είναι εάν οι μαθητές καλύπτουν την webcam τους όταν δεν την χρησιμοποιούν, βλέπε Εικόνα 34.



Εικόνα 33: Απαντήσεις στην ερώτηση "Μπλοκάρεις αριθμούς τηλεφώνου ή αιτήματα φιλίας που σου φαίνονται ύποπτα;;"



Εικόνα 34: Απάντηση με Ναι ή Όχι στην ερώτηση "Καλύπτεις πάντα την webcam (βιντεοκάμερα που μεταφέρει την εικόνα σε πραγματικό χρόνο προς ή μέσω ενός υπολογιστή) σου όταν δεν την χρησιμοποιείς;"

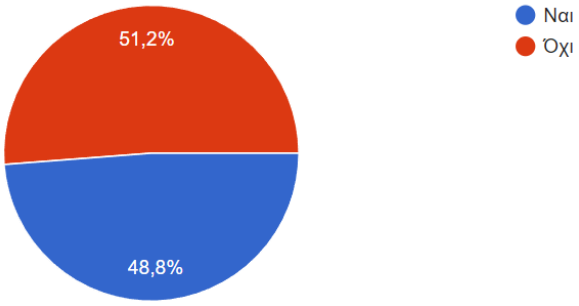
Ένα ζευγάρι ερωτήσεων που είναι αρκετά σημαντικό είναι αυτό που αφορούσε το cyber stalking. Οι συμμετέχοντες ερωτήθηκαν αν έχουν δεχτεί και αν έχουν πραγματοποιήσει οι ίδιοι cyber stalking. Συγκεκριμένα, 11 στους 41 απάντησαν ότι έχουν δεχτεί και 9 στους 41 ότι έχουν πραγματοποιήσει οι ίδιο cyber stalking σε κάποιον άλλο. Παράλληλα, ενδιαφέρον παρουσιάζουν οι απαντήσεις στην ακόλουθη ερώτηση, "Αν μιλήσεις με κάποιον σε ένα game και ισχυριστεί ότι έχει μία αποκαλυπτική φωτογραφία σου και ότι θα τη στείλει στην οικογένεια σου αν δεν του στείλεις και άλλες παρόμοιες, τι κάνεις;", καθώς το 34,1% των συμμετεχόντων απάντησαν ότι δεν θα απευθυνθούν σε κανέναν και θα διαγράψουν το μήνυμα, Εικόνα 35.

Εικόνα 35: Απαντήσεις στην ερώτηση "Αν μιλήσεις με κάποιον σε ένα game και ισχυριστεί ότι έχει μία αποκαλυπτική φωτογραφία σου και ότι θα τη στείλει στην οικογένεια σου αν δεν του στείλεις και άλλες παρόμοιες, τι κάνεις;"

Τέλος, 32 στους 41 μαθητές δήλωσαν ότι αν λάμβαναν ένα μήνυμα από έναν φίλο τους το οποίο τους λέει να το κοινοποιήσουν σε άλλους 10 φίλους για να κερδίσουν κάτι, θα το διέγραφαν και θα ενημέρωναν τον φίλο ότι πιθανά να έχει χακαριστεί ο λογαριασμός του. Στην ερώτηση αυτή 7 απάντησαν ότι θα το έστελναν σε 10 φίλους τους γιατί μπορεί να μην είναι fake μήνυμα, ενώ 2 θα το έστελναν σε περισσότερους από 10.

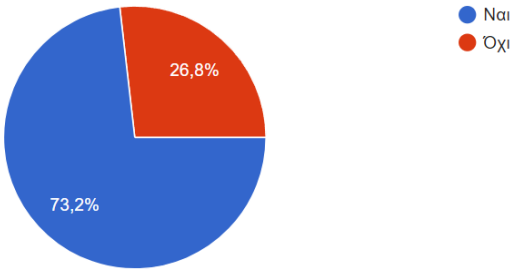
3.2.2.3 Κωδικοί πρόσβασης

Από την έρευνα αυτή διαπιστώθηκε ότι ο τρόπος με τον οποίο οι συμμετέχοντες επιλέγουν κωδικούς πρόσβασης διαφέρει από άτομο σε άτομο. Στην Εικόνα 36 βλέπει κανείς αν οι μαθητές επιλέγουν για κωδικούς ασφαλείας του κινητού τους κωδικούς όπως 1234 ή 1111 ή κάποιον παρόμοιο.



Εικόνα 36: Απάντηση Ναι ή Όχι στην ερώτηση "Έχεις χρησιμοποιήσει ή χρησιμοποιείς σαν κωδικό ασφαλείας του κινητού σου το 1234 ή 1111 ή κάποιον παρόμοιο;"

Επιπλέον, οι συμμετέχοντες ερωτήθηκαν εάν έχουν αλλάξει ποτέ τον κωδικό τους στα μέσα κοινωνικής δικτύωσης. Οι 18 στους 41 απάντησαν ότι τον αλλάζουν συχνά, οι 17 στους 41 ότι τον έχουν αλλάξει 1 φορά και οι 6 στους 41 ότι δεν τον έχουν αλλάξει ποτέ. Παράλληλα, 22 στους 41 μαθητές απάντησαν ότι οι κωδικοί τους φροντίζουν να είναι μοναδικοί και κρυφοί από όλους. Οι 17 υποστήριξαν ότι οι κωδικοί τους είναι πολλοί δύσκολοι, ενώ οι 2 φροντίζουν να μην τους μοιράζονται με κανέναν εκτός από τους γονείς τους. Επίσης, 30 μαθητές υποστήριξαν ότι χρησιμοποιούν στους κωδικούς ασφαλείας τους αριθμούς, πεζά και κεφαλαία γράμματα και σύμβολα, Εικόνα 37.



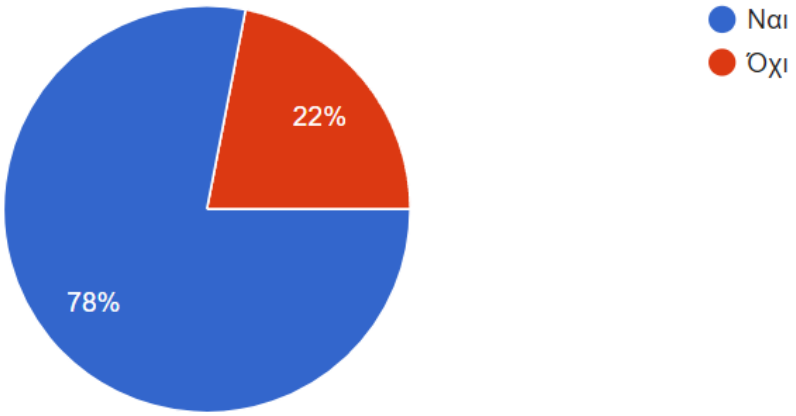
Εικόνα 37: Απάντηση Ναι ή Όχι στην ερώτηση "Χρησιμοποιείς στους κωδικούς ασφαλείας σου αριθμούς, πεζά και κεφαλαία γράμματα και σύμβολα;"

Μία ακόμη ερώτηση του ερωτηματολογίου σχετική με τους κωδικούς ασφαλείας ήταν η "Χρησιμοποιείς password manager (διαχειριστής κωδικών πρόσβασης τον οποίο οι χρήστες χρησιμοποιούν για να αποθηκεύουν και να διαχειρίζονται τους κωδικούς τους) για να σου υπενθυμίζει τους κωδικούς σου; ". Τα αποτελέσματα παρουσιάζονται στον Πινακα 17.

Πίνακας 17: Απαντήσεις στην ερώτηση "Χρησιμοποιείς password manager για να σου υπενθυμίζει τους κωδικούς σου; "

Προτεινόμενες Επιλογές	Πλήθος μαθητών που επέλεξαν την απάντηση	Ποσοστό Επιλογής
Ναι	17	41,5%
Όχι, τους θυμάμαι	11	26,8%
Όχι, χρησιμοποιώ τον ίδιο κωδικό ασφαλείας	10	24,4%
Όχι δεν γνωρίζω ότι υπάρχει	3	7,3%

Επίσης, μόνο το 22% δεν χρησιμοποιεί και άλλους τρόπους για να διατηρεί ασφαλή τον λογαριασμό του εκτός από τον κωδικό ασφαλείας (Εικόνα 38).



Εικόνα 38: Απάντηση Ναι ή Όχι στην ερώτηση "Χρησιμοποιείς εκτός από τον κωδικό ασφαλείας των λογαριασμών σου και άλλους τρόπους για να τους διατηρείς ασφαλείς; (πχ sms στο κινητό, ειδοποίηση στο email);"

Τέλος, σχεδόν όλοι οι μαθητές υποστήριξαν ότι ο κωδικός " 5pa@Ssword" είναι πιο ασφαλής από τους "paSsword","p@ssword" και "password456" οι οποίοι συνέλεξαν από μία ψήφο.

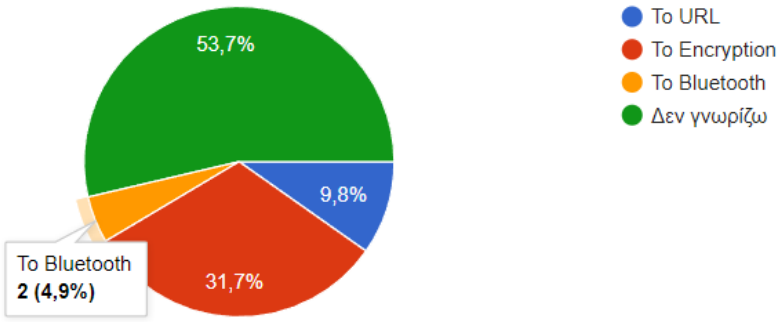
3.2.2.4 Δεδομένα χρήστη

Στο ερωτηματολόγιο υπήρχαν αρκετές ερωτήσεις σχετικές με τα δεδομένα των χρηστών στον κυβερνοχώρο. Μία τέτοια ερώτηση αφορούσε τα cookies και μέσα από πολλές επιλογές οι συμμετέχοντες/ουσες κλήθηκαν να επιλέξουν αν τα cookies μπορούν να παρακολουθήσουν την διαδικτυακή συμπεριφορά κάποιου, βλέπε Πίνακα 18.

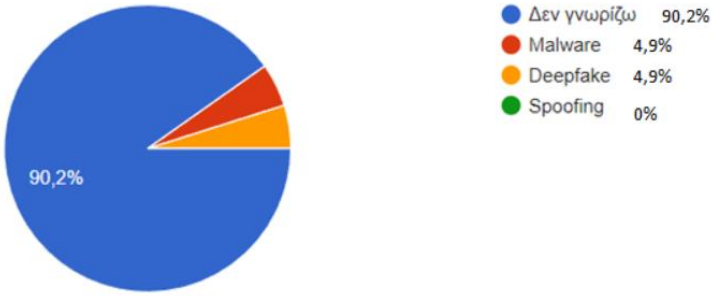
Πίνακας 18: Απαντήσεις στην ερώτηση "Τα "cookies" μπορούν να παρακολουθήσουν την διαδικτυακή σου δραστηριότητα;"

Προτεινόμενες Επιλογές	Πλήθος μαθητών που επέλεξαν την απάντηση	Ποσοστό Επιλογής
Μπορούν να δουν την τοποθεσία σου	1	2,4%
Μπορούν να παρακολουθούν τους ιστότοπους που επισκέπτεστε	9	22%
Μπορούν να καταγράψουν το ιστορικό αναζήτησης στον ιστό	1	2,4%
Όλα τα παραπάνω	21	51,2%
Τίποτα από τα παραπάνω	2	4,9%
Δεν γνωρίζω τι είναι τα "cookies"	7	17,1%

Δύο ακόμη ερωτήσεις που παρουσιάζουν ενδιαφέρον είναι (1) "Τι προστατεύει τα δεδομένα που στέλνεις σε άλλους;" και (2) "Πως λέγεται το λογισμικό που μπορεί να βλάψει τη συσκευή σας και να κλέψει τις πληροφορίες σας;". Τα αποτελέσματα φαίνονται στις Εικόνες 39 και 40 αντίστοιχα.



Εικόνα 39: Απαντήσεις στην ερώτηση "Τι προστατεύει τα δεδομένα που στέλνεις σε άλλους;"



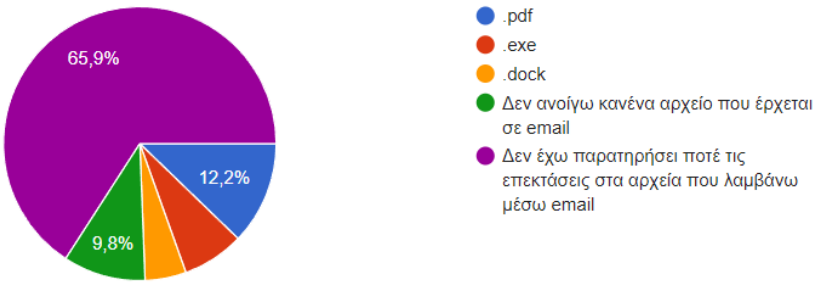
Εικόνα 40: Απαντήσεις στην ερώτηση "Πως λέγεται το λογισμικό που μπορεί να βλάψει τη συσκευή σας και να κλέψει τις πληροφορίες σας;"

Το ερωτηματολόγιο έθετε στους συμμετέχοντες/ουσες μία ερώτηση σχετική με το τι αποτελεί μέρος του ψηφιακού αποτυπώματος. Οι απαντήσεις που δόθηκαν φαίνονται στον Πίνακα 19.

