

ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ
ΣΧΟΛΗ ΕΠΙΣΤΗΜΗΣ ΤΗΣ ΠΛΗΡΟΦΟΡΙΑΣ & ΠΛΗΡΟΦΟΡΙΚΗΣ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ



ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

**Δημιουργία ενός σοβαρού παιχνιδιού για την
κυβερνοασφάλεια**

Χριστίνα Γ. Κρυελέση, Π2017129

Επιβλέπουσα καθηγήτρια : Ελένη Χριστοπούλου

Κέρκυρα, Σεπτέμβριος 2021

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Δημιουργία ενός σοβαρού παιχνιδιού για την κυβερνοασφάλεια

Τριμελής Επιτροπή

Μιχαήλ Στεφανιδάκης
Αναπληρωτής Καθηγητής
Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Χριστόφορος Νταντογιάν
Επίκουρος Καθηγητής
Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Ελένη Χριστοπούλου
ΕΔΙΠ
Τμήμα Πληροφορικής, Ιόνιο Πανεπιστήμιο

Η παρούσα εργασία εκπονήθηκε στο πλαίσιο των σπουδών για την απόκτηση πτυχίου που απονέμει το Τμήμα Πληροφορικής της Σχολής Επιστήμης της Πληροφορίας και Πληροφόρησης του Ιονίου Πανεπιστημίου.

Ευχαριστίες

Θεωρώ μεγάλη ανάγκη να ευχαριστήσω τους ανθρώπους που με βοήθησαν στην εκπόνηση της πτυχιακής εργασίας μου, παρέχοντας μου υλική και ψυχολογική υποστήριξη. Αρχικά, θέλω να ευχαριστήσω την επιβλέπουσα καθηγήτρια, την κα. Ελένη Χριστοπούλου, για την βοήθεια και την καθοδήγηση που μου παρείχε για την εκπόνηση της παρούσας πτυχιακής, αλλά και τους επιβλέποντες καθηγητές της εργασίας, κ. Μιχαήλ Στεφανιδάκη και Χριστόφορο Νταντογιάν που μου έδωσαν την ευκαιρία να ασχοληθώ με το θέμα της ασφάλειας και της ανάπτυξης παιχνιδιού, ώστε να κάνω μια εμπεριστατωμένη έρευνα γύρω από το συγκεκριμένο θέμα ώστε και να αναπτύξω την πτυχιακή μου. Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου, τον αδερφό μου και την Θεοδώρα, για την αμέριστη ηθική και υλική συμπαράσταση που μου παρείχαν κατά την διάρκεια των σπουδών μου.

Περίληψη

Η εργασία αυτή αναφέρεται στην δημιουργία ενός σοβαρού παιχνιδιού για την κυβερνοασφάλεια που απευθύνεται σε υπαλλήλους επιχειρήσεων σε ένα πρόγραμμα εκπαίδευσης και ευαισθητοποίησης για την ασφάλεια. Είναι ένα παιχνίδι που ενσωματώνει στοιχεία gamification (παιχνιδοποίησης) και ανήκει στην κατηγορία παιχνίδια ρόλων (role playing games). Ο παίκτης αναλαμβάνει το ρόλο του υπαλλήλου μιας εταιρείας (όπως και στην πραγματική του ζωή) με βασικό σκοπό να μάθει διάφορες έννοιες, ποικίλους κινδύνους που υπάρχουν στον κυβερνοχώρο και τρόπους προφύλαξης σχετικά με την κυβερνοασφάλεια έτσι ώστε να ενδυναμώσει τον χαρακτήρα του παιχνιδιού για να καταφέρει να προστατευτεί από προβλήματα ασφάλειας. Ένα από τα σενάρια που σχεδιάστηκαν, υλοποιήθηκε και έχει να κάνει με την επίθεση ηλεκτρονικού ψαρέματος.

Οι εργαζόμενοι γίνονται συχνότερα στόχος επιθέσεων, καθώς αποτελούν μια από τις σημαντικότερες ευπάθειες του κυβερνοχώρου και, ως εκ τούτου, πρέπει να είναι πλήρως ενημερωμένοι σχετικά με τον ρόλο τους στην εξασφάλιση ασφάλειας της εταιρείας. Τα τελευταία χρόνια στη κοινωνία της Πληροφορίας οι ειδικοί της ασφάλειας επικεντρώνονται περισσότερο στους ανθρώπους από ότι στην τεχνολογία. Όσο ακόμα παίζει και ο άνθρωπος σημαντικό ρόλο στην διεκπεραίωση των εργασιών ενός οργανισμού, για να δούμε κατά πόσο ασφαλής είναι ένας οργανισμός χρειάζεται να ελέγξουμε την κατάρτιση και την εκπαίδευση ασφαλείας όχι μόνο του προσωπικού πληροφορικής αλλά όλων όσων συμμετέχουν. Έτσι έχει αποδειχθεί υποχρεωτικό κριτήριο στα διεθνή πρότυπα διαχείρισης της Ασφάλειας πληροφοριών, η ευαισθητοποίηση και η εκπαίδευση σε θέματα ασφάλειας όλων των υπαλλήλων μιας επιχείρησης. Για αυτό το λόγο πολλές επιχειρήσεις προσπαθούν μέσω του e-learning, να επιμορφώσουν τους υπαλλήλους τους ώστε να ασφαλιστούν οι ίδιες. Ο αλληλεπιδραστικός κόσμος των βιντεοπαιχνιδιών είναι πολύ δημοφιλής τρόπος ευαισθητοποίησης των υπαλλήλων στο εξωτερικό και το ιδανικό μέσο εκπαίδευσης. Το παιχνίδι που δημιουργήθηκε σε αυτή την εργασία επικεντρώνεται στη ευαισθητοποίηση των υπαλλήλων μιας επιχείρησης σε βασικές έννοιες που δεν γνωρίζουν ή πρέπει να εμβραθύνουν για την ατομική ασφάλεια τους αλλά και για το σύνολο της επιχείρησης, στον κυβερνοχώρο. Κύριος σκοπός είναι η βελτίωση των τεχνικών δεξιοτήτων και η ενίσχυση της ευαισθητοποίησης σχετικά με την ασφάλεια, των εργαζομένων του οργανισμού / επιχείρησης για την ανάπτυξη και εφαρμογή ώριμης κουλτούρας απέναντι στους κινδύνους που ευδοκιμούν στον κυβερνοχώρο.

Το παιχνίδι που αναπτύχθηκε ονομάστηκε SAGE και είναι ένα point & click (εκεί που δείχνεις κάνεις κλικ) παιχνίδι που προσομοιώνει το γραφείο ενός υπαλλήλου και συγκεκριμένα την οθόνη του υπολογιστή του. Για την ανάπτυξη του χρησιμοποιήθηκε η παιχνιδομηχανή Godot 3. Αναδεικνύει σενάρια που συμβαίνουν στον πραγματικό κόσμο και σχεδιάστηκε για την επιμόρφωση των υπαλλήλων μιας εταιρείας, οργανισμού ή επιχείρησης. Οι παίκτες εμπλεκόμενοι σε αυτό το εικονικό περιβάλλον από τη μία πλευρά αναλαμβάνουν οι ίδιοι τον κυρίαρχο ρόλο στο παιχνίδι, αλλά βλέπουν και με πιο σφαιρική εικόνα και σχεδόν αμέσως, τις επιπτώσεις και το μέγεθος των συνεπειών πάνω στη εταιρεία, που φέρνουν οι δικές τους καθημερινές αποφάσεις και κινήσεις, αλλά και των άλλων, κυρίως για όταν βρίσκονται στο περιβάλλον της εργασίας τους. Με τη χρήση αυτού του παιχνιδιού ως μέρος ενός προγράμματος ευαισθητοποίησης σε θέματα ασφάλειας που υπάρχει ήδη ή ως μοναδικό εργαλείο, οι εταιρείες θα μπορέσουν να ευαισθητοποιούν πραγματικά τους υπαλλήλους τους στην ασφάλεια των πληροφοριών και όχι απλώς να μεταφέρουν γνώσεις.

Λέξεις κλειδιά: κυβερνοασφάλεια σε οργανισμούς, gamification, ευαισθητοποίηση σχετικά με την ασφάλεια, serious games, cyber security, σχεδιασμός παιχνιδιού, security awareness improvement, information security program, game-based learning.

Περιεχόμενα

Πίνακας εικόνων	9
1. Εισαγωγή	12
1.1 Σκοπός	12
1.2 Στόχοι	12
1.3 Συνεισφορά/ Συμβολή	12
1.4 Διάρθρωση	13
2. Βιβλιογραφική επισκόπηση (Κυβερνοασφάλεια και κυβερνοεπιθέσεις)	14
2.1 Η έννοια του κυβερνοχώρου και κυβερνοπόλεμος	14
2.2 Είδη επιθέσεων	15
2.2.1 Phishing	15
2.2.1.1 Σχετικές μελέτες	16
2.2.1.2 Αναγνώριση μηνυμάτων phishing	17
2.2.2 Κωδικός πρόσβασης	18
2.2.3 Έλεγχος πρόσβασης	19
2.2.4 Wi-fi hotspots	20
2.2.5 Social engineering	21
2.2.6 Ransomware	23
2.2.7 GDPR (General Data Protection Regulation)	24
2.3 Επιχειρήσεις και κυβερνοασφάλεια	26
3. Παιχνιδοποίηση της ευαισθητοποίησης στην κυβερνοασφάλεια	29
3.1 Σοβαρά Παιχνίδια	29
3.2 Εκπαίδευση/ Μάθηση	30
3.3 Αρχές σχεδιασμού βιντεοπαιχνιδιών	32
3.3.2 Στάδια παραγωγής ενός videogame	34
3.3.3 Κατηγορίες	35
3.4 Παιχνιδοποίηση και Ασφάλεια Υπολογιστών	36
3.4.1 Προσεγγίσεις/ Υλοποιήσεις Παιχνιδοποίησης	37
3.4.2 Παρατήρηση άλλων παιχνιδιών εκπαίδευσης υπαλλήλων σε θέματα ασφάλειας	38
4. Μεθοδολογία και Σενάρια Παιχνιδιού	40
4.1.1 Πρόβλημα	40
4.1.2 Λύση	40
4.2 Σενάρια	41
4.2.1 Σενάριο - Ηλεκτρονικό ψάρεμα	41
4.2.1.1 Εισερχόμενο email ηλεκτρονικού ψαρέματος	41
4.2.1.2 Διάκριση μηνυμάτων ηλεκτρονικού ψαρέματος	42
4.2.2 Σενάριο - Κωδικός πρόσβασης	43
4.2.2.1 Αφορμή επιλογής σεναρίου “Κωδικός πρόσβασης”	43
4.2.2.2 Σενάριο	43
4.2.3 Σενάριο - Δημόσιο WiFi	44
4.2.3.1 Αφορμή επιλογής σεναρίου “Δημόσιο WiFi”	44

4.2.3.2 Σενάριο	45
4.2.4 Σενάριο - Κοινωνική Μηχανική	45
4.2.4.1 Αφορμή επιλογής σεναρίου “Κοινωνική Μηχανική”	45
4.2.4.2 Σενάριο	46
4.2.5 Σενάριο - Ransomware μέσω USB	46
4.2.5.1 Αφορμή επιλογής σεναρίου “Ransomware μέσω USB”	46
4.2.5.2 Σενάριο	47
4.2.6 Σενάριο - Ιδιωτικότητα και GDPR	47
4.2.6.1 Αφορμή επιλογής σεναρίου “Ιδιωτικότητα και GDPR”	47
4.2.6.2 Σενάριο	48
5. Security Awareness Game for Employees (SAGE)	49
5.1.1 Αρχικές Σκέψεις	49
5.1.2 Τελικός Σχεδιασμός	51
6. Στάδια Υλοποίησης Παιχνιδιού	54
6.1.1 Έρευνα υπαρχουσών παιχνιδομηχανών	54
6.1.2 Έρευνα υπαρχουσών εργαλείων σχεδιασμού	55
6.2. Υλοποίηση	57
6.2.1. Δημιουργία νέου έργου με την Godot	57
6.2.2 Ρυθμίσεις	59
6.2.3 Input Map	60
6.2.4 Σκηνές	60
6.2.5 Σχεδιασμός Πρώτου Σεναρίου	63
6.2.5.1 Αρχική οθόνη (Title Screen)	63
6.2.5.2 Σκηνή Email.tscn	68
6.2.5.3. Σκηνή «EmailPlatform.tscn»	72
6.2.5.4 Σκηνή «PhishingEmail.tscn»	73
6.2.5.5 Σκηνή «MalwareSite.tscn»	74
6.2.5.6 Σκηνή «Ignored.tscn»	75
6.2.5.7 Σκηνή «Think.tscn»	76
6.2.5.8 Σκηνή «Phished.tscn»	77
6.2.5.9 Σκηνή «PhishingEnd.tscn»	78
6.2.5.10 autoloads	79
6.2.5.10. Σκηνή «Options.tscn»	82
6.2.6 Πλατφόρμες έκδοσης	83
6.2.7 η Διεπαφή του Παιχνιδιού	84
6.2.8 Πρωτότυπο	89
6.2.8.1 Εισαγωγική οθόνη	89
6.2.8.2 Επιλογές του παιχνιδιού	90
6.2.8.3 Η πρόοδος στο Παιχνίδι	91
7. Αξιολόγηση	94
7.1 Ποσοτική έρευνα	94
7.2 Δημογραφικά στοιχεία των συμμετεχόντων	94
7.3 Αποτελέσματα της έρευνας	94

8. Συμπεράσματα-μελλοντικές προεκτάσεις	97
8.1 Συμπεράσματα	97
8.2 Μελλοντικές προεκτάσεις	97
9. Βιβλιογραφία	99
Παράρτημα (ερωτηματολόγιο αξιολόγησης)	104
Ερωτήσεις	104
Απαντήσεις	108