Πίνακας 19: Απαντήσεις στην ερώτηση "Τι από τα παρακάτω αποτελεί μέρος του ψηφιακού αποτυπώματος"

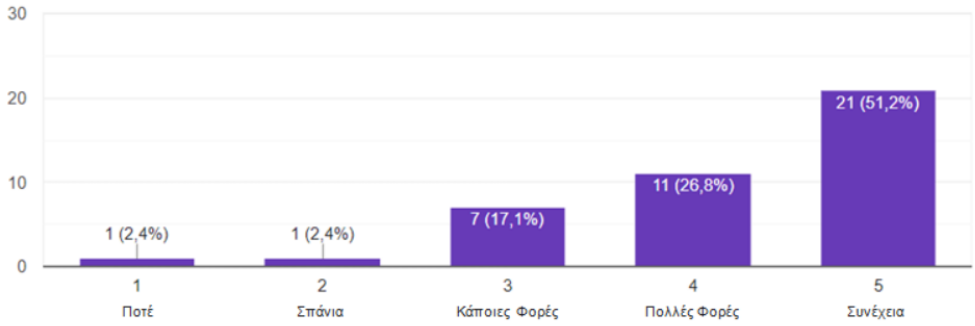
Προτεινόμενες Επιλογές	Πλήθος μαθητών που επέλεξαν την απάντηση	Ποσοστό Επιλογής
Τα παιχνίδια και οι εφαρμογές που χρησιμοποιείς	0	0%
Τα μηνύματα σου και αυτά που ποστάρεις στα social media	4	9,8%
Οι ιστοσελίδες που επισκέπτεσαι	6	16,4%
Όλα τα παραπάνω	14	34,1%
Δεν γνωρίζω τι είναι το "ψηφιακόαποτύπωμα – digital footprint",	16	39%
Τίποτα από τα παραπάνω	1	2,4%

Εντύπωση προκαλεί η σύγκριση δύο ερωτήσεων τους ερωτηματολογίου. Η πρώτη ερώτηση ζητούσε από τους συμμετέχοντες να απαντήσουν με "Ναι" ή "Όχι" στην ερώτηση "Γνωρίζεις τι σημαίνει η επέκταση .exe.file σε ένα αρχείο;" με το 48,8% να απαντάει ναι. Το ιδιαίτερα μεγάλο ποσοστό θετικών απαντήσεων σε αυτή την ερώτηση έρχεται σε αντιδιαστολή με την επόμενη (Εικόνα 41), στην οποία φαίνεται ότι μόνο το 7,3% απάντησαν ότι δεν θα άνοιγαν ένα με επέκταση .exe.



Εικόνα 41: Απαντήσεις στην ερώτηση "Προσέχεις πάντα την επέκταση σε συνημμένα που μπορεί να λάβεις σε ένα email. Δεν ανοίγεις ποτέ αρχεία:"

Παράλληλα, στην ερώτηση "Έχεις συνδεθεί ποτέ σε δημόσιο δίκτυο Wi-Fi το οποίο μπορεί να μην ζητάει κωδικό;" οι απαντήσεις δόθηκαν σε κλίμακα Likert και αποτυπώνονται στην Εικόνα 42.



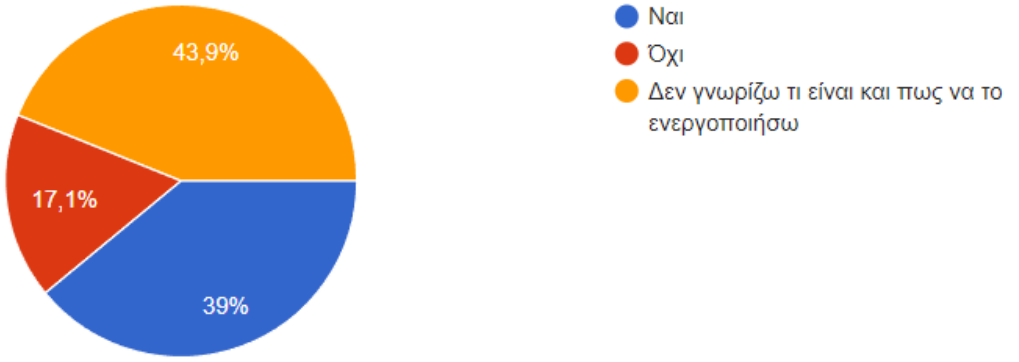
Εικόνα 42: Απαντήσεις στην ερώτηση "Έχεις συνδεθεί ποτέ σε δημόσιο δίκτυο Wi-Fi το οποίο μπορεί να μην ζητάει κωδικό;"

Επίσης, αξιοσημείωτο είναι το γεγονός ότι το 68,3% των ερωτηθέμενων απάντησε πως κρατάει backups των σημαντικών αρχείων. Επιπλέον, το ερωτηματολόγιο έθετε και κάποιες ερωτήσεις σχετικές με τα spam μηνύματα οι απαντήσεις σε μία από αυτές φαίνονται στον Πίνακα 20.

Πίνακας 20: Απαντήσεις στην ερώτηση "Τι από τα παρακάτω κάνεις όταν λάβεις ένα spam email"

Προτεινόμενες Επιλογές	Πλήθος μαθητών που επέλεξαν την απάντηση	Ποσοστό Επιλογής
Κοινοποίηση στους φίλους μου αλλά τους προειδοποιώ ότι είναι spam	3	7,3%
Δεν ανοίγω τα links και το επισημαίνω ως spam	22	53,7%
Το διαγράφω αμέσως	16	39%

Εντύπωση προκαλούν και οι απαντήσεις, που φαίνονται στην Εικόνα 43, οι οποίες αφορούν την ερώτηση "Έχεις ενεργοποιημένο το Spam Filter με σκοπό να μην σου έρχονται ανεπιθύμητα μηνύματα;" στην οποία το 43,9% δεν γνωρίζει τι είναι το Spam Filter και πώς να το ενεργοποιήσει. Τέλος, αξίζει να σημειωθεί ότι 39 στους 41 μαθητές θα ενημέρωναν τους γονείς τους αν αγόραζαν κάτι με την πιστωτική τους και αυτό αποδεικνύονταν ότι ήταν απάτη, ενώ μόνο 2 θα διέγραφαν απλά το λογαριασμό.



Εικόνα 43: Απαντήσεις στην ερώτηση "Έχεις ενεργοποιημένο το Spam Filter με σκοπό να μην σου έρχονται ανεπιθύμητα μηνύματα;"

3.2.3 Ερωτήσεις σύντομης ανάπτυξης

Το δεύτερο μέρος του ερωτηματολογίου προ-ερωτήσεων απαρτιζόταν από 4 ερωτήσεις σύντομης ανάπτυξης. Πριν τις ερωτήσεις αυτές υπήρχε ένα εισαγωγικό σημείωμα το οποίο ανέφερε ρητά ότι είναι αποδεκτές οι απαντήσεις «δεν γνωρίζω κάποια έννοια». Η πρώτη ερώτηση ζητούσε από τους μαθητές να αναφέρουν σύντομα τι γνωρίζουν για το ηλεκτρονικό ψάρεμα. Οι απαντήσεις στην ερώτηση αυτή παρουσιάζονται στον Πίνακα 21.

Πίνακας 21: Απαντήσεις στην ερώτηση "Τι γνωρίζεις για το ηλεκτρονικό ψάρεμα;"

Απαντήσεις	Πλήθος μαθητών που επέλεξαν την απάντηση	Ποσοστό Επιλογής
Ενδεικτικές απαντήσεις: "*δεν γνωρίζω κάτι*", " *Δεν έχω ιδέα* ", " *Δεν γνωρίζω τι είναι αυτή η έννοια* "	31	75,6%
Ενδεικτικές απαντήσεις: "*Όταν κάποιος προσπαθεί να σου κλέψει στοιχεία*", "*Όταν κάποιος προσπαθεί να σου κλέψει στοιχεία και πραγματοποιείται ηλεκτρονικά*"	5	12,2%
Ενδεικτικές απαντήσεις: *"είναι όταν ένα άτομο εξαπατά κάποιον άλλον δίνοντας ψεύτικες πληροφορίες για τον εαυτό του"*	1	2,4%
Ενδεικτικές απαντήσεις: *"όταν άτομα εξαπατούν άλλους μέσω του διαδικτύου δίνοντας ψεύτικες πληροφορίες για αυτούς"*	1	2,4%
Ενδεικτικές απαντήσεις: *"μερικά άτομα επικοινωνούν με αγνώστους για να αποσπάσουν προσωπικές τους πληροφορίες, όπως είναι ο αριθμός της πιστωτικής τους κάρτα"*	1	2,4%
Ενδεικτικές απαντήσεις: *"είναι κάτι επικίνδυνο"*	1	2,4%
Ενδεικτικές απαντήσεις: *"phishing είναι η διαδικτυακή απάτη κατά την οποία διάφορα άτομα πέφτουν θύματα άλλων με σκοπό να αποσκοπήσουν χρήματα και να εξυπηρετήσουν συμφέροντα"*	1	2,4%

Η δεύτερη ερώτηση ζητούσε από τους μαθητές να γράψουν σύντομα τι γνωρίζουν για τον έλεγχο ταυτότητας δύο παραγόντων και αν αξιοποιούν multi-factor authentication;. Οι απαντήσεις στην ερώτηση αυτή παρουσιάζονται στον Πίνακα 22.

Πίνακας 22: Απαντήσεις στην ερώτηση "Τι γνωρίζεις για τον έλεγχο ταυτότητας 2 παραγόντων. Αξιοποιείς το multi-factor authentication;"

Απαντήσεις	Πλήθος μαθητών που επέλεξαν την απάντηση	Ποσοστό Επιλογής
Ενδεικτική απάντηση: "*Οταν για την επιβεβαίωση του λογαριασμού μου εκτός από κωδικό μου ζητά και επιβεβαίωση από sms"*και ένας άλλος/η *"Ναι χρησιμοποιώ επιβεβαίωση μέσω email"*	1	2,4%
Ενδεικτική απάντηση: *"Ναι, χρησιμοποιώ επιβεβαίωση μέσω email"*	1	2,4%
Ενδεικτικές απαντήσεις: *"δεν γνωρίζω", "δεν ξέρω"*	39	95,1%

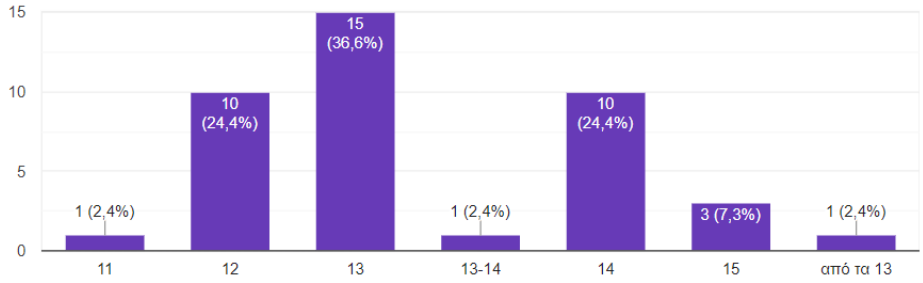
Αξίζει να σημειωθεί ότι κανένας δεν απάντησε στο δεύτερο σκέλος της ερώτησης. Εντοπίζεται εδώ η αντίθεση των απαντήσεων αυτής της ερώτησης με την ερώτηση 20 του πρώτου μέρους του συγκεκριμένου ερωτηματολογίου *"Χρησιμοποιείς εκτός από τον κωδικό ασφαλείας των λογαριασμών σου και άλλους τρόπους για να τους διατηρείς ασφαλείς; (πχ sms στο κινητό, ειδοποίηση στο email)"* στην οποία το 78% είχε απαντήσει θετικά.

Η τρίτη και η τέταρτη ερώτηση ζητούσε από τους μαθητές να αναφέρουν από ποια ηλικία και έπειτα θεωρούν φρόνιμο κάποιος ανήλικος να έχει λογαριασμό στα μέσα κοινωνικής δικτύωσης και από ποια ηλικία είχαν οι ίδιοι, αντίστοιχα. Οι απαντήσεις στην τρίτη ερώτηση φαίνονται στον Πίνακα 23.

Πίνακας 23: Απαντήσεις στην ερώτηση "Από ποια ηλικία και έπειτα θεωρείς φρόνιμο κάποιος ανήλικος να έχει λογαριασμό στα μέσα κοινωνικής δικτύωσης "

Απαντήσεις	Πλήθος μαθητών που επέλεξαν την απάντηση	Ποσοστό Επιλογής
23 χρονών	1	2,4%
17 χρονών	1	2,4%
16 χρονών	4	9,7%
15 χρονών	13	31,7%
14 χρονών	10	24,4%
14-15	1	2,4%
13 χρονών	7	17,1%
13-14 χρονών	1	2,4%
12-13 χρονών	1	2,4%
7 χρονών	1	2,4%
"*δεν ξέρω*"	1	2,4%

Στην τέταρτη ερώτηση στην οποία οι συμμετέχοντες κλήθηκαν να απαντήσουν από ποια ηλικία οι ίδιοι είχαν λογαριασμό οι περισσότεροι, 16 απάντησαν την ηλικία των δεκατριών ετών, ενώ σε αντίθεση με πριν μόνο τρεις δήλωσαν ότι ο πρώτος τους λογαριασμός έγινε στα 15. Οι απαντήσεις στην ερώτηση αυτή φαίνονται στην Εικόνα 44.



Εικόνα 44: Απαντήσεις στην ερώτηση "Από ποια ηλικία είχες εσύ social media;"

3.3 Αποτελέσματα ερωτηματολογίου μετά-ερωτήσεων

3.3.1 Εισαγωγή και δημογραφικά στοιχεία

Το ερωτηματολόγιο μετά-ερωτήσεων τέθηκε τελευταίο σε εφαρμογή. Πριν από αυτό προηγήθηκαν οι απαντήσεις στο ερωτηματολόγιο προ-ερωτήσεων και η χρήση των παιχνιδιών από τους μαθητές/τριες. Όλοι οι μαθητές/τριες αφού διάβασαν το εισαγωγικό σημείωμα έδωσαν τη συγκατάθεση τους για την επεξεργασία των απαντήσεων για τις ανάγκες της έρευνας. Επομένως, δέχτηκαν να συμμετέχουν στο ερωτηματολόγιο 41 μαθητές. Από αυτούς οι 24 συμπλήρωσαν στην φόρμα το φύλο άντρας και 17 γυναίκα. Τέλος, όλοι οι συμμετέχοντες είχαν την ίδια ηλικία αυτή των 16 ετών.

Μετά τις ερωτήσεις συλλογής δημογραφικών στοιχείων ακολούθησαν οι ερωτήσεις πολλαπλών επιλογών. Οι συμμετέχοντες έπρεπε να απαντήσουν σε κάθε ερώτηση του ερωτηματολογίου, καθώς όλες ήταν υποχρεωτικές. Το ερωτηματολόγιο αποτελούνταν από τρεις κατηγορίες ερωτήσεων. Πρώτον απαρτιζόταν από εννέα ερωτήσεις που αφορούσαν την εμπειρία του χρήστη από τα παιχνίδια. Δεύτερον, περιελάμβανε δύο ερωτήσεις ευχρηστίας των παιχνιδιών που κλήθηκαν να παίξουν οι συμμετέχοντες/ουσες πρωτού απαντήσουν στο ερωτηματολόγιο. Τέλος, τρίτη κατηγορία ερωτήσεων ήταν αυτή του εντοπισμού των μαθησιακών αποτελεσμάτων μέσα από 10 ερωτήσεις.

3.3.2 Ερωτήσεις εμπειρίας χρήστη

Η παρούσα ενότητα αφορούσε ερωτήσεις σχετικές με το σχεδιασμό των παιχνιδιών, το αν χρειάστηκαν βοήθεια για να παίξουν το παιχνίδι και αν χρειάζονταν γνώσεις σχετικές με το θέμα το οποίο πραγματεύονταν τα παιχνίδια. Επιπλέον, υπήρχαν ερωτήσεις όπως *"Θα μπορούσαν εύκολα όλοι οι συμμαθητές σου να παίξουν το παιχνίδι;"* και *"Θα συνιστούσες το παιχνίδι σε μαθητές μικρότερης ηλικίας;"*. Επιπλέον,

μέσα από απαντήσεις σε ερωτήσεις αυτής της ενότητας μπορεί να διαπιστωθεί εάν τα παιχνίδια φάνηκαν διασκεδαστικά ή μονότονα, αν σχετίζονται με τα ενδιαφέροντα των μαθητών και αν θα ήταν χρήσιμο να μάθει κανείς περισσότερες πληροφορίες για την ασφάλεια και το απόρρητο μέσω της χρήσης αυτών των παιχνιδιών. Οι απαντήσεις των ερωτήσεων εμπειρίας χρήστη δόθηκαν για κάθε παιχνίδι ξεχωριστά.

Στον Πίνακα 24 παρουσιάζονται για κάθε ερώτηση της ομάδας ερωτήσεις εμπειρίας χρήστη και για κάθε παιχνίδι ξεχωριστά η μέση τιμή, η διάμεσος και η τυπική απόκλιση. Στις στήλες έξι με δέκα φαίνεται το πλήθος των μαθητών που έδωσαν την απάντηση της στήλης και το ποσοστό.

Πίνακας 24: Απαντήσεις στις ερωτήσεις εμπειρίας χρήστη

Ερώτηση	Παιχνίδι	Μέση τιμή	Τυπική απόκλιση	Διάμεσος	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα Πολύ
Ο σχεδιασμός του παιχνιδιού (γραφικά κ.α.) σου φάνηκε ελκυστικός;	Space Shelter	4,29	0,78	4	0(0%)	2(4,9%)	2(4,9%)	19(46,3%)	18(43,9%)
	Be Internet Awesome	4,1	0,92	4	1(2,4%)	0(0%)	9(21,9%)	15(36,6%)	16(39%)
Χρειάστηκε να έχεις προϋπάρχουσες γνώσεις για να παίξεις το παιχνίδι;	Space Shelter	2,05	1,38	1	22(53,6%)	6(14,6%)	6(14,6%)	3(7,3%)	4(9,8%)
	Be Internet Awesome	2,05	1,38	1	22(53,6%)	6(14,6%)	6(14,6%)	3(7,3%)	4(9,8%)
Χρειάστηκες βοήθεια από κάποιον καθηγητή για να παίξεις το παιχνίδι;	Space Shelter	1,24	0,73	1	35(85,4%)	4(9,8%)	1(2,4%)	0(0%)	1(2,4%)
	Be Internet Awesome	1,29	0,84	1	35(85,4%)	3(7,3%)	1(2,4%)	1(2,4%)	0(0%)
Θα μπορούσαν εύκολα όλοι οι συμμαθητές σου να παίξουν το παιχνίδι;	Space Shelter	4,37	0,86	5	0(0%)	2(4,9%)	4(9,8%)	12(29,3%)	23(56,1%)
	Be Internet Awesome	4,32	0,86	5	0(0%)	1(2,4%)	7(17,1%)	11(26,8%)	22(53,6%)
Σου φάνηκε το παιχνίδι μονότονο;	Space Shelter	1,46	0,98	1	32(78%)	2(4,9%)	5(12,2%)	1(2,4%)	1(2,4%)
	Be Internet Awesome	2,39	1,16	3	13(31,7%)	7(17,1%)	14(34,1%)	6(14,6%)	1(2,4%)
Θα συνιστούσες το παιχνίδι σε μαθητές μικρότερης ηλικίας;	Space Shelter	3,83	1,12	4	1(2,4%)	5(12,2%)	8(19,5%)	13(31,7%)	14(34,1%)
	Be Internet Awesome	3,93	1,03	4	0(0%)	5(12,2%)	8(19,5%)	13(31,7%)	15(36,6%)
Διασκέδασες παίζοντας το παιχνίδι;	Space Shelter	4,1	0,94	4	1(2,4%)	1(2,4%)	7(17,1%)	16(39%)	16(39%)
	Be Internet Awesome	3,76	1,09	4	2(4,9%)	3(7,3%)	9(21,9%)	16(39%)	11(26,8%)
Σχετίζεται το παιχνίδι με τα ενδιαφέροντα σου;	Space Shelter	3,49	1,29	4	5(12,2%)	4(9,8%)	7(17,1%)	16(39%)	9(21,9%)
	Be Internet Awesome	3,29	1,27	4	6(14,6%)	4(9,8%)	9(21,9%)	16(39%)	6(14,6%)
Θα πρότεινες να μάθει κανείς περισσότερες πληροφορίες σχετικά με την ασφάλεια και το απόρρητο μέσω της χρήσης του παιχνιδιού;	Space Shelter	4,41	0,74	5	0(0%)	2(4,9%)	0(0%)	18(43,9%)	21(51,2%)
	Be Internet Awesome	4,24	0,83	4	0(0%)	2(4,9%)	4(9,8%)	17(41,5%)	18(43,9%)

3.3.3 Ερωτήσεις Ευχρηστίας

Η παρούσα ενότητα αφορούσε ερωτήσεις σχετικές με την ευχρηστία των παιχνιδιών. Οι ερωτήσεις και οι απαντήσεις παρουσιάζονται για κάθε παιχνίδι ξεχωριστά στον Πίνακα 25. Στον Πίνακα 25 παρουσιάζονται για κάθε ερώτηση της ομάδας ερωτήσεις ευχρηστίας και για κάθε παιχνίδι ξεχωριστά η μέση τιμή, η διάμεσος και η τυπική απόκλιση. Στις στήλες έξι με δέκα φαίνεται το πλήθος των μαθητών που έδωσαν την απάντηση της στήλης και το ποσοστό.

Πίνακας 25: Απαντήσεις στις ερωτήσεις ευχρηστίας

Ερώτηση	Παιχνίδι	Μέση τιμή	Τυπική απόκλιση	Διάμεσος	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα Πολύ
Παρέχει το παιχνίδι καθοδήγηση και επαρκή βοήθεια;	Space Shelter	4,02	1,06	4	2(4,9%)	1(2,4%)	7(17,1%)	15(36,6%)	16(39%)
	Be Internet Awesome	4,17	0,8	4	0(0%)	1(2,4%)	7(17,1%)	17(41,5%)	16(39%)
Παρέχει το παιχνίδι ουσιαστική ανατροφοδότηση σχετικά με τις επιλογές που κάνεις κατά τη διάρκεια;	Space Shelter	3,9	1,09	4	2(4,9%)	2(4,9%)	8(19%)	15(36,6%)	14(34,1%)
	Be Internet Awesome	4	1,05	4	1 (2,4%)	3(7,3%)	7(17,1%)	14(34,1%)	16(39%)

3.3.4 Ερωτήσεις μαθησιακών αποτελεσμάτων

Η παρούσα ενότητα αφορούσε ερωτήσεις σχετικές με τα μαθησιακά αποτελέσματα από τη χρήση των παιχνιδιών. Αρχικά, οι συμμετέχοντες κλήθηκαν να απαντήσουν αν ολοκλήρωσαν και τα δύο παιχνίδια. Το Space Shelter είχε πλήρη επιτυχία καθώς όλοι οι μαθητές/τριες κατάφεραν να το ολοκληρώσουν. Αντίθετα το Be Internet Awesome-Reality River δεν ολοκληρώθηκε από 6 μαθητές/τριες, λόγω έλλειψης χρόνου.

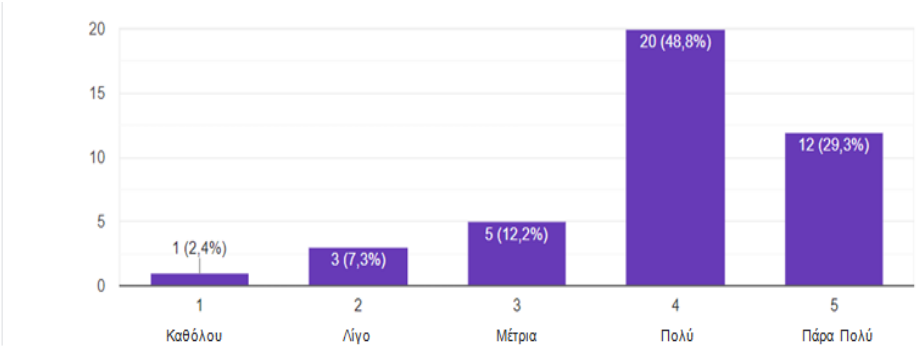
Σε κάποιες ερωτήσεις οι μαθητές/τριες κλήθηκαν να απαντήσουν για κάθε παιχνίδι χωριστά στην κλίμακα Likert. Τα αποτελέσματα των ερωτήσεων φαίνονται στον Πίνακα 26. Στον Πίνακα 26 παρουσιάζονται για κάθε ερώτηση της ομάδας ερωτήσεις εμπειρίας χρήστη και για κάθε παιχνίδι ξεχωριστά η μέση τιμή, η διάμεσος και η τυπική απόκλιση. Στις στήλες έξι με δέκα φαίνεται το πλήθος των μαθητών που έδωσαν την απάντηση της στήλης και το ποσοστό.

Πίνακας 26: Απαντήσεις στις ερωτήσεις μαθησιακών αποτελεσμάτων

Ερώτηση	Παιχνίδι	Μέση τιμή	Τυπική απόκλιση	Διάμεσος	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα Πολύ
Θα μπορούσε το παιχνίδι να χρησιμοποιηθεί ως συμπλήρωμα στην εκπαιδευτική διαδικασία;	Space Shelter	4,34	0,83	5	0(0%)	2(4,9%)	3(7,3%)	15(36,6%)	21(51,2%)
	Be Internet Awesome	4,24	0,89	4	1(2,4%)	0(0%)	6(14,6%)	15(36,6%)	19(46,3%)
Έμαθες ενδιαφέρουσες πληροφορίες που δεν γνώριζες μέσα από το παιχνίδι;	Space Shelter	4,1	0,89	4	0(0%)	2(4,9%)	8(19,5%)	15(36,6%)	16(39%)
	Be Internet Awesome	4,02	0,85	4	0(0%)	2(4,9%)	8(19,5%)	18(43,9%)	13(31,7%)
Σε βοήθησε το παιχνίδι να αναγνωρίσεις τη σημαντικότητα της προστασίας του απορρήτου σου;	Space Shelter	4,32	0,72	4	0(0%)	0(0%)	6(14,6%)	16(39%)	19(46,3%)
	Be Internet Awesome	4,22	0,85	4	0(0%)	2(4,9%)	5(12,2%)	16(39%)	18(43,9%)
Σε ώθησε το παιχνίδι να αλλάξεις τη στάση σου απέναντι στον τρόπο με τον οποίο αντιλαμβανόσουν την διαδικτυακή ασφάλεια και το απόρρητο πριν να παίξεις;"	Space Shelter	3,76	1,14	4	2(4,9%)	3(7,3%)	11 (26,8%)	12(29,2%)	13(31,7%)
	Be Internet Awesome	3,76	1,09	4	1(2,4%)	4(9,7%)	12 (29,2%)	11(26,8%)	13(31,7%)
Το παιχνίδι σου φάνηκε διασκεδαστικό αλλά και συνάμα χρήσιμο ως προς τις γνώσεις που σου προσέφερε;"	Space Shelter	3,93	0,91	4	0(0%)	3(7,3%)	9(21,9%)	17(41,5%)	12(29,2%)
	Be Internet Awesome	3,78	1,06	4	1(2,4%)	5(12,2%)	7(17,1%)	17(41,5%)	11(26,8%)
Σε παρακίνησε το παιχνίδι να αναζητήσεις περισσότερες πληροφορίες για την ασφάλεια και το απόρρητο στο διαδίκτυο;"	Space Shelter	3,63	1,13	4	1(2,4%)	7(17,1%)	9(21,9%)	13(31,7%)	11(26,8%)
	Be Internet Awesome	3,68	1,01	4	0(0%)	6(14,6%)	11(26,8%)	14(34,1%)	10(24,4%)