Πίνακας εικόνων

Εικόνα 1. Οντολογικό μοντέλο επίθεσης κοινωνικής μηχανικής (Mouton, 2016).....σελ. 18	σελ. 18
Εικόνα 2. Συσκευές που μπορούν να επηρεαστούν από ransomware (Hassan, 2019).σελ. 19	σελ. 19
Εικόνα 3. «Το ταξίδι του Έρωτα» και οι τρεις πράξεις μιας ιστορίας σελ.31	σελ. 31
Εικόνα 4. Πρώτη ενδεικτική σκηνή του παιχνιδιού (σχέδιο στο χαρτί) σελ. 46	σελ. 46
Εικόνα 5. Χαρακτήρας σε αλληλεπίδραση με το γραφείο του.....σελ. 47	σελ. 47
Εικόνα 6. Ο εικονικός υπολογιστής (σχέδιο στο χαρτί) σελ. 47	σελ. 47
Εικόνα 7. Οθόνες ηλεκτρονικού ταχυδρομείου (σχέδιο στο χαρτί) σελ. 48	σελ. 48
Εικόνα 8. Χάρτης παιχνιδιού (σχέδιο στο χαρτί) σελ. 49	σελ. 49
Εικόνα 9. Σκηνή παύσης με τις διαθέσιμες επιλογές (σχέδιο στο χαρτί) σελ. 49	σελ. 49
Εικόνα 10. Διάγραμμα ροής παιχνιδιού, σε στάδιο μελέτης (σχέδιο στο χαρτί) σελ. 50	σελ. 50
Εικόνα 11. Διαφορά μεταξύ raster και vector γραφικών σελ. 53	σελ. 53
Εικόνα 12. Νέο έργο (New Project) στη Godot σελ. 55	σελ. 55
Εικόνα 13. Δημιουργία νέου φακέλου (Create Folder) σελ. 55	σελ. 55
Εικόνα 14. Περιβάλλον Godot 3 σελ. 56	σελ. 56
Εικόνα 15. Γενικές ρυθμίσεις οθόνης (Display) σελ. 56	σελ. 56
Εικόνα 16. Stretch options σελ. 60	σελ. 60
Εικόνα 17. Input Map, προσθήκη της παύσης σελ. 60	σελ. 60
Εικόνα 18. Περιβάλλον σκηνών σελ. 61	σελ. 61
Εικόνα 19. Σήματα (signals) κουμπιού «Exit» σελ. 62	σελ. 62
Εικόνα 20. Συνάρτηση εκκίνησης διαδικασιών με το πάτημα του κουμπιού σελ. 62	σελ. 62
Εικόνα 21. Καθορισμός κύριας σκηνής (main scene) σελ. 63	σελ. 63
Εικόνα 22. <i>TitleScreen.tscn</i> σελ. 63	σελ. 63
Εικόνα 23. κόμβος Control→ <i>TitleScreen.tscn</i> σελ. 64	σελ. 64
Εικόνα 24. κόμβος Background→ <i>TitleScreen.tscn</i> σελ. 65	σελ. 65
Εικόνα 25. Containers (<i>TitleScreen.tscn</i>) σελ. 65	σελ. 65
Εικόνα 26. <i>GameButton.tscn</i> σελ. 66	σελ. 66
Εικόνα 27. <i>TitleScreen.gd</i> σελ. 67	σελ. 67
Εικόνα 28. <i>ExitButton</i> σελ. 67	σελ. 67
Εικόνα 29. <i>MenuButton.gd</i> σελ. 67	σελ. 67
Εικόνα 30. <i>NewGameButton</i> (Inspector load script) σελ.68	σελ. 68
Εικόνα 31. <i>NewGameButton</i> (Inspector Script Variables) σελ.68	σελ. 68
Εικόνα 32. <i>Email.tscn</i> σελ.69	σελ. 69
Εικόνα 33. <i>AnimationPlayer</i> (<i>Email.tscn</i>) σελ.69	σελ. 69
Εικόνα 34. <i>Property Track</i> (<i>AnimationPlayer</i>) σελ.69	σελ. 69

Εικόνα 35. Animated node (AnimationPlayer)	σελ. 70
Εικόνα 36. rect_scale (AnimationPlayer)	σελ. 70
Εικόνα 37. popup (AnimationPlayer)	σελ. 70
Εικόνα 38. popup timetable (AnimationPlayer)	σελ. 71
Εικόνα 39. popup pivot_offset (AnimationPlayer)	σελ. 71
Εικόνα 40. <i>Email.gd</i>	σελ. 71
Εικόνα 41. <i>EmailPlatform.tscn</i>	σελ. 72
Εικόνα 42. Choice1open button (<i>EmailPlatform</i>)	σελ. 72
Εικόνα 43. NewOne button (<i>EmailPlatform</i>)	σελ. 73
Εικόνα 44. <i>EmailPlatform.gd</i>	σελ. 73
Εικόνα 45. <i>PhishingEmail.tscn</i>	σελ. 74
Εικόνα 46. <i>PhishingEmail.gd</i>	σελ. 74
Εικόνα 47. <i>MalwareSite.tscn</i>	σελ. 74
Εικόνα 48. <i>MalwareSite.gd</i>	σελ. 75
Εικόνα 49. Buttons (<i>MalwareSite</i>)	σελ. 75
Εικόνα 50. <i>Ignored.tscn</i>	σελ. 75
Εικόνα 51. <i>Ignored.gd</i>	σελ. 76
Εικόνα 52. <i>Think.tscn</i>	σελ. 76
Εικόνα 53. <i>Think.gd</i>	σελ. 76
Εικόνα 54. <i>Phished.tscn</i>	σελ. 77
Εικόνα 55. <i>Phished.gd</i>	σελ. 77
Εικόνα 56. <i>Home.tscn</i> και <i>Home.gd</i>	σελ. 78
Εικόνα 57. <i>Deleted.tscn</i> και <i>Deleted.gd</i>	σελ. 78
Εικόνα 58. <i>ReportedDeleted.tscn</i> και <i>ReportedDeleted.gd</i>	σελ. 78
Εικόνα 59. <i>PhishingEnd.tscn</i>	σελ. 79
Εικόνα 60. <i>PhishingEnd.gd</i>	σελ. 79
Εικόνα 61. <i>MusicController.gd</i>	σελ. 80
Εικόνα 62. <i>Autoload settings</i>	σελ. 80
Εικόνα 63. <i>Remote panel</i>	σελ. 81
Εικόνα 64. <i>Pause.gd</i>	σελ. 81
Εικόνα 65. <i>Pause.tscn</i>	σελ. 82
Εικόνα 66. <i>Options.tscn</i>	σελ. 83
Εικόνα 67. <i>Options.gd</i>	σελ. 83
Εικόνα 68. Γενικές ρυθμίσεις για εξαγωγή σε πλατφόρμα android	σελ. 84
Εικόνα 69. Περιβάλλον του Inkscape	σελ. 85
Εικόνα 70. Νέο έργο στο Inkscape	σελ. 85
Εικόνα 71. Ιδιότητες εγγράφου (Inkscape)	σελ. 86

Εικόνα 72. Εικονογραφήσεις συγχρονισμού χειλιών (Inkscape)	σελ. 86
Εικόνα 73. Χαρακτήρας - γραφείο (Inkscape)	σελ. 87
Εικόνα 74. Λειτουργίες διαδρομής και λογότυπο (Inkscape)	σελ. 87
Εικόνα 75. επιλογέας χρωμάτων (color picker, Inkscape)	σελ. 88
Εικόνα 76. Σχέδια παιχνιδιού (α) (Inkscape)	σελ. 88
Εικόνα 77. Σχέδια παιχνιδιού (β) (Inkscape)	σελ. 89
Εικόνα 78. Διάγραμμα σκηνών	σελ. 89
Εικόνα 79. Πρώτη οθόνη διεπαφής χρήστη - SAGE	σελ. 90
Εικόνα 80. Οθόνη παύσης παιχνιδιού	σελ. 90
Εικόνα 81. Οθόνη Ρυθμίσεων	σελ. 91
Εικόνα 82. Πρώτη οθόνη σεναρίου Phishing	σελ. 91
Εικόνα 83. Δεύτερη οθόνη σεναρίου Phishing (μόνο “αφήγηση”)	σελ. 92
Εικόνα 84. Δεύτερη οθόνη σεναρίου Phishing (ολοκληρωμένη)	σελ. 92
Εικόνα 85. Οθόνη επιλογής “1.Άνοιγμα και διάβασμα” (Phishing).....	σελ. 93
Εικόνα 86. Ερώτηση 8	σελ. 95
Εικόνα 87. Ερώτηση 9	σελ. 95
Εικόνα 88. Ερώτηση 10	σελ. 95
Εικόνα 89. Ερώτηση 20	σελ. 96

1. Εισαγωγή

1.1 Σκοπός

Στην εποχή μας διαπράττονται διαρκώς κυβερνοεγκλήματα που πλήττουν εκτός των άλλων και τις επιχειρήσεις. Για αυτό τον λόγο, είναι απαραίτητο οι επιχειρήσεις να έχουν γερά θεμέλια στις αρχές της ασφάλειας και να λαμβάνουν τα κατάλληλα μέτρα προστασίας ενάντια σε αυτές τις απειλές. Πέρα από τα λογισμικά και τα συστήματα ασφαλείας τα οποία υπάρχουν και οι επιχειρήσεις επιλέγουν για την προστασία τους, θα πρέπει να δίνουν ιδιαίτερη σημασία και στην θωράκιση του ανθρώπινου δυναμικού τους. Ένα πρόγραμμα εκπαίδευσης και ευαισθητοποίησης για την ασφάλεια γίνεται η πιο σημαντική γραμμή άμυνας για τη διασφάλιση των δεδομένων ενός οργανισμού από εσωτερικές και εξωτερικές επιθέσεις (Hassan, 2019).

1.2 Στόχοι

Η ευαισθητοποίηση των υπαλλήλων δεν γίνεται να περιορίζεται μόνο σε ενημερωτικά φυλλάδια και παρουσιάσεις, καθώς όπως φαίνεται από έρευνες, δεν επιφέρουν το επιθυμητό αποτέλεσμα, αφού δεν δίνουν κίνητρο στους υπαλλήλους να εμπλακούν και να συνειδητοποιήσουν την σοβαρότητα των απειλών. Χρειάζεται να ληφθούν πιο δραστικά μέτρα από τις επιχειρήσεις. Παράλληλα, έρευνες δείχνουν πως η εκπαίδευση μέσω παιχνιδιών έχει θετικά αποτελέσματα σε διάφορους τομείς εκτός των άλλων και στον χώρο της ασφάλειας. Τα σοβαρά παιχνίδια παρέχουν ένα εικονικό περιβάλλον με καλά ορισμένους κανόνες, αλληλεπίδραση και άμεση ανάδραση των επιπτώσεων των πράξεων του παίκτη (Αναγνώστου, 2009), ιδανικά στοιχεία για την εκπαίδευση και ευαισθητοποίηση υπαλλήλων σε θέματα ασφάλειας.

1.3 Συνεισφορά/ Συμβολή

Με αυτό υπόψη, σχεδιάστηκε και αναπτύχθηκε ένα παιχνίδι, το «SAGE» το οποίο μπορεί να υποστηριχθεί μέσω web browser (περιηγητή) αλλά και από κινητή συσκευή . Είναι ένα σοβαρό και εκπαιδευτικό παιχνίδι που μπορεί να δοθεί σε υπαλλήλους επιχειρήσεων και μέσα από την βιωματική μάθηση να ευαισθητοποιηθούν για κάποιες πολύ σημαντικές τακτικές ασφάλειας στο περιβάλλον εργασίας τους. Έχει ως στόχο την γνωριμία των εργαζομένων με κάποιες πολύ βασικές έννοιες, όπου ο εργαζόμενος έρχεται αντιμέτωπος πολλές φορές στην προσωπική του ζωή αλλά και ιδιαίτερα στο περιβάλλον εργασίας του. Η κεντρική ιδέα του παιχνιδιού είναι η ύπαρξη διαφορετικών σεναρίων για κάθε έννοια και γεγονός που θέλουμε να θίξουμε τα οποία βοηθούν τον παίκτη να βιώσει εικονικά κάποιες καταστάσεις. Κάποια από τα σενάρια είναι πολύ κοινά και είναι πιθανόν να τα έχει συναντήσει στην πραγματική του ζωή, ίσως όμως, πριν έρθει σε επαφή με το παιχνίδι δεν είχε αντιληφθεί τη βαρύτητα των αποφάσεων που λαμβάνει και το αντίκτυπο τους στην επιχείρηση που εργάζεται. Αυτός είναι ο βασικός ρόλος του παιχνιδιού, πέρα από την εκπαίδευσή του σε θέματα ασφάλειας, να δείξει στον παίκτη σε άμεσο χρόνο, μέσα σε λίγα λεπτά, τα αποτελέσματα των αποφάσεων του. Συνεπώς, εάν ο παίκτης κάνει γρήγορες και επιπόλαιες κινήσεις, θα δημιουργήσει το κατάλληλο περιβάλλον, δίνοντας την ευκαιρία σε

ένα κακόβουλο χρήστη να ενεργήσει, εκμεταλλευόμενος κάποιο κενό ή αδυναμία που δημιουργήθηκε και τελικά να ζημιώσει τον ίδιο και την επιχείρηση.

1.4 Διάρθρωση

Η δομή της εργασίας είναι η ακόλουθη. Το κεφάλαιο δύο αναφέρεται στη κυβερνοασφάλεια, στα συνηθέστερα είδη επιθέσεων και στην ασφάλεια των επιχειρήσεων. Το 3ο κεφάλαιο πραγματεύεται τα σοβαρά παιχνίδια και τα δωμάτια διαφυγής, το ρόλο τους στην εκπαίδευση και την ευαισθητοποίηση σε θέματα ασφάλειας μέσω παιχνιδιών. Στο τέταρτο κεφάλαιο είναι η μεθοδολογία της εργασίας με τα σενάρια που έχουν σχεδιαστεί για το παιχνίδι και στο πέμπτο κεφάλαιο αναλύεται ο σχεδιασμός του παιχνιδιού. Το έκτο κεφάλαιο πραγματεύεται τον τρόπο υλοποίησης και παρουσιάζει το τελικό παιχνίδι. Τέλος, στο Κεφάλαιο έξι είναι τα συμπεράσματα και οι μελλοντικές βελτιώσεις και στο οκτώ η βιβλιογραφία που χρησιμοποιήθηκε για την υλοποίηση αυτής της εργασίας.

2. Βιβλιογραφική επισκόπηση (Κυβερνοασφάλεια και κυβερνοεπιθέσεις)

2.1 Η έννοια του κυβερνοχώρου και κυβερνοπόλεμος

Θα μπορούσαμε να ορίσουμε τον κυβερνοχώρο ως ένα συνθετικό κόσμο που απαρτίζεται από την παράθεση δεδομένων σε έναν πολυδιάστατο χώρο, τον οποίο χρήστες μπορούν να χειριστούν, να πλοηγηθούν, να εξερευνήσουν και, κυρίως, να επικοινωνήσουν μεταξύ τους με τη βοήθεια της πληροφορικής (του διαδικτύου και των ηλεκτρονικών υπολογιστών) (Μπασδαράς, 2017). Κατά την περιήγηση στον ιστό, υπάρχουν πολλοί τρόποι με τους οποίους οι χρήστες ενδέχεται να θέσουν τον εαυτό τους σε κίνδυνο. Αυτές μπορεί να περιλαμβάνουν αλληλεπίδραση με ιστότοπους που είναι ανεπαρκώς κωδικοποιημένοι, δημιουργία αδύναμων κωδικών πρόσβασης και λήψη δεδομένων από ιστότοπους που περιέχουν κακόβουλα αρχεία (Γιουφτσιάδης, 2020; Scholofield, 2019).

Οι εγκληματικές ενέργειες που διαπράττονται στον κυβερνοχώρο ονομάζεται κι αλλιώς κυβερνοπόλεμος και αποτελεί ένα όπλο με μικρό κόστος, πού βασίζεται στην εφευρετικότητα και τη γνώση των τρωτών σημείων των συστημάτων, και έχει πανίσχυρα αποτελέσματα. Αποτελεί μία ιδιαίτερα σημαντική ασύμμετρη απειλή για την εθνική ασφάλεια και την ευημερία των κρατών, και φυσικά απειλεί και την επιτυχία των επιχειρήσεων. Ένας σύντομος ορισμός είναι ότι «ο κυβερνοπόλεμος είναι κάθε ενέργεια που λαμβάνει χώρα στον κυβερνοχώρο και έχει στόχο την βλάβη, τον αποκλεισμό και τη μείωση της ισχύος μιας χώρας ή ενός μη κρατικού δρώντα (προσώπου, εταιρείας, οργανισμού)». Ο σκοπός των κυβερνοεπιθέσεων είναι πάντοτε συγκεκριμένος και μπορεί να αφορά την εκμετάλλευση (exploitation), παραπλάνηση (deception), καταστροφή (destruction) ή διακοπή λειτουργίας (denial of service) (Μπασδαράς, 2017).

Τα κυριότερα μέσα που χρησιμοποιούνται για την επίτευξη του στόχου σε μια κυβερνοεπίθεση, είναι το κακόβουλο λογισμικό (malware) που συνίσταται σε ιούς, σκουλήκια, δούρειος ίππους και κατασκοπευτικό λογισμικό και τα δίκτυα ρομπότ (botnet) τα οποία είναι μηχανήματα-προσωπικοί υπολογιστές που έχουν εσκεμμένα μολυνθεί με κακόβουλο λογισμικό, εν αγνοία των ιδιοκτητών και οργανώνονται σε δίκτυο ρομπότ από τους hackers, που τα κατευθύνουν ώστε να μολύνουν και άλλους χρήστες ανοίγοντας μία κερκόπορτα μέσω της οποίας δίνονται να δίνουν εντολές επίθεσης, άρνησης εξυπηρέτησης (DDos - denial of service attacks). Ολοένα και πιο δημοφιλής τακτική κυβερνοεπίθεσης αποτελεί το ηλεκτρονικό ψάρεμα (phishing), μέσω της δημιουργίας πλαστών τοποθεσιών ιστού ή της αποστολής μηνυμάτων ηλεκτρονικού ταχυδρομείου, που παρουσιάζονται ως μηνύματα γνωστών νόμιμων εταιρειών ή οργανισμών, εξαπατώντας τους χρήστες για να τους δώσουν εμπιστευτικά απόρρητα δεδομένα τους, προσωπικά στοιχεία και κωδικούς πρόσβασης (Μπασδαράς, 2017).

Ο όρος "ηλεκτρονική απάτη" αναφέρεται σε «κάθε τύπο συστήματος απάτης που χρησιμοποιεί μηνύματα ηλεκτρονικού ταχυδρομείου, ιστότοπους, χώρους συνομιλίας ή πίνακες μηνυμάτων για την υποβολή απατηλών προσκλήσεων σε υποψήφια θύματα, τη διεξαγωγή δόλιας συναλλαγής ή τη μετάδοση προϊόντων απάτης σε χρηματοπιστωτικά ιδρύματα ή σε τρίτους που συνδέονται με το σύστημα». Οι απάτες στο Διαδίκτυο ενδέχεται να περιλαμβάνουν ανεπιθύμητα μηνύματα, απάτες, λογισμικό υποκλοπής spyware, κλοπή

ταυτότητας και απάτη ηλεκτρονικού "ψαρέματος" (phishing) (Alanezi, 2015). Η ηλεκτρονική απάτη έχει τα γενικά κοινά παραπλανητικά χαρακτηριστικά ενός εγκλήματος που διαπράττεται στον κυβερνοχώρο σε μια επιχειρηματική σχέση για προσωπικά κέρδη. Σκοπός της είναι η εξαπάτηση μέσω ψευδών πληροφοριών, ισχυρισμού ή καταστολής της αλήθειας (Brenner, 2012). Γενικά, μπορούμε να περιγράψουμε την ηλεκτρονική απάτη ως τη χρήση διαδικτυακών εγκαταστάσεων για την πραγματοποίηση αμφίβολων επιχειρηματικών συναλλαγών με σκοπό την εξαπάτηση προσώπων, οργανισμών, ακόμα και κυβερνήσεων (Γιουφτσιάδης, 2020).

2.2 Είδη επιθέσεων

Σε αυτό το κεφάλαιο περιγράφονται κάποιες από τις πιο συχνές απειλές στον κυβερνοχώρο που στοχεύουν τις επιχειρήσεις και στις οποίες έχουν βασιστεί τα σενάρια που έχουν δημιουργηθεί. Τα σενάρια έχουν να κάνουν με το ηλεκτρονικό ψάρεμα (phishing), τον κωδικό πρόσβασης (password), τον έλεγχο πρόσβασης, τα δημόσια σημεία πρόσβασης στο διαδίκτυο (wifi), την κοινωνική μηχανική (social engineering), το ransomware (κακόβουλο λογισμικό εκβιασμού) μέσω usb και τον GDPR και αναλύονται στο κεφάλαιο τέσσερα.

2.2.1 Phishing

Η πρώτη κατηγορία απειλών είναι απειλές που σχετίζονται με τη χρήση κοινωνικοτεχνικών μεθόδων και τεχνικών όπως το phishing (ηλεκτρονικό ψάρεμα), οι οποίες προκαλούν ότι οι ίδιοι οι χρήστες, αγνοώντας τις ενέργειές τους, αποτελούν απειλή για τον οργανισμό (Podgórski, 2020).

Το ηλεκτρονικό "ψάρεμα" (Phishing) είναι «ένας ειδικός τύπος ανεπιθύμητης αλληλογραφίας (spam) που αποσκοπεί στην εξαπάτηση του χρήστη με στόχο να εξάγει προσωπικές του πληροφορίες ή τις πληροφορίες λογαριασμού του, με σκοπό την παραβίαση του λογαριασμού του και τη διάπραξη κλοπής ταυτότητας ή απάτης» (Γιουφτσιάδης, 2020).

Συνήθως, παραδίδεται μέσα από ένα ψευδές μήνυμα ηλεκτρονικού ταχυδρομείου και το e-mail φαίνεται να προέρχεται από μια νόμιμη πηγή, για παράδειγμα το PayPal, την τράπεζα του χρήστη, κρατικά τμήματα κλπ (Γιουφτσιάδης, 2020). Συχνά, μέσα στο κείμενο παρατίθεται και ένας σύνδεσμος προς πλάστη ιστοσελίδα, η οποία πλασάρεται ως η επίσημη ιστοσελίδα του αποστολέα. Πηγαίνοντας στην ιστοσελίδα αυτή, το θύμα καλείται να συμπληρώσει τα στοιχεία του, με την παραπλανητική αφορμή, για παράδειγμα, να μην απενεργοποιηθεί ο λογαριασμός του. Την ίδια ώρα οι κακόβουλοι χρήστες που κρύβονται πίσω από το ψεύτικο μήνυμα αποκτούν πρόσβαση στα στοιχεία αυτά και στη συνέχεια μπορούν να κάνουν ηλεκτρονικές απάτες εις βάρος του πραγματικού ιδιοκτήτη αυτών των στοιχείων (Κουτσοδόντης, 2016). Εναλλακτικά, ένας εισβολέας μπορεί να συνοδεύσει ένα μήνυμα με κακόβουλο συνημμένο για να εκμεταλλευτεί ένα ευάλωτο σύστημα χρήστη, με το κείμενο στο σώμα του μηνύματος να χρησιμοποιείται στη συνέχεια για να ενθαρρύνει τον χρήστη να ανοίξει το συνημμένο. Αυτή είναι μια ευρέως χρησιμοποιούμενη τεχνική στη διάδοση κακόβουλου λογισμικού όπως τα worms και οι Δούρειοι Ίπποι (Trojan horses) (Karakasiliotis, 2006).

Υπάρχουν δύο συνήθεις τύποι ηλεκτρονικού "ψαρέματος" (phishing), το ίδιο το "phishing" και η πλαστογράφηση (spoofing) (McQuade, 2009). Η διαφορά μεταξύ phishing και spoofing είναι ότι το τελευταίο χρησιμοποιεί ψεύτικες εκδόσεις νόμιμων ιστοτόπων, ενώ η απάτη μέσω phishing πραγματοποιείται μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου. Το

ηλεκτρονικό ψάρεμα (phishing) και πλαστογράφηση (spoofing) είναι δύο διαφορετικές τεχνικές ηλεκτρονικής απάτης. Στην μία περίπτωση κάποιος κατεβάζει κακόβουλο λογισμικό στον υπολογιστή ή το προσωπικό δίκτυο του χρήστη ενώ στο spoofing γίνεται παραβίαση ευαίσθητων οικονομικών στοιχείων μέσω διαδικτύου. Ουσιαστικά το phishing είναι μια μέθοδος ανάκτησης στοιχείων, ενώ η πλαστογράφηση (spoofing) είναι ένας τρόπος παράδοσης στοιχείων (Alanezi, 2015) (Γιουφτσιάδης, 2020).

Σε επιθέσεις ηλεκτρονικού ψαρέματος, εφαρμόζονται επιδραστικές μέθοδοι για την εκπλήρωση αιτημάτων από τον επιτιθέμενο προς το θύμα ή τα θύματα. Αυτές, μπορούν να εφαρμοστούν μέσω της τεχνικής της σημασιολογικής εξαπάτησης (Fette et al. 2006), η οποία επιτυγχάνεται μέσω της γλώσσας που χρησιμοποιείται στο σώμα κειμένου ενός μηνύματος ηλεκτρονικού ταχυδρομείου (Karakasiliotis, 2006). Η οπτική εξαπάτηση στις επιθέσεις ηλεκτρονικού ψαρέματος μπορεί να επιτευχθεί μέσω πολλών κόλπων για να φαίνεται το μήνυμα ηλεκτρονικού ταχυδρομείου νόμιμο, όπως η απόκρυψη μιας δόλιας διεύθυνσης URL, η αντιγραφή και η χρήση του λογότυπου και η κλοπή κώδικα HTML από έναν γνήσιο ιστότοπο προκειμένου να δημιουργηθεί ένας ψεύτικος παριστάνοντας τον. Περαιτέρω τεχνικές που μπορούν να χρησιμοποιηθούν για να κερδίσουν την εμπιστοσύνη του χρήστη περιλαμβάνουν την πλαστογραφία της διεύθυνσης ηλεκτρονικού ταχυδρομείου του αποστολέα και την παρουσίαση διευθύνσεων URL που περιέχουν «https» στο μήνυμα για να προτείνουν έναν ασφαλή σύνδεσμο. Ο ψεύτικος ιστότοπος μπορεί να περιέχει εύλογους δείκτες ασφαλείας, για να μπερδέψει το θύμα, όπως το εικονίδιο λουκέτου για να υποδηλώσει μια ασφαλή συνεδρία και κατάχρηση εικόνων σφραγίδων ασφαλείας (όπως τα λογότυπα VeriSign και TRUSTe) (Karakasiliotis, 2006). Εάν είναι επιτυχής, το ηλεκτρονικό ψάρεμα επιτρέπει στους εγκληματίες στον κυβερνοχώρο να έχουν ελεύθερη πρόσβαση είτε σε δεδομένα πελατών (μειώνεται η εμπιστοσύνη προς την επιχείρηση) είτε εσωτερική υποδομή και ευαίσθητα έγγραφα μιας επιχείρησης. Τα κύρια περιουσιακά στοιχεία της επιχείρησης που πλήττονται είναι: ηλεκτρονικοί υπολογιστές, κινητά τηλέφωνα και γενικά όποια συσκευή μπορεί να λάβει και να ανοίξει τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου (Κουτρώσιος, 2019).

Μία ακόμη πιο απειλητική μορφή επίθεσης, παρόμοια με το phishing αλλά πιο επικίνδυνη, είναι το λεγόμενο Pharming. Ένα ειδικό πρόγραμμα εκμεταλλεύεται κενά ασφαλείας του συστήματος, διεισδύει στον υπολογιστή του θύματος και το επηρεάζει, με τρόπο όπου, ακόμα κι αν ο χρήστης πληκτρολογεί τη σωστή διεύθυνση του διαδικτυακού τόπου που θέλει να επισκεφτεί, θεωρώντας πως βρίσκεται σε ασφαλή χώρο, ο συγκεκριμένος υπολογιστής να τον κατευθύνει μόνο σε πλαστές ιστοσελίδες. Ειδικότερα, αν πρόκειται για ιστοσελίδα τράπεζας, η προσπάθεια του θύματος να πραγματοποιήσει τις συναλλαγές του μέσω on-line banking θα καταλήξει στο να έχει μεταφέρει το χρηματικό ποσό στους δράστες (pharmers) (Καραδούκας, 2019). Το Vishing και το smishing είναι οι παραλλαγές τηλεφώνου και μηνυμάτων SMS του phishing. Οποιαδήποτε από τις επιλογές μπορεί να παρέχει στον απατεώνα πρόσβαση στις ευαίσθητες πληροφορίες των πελατών ή της επιχείρησής (Erps, 2017).