Σε μία από τις τελευταίες ερωτήσεις του ερωτηματολογίου μετά-ερωτήσεων οι μαθητές/τριες κλήθηκαν να απαντήσουν εάν τα παιχνίδια αποτέλεσαν ένα έναυσμα στο να αλλάξουν τη συμπεριφορά τους στον κυβερνοχώρο. Με 32 μαθητές να επιλέγουν πολύ ή πάρα πολύ και μόνο έναν να επιλέγει καθόλου μπορεί να διαπιστώσει κανείς ότι οι ενασχόληση των μαθητών με αυτά τα παιχνίδια είναι ικανή να τους παροτρύνει να

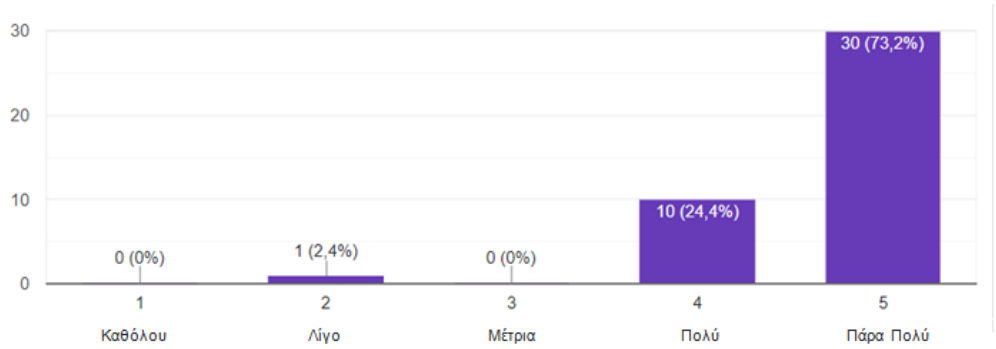
βελτιώσουν την διαδικτυακή τους συμπεριφορά. Τα αποτελέσματα της ερώτηση αυτής παρουσιάζονται στην Εικόνα 45.



Εικόνα 45: Απαντήσεις στην ερώτηση "Μετά την ενασχόληση σου με τα παιχνίδια σκοπεύεις να αλλάξεις την διαδικτυακή σου συμπεριφορά;"

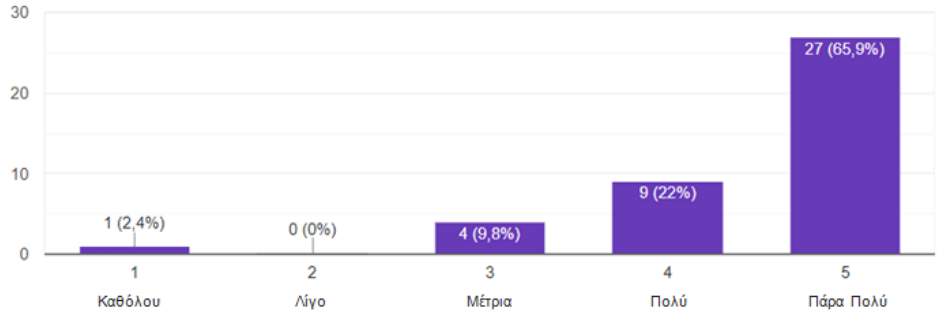
Σε αυτό το σημείο αξίζει να σημειωθεί ότι το 92,7% των μαθητών δήλωσε ότι θα ήθελε να γνωρίζει πληροφορίες σχετικές με την προστασία του απορρήτου στο διαδίκτυο χρησιμοποιώντας εκτός από παραδοσιακούς τρόπους μάθησης (σχολικό βιβλίο) και παιχνίδια. Μόνο τρεις μαθητές υποστήριξαν ότι θα προτιμούσαν την εκμάθηση εννοιών μέσω παραδοσιακών τρόπων διδασκαλίας χωρίς την αξιοποίηση παιχνιδιών με σκοπό την εκμάθηση νέων εννοιών.

Παράλληλα, εντυπωσιακή είναι και η συμφωνία των μαθητών ως προς το ενδιαφέρον τους να μάθουν περισσότερες πληροφορίες σχετικά με την ασφάλεια και το απόρρητο μέσω της χρήσης και άλλων παιχνιδιών (Εικόνα 46).



Εικόνα 46: Απαντήσεις στην ερώτηση "Θα σε ενδιέφερε να μάθεις περισσότερες πληροφορίες σχετικά με την ασφάλεια και το απόρρητο μέσω της χρήσης άλλων παιχνιδιών;"

Τέλος, τέθηκε στους μαθητές το ερώτημα εάν θεωρούν ότι αν έπαιζαν και άλλα παιχνίδια με επίκεντρο το διαδικτυακό απόρρητο και την προστασία των δεδομένων τους θα μπορούσαν να προστατευτούν καλύτερα στον κυβερνοχώρο. Σε αυτή την ερώτηση οι απαντήσεις παρουσιάζουν μία πιο διαφορετική εικόνα από τις προηγούμενες ερωτήσεις. Αναλυτικά φαίνονται στην Εικόνα 47.



Εικόνα 47: Απαντήσεις στην ερώτηση "Θεωρείς ότι αν έπαιζες και άλλα παιχνίδια με επίκεντρο το διαδικτυακό απόρρητο και την προστασία των δεδομένων σου θα μπορούσες να προστατευτείς καλύτερα στον διαδικτυακό χώρο;"

3.4 Συμπεράσματα της εμπειρικής μελέτης

3.4.1 Εισαγωγή

Στην ενότητα αυτή παρουσιάζονται τα συμπεράσματα που εξήχθησαν για τα ερευνητικά ερωτήματα της εμπειρικής μελέτης, πραγματοποιώντας ταυτόχρονα και μία σύνθεση των απαντήσεων των ερωτηματολογίων.

3.4.2 Ε.Ε.Μ.1. Ποια είναι η στάση των μαθητών απέναντι στην μάθηση μέσω παιχνιδιών σοβαρού σκοπού;

Οι μαθητές έδειξαν ιδιαίτερο ενδιαφέρον για τη μάθηση μέσω παιχνιδιού. Οι περισσότεροι από αυτούς εξέφρασαν την επιθυμία τους να συλλέγουν γνώσεις και πληροφορίες όχι μόνο με παραδοσιακούς τρόπους μάθησης αλλά και με παιχνίδια. Θα προτιμούσαν αν εκτός από το σχολικό βιβλίο αξιοποιούσαν και τη μάθηση μέσω παιχνιδιών. Αυτή η αντίδραση των μαθητών απαντά και στην τρίτη ερώτηση που θέτει η εμπειρική μελέτη εάν οι μαθητές προτιμούν να μαθαίνουν για την προστασία της ιδιωτικότητας τους μόνο μέσα από παραδοσιακούς τρόπους εκπαίδευσης, σχολικό βιβλίο, ή συνδυαστικά με παιχνίδια σοβαρού σκοπού.

Επιπρόσθετα, αναφέροντας ότι τα παιχνίδια τους έκαναν γνωστές πληροφορίες σχετικές με την ασφάλεια και το απόρρητο στο διαδίκτυο που δεν γνώριζαν ήδη, επιβεβαιώνει ότι τα παιχνίδια μπορούν να αξιοποιηθούν ως συμπληρωματικά εργαλεία μάθησης. Άλλωστε οι μαθητές επέδειξαν ιδιαίτερο ενδιαφέρον ως προς αυτά και το περιεχόμενο τους και οι περισσότεροι από αυτούς υπογράμμισαν ότι αν είχαν την ευκαιρία να παίξουν και άλλα με παρεμφερές περιεχόμενο θα είχαν τη δυνατότητα να συλλέξουν περισσότερες πληροφορίες σχετικές με την ασφάλεια και το απόρρητο στο διαδίκτυο. Έτσι θα μπορούσαν να προστατέψουν καλύτερα τους εαυτούς στον κυβερνοχώρο.

3.4.3 Ε.Ε.Μ.2. Ποια είναι η στάση των μαθητών απέναντι στην προστασία των προσωπικών τους δεδομένων και γενικότερα την προστασία τους στον κυβερνοχώρο;

Η τωρινή στάση των μαθητών απέναντι στην προστασία των προσωπικών τους δεδομένων και γενικότερα την προστασία τους στον κυβερνοχώρο δημιουργεί ορισμένους προβληματισμούς. Από κάποιες απαντήσεις συμμετεχόντων/ουσών στο ερωτηματολόγιο των προ-ερωτήσεων φαίνεται ότι η στάση αρκετών νεαρών χρηστών των μέσων κοινωνικής δικτύωσης δεν διαφυλάσσει την προστασία τους στο διαδίκτυο.

Αρχικά, βλέποντας ότι η πλειοψηφία των μαθητών αισθάνεται σημαντική την ανάγκη προστασίας του απορρήτου στο διαδίκτυο περιμένει κανείς να δει μία πολύ υπεύθυνη διαδικτυακή συμπεριφορά. Όμως σχεδόν οι μισοί μαθητές υποστήριξαν ότι χρησιμοποιούν ως κωδικό ασφαλείας έναν εύκολα εντοπίσημο συνδυασμό. Επιπλέον, βλέποντας τις απαντήσεις στην ερώτηση που αφορούσε τους ακολούθους στα μέσα κοινωνικής δικτύωσης εντοπίζει κάποιος ότι αρκετοί είναι αυτοί που αποδέχονται οποιονδήποτε. Οι περισσότεροι ωστόσο αποδέχονται προφίλ χωρίς να φιλτράρουν αν οι υποψήφιοι ακόλουθοι ενδιαφέρονται για την προστασία του διαδικτυακού τους απορρήτου. Σε αυτή την ερώτηση κανείς δεν απάντησε ότι έχει κλειστό προφίλ και αποδέχεται μόνο άτομα τα οποία ενδιαφέρονται και εκείνα για το απόρρητο. Αυτό έρχεται σε αντιδιαστολή με το γεγονός ότι σχεδόν όλοι οι μαθητές υποστήριξαν ότι είναι αναγκαίο να προστατεύει κανείς τα προσωπικά του δεδομένα στο διαδίκτυο.

Παράλληλα, αυτή η αντίθεση εντοπίζεται στο γεγονός ότι σχεδόν όλοι οι μαθητές έχουν μοιραστεί ή μοιράζονται τα μέρη που τους αρέσει να συχνάζουν στα μέσα κοινωνικής δικτύωσης. Επίσης, ανησυχία σχετικά με το απόρρητο μπορεί να προκαλέσει

και το γεγονός ότι 68,3% του δείγματος αποδέχεται κάποιον στα μέσα κοινωνικής δικτύωσης απλά και μόνο επειδή το προφίλ μπορεί να είναι αληθοφανές.

Ανησυχία προκαλεί, επιπλέον, ότι το 26,8% του δείγματος έχει συναντήσει κάποιον άγνωστο που έμαθε μέσω των μέσων κοινωνικής δικτύωσης. Οι ανησυχίες επίσης αυξάνονται όταν διαπιστώνεται ότι αντίστοιχο ποσοστό μαθητών έχει δεχτεί cyber stalking. Εντύπωση προκαλεί ότι 9 από τους μαθητές/τριες έχουν παρακολουθήσει ή και ενοχλήσει κάποιον συστηματικά μέσα από τις πλατφόρμες κοινωνικής δικτύωσης.

Ταυτόχρονα, δυσαρέσκεια προκαλεί η ενδεχόμενη αντίδραση 16 μαθητών/τριών στην περίπτωση στην οποία κάποιος, σε ένα online game, ισχυριστεί ότι έχει μία αποκαλυπτική φωτογραφία τους και ότι θα τη στείλει στην οικογένεια τους αν δεν λάβει και άλλες παρόμοιες. Οι συγκεκριμένοι μαθητές/τριες δήλωσαν ότι δεν θα απευθυνθούν σε κάποιον ενήλικα ή στην αστυνομία. Αντίθετα οι 14 απάντησαν ότι δεν θα μιλούσαν σε κανέναν και θα διέγραφαν το μήνυμα, ενώ 2 θα έστελναν περισσότερες φωτογραφίες.

3.4.4 E.E.M.4. Οι μαθητές χρειάζονται βοήθεια για να ασχοληθούν με το διαδικτυακό περιβάλλον (παιχνίδι σοβαρού σκοπού) ή μπορούν να χρησιμοποιήσουν αυτά τα παιχνίδια μόνοι τους εκτός του σχολικού ωραρίου ως συμπληρωματική μάθηση;

Η ερώτηση αυτή απαντάται στις αρχικές ερωτήσεις του ερωτηματολογίου μετά-ερωτήσεων. Εντοπίστηκε, λοιπόν, ότι οι περισσότεροι μαθητές δεν χρειάστηκαν βοήθεια για κανένα από τα παιχνίδια αυτά. Άλλωστε, αρκετοί εξέφρασαν ότι δεν χρειάστηκαν ιδιαίτερες προϋπάρχουσες γνώσεις για την ενασχόληση τους με τα παιχνίδια. Παράλληλα, η πλειοψηφία υποστήριξε ότι και άλλοι συμμαθητές τους ακόμη και μικρότερης ηλικίας θα μπορούσαν να παίξουν τα παιχνίδια. Έτσι μπορεί να επιβεβαιωθεί ότι αυτά τα παιχνίδια θα μπορούσαν να αξιοποιηθούν ως συμπληρωματική μάθηση εκτός του σχολικού ωραρίου χωρίς την επίβλεψη-βοήθεια κάποιου εκπαιδευτικού.