2.2.1.1 Σχετικές μελέτες

Έρευνες δείχνουν πως όσο περνάει ο καιρός τόσο αυξάνονται τα ποσοστά ηλεκτρονικού ψαρέματος (phishing). Το 2019, το μερίδιο του οικονομικού ηλεκτρονικού ψαρέματος (phishing) αυξήθηκε από 44,7% το 2018, σε 51,4% (Γιουφτσιάδης, 2020) και έρευνα του Κουτρώσιος (2019), έδειξε πως το 80,6% των μικρομεσαίων επιχειρήσεων στην

Κύπρο έλαβε μήνυμα ηλεκτρονικού ταχυδρομείου spam/ phishing. Επίσης, υπάρχουν αρκετές μελέτες περίπτωσης για τέτοιους είδους επιθέσεις, που έχουν καταγραφεί και οι “ζημιές” που έχουν υποστεί επιχειρήσεις. Παράδειγμα είναι η επίθεση στη Γερμανική χαλυβουργία το 2014 όπου εισβολέας χρησιμοποίησε ένα e-mail phishing για να αποκτήσει πρόσβαση στο εταιρικό δίκτυο, με αποτέλεσμα να εγκατασταθεί σε αυτό (Κουτσοδόντης, 2016). Ταυτόχρονα σύμφωνα με στατιστικά στοιχεία CERT (πολωνικό τμήμα) περισσότερο από το 44% όλων των περιστατικών που χειρίστηκε ο οργανισμός το 2018 αφορούσαν ηλεκτρονικό ψάρεμα και η έκθεση ISTR 2019 της Symantec αναφέρει ότι οι οργανισμοί δημόσιας διοίκησης λαμβάνουν ένα κακόβουλο e-mail ανά 302 e-mail (Podgórski, 2020).

Διεξάγονται και έρευνες που μας δίνουν πληροφορίες σχετικά με την ευαισθητοποίηση πολιτών και εργαζομένων. Μέσα από έρευνα (Karakasiliotis, 2006), η οποία περιελάμβανε 20 ερωτήσεις, όπου η κάθε μία παρουσίαζε στον συμμετέχοντα ένα μήνυμα ηλεκτρονικού ταχυδρομείου και ζητούσε από αυτόν να κρίνει τη νομιμότητά του. Το συνολικό επίπεδο σωστής ταξινόμησης (δηλ. Ένδειξη «νόμιμο» για γνήσια μηνύματα και «παράνομο» για ψεύτικα) ήταν 42%, ενώ η εσφαλμένη ταξινόμηση ήταν 32%. Αυτό, μαζί με το επιπλέον 26% των απαντήσεων «δεν γνωρίζω», απεικονίζει σαφώς το επίπεδο σύγχυσης μεταξύ των συμμετεχόντων. Η έρευνα των Ali et al., (2017) ανέλυσε τη συμπεριφορά περισσότερων από 100 χρηστών διαδικτυακών τραπεζών και υπολόγισε τις επιπτώσεις των απειλών του κυβερνοχώρου σε αυτούς τους χρήστες. Το 6% γνωρίζει το ηλεκτρονικό ψάρεμα (phishing), ενώ το υπόλοιπο 6% επιβεβαίωσε ότι έλαβε γνώση σχετικά με το ηλεκτρονικό ψάρεμα μέσω τηλεφωνικής κλήσης (phishing over VOIP, vishing) (Γιουφτσιάδης, 2020).

Από την άλλη πλευρά, σε μελέτη, που το αντικείμενο ήταν μια μονάδα πανεπιστημίου που απασχολεί πάνω από 340 άτομα, δεν ανέφερε ευρύτερες προσπάθειες χρήσης της μεθόδου, ηλεκτρονικό "ψάρεμα". Χάρη στην καλή ευαισθητοποίηση των χρηστών και την ευρεία εκστρατεία σχετικά με αυτό το ζήτημα, η μονάδα δεν υπέστη επικίνδυνα αποτελέσματα. Θα πρέπει επίσης να σημειωθεί ότι η υψηλή ευαισθητοποίηση των χρηστών είχε συχνά ως αποτέλεσμα την αναφορά τέτοιων περιστατικών στις σχετικές υπηρεσίες και μια γρήγορη απάντηση με τη μορφή κατάλληλων μηνυμάτων σε όλους τους υπαλλήλους που αποστέλλονται από το τμήμα πληροφορικής (Podgórski, 2020).

Μέσα από αυτές τις ενδεικτικές έρευνες, μπορούμε να διακρίνουμε το μέγεθος της απειλής, της αμάθειας των πολιτών και των εργαζομένων, καθώς και την σημασία της ευαισθητοποίησης πάνω σε αυτή την απειλή όπως είδαμε από την έρευνα του (Podgórski, 2020) όπου εστιάζει και η εργασία αυτή.

2.2.1.2 Αναγνώριση μηνυμάτων phishing

Η διάκριση μηνυμάτων ηλεκτρονικού ψαρέματος από την πραγματική αλληλογραφία, σταδιακά γίνεται όλο και πιο δύσκολο για όσους στοχοποιούνται. Αυτό μπορεί να σχετίζεται άμεσα με την πρόοδο στην κοινωνική μηχανική και τις μεθόδους εξαπάτησης που χρησιμοποιούνται από τους επιτιθέμενους (Karakasiliotis, 2006). Ωστόσο υπάρχουν κάποια σημεία άξια, ιδιαίτερης προσοχής τα οποία πολλές φορές σηματοδοτούν πως ένα μήνυμα δεν είναι αληθινό. Σημεία στα οποία έδωσαν προσοχή ερωτηθέντες στην έρευνα του Karakasiliotis (2006) ώστε να κάνουν την κατάταξη, ήταν οι οπτικοί παράγοντες όπως λογότυπα, πανό (banner), εμπορικά σήματα, υποσέλιδο, γραμματοσειρές και σύμβολα πνευματικών δικαιωμάτων, τα τεχνικά στοιχεία όπως η ύπαρξη του «http» ή «https» στην

αρχή του URL, και η γλώσσα και τα χαρακτηριστικά που σχετίζονται με το περιεχόμενό της όπως γλωσσικά λάθη, απεύθυνση σε προσωπικό επίπεδο (π.χ. η παρουσία (ή η απουσία) του όνομα παραλήπτη στο μήνυμα ηλεκτρονικού ταχυδρομείου ή άλλες προσωπικές πληροφορίες) (Karakasiliotis, 2006). Υπάρχουν βέβαια και αρκετά προγράμματα περιήγησης τα οποία αναγνωρίζουν τους ιστοτόπους στους οποίους παραπέμπουν τα παραπλανητικά μηνύματα, ωστόσο αυτό δεν συμβαίνει με ποσοστό επιτυχίας 100% (Καραδούκας, 2019).

Η πιο σημαντική προτεραιότητα για τη βιομηχανία γενικότερα είναι να διασφαλίσει επαρκή επίγνωση και αντιμετώπιση της απειλής του ηλεκτρονικού ψαρέματος. Αυτό δεν ισχύει μόνο για τους χρήστες που ενδέχεται να λάβουν τα μηνύματα, αλλά και για τους οργανισμούς που ενδέχεται να διαπιστώσουν ότι η μάρκα (επωνυμία) τους παραβιάζεται (Karakasiliotis, 2006). Για να αποφύγει να λαμβάνει τέτοιου είδους μηνύματα ηλεκτρονικού ταχυδρομείου, κάθε επιχείρηση θα πρέπει να εφαρμόσει ένα επιθετικό φιλτράρισμα ανεπιθύμητων μηνυμάτων, ώστε να μην εμφανίζονται στα εισερχόμενα μηνύματα των χρηστών καθώς και να ευαισθητοποιεί τους εργαζομένους γύρω από την ασφάλεια του ηλεκτρονικού ταχυδρομείου μέσω περιοδικής εκπαίδευσης τους ώστε να είναι σε θέση να ξεχωρίσουν ένα ανεπιθύμητο μήνυμα ηλεκτρονικού ταχυδρομείου (Κουτρώτσιος, 2019). Αυτό μπορεί να επιτευχθεί μέσω διαφόρων εργαλείων που διατίθενται στη σύγχρονη αγορά, τα οποία προσομοιώνουν επιθέσεις αυτής της κατηγορίας, ώστε να καλυφθούν οι αδυναμίες του δικτύου και των Συστημάτων και να πλήξουν την αυθεντικοποίηση και την εξουσιοδότηση τους πραγματοποιώντας τον τεχνικό έλεγχο “penetration testing”. Τέτοια εργαλεία είναι για παράδειγμα, το Metasploit που διατίθενται δωρεάν και σε εμπορική έκδοση και το εμπορικό πακέτο της Tenable Network Security “Nessus Vulnerability Scanner” (Κουτσοδόντης, 2016). Πέρα από την χρήση αυτών των εργαλείων μπορούν να αξιοποιηθούν εναλλακτικές μέθοδοι μάθησης για την εκπαίδευση των εργαζομένων (που θα αναλυθούν στο επόμενο κεφάλαιο).

2.2.2 Κωδικός πρόσβασης

Ως μη εξουσιοδοτημένη χρήση χαρακτηρίζονται οι επιθέσεις κατά τις οποίες ένας μη εξουσιοδοτημένος χρήστης προσπαθεί να αποκτήσει πρόσβαση σε προστατευμένους πόρους, στους οποίους εφαρμόζεται ελεγχόμενη πρόσβαση. Ο πιο απλός τρόπος εκδήλωσης της επίθεσης αυτής είναι μέσα από την υποκλοπή του μυστικού προσωπικού κωδικού (password) κάποιου εξουσιοδοτημένου χρήστη (Κουτσοδόντης, 2016). Όπως όλα δείχνουν, η κοινωνία εξαρτάται ολοένα και περισσότερο από το Διαδίκτυο για τις τραπεζικές εργασίες και το ηλεκτρονικό εμπόριο. Οι τυπικές συναλλαγές περιλαμβάνουν την ανταλλαγή προσωπικών πληροφοριών, όπως διευθύνσεις σπιτιού, στοιχεία πιστωτικής κάρτας (Scholefield, 2019) και προσωπικά δεδομένα πελατών που διαχειρίζονται οι επιχειρήσεις. Για την παραβίαση κωδικών πρόσβασης υπάρχουν προγράμματα που σε μικρό χρονικό διάστημα δοκιμάζουν συνδυασμό χαρακτήρων και αριθμών με απώτερο σκοπό την ανακάλυψη του μυστικού προσωπικού κωδικού. Ένας άλλος τρόπος είναι η παρακολούθηση του τι εισάγει κάποιος μέσω του πληκτρολογίου (key stroke monitoring) με τη βοήθεια ειδικών προγραμμάτων και η αποθήκευση των αποτελεσμάτων σε αρχείο (Κουτσοδόντης, 2016).

Για την μείωση του φαινομένου της μη εξουσιοδοτημένης χρήσης από τρίτους, οι οργανισμοί πρέπει να προστατεύουν τα συστήματα και τα δεδομένα μέσω ισχυρού ελέγχου ταυτότητας που βασίζεται σε περισσότερα από κάτι που γνωρίζει ο χρήστης (κωδικός πρόσβασης). Θα πρέπει να υπάρχει τουλάχιστον ένας άλλος παράγοντας ελέγχου ταυτότητας, όπως κάτι που έχει ο χρήστης (π.χ., διακριτικό σύνδεσης υπολογιστή) ή/και με

κάποιο βιομετρικό χαρακτηριστικό (Erps, 2017). Η αντικατάσταση παρελθοντικών κωδικών πρόσβασης και ο συνδυασμός πολλών παραγόντων αυθεντικοποίησης είναι μια τακτική σίγουρα κερδοφόρα για την προστασία των οργανισμών. Βέβαια παρά την εισαγωγή βιομετρικών μηχανισμών ελέγχου ταυτότητας όπως συστήματα που βασίζονται σε δακτυλικά αποτυπώματα (Μπασδαράς, 2017), οι κωδικοί πρόσβασης εξακολουθούν να αποτελούν τον κύριο μηχανισμό ελέγχου ταυτότητας για την πρόσβαση σε τέτοιες υπηρεσίες, επομένως είναι σημαντικό να διασφαλιστεί ότι οι χρήστες παραμένουν ασφαλείς στο διαδίκτυο κατά τη χρήση κωδικών πρόσβασης (Scholefield, 2019).

Πραγματοποιούνται ήδη μία σειρά από προσπάθειες για την αύξηση της ασφάλειας κωδικού πρόσβασης τελικού χρήστη. Μία κοινή μέθοδος ευαισθητοποίησης σύμφωνα με τον Scholefield, περιλαμβάνει τη χρήση μετρητών κωδικού πρόσβασης που συνήθως τοποθετούνται δίπλα σε φόρμες σε μία ιστοσελίδα για να δώσουν στους χρήστες μία γενική ένδειξη της ισχύος του κωδικού πρόσβασης. Αν και είναι πολύ δημοφιλής μέθοδος, δεν είναι απόλυτα σίγουρο πως σε όλες τις ιστοσελίδες αυτοί οι μετρητές αναδεικνύουν την πραγματική ισχύ του κωδικού. Την ίδια στιγμή όμως φαίνεται πως “κάθε μηχανισμός ανατροφοδότησης μπορεί να επηρεάσει τους χρήστες στο να δημιουργήσουν κωδικούς πρόσβασης με υψηλότερη εντροπία”. Με το σκεπτικό αυτό έχει ερευνηθεί και φαίνεται να αποδίδουν, οι εκκλήσεις φόβου για την επιλογή ισχυρότερων κωδικών ως μέθοδος ευαισθητοποίησης των τελικών χρηστών για την ασφάλεια. Η τεχνική αυτή χρησιμοποιεί πειστικά μηνύματα που ενημερώνουν τον χρήστη για όλες τις αρνητικές συνέπειες που θα έχει εάν δεν επιλέξει έναν ισχυρό κωδικό (Scholefield, 2019).