3.4.5 E.E.M.5. Είναι αποτελεσματική τελικά η εκπαίδευση μέσω της χρήσης παιχνιδιών σοβαρού σκοπού (Digital Game-Based Learning - DGBL) στην ανάπτυξη δεξιοτήτων προστασίας στον κυβερνοχώρο;

Η απάντηση στην ερώτηση αυτή εντοπίζεται στην ενότητα με τις ερωτήσεις μαθησιακών αποτελεσμάτων του ερωτηματολογίου μετά-ερωτήσεων. Συγκεκριμένα, για

τα παιχνίδια που αξιοποιεί η παρούσα ερευνητική μελέτη προκύπτει ότι η εκπαίδευση μέσω της χρήσης παιχνιδιών σοβαρού σκοπού (Digital Game-Based Learning - DGBL) στην ανάπτυξη δεξιοτήτων προστασίας στον κυβερνοχώρο των μαθητών/τριών ήταν αποτελεσματική.

Συγκεκριμένα, οι περισσότεροι μαθητές δήλωσαν ότι έμαθαν πληροφορίες που δεν γνώριζαν και ότι συμφωνούν πως τα παιχνίδια θα μπορούσαν να αξιοποιηθούν στην εκπαιδευτική διαδικασία. Μέσω των παιχνιδιών αυτών οι μαθητές εμπέδωσαν σε μεγάλο βαθμό τη σημαντικότητα της προστασίας του απορρήτου τους στο διαδίκτυο. Ταυτόχρονα, αρκετοί εξέφρασαν ότι θα αλλάξουν την στάση τους απέναντι στην προστασία τους μετά την ενασχόληση τους με αυτά.

Επιπλέον, αρκετοί είναι αυτοί οι οποίοι μετά την ενασχόληση τους με τα παιχνίδια δήλωσαν ότι παρακινήθηκαν να ψάξουν περαιτέρω πληροφορίες σχετικές με το θέμα στο διαδίκτυο.Παράλληλα, οι περισσότεροι συμμετέχοντες/ουσες εξέφρασαν ότι τα παιχνίδια ήταν ικανά να τους παρακινήσουν να έχουν μία πιο υπεύθυνη διαδικτυακή συμπεριφορά.

Από τα παραπάνω προκύπτει ότι ο σκοπός του DGBL ως προς την ανάπτυξη δεξιοτήτων προστασίας στον κυβερνοχώρο επιτεύχθηκε μέσω αυτών των παιχνιδιών στην πλειοψηφία των μαθητών/τριών. Με αυτόν τον τρόπο απαντάται και το έκτο ερώτημα της εμπειρικής μελέτης που είναι αν η εφαρμογή παιχνιδιών συμβάλλει στην ευαισθητοποίηση σχετικά με το απόρρητο και στην αλλαγή της συμπεριφοράς των μαθητών/τριών.

3.4.6 Ε.Ε.Μ.7. Ποια είναι η στάση των μαθητών απέναντι στην ασφάλεια και το απόρρητο στο διαδίκτυο, πριν και ποια μετά την εφαρμογή των παιχνιδιών;

Την τελευταία ερώτηση της εμπειρικής μελέτης απαντούν οι προηγούμενες ενότητες. Περιληπτικά, από τις απαντήσεις του ερωτηματολογίου προ-ερωτήσεων προέκυψε ότι η στάση των μαθητών πριν την ενασχόληση τους με τα παιχνίδια δεν είναι ικανή να προστατέψει σημαντικά το απόρρητο και τα προσωπικά δεδομένα τους. Αν και οι μαθητές είχαν εκφράσει εξαρχής ότι θεωρούν πολύ σημαντική την ανάγκη προστασίας του απορρήτου τους μετά τη χρήση των παιχνιδιών διαπίστωσαν ότι χρειάζεται να αλλάξουν στοιχεία της διαδικτυακής τους συμπεριφοράς με σκοπό να το προστατεύουν υπεύθυνα.

Διαπιστώθηκε, από τους ίδιους τους μαθητές/τριες, ότι η προϋπάρχουσα στάση τους απέναντι στην ασφάλεια και το απόρρητο στο διαδίκτυο χρειάζεται αλλαγή και αυτό επιβεβαιώνεται από τις απαντήσεις τους μετά την ενασχόληση τους με τα παιχνίδια.

4 Επίλογος

4.1 Σύνοψη και συμπεράσματα

Η διπλωματική αυτή εργασία χωρίζεται σε τέσσερα κεφάλαια. Στο πρώτο κεφάλαιο, αυτό της εισαγωγής, αρχικά διατυπώνεται η σημαντικότητα του θέματος. Γίνεται γνωστό το γεγονός ότι τα παιχνίδια σοβαρού σκοπού εξυπηρετούν διάφορους σκοπούς. Ένας από αυτούς είναι η αλλαγή της συμπεριφοράς των παικτών με στόχο την ευαισθητοποίηση τους σε διάφορα θέματα. Χρειάζεται να σημειωθεί ότι η παρούσα εργασία επικεντρώνεται σε παιχνίδια σοβαρού σκοπού με περιεχόμενο τα προσωπικά δεδομένα και την προστασία του απορρήτου στον κυβερνοχώρο. Η σημαντικότητα του θέματος έγκειται στην ανάγκη να διαπιστωθεί εάν η εφαρμογή των παιχνιδιών σοβαρού σκοπού στα πλαίσια της εκπαίδευσης είναι ικανή να αλλάξει τη στάση των μαθητών στα ζητήματα της προστασίας των προσωπικών δεδομένων και του απορρήτου στο διαδίκτυο.

Οι στόχοι της εργασίας αυτής είναι δύο. Πρώτον η εργασία ερευνά υπάρχοντα παιχνίδια σοβαρού σκοπού με περιεχόμενο τα προσωπικά δεδομένα και την προστασία του απορρήτου στον κυβερνοχώρο. Δεύτερον διερευνά εάν η εφαρμογή παιχνιδιών, με αυτό το περιεχόμενο, σε μαθητές είναι ικανή να συμβάλλει στην ευαισθητοποίηση τους σχετικά με αυτά τα ζητήματα και στην αλλαγή της συμπεριφοράς τους. Ο πρώτος στόχος επιτυγχάνεται μέσα από την βιβλιογραφική επισκόπηση και ο δεύτερος στόχος μέσα από την εμπειρική μελέτη.

Η βιβλιογραφική επισκόπηση αναπτύσσεται στο δεύτερο κεφάλαιο. Μέσα από αυτό το κεφάλαιο επιδιώκεται να απαντηθούν ορισμένα ερωτήματα. Καταρχάς, η βιβλιογραφική επισκόπηση ακολουθεί τη μεθοδολογία PRISMA, θέτοντας το κατάλληλο ερώτημα στη βάση δεδομένων Google Scholar. Μετά την καταγραφή της μεθοδολογίας της βιβλιογραφικής επισκόπησης αναλύεται η έννοια της παιχνιδοποίησης και των παιχνιδιών σοβαρού σκοπού, εξηγώντας ότι τα παιχνίδια αυτά δεν επιδιώκουν αποκλειστικά την ψυχαγωγία των παικτών αλλά και άλλους σκοπούς. Γίνεται γνωστό, επίσης, το γεγονός ότι η τεχνολογία εκτός από οφέλη καιροφυλακτεί και κινδύνους. Αναφορικά με τους κινδύνους αξίζει να σημειωθεί ότι σήμερα αν και πολλά παιδιά κάνουν συστηματική χρήση του διαδικτύου δεν έχουν ιδιαίτερα αναπτυγμένες δεξιότητες ασφάλειας και διαφύλαξης του απορρήτου τους σε αυτό. Το πρόβλημα αυτό μπορεί να αντιμετωπιστεί με τη βοήθεια παιχνιδιών σοβαρού

σκοπού. Η χρήση αυτών των παιχνιδιών ως εκπαιδευτικά εργαλεία με στόχο την κατανόηση εννοιών σχετικών με την ασφάλεια στον κυβερνοχώρο είναι δυνατό να αποτελέσει λύση στο πρόβλημα.

Έχουν αναπτυχθεί διάφορα είδη παιχνιδιών σοβαρού σκοπού με στόχο την ευαισθητοποίηση για την ασφάλεια στο διαδίκτυο. Παράλληλα, μεγάλο είναι και το πλήθος των παιχνιδιών σοβαρού σκοπού με περιεχόμενο σχετικό με το ηλεκτρονικό "ψάρεμα" (Phishing) και το Hacking. Επιπλέον, δεν είναι λίγα τα παιχνίδια εκείνα τα οποία στοχεύουν στην ευαισθητοποίηση των παικτών σε διάφορα ζητήματα απορρήτου στον κυβερνοχώρο. Συγκεκριμένα, παιχνίδια αυτής της κατηγορίας μπορεί να αφορούν γενικά την προστασία του απορρήτου στο διαδίκτυο ή μπορεί να επικεντρώνονται στο απόρρητο των ηλεκτρονικών συσκευών, στον κίνδυνο παραβίασης του απορρήτου στα μέσα κοινωνικής δικτύωσης ή στο απόρρητο της τοποθεσίας. Επιπλέον, τα παιχνίδια σοβαρού σκοπού αυτής της κατηγορίας μπορεί να έχουν περιεχόμενο σχετικό με τις πολιτικές απορρήτου ή τα cookies. Τέλος, έχουν αναπτυχθεί και διάφορα παιχνίδια μέσα από τα οποία επιδιώκεται η αντιμετώπιση του προβλήματος της έλλειψης προστασίας των προσωπικών δεδομένων των χρηστών του διαδικτύου.

Στο τέλος του κεφαλαίου της βιβλιογραφικής επισκόπησης απαντώνται ερωτήματα σχετικά με τα παιχνίδια σοβαρού σκοπού που εντοπίστηκαν. Η εργασία απαντά ποια παιχνίδια έχουν αναπτυχθεί με περιεχόμενο σχετικό με την ασφάλεια και το απόρρητο στο διαδίκτυο και σε ποιους απευθύνονται. Επιπλέον, απαντά στο ερώτημα που αφορά την εμπειρία των χρηστών από την ασχολία τους με τα παιχνίδια. Επίσης, δίνεται απάντηση στο ερώτημα αν αυτά τα παιχνίδια είναι αποτελεσματικά και κατάλληλα να επιτύχουν το επιδιωκόμενο μαθησιακό αποτέλεσμα. Οι απαντήσεις στα δύο τελευταία ερωτήματα συλλέχθηκαν από τις αξιολογήσεις των παιχνιδιών οι οποίες εντοπίστηκαν στη βιβλιογραφία. Εκεί παρατηρήθηκε ότι υπάρχουν παιχνίδια τα οποία δεν έχουν τεθεί σε διαδικασία αξιολόγησης. Επιπλέον, διαπιστώθηκε ότι η αξιολόγηση πολλών παιχνιδιών έγινε, τις περισσότερες φορές, είτε από ειδικούς είτε από μικρό δείγμα παικτών.

Το κεφάλαιο της βιβλιογραφικής επισκόπησης διαδέχεται η εμπειρική μελέτη. Αρχικά, διατυπώνονται τα ερωτήματα που καλείται να απαντήσει η εμπειρική μελέτη καθώς και η μεθοδολογία την οποία ακολουθεί η οποία περιλαμβάνει την επιλογή των κατάλληλων παιχνιδιών και την δημιουργία των ερωτηματολογίων τα οποία εφαρμόστηκαν σε 41 μαθητές Β' τάξης Γενικού Λυκείου. Υπενθυμίζεται, εδώ, ότι οι

μαθητές απάντησαν πρώτα στο ερωτηματολόγιο προ-ερωτήσεων, έπειτα έπαιξαν δύο παιχνίδια και τέλος απάντησαν στο ερωτηματολόγιο μετά-ερωτήσεων. Έπειτα ακολουθούν τα αποτελέσματα του ερωτηματολογίου προ-ερωτήσεων. Από τις απαντήσεις προέκυψαν κάποια αξιοσημείωτα πράγματα. Ένα από αυτά είναι το γεγονός ότι το 46,3% των μαθητών δεν έχει παίξει ποτέ εκπαιδευτικά παιχνίδια στα πλαίσια του μαθήματος της Πληροφορικής. Μία ακόμη ενδιαφέρουσα πληροφορία που εξάχθηκε ήταν ότι όλοι οι μαθητές έχουν λογαριασμό σε τουλάχιστον ένα μέσο κοινωνικής δικτύωσης αλλά κανείς τους δεν προσέχει να έχει ακόλουθους που να ενδιαφέρονται πραγματικά για την προστασία του απορρήτου. Παράλληλα, σχεδόν οι μισοί, 48,8%, έχουν χρησιμοποιήσει έναν πολύ απλό κωδικό ασφαλείας ενώ το 51,2% των μαθητών εξέφρασε ότι πάντα συνδέεται σε δημόσια δίκτυα Wi-Fi ακόμη και όταν αυτά δεν ζητούν password για να επιτρέψουν την σύνδεση. Οι απαντήσεις αυτές όμως έρχονται σε αντίθεση με το γεγονός ότι το 83% των μαθητών θεωρεί ιδιαίτερα σημαντική την προστασία των προσωπικών δεδομένων στο διαδίκτυο.