2.2.3 Έλεγχος πρόσβασης

Πέρα από τη μη εξουσιοδοτημένη πρόσβαση λόγω ασθενή κωδικού πρόσβασης ή υποκλοπής αυτού, σημαντικό ρόλο σε μία επιχείρηση παίζει και ο έλεγχος πρόσβασης στα δεδομένα και στους πόρους ενός συστήματος για τους υπαλλήλους της (Κουτσοδόντης, 2016). Υπάρχει λόγος στο να υπάρχει επιφύλαξη και για εσωτερικές απειλές. Τα προβλήματα που προκαλούνται από κακόβουλα άτομα μπορεί να μην είναι άμεσα εμφανή, αλλά δεν πρέπει να αγνοηθούν. Το προσωπικό μιας επιχείρησης μπορεί να έχει αυξημένα προνόμια για πρόσβαση σε ευαίσθητες πληροφορίες και μπορεί να τα χρησιμοποιήσει για να επηρεάσει αρνητικά τον οργανισμό. Οι εξωτερικοί υπάλληλοι, οι εργολάβοι που επισκέπτονται ή το προσωπικό συντήρησης στο χώρο θα μπορούσαν επίσης να αποτελέσουν τέτοιο κίνδυνο για την επιχείρησή. Σε περίπτωση που τους δοθούν για παράδειγμα προσωρινοί κωδικοί πρόσβασης ή ενώ έχουν απομακρυνθεί από το ρόλο τους στην επιχείρηση, εάν εξακολουθούν να έχουν δικαιώματα πρόσβασης σε κοινόχρηστο αποθηκευτικό χώρο ή έγγραφα, έχουν τη δυνατότητα να αλλάζουν, να διαγράφουν ή να αλλοιώνουν με άλλον τρόπο ευαίσθητες πληροφορίες. Είτε καταστρέφουν είτε μοιράζονται οικονομικά αρχεία, πληροφορίες πελατών ή ίσως δικαιώματα ελέγχου ταυτότητας, οι ενέργειες τέτοιων ατόμων μπορούν να προκαλέσουν όλεθρο σε επιχειρήσεις όλων των μεγεθών (Erps, 2017).

Ακολουθώντας τους μηχανισμούς ασφαλείας που προβλέπονται ο έλεγχος πρόσβασης δεν θα είναι δύσκολο ζήτημα. Η πολιτική ασφαλείας θα διασφαλίσει πως ο ιδιοκτήτης κατέχει το δικαίωμα εκχώρησης δικαιωμάτων, δηλαδή μέσω της πολιτικής διακριτικού ελέγχου προσπέλασης (Discretionary Access Control, DAC) σε ομάδες βάσει κάποιων κοινών χαρακτηριστικών ή αρμοδιοτήτων. Της πολιτικής Υποχρεωτικού Ελέγχου Πρόσβασης (Mandatory Access Control, MAC) για τους διαχειριστές των πόρων και της

Πολιτικής Ρολοκεντρικού Ελέγχου Προσπέλασης (Role Based Access Control) που εστιάζει στους χρήστες και στις εργασίες που εκτελούν.(Κουτσοδόντης, 2016). Η γνώση και η κατανόηση της απειλής από κακοπροαίρετους εσωτερικούς μπορεί να είναι η μισή μάχη για να αποτρέψουν τις επιχειρήσεις να πέσουν θύματα εγκλημάτων στον κυβερνοχώρο δραστηριότητες. Οι ηγέτες πληροφορικής και οι ιδιοκτήτες επιχειρήσεων πρέπει να παραμένουν σε εγρήγορση ώστε οι χρήστες να έχουν μόνο τα δικαιώματα πρόσβασης που χρειάζονται και να είναι επιφυλακτικοί για τις νέες εξελίξεις σε τεχνικές απάτης, προκειμένου να διασφαλιστεί ότι οι επιχειρήσεις τους παραμένουν μπροστά από τις κακόβουλες προθέσεις των εγκληματιών στον κυβερνοχώρο (Erps, 2017).

2.2.4 Wi-fi hotspots

Σήμερα η πρόσβαση στο διαδίκτυο είναι κάτι το αυτονόητο. Οι περισσότεροι διαθέτουν κινητές συσκευές και χρησιμοποιούν το δημόσιο ασύρματο δίκτυο (wifi) και το δίκτυο κινητής τηλεφωνίας όταν βρίσκονται και σε εξωτερικούς χώρους. Το χρησιμοποιούν για ψυχαγωγία ενημέρωση, εργασία και όχι μόνο. Αυτό που θα πρέπει να αναλογιστούμε όλοι είναι το πόσο ασφαλή είναι τα ασύρματα δίκτυα που προσφέρονται δωρεάν ή μη, από καφετέριες, μαγαζιά κτλ. σε δημόσιους χώρους.

Η πρόσβαση στο δημόσιο wifi έχει πάντα το ρίσκο να θέσει σε κίνδυνο την ασφάλεια της συσκευής. Αυτά τα δίκτυα χρησιμοποιούνται από εκατομμύρια ανθρώπους σε καθημερινή βάση, μεταξύ των οποίων ορισμένοι από αυτούς μπορεί να είναι και χάκερ (Poojary, 2021). Τα hotspots τις περισσότερες φορές αφήνονται χωρίς κρυπτογράφηση, επομένως οι πληροφορίες παρουσιάζονται ανοιχτά και, χωρίς προειδοποίηση, μπορούν να συλλεχθούν (Watts, 2016). Τα δεδομένα που αποστέλλονται μέσω δημόσιου wifi μπορούν εύκολα να παραβιαστούν από τους επιτιθέμενους, επίσης εάν η συσκευή δεν προστατεύεται από κακόβουλο λογισμικό, τότε και η ίδια η συσκευή είναι πιο επιρρεπείς σε επίθεση (Poojary, 2021). Επιτήδαιοι μπορεί να στήσουν ένα WiFi access point και να αφήσουν την πρόσβαση σε αυτό δωρεάν ή ελεύθερη ώστε να προσελκύσουν θύματα. Εάν τα θύματα έχουν πρόσβαση στο διαδίκτυο χρησιμοποιώντας το συγκεκριμένο WiFi access point επιτρέπουν στον επιτήδαιο να παρακολουθεί όλη την κίνηση των θυμάτων στο διαδίκτυο, παίρνοντας πολύτιμες πληροφορίες, όπως κωδικούς πρόσβασης, ιστοσελίδες που σχετίζονται με την εργασία τους και όχι μόνο (Κουτρώτσιος, 2019). Ακόμη και η παραμικρή διαρροή μιας διεύθυνσης ηλεκτρονικού ταχυδρομείου θα μπορούσε να οδηγήσει τους εγκληματίες του κυβερνοχώρου, να μάθουν ολόκληρο το ψηφιακό αποτύπωμα ενός χρήστη (Watts, 2016).

Το κύριο περιουσιακό στοιχείο που πλήττεται αν συμβεί μια τέτοια “επίθεση” εις βάρος μιας επιχείρησης είναι τα ευαίσθητα δεδομένα της επιχείρησης. Τα ξενοδοχεία πολλές φορές προσφέρουν δωρεάν πρόσβαση του διαδικτύου μέσω του wifi δικτύου τους, το οποίο μπορεί να μολύνει τις συσκευές που είναι ενωμένες με αυτό με ιούς, spyware, worms και malware. Laptops που δεν έχουν ενημερωμένο firewall, anti-virus, anti-malware κ.α. μπορούν να μολυνθούν πολύ εύκολα από τέτοιου είδους δίκτυα. Αργότερα, όταν ο υπάλληλος ενώσει τη μολυσμένη συσκευή του στο δίκτυο της επιχείρησης, μπορεί να μολύνει όλο το δίκτυο αυτής (Κουτρώτσιος, 2019).

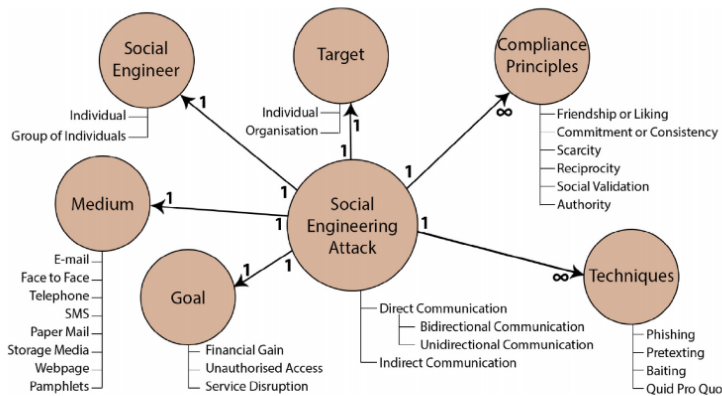
Οι χρήστες αυτών των δικτύων θα πρέπει να είναι ιδιαίτερα προσεκτικοί. Θα πρέπει να αποφεύγουν οι υπάλληλοι την απερίσκεπτη χρήση wifi hotspot, να είναι ενημερωμένοι ώστε να διαλέγουν πάντα κρυπτογραφημένη σύνδεση αλλά και να χρησιμοποιούν VPN (virtual private network) (Κουτρώτσιος, 2019). Επιπλέον δεν πρέπει να συνδέονται σε

οποιοδήποτε άγνωστο σημείο ασύρματης πρόσβασης επειδή μερικές φορές οι εγκληματίες στον κυβερνοχώρο δημιουργούν έναν ψεύτικο διαδικτυακό σημείο πρόσβασης, που έχει παρόμοιο όνομα με τη καφετέρια ή το όνομα των καταστημάτων. Πριν από την πρόσβαση θα πρέπει να επικοινωνήσουν με τον ιδιοκτήτη ή υπάλληλο του καταστήματος, να ζητήσουν το σημείο πρόσβασης Wi-Fi και να αποφεύγουν τη μεταφορά κρίσιμων δεδομένων και πληροφοριών μέσω αυτού του δικτύου (Poojary, 2021). Τέλος, οι επιχειρήσεις θα πρέπει σε όλες τις συσκευές που της ανήκουν, όπως laptops, κινητά τηλέφωνα, tablets κ.α. να έχει ενημερωμένα προγράμματα ασφάλειας, όπως anti-virus, anti-malware, anti-spyware και firewall. Επίσης θα ήταν καλό να υπάρχει μία πολιτική που να απαγορεύει στους υπαλλήλους της επιχείρησης να απενεργοποιούν τα παραπάνω προγράμματα στις συσκευές τους (Κουτρώσιος, 2019).

2.2.5 Social engineering

Η κοινωνική μηχανική αποτελεί σημαντική απειλή για την ασφάλεια των συστημάτων και των δεδομένων. Μια επίθεση κοινωνικής μηχανικής στοχεύει στο ανθρώπινο στοιχείο ως αδυναμία, χρησιμοποιώντας διάφορες τεχνικές χειραγώγησης για την εξαγωγή ευαίσθητων πληροφοριών (Mouton, 2016). Ο Harl (1997) ορίζει την τεχνική ως «η τέχνη και η επιστήμη να κάνεις τους ανθρώπους να συμμορφώνονται με τις επιθυμίες σου» και μπορούν να εντοπιστούν πολυάριθμες περιπτώσεις στις οποίες χρησιμοποιούνται συναφείς μέθοδοι από τους επιτιθέμενους για να συμβάλουν στον συμβιβασμό ενός συστήματος ή στην απόκτηση πληροφοριών (Karakasiliotis, 2006). Οι εταιρείες που διαθέτουν ευαίσθητα δεδομένα πελατών γνωρίζουν τις πιο συνηθισμένες πρακτικές που εκτελούνται από χάκερ κοινωνικής μηχανικής. Οι χάκερ επίθεσης κοινωνικής μηχανικής χρησιμοποιούν διάφορες ενημερωμένες μεθόδους για τη λήψη προσωπικών πληροφοριών. Πέντε συνηθισμένες σύγχρονες επιθέσεις περιλαμβάνουν το ηλεκτρονικό ψάρεμα (phishing), το δόλωμα, το quid pro quo (ανταλλαγή αγαθών και υπηρεσιών), το πρόσχημα και το piggybacking (Aldawood, 2019). Το ηλεκτρονικό "ψάρεμα" είναι ίσως η πιο γνωστή μορφή hacking "ψευδούς εμπιστοσύνης" (Epps, 2017).

Ερευνητές στο κομμάτι αυτό διαπίστωσαν ότι οι επιθέσεις κοινωνικής μηχανικής που είναι παρόμοιες, όσον αφορά το είδος της επικοινωνίας (άμεση ή έμμεση), το μέσο, τον στόχο, τις αρχές και τις τεχνικές συμμόρφωσης, μοιράζονται ένα παρόμοιο σύνολο βημάτων και φάσεων σε όλη την επίθεση κοινωνικής μηχανικής. Ο κοινωνικός μηχανικός μπορεί να είναι είτε ένα άτομο είτε μια ομάδα ατόμων. Ο στόχος μπορεί να είναι είτε ένα άτομο είτε ένας οργανισμός (Mouton, 2016). Υπάρχουν κάποιες βασικές τάσεις ανθρώπινης συμπεριφοράς που μπορεί να επηρεάσουν τη συμμόρφωση με ένα αίτημα κάποιου (Karakasiliotis, 2006). Οι αρχές συμμόρφωσης (φιλία ή συμπάθεια, δέσμευση ή συνέπεια, έλλειψη, αμοιβαιότητα, κοινωνική επικύρωση, εξουσία) αναφέρονται στους λόγους για τους οποίους ένας στόχος συμμορφώνεται με το αίτημα του εισβολέα (Mouton, 2016). Επιπλέον, στον τομέα της τεχνολογίας της πληροφορίας, ο Stevens (2000) αναφέρεται σε χαρακτηριστικά συμπεριφοράς όπως η «συμμόρφωση» και η «επιθυμία να βοηθήσουμε», ενώ οι Jordan και Goudey (2005) αναφέρονται σε παράγοντες «απειρίας» και «περιέργειας» που μπορούν να εκμεταλλευτούν (Karakasiliotis, 2006).



Εικόνα 1. Οντολογικό μοντέλο επίθεσης κοινωνικής μηχανικής (Mouton, 2016)

Το μοντέλο επίθεσης του Mitnick έχει τέσσερις φάσεις: έρευνα, ανάπτυξη σχέσεων και εμπιστοσύνης, εκμετάλλευση εμπιστοσύνης και χρήση πληροφοριών (Mouton, 2016). Κάποια σενάρια επίθεσης κοινωνικής μηχανικής είναι, ο εισβολέας να προσπαθεί να αποκτήσει οικονομικό όφελος στέλνοντας μηνύματα ηλεκτρονικού ταχυδρομείου που ζητούν από μια ομάδα ατόμων να κάνουν μια μικρή κατάθεση σε έναν τραπεζικό λογαριασμό που ανήκει στον εισβολέα (π.χ. ως φιλανθρωπικός οργανισμός που ζητά δωρεές ή μέσω ενός ψεύτικου ιστότοπου που πουλάει εισιτήρια για ένα αθλητικό γεγονός). Ή μπορεί να επιχειρεί να λάβει διαπιστευτήρια σύνδεσης από μια ομάδα ατόμων που χρησιμοποιούν όλα ένα συγκεκριμένο σύστημα ή προϊόν που παρέχεται από έναν οργανισμό. Ή ακόμη να στείλει υπερ-σύνδεση σε SMS στο οποίο θα ζητηθεί από το άτομο να κάνει κλικ για να λάβει τη δωρεάν ενημέρωση του συστήματος, η πρώτη οθόνη που θα βλέπει το άτομο αφού κάνει κλικ στο σύνδεσμο θα είναι μια οθόνη σύνδεσης παρόμοια με αυτή που έχει συνηθίσει. Χρησιμοποιώντας τις αρχές δέσμευσης και συνέπειας, ο χρήστης θα εμπιστευτεί τον ιστότοπο με οικεία εμφάνιση και θα εισαγάγει τα διαπιστευτήριά του (Mouton, 2016).