Μετά την ανάλυση των απαντήσεων του ερωτηματολογίου προ-ερωτήσεων ακολούθησε η ανάλυση των απαντήσεων του ερωτηματολογίου μετά-ερωτήσεων. Το ερωτηματολόγιο αυτό αποτελούνταν από ερωτήσεις τριών κατηγοριών. Η πρώτη κατηγορία ερωτήσεων αφορούσε την εμπειρία του χρήστη από την ενασχόληση του με τα παιχνίδια. Συγκεκριμένα, περιελάμβανε ερωτήσεις σχετικές με τον σχεδιασμό των παιχνιδιών, το αν χρειάστηκαν βοήθεια και γνώσεις για να τα παίξουν, αν τους φάνηκαν ενδιαφέροντα ή μονότονα και αν θα πρότειναν σε άλλους να μάθουν πληροφορίες για την ασφάλεια και το απόρρητο στο διαδίκτυο παίζοντας αυτά τα παιχνίδια. Αξίζει να σημειωθεί ότι πάνω από το 80% των μαθητών θα πρότειναν σε άλλους παίξουν αυτά τα παιχνίδια. Η δεύτερη κατηγορία ερωτήσεων περιελάμβανε ερωτήσεις σχετικές με την ευχρηστία των παιχνιδιών. Μέσα από αυτές διαπιστώθηκε ότι περισσότερο από το 70% των μαθητών έμεινε ικανοποιημένο από την βοήθεια, την καθοδήγηση και την ανατροφοδότηση που έλαβε κατά τη διάρκεια ενασχόλησης του με τα παιχνίδια.

Η τελευταία κατηγορία περιελάμβανε ερωτήσεις σχετικές με τα μαθησιακά αποτελέσματα από την ενασχόληση με τα παιχνίδια. Οι περισσότεροι μαθητές, πάνω από το 80%, εξέφρασαν ότι τα παιχνίδια αυτά θα ήταν χρήσιμο να αξιοποιηθούν ως συμπλήρωμα στην εκπαιδευτική διαδικασία. Επίσης, το 75% των μαθητών έμαθε ενδιαφέρουσες πληροφορίες που δεν γνώριζε και το 80%, περίπου, αναγνώρισε την σημαντικότητα της διαφύλαξης του απορρήτου μετά την ενασχόληση με τα παιχνίδια.

Παράλληλα, το 58%, περίπου, δήλωσε ότι θα αλλάξει στάση απέναντι στον τρόπο αντίληψης του απορρήτου και της ασφάλειας ενώ ταυτόχρονα παρακινήθηκε να αναζητήσει περισσότερες πληροφορίες σχετικές με το θέμα. Επιπρόσθετα πάνω από το 60% είναι διατεθειμένο να αλλάξει την διαδικτυακή του συμπεριφορά. Επίσης, πάνω από το 90% των μαθητών δήλωσε ότι θα ήθελε να γνωρίσει περισσότερες πληροφορίες σχετικές με το θέμα αξιοποιώντας και παιχνίδια συμπληρωματικά με το σχολικό βιβλίο. Άλλωστε περισσότερο από το 80% των μαθητών εξέφρασε ότι αν έπαιζε και άλλα παιχνίδια σχετικά με την ασφάλεια και το απόρρητο στο διαδίκτυο θα μπορούσε να προστατευτεί αποτελεσματικότερα στον κυβερνοχώρο.

Στο τελευταίο μέρος της εμπειρικής μελέτης περιλαμβάνονται τα συμπεράσματα αυτής και απαντώνται τα ερωτήματα. Προέκυψε, λοιπόν, ότι οι μαθητές είχαν μία θετική στάση απέναντι στη μάθηση μέσω παιχνιδιών. Επιβεβαίωσαν ότι έμαθαν μέσα από τα παιχνίδια πληροφορίες που δεν γνώριζαν και ότι θα ήθελα να αξιοποιούνται τα παιχνίδια ως συμπληρωματικά εργαλεία μάθησης. Προτιμούν άλλωστε να χρησιμοποιούνται και παιχνίδια στην εκπαιδευτική διαδικασία με σκοπό αυτή να μην περιορίζεται αποκλειστικά σε παραδοσιακές μεθόδους. Επιπλέον, δηλώνοντας οι μαθητές ότι δεν χρειάστηκαν βοήθεια κατά την ενασχόληση τους με τα παιχνίδια εύκολα συμπεραίνει κανείς ότι μπορούν να αξιοποιηθούν ως συμπληρωματική μάθηση και εκτός του σχολικού πλαισίου. Παράλληλα, διαπιστώθηκε μέσα από την εμπειρική μελέτη ότι η υπάρχουσα στάση των μαθητών απέναντι στην προστασία των προσωπικών δεδομένων και γενικότερα την ασφάλεια στον κυβερνοχώρο δημιουργεί προβληματισμούς. Αν και οι μαθητές αναγνωρίζουν την αξία της προστασίας της ιδιωτικότητας τους ο τρόπος χρήσης των κοινωνικών δικτύων από μεριάς τους δεν την διαφυλάσσει ιδιαίτερα. Προκύπτει, λοιπόν, ότι η στάση πριν την ενασχόληση με τα παιχνίδια δεν ήταν ιδιαίτερα ικανή να προστατέψει το απόρρητο των παιδιών.

Τέλος, αποδείχτηκε ότι το Digital Game-Based Learning είναι αποτελεσματικό στην ανάπτυξη δεξιοτήτων προστασίας του απορρήτου και των προσωπικών δεδομένων στον διαδικτυακό χώρο. Αυτό επιβεβαιώνει το γεγονός ότι οι μαθητές δήλωσαν πως έμαθαν ενδιαφέρουσες πληροφορίες, συμφώνησαν ότι τα παιχνίδια είναι ωφέλιμο να αξιοποιούνται ως συμπληρωματική μάθηση, κινητοποιήθηκαν να αναζητήσουν νέες πληροφορίες και ευαισθητοποιήθηκαν στα θέματα προστασίας. Άλλωστε οι ίδιοι οι μαθητές μετά την ενασχόληση τους με τα παιχνίδια διαπίστωσαν ότι ο τρόπος με τον οποίο διαχειρίζονται το απόρρητο και τα προσωπικά δεδομένα τους στον κυβερνοχώρο

χρειάζεται αλλαγή. Εν κατακλείδι, η ενασχόληση των παιδιών με αυτά τα παιχνίδια ήταν ικανή να πετύχει την ευαισθητοποίηση σε θέματα ασφάλειας και προστασίας των προσωπικών δεδομένων καθώς και την αφύπνιση τους για αλλαγή της συμπεριφοράς τους.

4.2 Όρια και περιορισμοί της έρευνας

Σε αυτή την ενότητα πραγματοποιείται μία σύντομη αναφορά σε ατέλειες τις έρευνας. Όπως και στις περισσότερες μελέτες έτσι και σε αυτή εντοπίζονται κάποιες αστοχίες οι οποίες περιορίζουν την δυνατότητα απόλυτης αποδοχής των αποτελεσμάτων. Αρχικά, οι μαθητές που επιλέχθηκε να απαντήσουν στα ερωτηματολόγια και να ασχοληθούν με τα παιχνίδια ήταν μόνο 41. Επομένως, τα συμπεράσματα τα οποία προέκυψαν δεν μπορούν να διακρίνονται από απόλυτη ακρίβεια εάν γενικευτούν. Δεν είναι δυνατό τα αποτελέσματα τόσων λίγων, σε αριθμό, εφήβων να αντικατοπτρίζουν όλους τους μαθητές της Β' Λυκείου ή ακόμη και όλα τα παιδιά.

Επιπλέον, η επιλογή δύο παιχνιδιών και η διαπίστωση από τους περισσότερους μαθητές ότι επιτυγχάνουν τον σκοπό τους δεν μπορεί να σημαίνει ότι όλα τα παιχνίδια μπορούν να επιτύχουν τους σκοπούς τους. Παράλληλα, η εφαρμογή αυτών των ερωτήσεων στα ερωτηματολόγια δεν είναι ικανή τα αποκλείσει ότι υπάρχουν και άλλα κριτήρια να αξιολογήσει κανείς τη στάση των μαθητών απέναντι στην ασφάλεια και την προστασία των δεδομένων τους στο διαδίκτυο. Ταυτόχρονα, δεν αποκλείεται το γεγονός τα παιχνίδια να χρειάζεται να αξιολογούνται από περισσότερα κριτήρια σχετικά με την εμπειρία του χρήστη από αυτά, την ευχρηστία τους και τα μαθησιακά αποτελέσματα που προσφέρουν.

Συμπερασματικά, θα πρέπει να καταστεί σαφές ότι η έρευνα έχει ορισμένες ανεπάρκειες οι οποίες περιορίζουν τη δυνατότητα γενίκευσης και απόλυτης αποδοχής των αποτελεσμάτων της.

4.3 Μελλοντικές Επεκτάσεις

Η βιβλιογραφική επισκόπηση της διπλωματικής αυτής εργασίας επιβεβαιώνει την ύπαρξη μεγάλου πλήθους παιχνιδιών σοβαρού σκοπού με περιεχόμενο την ευαισθητοποίηση των παικτών σε θέματα ασφάλειας και προστασίας των προσωπικών δεδομένων στον κυβερνοχώρο. Διαπιστώθηκε όμως, ότι ορισμένα από τα παιχνίδια που εντοπίστηκαν δεν έχουν αξιολογηθεί ακόμη. Παράλληλα, κάποια από τα παιχνίδια έχουν εξεταστεί μόνο από ειδικούς. Επιπλέον, τα περισσότερα από αυτά έχουν αξιολογηθεί από

μικρό δείγμα ενδιαφερόμενων παικτών. Προτείνεται, λοιπόν, ως μελλοντική διαδικασία να αξιολογηθούν τα παιχνίδια τα οποία δεν έχουν αξιολογηθεί. Επιπλέον, θα ήταν χρήσιμο να εφαρμοστούν και να αξιολογηθούν τα παιχνίδια σε έναν μεγαλύτερο αριθμό παικτών στους οποίους απευθύνονται. Έτσι θα μπορούσε να διαπιστωθεί εάν πετυχαίνουν πράγματι τον σκοπό τους.

Η εμπειρική μελέτη της εργασίας κλήθηκε να αναγνωρίσει την στάση την οποία έχει ένα σύνολο μαθητών απέναντι στην προστασία του απορρήτου και των προσωπικών δεδομένων στο διαδίκτυο. Δυστυχώς εντοπίστηκε ότι οι μαθητές δεν προστατεύουν σημαντικά τα τις προσωπικές τους πληροφορίες αν και αναγνωρίζουν ότι είναι αναγκαία η προστασία τους. Αυτή η διαπίστωση έγινε και από τους ίδιους, μετά την ενασχόληση τους με παιχνίδια, με περιεχόμενο σχετικό με την προστασία των προσωπικών δεδομένων και την ασφάλεια στο διαδίκτυο. Η ενασχόληση τους με αυτά είχε ως αποτέλεσμα την ευαισθητοποίηση τους. Προτείνεται, λοιπόν, παιχνίδια σοβαρού σκοπού να ενσωματωθούν στην διαδικασία της εκπαίδευσης ως εργαλείο συμπληρωματικής μάθησης. Ακόμη όμως και αν αυτό δεν είναι εφικτό, προτείνεται να αξιοποιούνται τα παιχνίδια ως συμπληρωματική μάθηση στο σπίτι. Έτσι οι μαθητές θα έχουν την ευκαιρία να γνωρίσουν σημαντικές πληροφορίες εκτός του σχολικού ωραρίου παίζοντας παιχνίδια.

Βιβλιογραφία

Alhazmi, A. H., & Arachchilage, N. A. (2023). Evaluation of Game Design Framework Using a Gamified Browser-Based Application. *arXiv preprint arXiv:2306.07463* .

Allers, J., Drevin, G. R., Snyman, D. P., Kruger, H. A., & Drevin, L. (2021, June). Children's awareness of digital wellness: a serious games approach. In IFIP World Conference on Information Security Education (pp. 95-110). Charm Springer International Publishing.

Barnard-Wills, D., & Ashenden, D. (2015). Playing with privacy: Games for education and communication in the politics of online privacy. *Political Studies, 63(1), 142-160* .

Berger, E., & Sæthre, T. H. (2018). Privacity: A chatbot serious game to raise the privacy awareness of teenagers. *(Master's thesis, NTNU)* .

Bioglio, L., Capecchi, S., Peiretti, F., Sayed, D., Torasso, A., & Pensa, R. G. (2018). A social network simulation game to raise awareness of privacy among school children. *IEEE Transactions on Learning Technologies, 12(4), 456-469* .

Britnell, K. (2012). Cybersafety in the classroom: Looking toward the future. *Scan: The Journal for Edycators, 31 (1), 42-45* .

Chadwick, R., & Knight, P. (2010). Cybersmart: Learning Online Safety.

DeJong, S. (2020). *Generational Controls: Designing and implementing a serious intergerational escape game that analogizes data personalization, filter bubbles and echo chambers.* (Doctoral dissertation, Concordia University).

Diez, J. D., & Melcer, E. F. (2020). Cookie mania: a serious game for teaching internet cookies to high scool and college students. *In Serious Games: Joint International Conference, JCSG 2020, Stoke-on-Trent, UK, November 19-20, 2020, Proceedings 6 (pp. 69-77). Springer International Publishing* .

Fatima, R., Yasin, A., Liu, L., Wang, J., Afzal, W., & Yasin, A. (2019). Sharing information online rationally: An observation of user privacy concerns and awareness using serious game. *Journal of Information Security and Applications, 48, 102351* .

Gey, I., & Varvne, V. (2023). Informed Or Influenced?: Understanding if Implementing Defaults and Mappings in Privacy Notices Can Affect Users' Ability to Make Well-Informed and Deliberate Choices.

Hendrix, M., Al-Sherbaz, A., & Victoria, B. (2016). Game based cyber security training: are serious games suitable for cyber security training? *International Journal of Serious Games, 3(1), 53-61* .

Hill Jr, W. A., Fanuel, M., Yuan, X., Zhang, J., & Sajad, S. (2020). A survey of serious games for cybersecurity education and training.