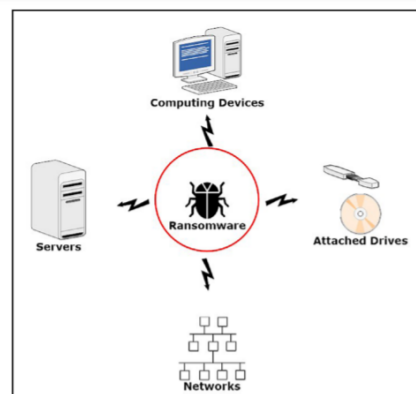
Η χρήση της κοινωνικής μηχανικής από εγκληματίες στον κυβερνοχώρο μπορεί να έχει καταστροφικές επιπτώσεις στις σύγχρονες επιχειρήσεις και είναι σίγουρα μια δραστηριότητα που πρέπει να προσέχουν οι ιδιοκτήτες επιχειρήσεων και οι ηγέτες της πληροφορικής (Erps, 2017). Λόγω της εκμετάλλευσης του ανθρώπινου στοιχείου από τους επιτιθέμενους, δεν υπάρχει «τέλειο» σύστημα ασφαλείας έναντι των απειλών κοινωνικής μηχανικής στις οποίες υπόκεινται οι οργανισμοί, αλλά η εκπαίδευση του ανθρώπινου δυναμικού για την αντιμετώπιση τέτοιων επιθέσεων είναι απαραίτητη. Η προκύπτουσα ανάγκη για αυξημένη ευαισθητοποίηση σχετικά με την ασφάλεια είναι σαφής, αλλά ο τρόπος επίτευξης αυτής της επίγνωσης θα μπορούσε να είναι μια δύσκολη διαδικασία λόγω της τεχνικής ανοικτότητας ή των χαρακτηριστικών συμπεριφοράς κάθε χρήστη (Karakasiliotis, 2006). Μικροί και μεγάλοι οργανισμοί επιλέγουν όλο και περισσότερο προγράμματα κατάρτισης και ευαισθητοποίησης με σύγχρονες μεθόδους, συμπεριλαμβανομένων σεναρίων προσομοίωσης πραγματικής ζωής, έχοντας υπόψη τις δημιουργικές δεξιότητες των χάκερ να σχεδιάσουν νέες απειλές για να εξαπατήσουν το ανθρώπινο στοιχείο, αποκαλύπτοντας σημαντικές πληροφορίες, εκτός από την ανάπτυξη τεχνικών εργαλείων για τον περιορισμό των πιθανών ζημιών που προκαλούνται από κυβερνοεπιθέσεις (Aldawood, 2019). Στόχος τους είναι να ενημερωθούν οι εργαζόμενοι για την κοινωνική μηχανική και τον τρόπο με τον οποίο μπορούν πραγματικά να χειριστούν μια τέτοια επίθεση βοηθώντας τους να σκεφτούν

στρατηγικά για το αν το μήνυμα είναι μια πιθανή επίθεση κοινωνικής μηχανικής ή όχι (Aldawood, 2019).

2.2.6 Ransomware

Το Ransomware είναι ένα είδος κακόβουλου λογισμικού που εμποδίζει τους χρήστες να έχουν πρόσβαση στους πόρους της υπολογιστικής τους συσκευής ή/και στα προσωπικά τους δεδομένα χρησιμοποιώντας διάφορες μεθόδους. Το Ransomware δεν σκοπεύει να προκαλέσει ζημιά στο σύστημα αρχείων του υπολογιστή, αντίθετα να το αφήσει σε λειτουργία για να εμφανίσει το σημείωμα λύτρων (δηλ. οδηγίες πληρωμής) στην οθόνη του θύματος και να δώσει έναν τρόπο στο θύμα να πληρώσει τα λύτρα. Τα δεδομένα στην υπολογιστική συσκευή του θύματος (είτε πρόκειται για υπολογιστή, διακομιστή, tablet, smartphone ή συσκευή Internet of Things) καθίστανται άχρηστα έως ότου ο κάτοχος της συσκευής πληρώσει λύτρα για να καταργήσει τον περιορισμό (Hassan, 2019).

Αυτό το διαβόητο στέλεχος κακόβουλου λογισμικού στοχεύει όχι μόνο τους απλούς τελικούς χρήστες, αλλά και τις κυβερνήσεις και τις επιχειρηματικές οργανώσεις σχεδόν σε κάθε τομέα. Ακόμη χειρότερα, το 2020, η πρώτη απώλεια ανθρώπινης ζωής ως αποτέλεσμα επιθέσεων ransomware αναφέρθηκε ότι έγινε στη Γερμανία (Security Magazine (2020), Oz (2021). Τα προαναφερθέντα περιστατικά έχουν ήδη καταστήσει το ransomware το νούμερο ένα πρόβλημα μεταξύ των φορέων απειλής και άμυνας (δηλαδή κυβερνήσεων, βιομηχανίας και ακαδημαϊκού χώρου) (Oz, 2021).



Εικόνα 2. Συσκευές που μπορούν να επηρεαστούν από ransomware (Hassan, 2019)

Το ransomware ονομάζεται επίσης ψηφιακός εκβιασμός (digital extortion or digital blackmail) και με βάση την μεθοδολογία που χρησιμοποιείται, ταξινομείται γενικά σε δύο τύπους, «Cryptographic Ransomware» και «Locker Ransomware». Ο «Locker» τύπος ransomware εμποδίζει το θύμα να έχει πρόσβαση στο σύστημά του κλειδώνοντας την οθόνη ή το πρόγραμμα περιήγησης και απαιτεί πληρωμή λύτρων για να ξεκλειδώσει το σύστημα και δεν κρυπτογραφεί τα δεδομένα του συστήματος ή των χρηστών (Oz, 2021). Οι σύγχρονες ransomware επιθέσεις χρησιμοποιούν κρυπτογράφηση (Cryptographic Ransomware) για να κλειδώσουν εντελώς τα προσωπικά αρχεία του θύματος καθιστώντας το μη ανακτήσιμο χωρίς το σχετικό κλειδί αποκρυπτογράφησης (Hassan, 2019).

Καθώς η εξάρτηση από την ψηφιακή τεχνολογία αυξάνεται, οι άνθρωποι βασίζονται όλο και περισσότερο στις υπολογιστικές τους συσκευές - είτε πρόκειται για υπολογιστή είτε

για κινητή συσκευή - για να οργανώσουν την εργασία και την προσωπική τους ζωή. Σε αυτές τις συσκευές αποθηκεύονται πολύτιμα προσωπικά δεδομένα, συμπεριλαμβανομένων συχνά εταιρικών δεδομένων που ενδέχεται να περιέχουν εμπορικά μυστικά ή επιχειρηματικές δραστηριότητες και προϋπολογισμούς που διατίθενται μόνο σε ψηφιακή μορφή. Αυτή η μετάβαση στην εποχή της πληροφορίας σημαίνει ότι μια επιτυχημένη επίθεση ransomware εναντίον ενός απροστάτευτου συστήματος μπορεί να έχει καταστροφικές συνέπειες (Hassan, 2019).

Το Ransomware προχωρά μέσω τριών μεγάλων βημάτων μόλις διαπεράσει μια επιχειρηματική οντότητα. Πρώτον, ο εισβολέας απελευθερώνει το κακόβουλο λογισμικό και μόλις μολύνει ένα χρήστη ή δίκτυο, ένα κλειδί στο κακόβουλο λογισμικό κρυπτογραφεί τα δεδομένα του θύματος. Δεύτερον, το κακόβουλο λογισμικό αποστέλει ένα μήνυμα προς το θύμα με πληροφορίες για το πώς να προχωρήσει. Ο εισβολέας υπόσχεται να παρέχει λογισμικό ή έναν κωδικό πρόσβασης για να ξεκλειδώσει τα δεδομένα μόλις πληρωθεί το αντίτιμό του. Τέλος, όταν ο εισβολέας λάβει ξανά την πληρωμή, μπορεί να ανταλλάξει τα δεδομένα των ομήρων ως κλειδί για την κρυπτογράφηση (Wade, 2021). Έτσι εκβιάζοντας το θύμα και εκμεταλλεύοντας την μεγάλη αξία των δεδομένων καταφέρνει να αποσπάσει το χρηματικό ποσό που ζητά.

Μία περίπτωση κακόβουλου λογισμικού ransomware μέσω επίθεσης πλαστοπροσωπίας είναι αυτή της φωτογράφισης ιστοσελίδας δίωξης Ηλεκτρονικού Εγκλήματος και στην οθόνη του χρήστη εμφανιζόταν η συγκεκριμένη σελίδα με ένα μήνυμα που απαιτούσε το ποσό των 100 ευρώ μέσω προπληρωμένης κάρτας για να λειτουργήσει ξανά υπολογιστής, ο οποίος είχε μπλοκαριστεί «εικονικά» λόγω παράνομης χρήσης διαδικτύου (Κουτσοδόντης, 2016).

Τα συμπτώματα που εμφανίζονται μετά από μια τέτοια επίθεση μπορεί να είναι αδυναμία ανοίγματος αρχείων, αντικατάσταση φόντου επιφάνειας εργασίας με μια σημείωση λύτρων, κλείδωμα υπολογιστή και αδυναμία εισόδου στην επιφάνεια εργασίας, κάλυψη ολόκληρης της οθόνης εμφανίζοντας σημείωμα λύτρων αιτώντας την πληρωμή αυτών σε περιορισμένο χρονικό διάστημα με την απειλή απώλειας των δεδομένων για πάντα και μετονομασία (π.χ. YOUR_FILES_ARE_ENCRYPTED.HTML και YOUR_FILES_ARE_ENCRYPTED.TXT), κρυπτογράφηση αρχείων και αλλοίωση ή αφαίρεση της επέκτασης (Hassan, 2019).

Τέλος, ο έλεγχος πρόσβασης που αναλύθηκε παραπάνω (στο 2.2.3) είναι απαραίτητος και αν δεν τηρείται μπορεί να βοηθήσει ακόμα περισσότερο στη διενέργεια αυτής της επίθεσης. Εάν οι κοινωνικοί μηχανικοί είναι σε θέση να αποκτήσουν πρόσβαση μέσω αγνώστου προσωπικού, οι εταιρείες ενδέχεται να υποφέρουν από τις πρόσφατες επιθέσεις ransomware. Μόλις οι επιτιθέμενοι παγώσουν έναν οργανωτικό σταθμό εργασίας ή ένα σύστημα πληροφοριών, μια διαδικασία διαπραγμάτευσης μπορεί να αποτύχει και να οδηγήσει σε καταστροφή σημαντικών δεδομένων (Aldawood, 2019).

2.2.7 GDPR (General Data Protection Regulation)

Ο GDPR είναι ο πιο σκληρός νόμος στον κόσμο σε σχέση με την ιδιωτικότητα και την ασφάλεια. Αν και έχει συνταχθεί και εγκριθεί από την Ευρωπαϊκή Ένωση, επιβάλλει τους κανονισμούς σε οργανισμούς και επιχειρήσεις σε όλο τον κόσμο, εφόσον στοχεύουν ή συγκεντρώνουν δεδομένα σχετικά με κατοίκους της Ευρωπαϊκής Ένωσης. Ο κανονισμός

αυτός τέθηκε σε ισχύ στις 25 Μαΐου 2018 (Κουτρώσιος, 2019). Οι παραβιάσεις αυτού του κανονισμού έχουν ως αντίτιμο υψηλά πρόστιμα και κυρώσεις στους παραβάτες.

Με το νέο αυτό κανονισμό, η Ευρώπη σηματοδοτεί την αυστηρή στάση της όσον αφορά την ιδιωτικότητα και την ασφάλεια των δεδομένων, σε μία εποχή που οι περισσότεροι άνθρωποι εμπιστεύονται τα προσωπικά τους δεδομένα σε υπηρεσίες cloud (υπολογιστικού νέφους) και οι παραβιάσεις είναι ένα καθημερινό φαινόμενο. Ο GDPR είναι μεγάλος, αρκετά εκτεταμένος και ελαφρύς κανονισμός όσον αφορά τις ιδιαιτερότητες, καθιστώντας έτσι την συμμόρφωση μαζί του μία ιδιαίτερα δύσκολη διαδικασία, ιδιαίτερα για τις μικρομεσαίες επιχειρήσεις (Κουτρώσιος, 2019).

Για τις οντότητες που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα (δηλαδή ελεγκτές δεδομένων ή επεξεργαστές δεδομένων), η επιβολή του GDPR σημαίνει την εφαρμογή οργανωτικών και τεχνικών αλλαγών, συμπεριλαμβανομένης της ανάπτυξης εργαλείων που επιτρέπουν την επίδειξη της συμμόρφωσης με τον GDPR, το διορισμό αξιωματικών προστασίας δεδομένων (DPOs), διεξαγωγή του αντίκτυπου της ιδιωτικής ζωής αξιολογήσεις (PIA), η εκπαίδευση του προσωπικού, η εφαρμογή τεχνικών απο-ταυτοποίησης δεδομένων κ.λπ. (Tsohou, 2020).

Ο GDPR χωρίζεται σε δύο μέρη: το πρώτο μέρος αποτελείται από 173 αιτιολογικές σκέψεις που εξηγούν τα κίνητρα του κανονισμού και τα επιδιωκόμενα επιτεύγματα. το δεύτερο μέρος αποτελείται από 99 άρθρα που αντιπροσωπεύουν τον κώδικα. Ο κανονισμός GDPR εφαρμόζεται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα, είτε είναι αυτοματοποιημένα (έστω και εν μέρει) είτε όχι (Calabrò, 2019). Σύμφωνα με το GDPR εάν η επιχείρηση ή ο οργανισμός διαχειρίζεται δεδομένα καθορίζονται οι ακόλουθες αρχές σύμφωνα με το Άρθρο 5.1-2 :

- Νομιμότητα, δικαιοσύνη, διαφάνεια, δηλαδή, τα δεδομένα πρέπει να υποβάλλονται σε δίκαιη, νόμιμη και διαφανή επεξεργασία.
- Περιορισμός στόχου, δηλαδή, τα δεδομένα πρέπει να συλλέγονται μόνο για καθορισμένους, σαφείς και νόμιμους σκοπούς και δεν πρέπει να υποβάλλονται σε επεξεργασία αργότερα για άλλους σκοπούς.
- Ελαχιστοποίηση δεδομένων, δηλαδή, τα δεδομένα που υποβάλλονται σε επεξεργασία πρέπει να είναι σχετικά, επαρκή και περιορισμένα στο αναγκαίο για τους σκοπούς για τους οποίους υποβάλλονται σε επεξεργασία.
- Ακρίβεια, δηλαδή, τα δεδομένα που υποβάλλονται σε επεξεργασία πρέπει να είναι ακριβή και ενημερωμένα τακτικά.
- περιορισμός αποθήκευσης, δηλαδή, τα δεδομένα πρέπει να διαγραφούν μετά από περιορισμένο χρονικό διάστημα.
- Η ρητή συγκατάθεση του υποκειμένου (λογοδοσία), δηλαδή, τα δεδομένα μπορούν να συλλεχθούν και να υποβληθούν σε επεξεργασία μόνο εάν το υποκείμενο των δεδομένων δώσει τη ρητή συγκατάθεσή του (Calabrò, 2019; Κουτρώσιος, 2019).

Κάθε επιχείρηση και οργανισμός λοιπόν θα πρέπει να συμμορφώνεται με τον κανονισμό αυτόν, τηρώντας όλες τις αρχές ώστε να υπάρχει μία νόμιμη και δίκαιη διαδικασία. Οι επιχειρήσεις κρατούν πολλά ευαίσθητα και προσωπικά δεδομένα τα οποία απαιτούν λεπτό χειρισμό. Ακολουθώντας τις παραπάνω αρχές προστατεύουν τα δεδομένα των πελατών τους και απομακρύνονται από τον εύκολο στόχο κακόβουλων χρηστών που βρίσκουν ευκαιρίες επίθεσης μέσα από παραλείψεις και κενά ασφαλείας των επιχειρήσεις απέναντι στα απαραίτητα πρωτόκολλα.

2.3 Επιχειρήσεις και κυβερνοασφάλεια

Το διαδίκτυο χρόνο με τον χρόνο εξελίσσεται κάνοντας την καθημερινότητά μας πιο εύκολη καθώς μας βοηθάει σε πολλούς τομείς της ζωής μας. Στον επαγγελματικό χώρο, μας προσφέρει ταχύτητα στην εκτέλεση των απαραίτητων λειτουργιών και αποδοτικότερη εξυπηρέτηση με τελικό στόχο την ικανοποίηση των προσδοκιών της εταιρείας και των απαιτήσεων των πελατών της. Πιο συγκεκριμένα, την σημερινή εποχή το διαδίκτυο έχει βελτιώσει τα επίπεδα εργασίας στη ψηφιοποίηση, τη παγκοσμιοποίηση, τη κινητικότητα, τις ομάδες εργασίας και την αμεσότητα (Καραδούκας, 2019). Οι επιχειρήσεις και κυρίως οι μεγάλο επιχειρήσεις έχουν μετατρέψει έγγραφα και αρχεία που ήταν σε φακέλους στον φυσικό επαγγελματικό χώρο της, σε ψηφιακή μορφή στον κυβερνοχώρο αξιοποιώντας υπολογιστές και υπηρεσίες διαδικτύου όπως το cloud computing. Τα οφέλη από την σύνδεση της επιχείρησης με τον κόσμο του διαδικτύου είναι πάρα πολλά, όπως η αύξηση των δεδομένων χωρίς την κατάληψη επιπλέον φυσικού χώρου, την δυνατότητα απομακρυσμένης (εξ αποστάσεως) εργασίας των υπαλλήλων, την διαφήμιση της εταιρείας, επικοινωνία με περισσότερα κανάλια όπως το ηλεκτρονικό ταχυδρομείο, φόρμα επικοινωνίας στην ιστοσελίδα της επιχείρησης και μέσω των μέσων κοινωνικής δικτύωσης κτλ. Επιπλέον η αυτοματοποίηση είναι ένα πολύ θετικό στοιχείο αφού η συλλογή στοιχείων, η ενημέρωση κατάστασης μια ενέργειας όπως μιας παραγγελίας αλλά ακόμα και η κατάρτιση σε διάφορα θέματα μέσω ειδικών διαμορφωμένων ιστοσελίδων με εκπαιδευτικές παρουσιάσεις, βίντεο και τεστ αξιολόγησης για τους εργαζόμενους προσφέρει γρηγορότερη και πολλές φορές καλύτερη εξυπηρέτηση ανταποκρινόμενη στους γρήγορους σημερινούς ρυθμούς της κοινωνίας.

Όλες οι επιχειρήσεις χρησιμοποιούν πληροφορίες. Υπάρχουν κάποιες βασικές πληροφορίες που όλες οι επιχειρήσεις έχουν αλλά ανάλογα με το είδος τους, τις υπηρεσίες και τα προϊόντα που προσφέρουν διαφοροποιούνται από επιχείρηση σε επιχείρηση. Γενικά διαχειρίζονται πολύτιμες πληροφορίες για τους εργαζόμενους τους, φορολογικές πληροφορίες, πληροφορίες και δεδομένα των πελατών της, προσωπικές πληροφορίες, αριθμούς κοινωνικής ασφάλισης ή πιστωτικής κάρτας, για οικονομικά στοιχεία, ιατρικό ιστορικό, αξιολογήσεις εργαζομένων, απώρητα έγγραφα, εμπορικά μυστικά για πατέντες, σχέδια ανάπτυξης νέων προϊόντων τμήματος μάρκετινγκ, μελέτες του Τμήματος έρευνας και ανάπτυξης (Μπασδαράς, 2017) και άλλα, που έχουν τεράστια αξία. Οι πληροφορίες είναι ζωτικής σημασίας για την λειτουργία μιας επιχείρησης (Κουτρύσιος, 2019). Χωρίς τα δεδομένα και τις πληροφορίες της δεν μπορεί να προσφέρει τα προϊόντα και τις υπηρεσίες της και συνεπώς να λειτουργήσει.

Η αυξανόμενη χρήση του Διαδικτύου εκτός των θετικών επιδράσεων φέρνει και αρνητικά αποτελέσματα. Λόγω των σύγχρονων λύσεων cloud, των εφαρμογών δικτύου και της προοδευτικής ψηφιοποίησης, κάθε οργανισμός ανεξάρτητα από τον κλάδο εκτίθεται σε ορισμένους κινδύνους που σχετίζονται με τα δεδομένα του με σοβαρές επιπτώσεις στη δημόσια ασφάλεια. Σήμερα, δεν υπάρχει οργανισμός που να μην αγγίζει τα προβλήματα που σχετίζονται με την ασφάλεια των πληροφοριών. (Podgórski, 2020; Μπασδαράς, 2017).

Στον κυβερνοχώρο που έχουν ανοιχτεί μεγάλες και μικρές επιχειρήσεις πλέον, εγκυμονούν πολύ κίνδυνοι και χωρίς την κατάλληλη στρατηγική πρόληψης και προστασίας είναι σίγουρο πως κακόβουλοι χρήστες παραμονεύουν για κυβερνοεπιθέσεις, εκμεταλλευόμενοι αυτή την ευκαιρία. Στο παρελθόν ένας χάκερ συνήθως κυνηγούσε την αναγνώριση αλλά πλέον αυτό έχει αλλάξει. Σήμερα, οι κυβερνοεγκληματίες στοχεύουν σε

οικονομικά οφέλη και είναι περισσότερο οργανωμένοι. Το επίπεδο οργάνωσης του προκαλεί μεγάλη ανησυχία καθώς για να μπορέσουν να έχουν τέτοιο επίπεδο οργάνωσης σημαίνει ότι έχουν πολλούς πόρους (Κουτρώσιος, 2019). Αυτές οι απειλές μπορεί να σχετίζονται με την απώλεια ενός από τα τρία κύρια χαρακτηριστικά ασφάλειας: εμπιστευτικότητα, προσβασιμότητα και ακεραιότητα, αλλά μπορεί επίσης να σχετίζονται με απώλειες που προκύπτουν από τη μείωση της αποδοτικότητας των εργαζομένων (Podgórski, 2020).

Οι διαδικτυακές απειλές περιλαμβάνουν spam, phishing, ιούς, rootkits, και διάφορα είδη malware. Η διαφορά σήμερα με το παρελθόν είναι η αλλαγή στην φιλοσοφία των επιθέσεων και στον αριθμό συσκευών και υπηρεσιών που επηρεάζονται. Τα κακόβουλα λογισμικά (malwares) για παράδειγμα, είναι μεγάλο πρόβλημα για τις επιχειρήσεις, επειδή επηρεάζουν πολλαπλές συσκευές (Κουτρώσιος, 2019). Μολύνοντας μια συσκευή και συνδέοντας την στο εταιρικό δίκτυο θα μεταφέρει το malware σε όλες τις άλλες συνδεδεμένες, σε αυτό το δίκτυο, συσκευές. Το κακόβουλο λογισμικό μπορεί να προκαλέσει τυχόν “εφέ” προγραμματισμένα από τον δημιουργό, τα οποία μπορεί να οδηγήσουν σε κλοπή δεδομένων, τροποποίηση ή πιο συχνά μπορεί να χρησιμοποιηθούν για εκβιασμό λόγω κρυπτογράφησης δεδομένων. Στη συνέχεια, ξεκινά η διαδικασία συλλογής λύτρων που σχετίζονται με την ανάκτηση κρυπτογραφημένων δεδομένων (Dobran, 2019). Οι στατιστικές δείχνουν ότι πρόκειται για μια ιδιαίτερα κερδοφόρα επιχείρηση για τους επιτιθέμενους (Podgórski, 2020).

Οι επενδύσεις στην κυβερνοασφάλεια δεν είναι πολυτέλεια αλλά αναγκαία επένδυση, γιατί η δυσλειτουργία της επιχείρησης ή η παραβίαση και υποκλοπή στοιχείων έχει σημαντικά μεγαλύτερο κόστος. Παίρνοντας τα κατάλληλα μέτρα οι επιχειρήσεις μπορούν να ελαχιστοποιήσουν τους κινδύνους που εγκυμονούν. Κίνδυνος για μια επιχείρηση μπορεί να είναι χρηματοοικονομικές ζημιές λόγω απρόβλεπτων γεγονότων, αλλοίωση της εικόνας (φήμης) της επιχείρησης, απώλεια εμπιστοσύνης και αξιοπιστίας των παροχών προς τους πελάτες της μεταβάλλοντας τα προσδοκώμενα αποτελέσματα (Μπασδαράς, 2017; Erps, 2017). Η μεγαλύτερη επίπτωση που μπορεί να έχει μετά από μια κυβερνοεπίθεση είναι δημιουργία πανικού λόγω πιθανής απώλειας, καταστροφής προσωπικών δεδομένων ή αδύνατης εισχώρησης σε προσωπικές πληροφορίες (Μπασδαράς, 2017).

Κύρια μέριμνα των επιχειρήσεων είναι η ελαχιστοποίηση των κινδύνων που οδηγούν σε αρνητικές συνέπειες της επιχείρησης με αποτέλεσμα την δυσλειτουργία της. Προτεραιότητα αξίζει να δοθεί στα μέτωπα τα οποία είναι πιο ευάλωτα σε κυβερνοεπιθέσεις με μεγάλες επιπτώσεις για την επιχείρηση (άξονας προετοιμασίας) (Μπασδαράς, 2017). Για την εκπλήρωση του στόχου αυτού πρέπει να οχυρωθεί η ασφάλεια της επιχείρησης. Η ασφάλεια, των πληροφοριών που διατηρεί, είναι τμήμα αυτής και στηρίζεται στις βασικές απαιτήσεις του τριγώνου CIA, εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα (confidentiality, integrity, availability) και πρέπει να διασφαλίζεται η ύπαρξη του σε κάθε σύστημα (Κουτρώσιος, 2019). Όλες οι ενέργειες διασφάλισης των πληροφοριών, των συστημάτων και των δικτύων από κάθε είδους απειλής, σύμφωνα με το Υπουργείο Άμυνας των ΗΠΑ, ορίζεται ως κυβερνοασφάλεια. Υπό τον άξονα της προστασίας η επιχείρηση πρέπει να λάβει τεχνολογικά μέτρα, διαδικασίες, οργάνωση αλλά και εγρήγορση, μέσω κατάλληλης και συνεχούς ενημέρωσης του ανθρώπινου δυναμικού. Τέλος, αφού έχει προετοιμαστεί και προστατευτεί, για να αντιμετωπίσει σωστά μια επίθεση θα πρέπει να την ανιχνεύσει και να την εντοπίσει (Μπασδαράς, 2017).

Η συνεχής εξέλιξη της τεχνολογίας συμπορεύεται με την εξέλιξη των κυβερνοεπιθέσεων με αποτέλεσμα την δύσκολη διαχείριση των επιθέσεων (Μπασδαράς, 2017). Επιπρόσθετα, τα τεχνολογικά μέσα προστασίας (λογισμικά κατα των ιών, προγράμματα, συστήματα firewall κτλ.) δεν επαρκούν για την ασφάλεια μιας επιχείρησης. Χρειάζεται να δοθούν τα απαραίτητα εναύσματα στο ανθρώπινο δυναμικό που την απαρτίζει, αφού αυτό φαίνεται να είναι το πιο ευάλωτο μέτωπο της (Mouton, 2016); Κουτρύσιος, 2019).