Jaccheri, L., Mishra, D., Houmb, S. H., Omerovic, A., & Papavlasopoulou, S. (2017). SikkerhetsLøypa-Knowledge Toward Sustainable and Secure Paths of Creative and Critical Digital Skills. *In Entertainment Computing-ICEC 2017: 16th IFIP TC 14 International Conference, Tsukuba City, Japan, September 18-21, 2017, Proccedings 16 (pp 157-168). Springer International Publishing.*

James, C. (2009). Young people, ethics, and the new digital media: A synthesis from the GoodPlay Project (p. 128). The MIT Press.

Karagiannis, S. (2022). Systematic Design, Deployment and Evaluation of Gamefied Cybersecurity Learning Environments. (Doctoral dissertation, Ιόνιο Πανεπιστήμιο. Σχολή Επιστήμης της Πληροφορίας και Πληροφορικής. Τμήμα Πληροφορικής).

Karagiannis, S., Papaioannou, T., Magkos, E., & Tsohou, A. (2020, November). Game-Based Information Security/Privacy Education and Awareness: Theory and Practice. *In European, Mediterranean, and Middle Eastern Conference on Information Systems. Cham: Springer international Publishing* , σσ. 509-525 .

Katsantonis, M., & Mavridis, I. (2021). Evaluation of HackLearn COFELET game user experience for cybersecurity education. *International Journal of Serious Games, 8(3), 3-24.*

Lareki, A., de Morentin, J. I., Altuna, J., & Amenabar, N. (2017). Teenagers' perception of risk behaviors regarding digital technologies. Computers in Human Behavior, 68, 395-402.

Löffler, E., Schneider, B., Zanwar, T., & Asprion, P. M. (2021). Cysecescape 2.0-- a virtual escape room to raise cybersecurity awareness. *International Journal of Serious Games, 8(1), 59-70* .

Manotipya, P., & Ghazinour, K. (2020). Children's online privacy from parents' perspective. *Procedia Computer Science, 177, 178-185.*

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & Group*, &. P. (2009). Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. Annals of internal medicine, 151(4), 264-269.

Nahmias, Y., Feldman, D. K., Richter, G., & Raban, D. R. (2020). Games of Terms. *Vt L. Rev., 45, 387* .

Nicolaidou, I., & Venizelou, A. (2020). Improving children's E-safety skils through an interactive learning environment: A quasi-experimental study. *Multimodal Technologies and Interaction, 492), 10.*

Papaioannou, T., Tsohou, A., Bounias, G., & Karagiannis, S. (2022, October). A constructive approach for raising information privacy competences: The case of escape room games. *In International Conference on Trust and Privacy in Digital Business (pp. 33-49). Cham: Springer International Publishing.*

Pape, S., Klauer, A., & Rebler, M. (2021). Leech: Let's Expose Evidently bad data Collecting Habits - Towards a Serious Game on Understanding Privacy Policies.

Pensa, R. G., Di Blasi, G., & Bioglio, L. (2019). Network-aware privacy risk estimation in online social network. *Social Network Analysis and Mining, 9, 1-15.*

Pulido, M. A., Johnson, C. W., & Alzahrani, A. (2021). Security Awareness Level Evaluation of Healthcare Participants Through Educational Games. *International Journal of Serious Games 8(3), 25-41* .

Roepke, R., & Schroeder, U. (2019). The Problem with Teaching Defence against the Dark Arts: a Review og Game-based Learning Applications and Serious Games for Cyber Security Education. *CSEDU (2), 58-66.*

Sandovar, A., Braad, E., Streicher, A., & Söbke, H. (2016). Ethical stewardship: Designing serious games seriously. In Entertainment Computing and Serious Games: International Gl-Dagstuhl Seminar 15283, Dagstuhl Castle, Germany, July 5-10, 2015. Springer International Publishing.

Solberg, D. F. (2018). SPRIG: Serious Privacy Game Workshop. *(Master's thesis, NTNU)* .

Stellmacher, C., Ternieten, J., Soroco, D., & Schöning, J. (2022). Escaping the Privacy Paradox: Evaluating the Learning Effects of Privacy Policies With Serious Games. *Proceedings of the ACM on Human-Computer Interaction, 6(CHI PLAY), 1-20* .

Thieu, H. Q. (2019). *Location Stalker: A Serious Mobile Game to Raise Awareness Towards Location Privacy.* (Master's thesis, NTNU).

Treiblmaier, H., Putz, L. M., & Lowry, P. B. (2018). Transactions on Human-Computer Interaction. Interaction. 10(3), 129-163.

Underhay, L., Pretorius, A., & Ojo, S. (2016, May). Game-based enabled e-learning model for e-Safety education. *In 2016 IST-Africa Week Conference (pp. 1-7). IEEE.*

Williams, M., Nurse, J. R., & Creese, S. (2019). Smartwatch games: Encuraging privacy-protective behaviour in a longidinal study. *Computers in Human Behavior, 99, 38-54* .

Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR), 54(1), 1-39* .

Παράρτημα Α - Ερωτήσεις ερωτηματολογίων

Α.1 Ερωτήσεις ερωτηματολογίου προ-ερωτήσεων

Το ακόλουθο ερωτηματολόγιο χρησιμοποιείται ως ερευνητικό εργαλείο στο πλαίσιο εκπόνησης της διπλωματικής μου εργασίας για το μεταπτυχιακό του Διιδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών Δίκαιο και Πληροφορική του Πανεπιστημίου Μακεδονίας.

Η αποχώρηση από το ερωτηματολόγιο μπορεί να πραγματοποιηθεί αν πάσα στιγμή χωρίς κάποια συνέπεια.

Σκοπός του παρόντος ερωτηματολογίου είναι η εξέταση της στάσης των νεαρών απέναντι στην διαφύλαξη της ασφάλειας και του απορρήτου τους στον κυβερνοχώρο.

Το ερωτηματολόγιο έχει τέτοια σύνθεση η οποία διαφυλάσσει την ανωνυμία των ερωτώμενων.

Παρακαλώ απαντήστε στις ερωτήσεις με ειλικρίνεια, ώστε να εξαχθούν τα ακριβέστερα δυνατά αποτελέσματα.

* Υποδεικνύει απαιτούμενη ερώτηση

Συγκατάθεση *

Αν δεν επιθυμείς να δώσεις την συγκατάθεση σου χρειάζεται να αποχωρήσεις από την έρευνα

1. Ζητείται η συγκατάθεση σου για την επεξεργασία των απαντήσεων για της ανάγκες της έρευνας και ενδεχόμενης δημοσίευσης.

Δημογραφικά Στοιχεία Να επισημαίνεται μόνο μία απάντηση.

2. Ηλικία *

- ◯ 14
- ◯ 15
- ◯ 16
- ◯ 17

3. Φύλο*

- ◯ Άνδρας
- ◯ Γυναίκα

Α. Ερωτήσεις Πολλαπλών Επιλογών

Α.1 Έχεις παίξει εκπαιδευτικά παιχνίδια στα πλαίσια του μαθήματος της πληροφορικής; (Likert). *

	1	2	3	4	5	
Ποτέ	◯	◯	◯	◯	◯	Συνέχεια

Α.2 Αισθάνεσαι σημαντική την ανάγκη προστασίας του απορρήτου σου και των προσωπικών σου δεδομένων; (Likert). *

	1	2	3	4	5	
Καθόλου	◯	◯	◯	◯	◯	Πάρα πολύ

Α.3 Έχεις χρησιμοποιήσει ή χρησιμοποιείς σαν κωδικό ασφαλείας του κινητού σου το 1234 ή 1111 ή κάποιον παρόμοιο; *

- ◯ Ναι
- ◯ Όχι

Α.4 Έχεις λογαριασμό σε κάποιο/κάποια από τα ακόλουθα social media; *
Σε αυτή την ερώτηση μπορείς να επιλέξεις περισσότερα από ένα

- ☐ Facebook
- ☐ Youtube
- ☐ Instagram
- ☐ TikTok
- ☐ Δεν έχω social media
- ☐ Άλλο: _____

Α.5 Ποιος μπορεί να σε ακολουθήσει στα social media; *

- ◯ Όποιος θέλει. Έχω ανοιχτό προφίλ και μπορεί να με ακολουθήσει ο καθένας
- ◯ Όποιος θέλει. Έχω κλειστό προφίλ, για να δει κάποιος το περιεχόμενο μου χρειάζεται πρώτα με ακολουθήσει, αλλά πολλούς από τους ακολούθους μου δεν τους γνωρίζω και συνήθως αποδέχομαι όλα τα αιτήματα
- ◯ Μόνο κάποιος που γνωρίζω εγώ ή που έχουμε κοινούς γνωστούς στα social. Έχω κλειστό προφίλ, πολλούς από τους ακολούθους τους γνωρίζω και με άλλους έχουμε κοινούς γνωστούς στα social
- ◯ Μόνο κάποιος που γνωρίζω πολύ καλά. Ακολουθώ και με ακολουθούν άτομα που γνωρίζω πολύ καλά
- ◯ Ακολουθώ και με ακολουθούν άτομα που γνωρίζω πολύ καλά και ενδιαφερόμαστε όλοι για την προστασία των προσωπικών μας δεδομένων
- ◯ Δεν έχω social media

Α.6 Έχεις μοιραστεί στα social media τα μέρη που σου αρέσει να συχνάζεις; *

- ◯ Ναι
- ◯ Όχι

Α.7 Το "tik tok" σου δίνει την ευκαιρία να μιλάς με αγνώστους, να κάνεις ή να συμμετέχεις σε livestream και να βλέπεις αστεία αλλά και χρήσιμα βίντεο. Ποιοι είναι οι κίνδυνοι;

- ◯ Η τοποθεσία σου μπορεί να παρακολουθηθεί
- ◯ Άγνωστοι μπορούν να επικοινωνήσουν μαζί σου
- ◯ Μπορεί να πέσεις θύμα bulling
- ◯ Μπορεί να συναντήσεις κακή φρασεολογία και εξτρεμιστικές απόψεις
- ◯ Μπορεί να δεις ακατάλληλο περιεχόμενο
- ◯ Όλα τα παραπάνω
- ◯ τίποτα από τα παραπάνω

Α.8 Έχεις συναντήσει ποτέ κάποιον άγνωστο που γνώρισες online; *

- ◯ Ναι
- ◯ Όχι

Α.9 Δέχεσαι follow στο Instagram από άγνωστο. Τι κάνεις; * .

- ◯ Τον αποδέχεσαι
- ◯ Δεν τον αποδέχεσαι
- ◯ Ελέγχεις το προφίλ του και αν σου φανεί αληθινό τον αποδέχεσαι

Α.10 Μπλοκάρεις αριθμούς τηλεφώνου ή αιτήματα φιλίας που σου φαίνονται ύποπτα; (Likert) *

	1	2	3	4	5	
Ποτέ	◯	◯	◯	◯	◯	Πάντα

Α.11 Καλύπτεις πάντα την webcam (βιντεοκάμερα που μεταφέρει την εικόνα σε πραγματικό χρόνο προς ή μέσω ενός υπολογιστή) σου όταν δεν την χρησιμοποιείς;

- ◯ Ναι
- ◯ Όχι

Α.12 Έχεις δεχτεί ποτέ cyber stalking; (cyber stalking είναι η κατάσταση στην οποία κάποιος παρακολουθεί ή/και ενοχλεί κάποιον συστηματικά)

- ◯ Ναι
- ◯ Όχι

Α.13 Έχεις κάνει ποτέ cyber stalking; *

- ◯ Ναι
- ◯ Όχι

Α.14 Αν μιλήσεις με κάποιον σε ένα game και ισχυριστεί ότι έχει μία αποκαλυπτική φωτογραφία σου και ότι θα τη στείλει στην οικογένεια σου αν δεν του στείλεις και άλλες παρόμοιες, τι κάνεις; *

- ◯ Απευθύνεσαι σε κάποιον ενήλικα ή στην αστυνομία
- ◯ Δεν απευθύνεσαι σε κανέναν και διαγράφεις το μήνυμα
- ◯ Δεν απευθύνεσαι σε κανέναν και στέλνεις περισσότερες φωτογραφίες

Α.15 Αν λάβεις ένα μήνυμα από έναν φίλο σου το οποίο σου λέει να το κοινοποιήσεις σε άλλους 10 φίλους για να κερδίσεις κάτι, τι κάνεις; *

- ◯ Το διαγράφεις και ενημερώνεις το φίλο σου ότι μπορεί να τον χάκαραν
- ◯ Το στέλνεις σε άλλους γιατί μπορεί να μην είναι fake
- ◯ Το στέλνεις σε περισσότερους από 10 φίλους

Α.16 Έχεις αλλάξει ποτέ τον κωδικό σου στα social media από την ημέρα που δημιούργησες το προφίλ σου; *

- ◯ Όχι
- ◯ Ναι, τον έχω αλλάξει μία φορά
- ◯ Ναι τον αλλάζω συχνά

Α.17 Οι κωδικοί σου φροντίζεις να *

- ◯ Είναι πολύ δύσκολοι
- ◯ Μην τους μοιράζεσαι με κανέναν εκτός από τους γονείς σου
- ◯ Είναι μοναδικοί και κρυφοί από όλους

Α.18 Χρησιμοποιείς στους κωδικούς ασφαλείας σου αριθμούς, πεζά και κεφαλαία γράμματα και σύμβολα; *

- ◯ Ναι
- ◯ Όχι

Α.19 Χρησιμοποιείς password manager (διαχειριστής κωδικών πρόσβασης το οποίο οι χρήστες χρησιμοποιούν για να αποθηκεύουν και να διαχειρίζονται τους κωδικούς τους) για να σου υπενθυμίζει τους κωδικούς σου; *

- ◯ Ναι
- ◯ Όχι, τους θυμάμαι
- ◯ Όχι, χρησιμοποιώ τον ίδιο κωδικό ασφαλείας
- ◯ Όχι δεν γνωρίζω την ύπαρξη του

Α.20 Χρησιμοποιείς εκτός από τον κωδικό ασφαλείας των λογαριασμών σου και άλλους τρόπους για να τους διατηρείς ασφαλείς; (πχ sms στο κινητό, ειδοποίηση στο email) *

- ◯ Ναι
- ◯ Όχι

Α.21 Ποιος κωδικός είναι καλύτερος; *

- ◯ password456
- ◯ p@ssword
- ◯ paSsword
- ◯ 5pa@Ssword

Α.22 Τα "cookies" μπορούν να παρακολουθήσουν την διαδικτυακή σου δραστηριότητα; *

- ◯ Μπορούν να δουν την τοποθεσία σου
- ◯ Μπορούν να παρακολουθούν τους ιστότοπους που επισκέπτεστε
- ◯ Μπορούν να καταγράψουν το ιστορικό αναζήτησης στον ιστό
- ◯ Όλα τα παραπάνω
- ◯ Τίποτα από τα παραπάνω
- ◯ Δεν γνωρίζω τι είναι τα "cookies"

Α.23 Τι προστατεύει τα δεδομένα που στέλνεις σε άλλους;*

- ◯ Το URL
- ◯ Το Encryption
- ◯ Το Bluetooth
- ◯ Δεν γνωρίζω

Α.24 Τι από τα παρακάτω αποτελεί μέρος τους "ψηφιακού αποτυπώματος - digital footprint"; *

- ◯ Τα παιχνίδια και οι εφαρμογές που χρησιμοποιείς
- ◯ Τα μηνύματα σου και αυτά που ποστάρεις στα social media
- ◯ Οι ιστοσελίδες που επισκέπτεσαι
- ◯ Όλα τα παραπάνω
- ◯ Δεν γνωρίζω τι είναι το "ψηφιακό αποτύπωμα - digital footprint"
- ◯ Τίποτα από τα παραπάνω

Α.25 Πως λέγεται το λογισμικό που μπορεί να βλάψει τη συσκευή σας και να κλέψει τις πληροφορίες σας; *

- ◯ Δεν γνωρίζω
- ◯ Malware
- ◯ Deepfake
- ◯ Spoofing

Α.26 Γνωρίζεις τι σημαίνει η επέκταση .exe.file σε ένα αρχείο; *

- ◯ Ναι
- ◯ Όχι

Α.27 Έχεις συνδεθεί ποτέ σε δημόσιο δίκτυο Wi-Fi το οποίο μπορεί να μην ζητάει κωδικό; (Likert) *

	1	2	3	4	5	
Ποτέ	◯	◯	◯	◯	◯	Συνέχεια

Α.28 Κρατάς backups από σημαντικά αρχεία; *

- ◯ Ναι
- ◯ Όχι

Α.29 Προσέχεις πάντα την επέκταση σε συνημμένα που μπορεί να λάβω σε ένα email. Δεν ανοίγεις ποτέ αρχεία: *

- ◯ .pdf
- ◯ .exe
- ◯ .dock
- ◯ Δεν ανοίγω κανένα αρχείο που έρχεται σε email
- ◯ Δεν έχω παρατηρήσει ποτέ τις επεκτάσεις στα αρχεία που λαμβάνω μέσω email

Α.30 Όταν λαμβάνεις ένα spam (μαζική αποστολή ηλεκτρονικών μηνυμάτων) email *

- ◯ Το κάνεις share στους φίλους σου αλλά τους προειδοποιείς ότι είναι spam;
- ◯ Δεν ανοίγεις τα links και το επισημαίνεις ως spam;
- ◯ Το διαγράφεις αμέσως;

Α.31 Έχεις ενεργοποιημένο το Spam Filter με σκοπό να μην σου έρχονται ανεπιθύμητα
μηνύματα; *

- ◯ Ναι
- ◯ Όχι
- ◯ Δεν γνωρίζω τι είναι και πως να το ενεργοποιήσω

Α.32 Αν αγοράσεις κάτι με πιστωτική κάρτα και αποδειχτεί scam (απάτη) *

- ◯ Το αναφέρεις στους γονείς σου
- ◯ Διαγράφεις τον λογαριασμό και όλα καλά

Β. Ερωτήσεις Σύντομης Ανάπτυξης

Β.1 Πες με δύο λόγια τι γνωρίζεις για το phishing - ηλεκτρονικό "ψάρεμα"; *

Β.2 Τι γνωρίζεις για τον έλεγχος ταυτότητας δύο παραγόντων - 2-factor authentication; Εσύ αξιοποιείς το multi-factor authentication; *

Β.3 Από ποια ηλικία πιστεύεις ότι θα ήταν χρήσιμο ένας ανήλικος να έχει λογαριασμό στα social media; *

Β.4 Από ποια ηλικία είχες εσύ social media; *

Α.2 Ερωτήσεις ερωτηματολογίου μετά-ερωτήσεων

Το ακόλουθο ερωτηματολόγιο χρησιμοποιείται ως ερευνητικό εργαλείο στο πλαίσιο εκπόνησης της διπλωματικής μου εργασίας για το μεταπτυχιακό του Διιδρυματικού Προγράμματος Μεταπτυχιακών Σπουδών Δίκαιο και Πληροφορική του Πανεπιστημίου Μακεδονίας.

Η αποχώρηση από το ερωτηματολόγιο μπορεί να πραγματοποιηθεί αν πάσα στιγμή χωρίς κάποια συνέπεια.

Για να απαντήσει κανείς σε αυτό το ερωτηματολόγιο πρέπει πρώτα να έχει απαντήσει στο ερωτηματολόγιο προ-ερωτήσεων και να έχει παίξει τα παιχνίδια Space Shelter και Interland – Be Internet Awesome – Reality River της Google.

Σκοπός του παρόντος ερωτηματολογίου είναι η εξέταση της στάσης των νεαρών απέναντι στην διαφύλαξη της ασφάλειας και του απορρήτου τους στον κυβερνοχώρο.

Το ερωτηματολόγιο έχει τέτοια σύνθεση η οποία διαφυλάσσει την ανωνυμία των ερωτώμενων.

Παρακαλώ απαντήστε στις ερωτήσεις με ειλικρίνεια, ώστε να εξαχθούν τα ακριβέστερα δυνατά αποτελέσματα.

* Υποδεικνύει απαιτούμενη ερώτηση

Συγκατάθεση *

Αν δεν επιθυμείς να δώσεις την συγκατάθεση σου χρειάζεται να αποχωρήσεις από την έρευνα

1. Ζητείται η συγκατάθεση σου για την επεξεργασία των απαντήσεων για της ανάγκες της έρευνας και ενδεχόμενης δημοσίευσης.

Δημογραφικά Στοιχεία Να επισημαίνεται μόνο μία απάντηση.

2.Ηλικία*

- ◯ 14
- ◯ 15
- ◯ 16
- ◯ 17

3. Φύλο*

- ◯ Άνδρας
- ◯ Γυναίκα

Α. Ερωτήσεις Εμπειρίας Χρήστη

Απάντησε για κάθε παιχνίδι ξεχωριστά σε κλίμακα Likert

Α.1 Ο σχεδιασμός του παιχνιδιού (γραφικά κ.α.) σου φάνηκε ελκυστικός; *

	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
Space Shelter	◯	◯	◯	◯	◯
Be Internet Awesome	◯	◯	◯	◯	◯

Α.2 Χρειάστηκε να έχεις προϋπάρχουσες γνώσεις για να παίξεις το παιχνίδι; *

	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
Space Shelter	◯	◯	◯	◯	◯
Be Internet Awesome	◯	◯	◯	◯	◯

Α.3 Χρειάστηκες βοήθεια από κάποιον καθηγητή για να παίξεις το παιχνίδι; *

	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
Space Shelter	◯	◯	◯	◯	◯
Be Internet Awesome	◯	◯	◯	◯	◯

Α.4 Θα μπορούσαν εύκολα όλοι οι συμμαθητές σου να παίξουν το παιχνίδι; *

	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
Space Shelter	○	○	○	○	○
Be Internet Awesome	○	○	○	○	○

Α.5 Σου φάνηκε το παιχνίδι μονότονο; *

	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
Space Shelter	○	○	○	○	○
Be Internet Awesome	○	○	○	○	○

Α.6 Θα συνιστούσες το παιχνίδι σε μαθητές μικρότερης ηλικίας; *

	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
Space Shelter	○	○	○	○	○
Be Internet Awesome	○	○	○	○	○

Α.7 Διασκέδασες παίζοντας το παιχνίδι; *

	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
Space Shelter	○	○	○	○	○
Be Internet Awesome	○	○	○	○	○

Α.8 Σχετίζεται το παιχνίδι με τα ενδιαφέροντα σου; *

	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
Space Shelter	◯	◯	◯	◯	◯
Be Internet Awesome	◯	◯	◯	◯	◯

Α.9 Θα πρότεινες να μάθει κανείς περισσότερες πληροφορίες σχετικά με την ασφάλεια και το απόρρητο μέσω της χρήσης του παιχνιδιού; *

	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
Space Shelter	◯	◯	◯	◯	◯
Be Internet Awesome	◯	◯	◯	◯	◯

Β. Ερωτήσεις Ευχρηστίας

Απάντησε για κάθε παιχνίδι ξεχωριστά σε κλίμακα Likert

Β.1 Παρέχει το παιχνίδι καθοδήγηση και επαρκή βοήθεια; *

	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
Space Shelter	◯	◯	◯	◯	◯
Be Internet Awesome	◯	◯	◯	◯	◯

Β.2 Παρέχει το παιχνίδι ουσιαστική ανατροφοδότηση σχετικά με τις επιλογές που κάνεις κατά τη διάρκεια; *

	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
Space Shelter	○	○	○	○	○
Be Internet Awesome	○	○	○	○	○

Γ. Ερωτήσεις Εντοπισμού Μαθησιακών Αποτελεσμάτων

Απάντησε για κάθε παιχνίδι ξεχωριστά σε κλίμακα Likert

Ολοκλήρωσες το παιχνίδι; * (Σε αυτή την ερώτηση μπορείς να επιλέξεις περισσότερα από ένα. Αν έχεις ολοκληρώσει και τα 2 παιχνίδια επιλέγεις και τα δύο τετράγωνα.)

- ☐ Space Shelter
- ☐ Be Internet Awesome

Γ.1 Θα μπορούσε το παιχνίδι να χρησιμοποιηθεί ως συμπλήρωμα στην εκπαιδευτική διαδικασία;*

	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
Space Shelter	○	○	○	○	○
Be Internet Awesome	○	○	○	○	○

Γ.2 Έμαθες ενδιαφέρουσες πληροφορίες που δεν γνώριζες μέσα από το παιχνίδι; *

	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
Space Shelter	○	○	○	○	○
Be Internet Awesome	○	○	○	○	○

Γ.3 Σε βοήθησε το παιχνίδι να αναγνωρίσεις τη σημαντικότητα της προστασίας του απορρήτου σου;*

	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
Space Shelter	○	○	○	○	○
Be Internet Awesome	○	○	○	○	○

Γ.4 Σε ώθησε το παιχνίδι να αλλάξεις τη στάση σου απέναντι στον τρόπο με τονοποίο αντιλαμβανόσουν την διαδικτυακή ασφάλεια και το απόρρητο πριν να παίξεις;*

	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
Space Shelter	○	○	○	○	○
Be Internet Awesome	○	○	○	○	○

Γ.5 Το παιχνίδι σου φάνηκε διασκεδαστικό αλλά και συνάμα χρήσιμο ως προς τιςγνώσεις που σου προσέφερε;*

	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
Space Shelter	○	○	○	○	○
Be Internet Awesome	○	○	○	○	○

Γ.6 Σε παρακίνησε το παιχνίδι να αναζητήσεις περισσότερες πληροφορίες για τηνασφάλεια και το απόρρητο στο διαδίκτυο;*

	Καθόλου	Λίγο	Μέτρια	Πολύ	Πάρα πολύ
Space Shelter	○	○	○	○	○
Be Internet Awesome	○	○	○	○	○

Γ.7 Μετά την ενασχόληση σου με τα παιχνίδια σκοπεύεις να αλλάξεις την διαδικτυακή σου συμπεριφορά;*

	1	2	3	4	5	
Καθόλου	○	○	○	○	○	Πάρα πολύ

Γ.8 Θα ήθελες να γνωρίσεις πληροφορίες σχετικές με την προστασία τουαπορρήτου σου στο διαδίκτυο χρησιμοποιώντας μόνο παραδοσιακούς τρόπουςμάθησης (σχολικό βιβλίο) ή και μέσω παιχνιδιών;*

- ○ Προτιμώ την εκμάθηση εννοιών μέσω παραδοσιακών τρόπων διδασκαλίας
- ○ Προτιμώ την αξιοποίηση παιχνιδιών με σκοπό την εκμάθηση νέων εννοιών

Γ.9 Θα σε ενδιέφερε να μάθεις περισσότερες πληροφορίες σχετικά με την ασφάλεια και το απόρρητο μέσω της χρήσης άλλων παιχνιδιών;*

	1	2	3	4	5	
Καθόλου	○	○	○	○	○	Πάρα πολύ

Γ.10 Θεωρείς ότι αν έπαιζες και άλλα παιχνίδια με επίκεντρο το διαδικτυακόαπόρρητο και την προστασία των δεδομένων σου θα μπορούσες να προστατευτείςκαλύτερα στον διαδικτυακό χώρο;*

	1	2	3	4	5	
Καθόλου	○	○	○	○	○	Πάρα πολύ