Διάφορες πολιτικές για την επαγρύπνηση, ευαισθητοποίηση, εκπαίδευση, κατάρτιση και τον έλεγχο της συμπεριφοράς όλων των υπαλλήλων μπορούν να βοηθήσουν στην εξασφάλιση της ασφάλειας της επιχείρησης θωρακίζοντας την από απειλές, ανεξαρτήτως τον τομέα δραστηριοποίησης της. Στην πρώτη γραμμή άμυνας βρίσκεται το προσωπικό ασφαλείας (Μπασδαράς, 2017), όμως δυστυχώς δεν συγχρονίζονται στην ενημέρωση και στην κατάρτιση γνώσεων με τους επιτιθέμενους, αντίθετα μένουν πιο πίσω (Katsantonis, 2019). Στη συνέχεια ακολουθεί το υπόλοιπο προσωπικό το οποίο παρά τις υπενθυμίσεις των ειδικών διατηρούν μια στάση απάθειας (Benjamin, 2007). Αυτό μπορεί να αντιμετωπιστεί αυξάνοντας την ευαισθητοποίηση, γιατί γνωρίζοντας και κατανοώντας τις πιθανές επιπτώσεις της στάσης αυτής απέναντι σε μια επίθεση ελαχιστοποιείται ο κίνδυνος (Cook, 2016). Σημαντική προϋπόθεση είναι να εφαρμοστεί το οποιοδήποτε πρόγραμμα πρωτίστως από τα ανώτερα στελέχη της επιχείρησης για να δοθεί το παράδειγμα και στα υπόλοιπα επίπεδα, αυτό θα καθορίσει και την αποτελεσματικότητα αυτής της προσπάθειας (Wilson, 2003). Οι υπάλληλοι θα πρέπει να εκπαιδευτούν ώστε να αναγνωρίσουν την σημασία της ασφαλούς συμπεριφοράς στον κυβερνοχώρο, την σωστή διαχείριση των δεδομένων και των πληροφοριών, όπως και τους κανόνες και τις πολιτικές απορρήτου και ασφάλειας που διέπουν την εκάστοτε επιχείρηση και την αναγκαιότητα τήρησης τους (Κουτρύσιος, 2019; Oroszi, 2019).

Δεν είναι πάντα εύκολη η δημιουργία και η εφαρμογή ενός αποτελεσματικού προγράμματος ασφαλείας αφού εκτός από την προσοχή στην ανάδειξη κατάλληλου και χρήσιμου περιεχομένου πρέπει να επιλεγεί και ο κατάλληλος τρόπος παρουσίασης που θα κεντρίσει το ενδιαφέρον των υπαλλήλων (Oroszi, 2019). Όλες αυτές οι μέθοδοι ευαισθητοποίησης και κατάρτισης πάνω στην κυβερνοασφάλεια, πρέπει να ενημερώνονται ανά τακτά χρονικά διαστήματα. Επίσης, χρειάζεται η συνεχής και περιοδική διοργάνωση ευαισθητοποίησης ίσως μέσω κάποιας μηνιαίας εκστρατείας ασφαλείας που θα συνδυάζει παρουσιάσεις, αφίσες ή κόμικ, ερωτηματολόγια κ.α. για την διαρκή επαγρύπνηση των εργαζομένων σχετικά με τις απειλές του ανθρώπινου παράγοντα (Κουτρύσιος, 2019). Όμως πέρα από την επαγρύπνηση και την υπενθύμιση και υπόδειξη μεθόδων προστασίας, για παράδειγμα μια αφίσα που να τονίζει την χρήση ασφαλούς κωδικού πρόσβασης, θα πρέπει να υπενθυμίζονται και οι συνέπειες των επιθέσεων. Τέλος, για να αυξηθεί το ενδιαφέρον των υπαλλήλων μπορούν να χρησιμοποιηθούν εναλλακτικές και πιο σύγχρονες μορφές επιμόρφωσης για παράδειγμα μέσω ομαδικών στοιχείων όπως είναι τα δωμάτια διαφυγής και μέσω του gamification (Oroszi, 2019).

Συνοψίζοντας, η εξασφάλιση της ασφάλειας των πληροφοριών και γενικότερα της επιχείρησης, όποιο και αν είναι το μέγεθος της, είναι ζωτικής σημασίας και μπορεί να επιτευχθεί με τον συνδυασμό υψηλής ευαισθητοποίησης και υπευθυνότητας των εργαζομένων και της χρήση των τελευταίων μέτρων ασφαλείας (Podgórski, 2020).

3. Παιχνιδοποίηση της ευαισθητοποίησης στην κυβερνοασφάλεια

3.1 Σοβαρά Παιχνίδια

Το παιχνίδι είναι μια δομημένη δραστηριότητα που έχει συνήθως ως κύριο σκοπό την ψυχαγωγία. Υπάρχει σε όλους τους πολιτισμούς και η ιστορία του ξεκινάει από πολύ παλιά. Όσο περνάνε τα χρόνια, λόγω των εξελίξεων του πολιτισμού, της οικονομίας, της τεχνολογίας το παιχνίδι αλλάζει μορφές και στόχους. Έχει γίνει και εξακολουθεί να γίνεται άξιο προσοχής από πολλούς ερευνητές και διάφορους επιστημονικούς κλάδους. Δεν έχει μείνει στάσιμο αλλά έχει εξελιχθεί σε σημείο να θεωρείται μορφή τέχνης και έχει επεκταθεί στον ψηφιακό κόσμο. Το συναντάμε με διάφορες ονομασίες όπως ψηφιακό παιχνίδι, ηλεκτρονικό παιχνίδι, παιχνίδι υπολογιστή, βιντεοπαιχνίδια (video games) όπου παλαιότερα υπήρχαν διακριτικά χαρακτηριστικά αλλά σήμερα αυτές τις ονομασίες τις αντιμετωπίζουμε ισοδύναμα (Πολύζου, 2019).

Τα περισσότερα ηλεκτρονικά παιχνίδια θεωρούνται είτε προσομοιώσεις κάποιου πραγματικού κόσμου ή φανταστικού κόσμου είτε μεταφορά ενός παραδοσιακού παιχνιδιού σε ψηφιακό. Αυτά τα παιχνίδια έχουν τα τυπικά χαρακτηριστικά του παραδοσιακού παιχνιδιού με τους ορισμένους κανόνες, τον ή τους στόχους, την έναρξη και το τέλος με την νίκη ή την ήττα και ψυχαγωγούν μέσα από μια διαδραστική εμπειρία. Το μέσο που χρησιμοποιείται για την αλληλεπίδραση του παίκτη μαζί τους είναι οι ψηφιακές πλατφόρμες (υπολογιστής, διαδίκτυο, κονσόλες, φορητές συσκευές). Απαραίτητη προϋπόθεση για την λειτουργία τους είναι η ενεργή συμμετοχή του παίκτη (Πολύζου, 2019).

Η χρήση των παιχνιδιών έχει ξεπεράσει τον συνηθισμένο σκοπό της ψυχαγωγίας και συμβάλλει στην εκπαίδευση, ευαισθητοποίηση, επιμόρφωση κ.α. υποστηρίζοντας ποικίλους τομείς όπως της υγείας, της παιδείας, της ασφάλειας κ.α. (Benjamin, 2007). Αυτό συμβαίνει χάρη στην αναπαράσταση γεγονότων, καταστάσεων και ιστοριών, στην εξομίωση ενός πραγματικού περιβάλλοντος, στην περιήγηση και αλληλεπίδραση του παίκτη με το παιχνίδι, καθώς και του μηδενικού αντίκτυπου των πράξεων του και την ευκαιρία να μάθει από τις αστοχίες του (Αναγνώστου, 2009). Τα παιχνίδια τα οποία έχουν κι άλλους σκοπούς πέρα από την ψυχαγωγία ονομάζονται σοβαρά παιχνίδια (serious games) και εμφανίζουν πολλά παιδαγωγικά πλεονεκτήματα (Le Compte, 2015).

Τα σοβαρά παιχνίδια αποτελούνται από εικονικά περιβάλλοντα και προσομοιώσεις και εμπλέκουν τον παίκτη σε μια ιστορία/ σενάριο και δεν είναι απαραίτητο να περιορίζονται στον ψηφιακό κόσμο. Παρά τους εκπαιδευτικούς και παιδαγωγικούς σκοπούς που έχουν δεν θα πρέπει να χάνουν τη θεμελιώδη έννοια του παιχνιδιού (Hill, 2020). Φαίνεται ότι μπορούν να είναι χρήσιμα εκπαιδευτικά εργαλεία (Katsantonis, 2019) γι αυτό υπάρχει πλήθος προσεγγίσεων και υλοποιήσεων διαθέσιμα αλλά και εργαλεία ανάπτυξης αυτών.

Μια άλλη προσέγγιση παιχνιδιών είναι τα δωμάτια απόδρασης (escape rooms). Είναι ομαδικά παιχνίδια που έχουν ως σκοπό την απόδραση των παικτών από ένα δωμάτιο μέσα σε ορισμένο χρονικό όριο, εξερευνώντας τον χώρο και χρησιμοποιώντας διάφορα στοιχεία που κερδίζουν από την επίλυση γρίφων (Karageorgiou Z., Fotaris P., Christopoulou E., Mavrommati E. 2020). Από τη φύση τους προκαλούν δημιουργικότητα στην εκπαιδευτική διαδικασία και παρέχουν στους ανθρώπους ευκαιρίες να εξασκήσουν μια σειρά από

δεξιότητες επικοινωνίας και συνεργασίας (Karageorgiou Z., Mavrommati E., Christopoulou E., Fotaris P., 2019). Ξεκίνησαν να λειτουργούν σε φυσικό μέρος αλλά πλέον στις μέρες μας μπορούμε να τα βρούμε και στον ψηφιακό κόσμο. Στο φυσικό κόσμο οι παίκτες γίνονται πρωταγωνιστές της ιστορίας και άλλοι αποφασίζουν τον χώρο και τον χρόνο αφιέρωσης σε αυτή την εμπειρίας. Αρχικά ο χαρακτηρισμός ανταποκρινόταν στην ακριβή σημασία των λέξεων (απόδραση και δωμάτιο) αλλά στις μέρες μας η σημασία του έχει ξεφύγει από την αυστηρή του έννοια και αφορά οποιαδήποτε διαδραστική εμπειρία σε κλειστό χώρο ως τρόπο ψυχαγωγίας (Πολύζου, 2019). Οι παίκτες ίσως κληθούν να εξιχνιάσουν ένα έγκλημα, να σώσουν έναν χαρακτήρα του παιχνιδιού ή να βρουν έναν θησαυρό (Fotaris, 2019).

Τέλος, πέρα από την εμφάνιση των σοβαρών παιχνιδιών υπάρχει και το φαινόμενο του “gamification” όπου σύμφωνα με τον Oroszi (2019) είναι “η χρήση στοιχείων παιχνιδιού και σκέψης παιχνιδιού σε περιβάλλοντα εκτός παιχνιδιού για την αύξηση της συμπεριφοράς και της αφοσίωσης στόχου”. Η παιχνιδοποίηση (gamification) συνδυάζει στοιχεία παιχνιδιού (gaming elements) και τεχνικές σχεδιασμού παιχνιδιών (game design techniques) χωρίς το υπόλοιπο πλαίσιο παιχνιδιού. Επειδή η σχεδίαση ενός συστήματος παιχνιδοποίησης πρέπει να είναι πολύ προσεκτική υπάρχουν ορισμένα πλαίσια σχεδίασης. Ένα είναι το MDA που αποτελείται από τρία βασικά στοιχεία, την μηχανική (Mechanics) για την αλληλεπίδραση με τον παίκτη (δεδομένα, αλγόριθμοι, κανόνες και συστήματα), τη δυναμική (Dynamics) για την δημιουργία της εμπειρίας του παίκτη μέσα από τους κατάλληλους μηχανισμούς και την αισθητική (Aesthetics). Η αισθητική αφορά την ευχαρίστηση και τα συναισθήματα που μπορεί να αισθάνεται ο παίκτης και σε συνδυασμό με την μηχανική και την δυναμική διαμορφώνει την συνολική διασκέδαση του παιχνιδιού (Πολύζου, 2019). Εάν δοθεί προσοχή σε αυτά τα στοιχεία και στο πλαίσιο των σεναρίων που χρησιμοποιούνται, μελέτες δείχνουν πως το gamification έχει θετικές επιδράσεις (Cook, 2016). Επιπρόσθετα, η παιχνιδοποίηση έχει χαρακτηριστικά τα οποία βοηθούν στον ευγενή ανταγωνισμό, στις ανταμοιβές, στην ποσοτικοποίηση της συμπεριφοράς του παίκτη και στην αύξηση των κινήτρων σε περιβάλλον εκτός παιχνιδιού (Scholefield, 2019; Omar, 2021).

3.2 Εκπαίδευση/ Μάθηση

Η εκπαίδευση του ατόμου ξεκινά να δίνει τις βάσεις για την ανάπτυξη ενός ατόμου με γνώσεις, ικανότητες, δεξιότητες και αξίες από πολύ νεαρή ηλικία, ώστε να μπορέσει να ενταχθεί στο κοινωνικό σύνολο. Ξεκινάει με την πρωτοβάθμια εκπαίδευση (νηπιαγωγείο, δημοτικό σχολείο), συνεχίζει με την δευτεροβάθμια (γυμνάσιο, λύκειο) και την τριτοβάθμια (ανώτατα εκπαιδευτικά ιδρύματα). Μέσα από την εκπαίδευση ο άνθρωπος μαθαίνει πως να διαχειρίζεται καινούργια δεδομένα και καταστάσεις με βάση αυτά που ξέρει ήδη. Όμως η μάθηση δεν έχει σημείο τερματισμού. Σε όλα τα στάδια της ζωής το άνθρωπος μαθαίνει και έτσι καταφέρνει να ανταπεξέλθει στις αντιξοότητες που προκύπτουν αλλά και να εξελίσσεται μέσα στην κοινωνία.

Στην εποχή μας, όπου η τεχνολογία κάνει αλματώδη βήματα χρειάζονται οι κατάλληλες ενέργειες για την παροχή δια βίου μάθησης σε όλους, ώστε να αποκτήσουν τις δεξιότητες και ικανότητες που απαιτούνται την τρέχουσα περίοδο. Η ανάπτυξη των ηλεκτρονικών δεξιοτήτων είναι μία από τις σημαντικότερες επενδύσεις επειδή συμβάλλει σε μεγάλο βαθμό στην ενίσχυση της ανταγωνιστικότητας, της καινοτομίας και της κοινωνικής συνοχής στην ευρωπαϊκή οικονομία σύμφωνα με την Ευρωπαϊκή επιτροπή το 2017. Στην Ελλάδα ωστόσο οι δείκτες για την ψηφιακή ικανότητα για το 2019 ήταν κάτω από το μέσο όρο της Ευρωπαϊκής Ένωσης σύμφωνα με τις εκθέσεις της Ψηφιακής Αγοράς. Επίσης η

συμμετοχή των ενηλίκων στη συνεχιζόμενη εκπαίδευση (προγράμματα "διά βίου μάθησης") εμφάνισαν χαμηλές επιδόσεις (Παναγιώταρου, 2020).

Οι τεχνικές διδασκαλίας είναι πολλές και διαφορετικές και εξαρτώνται από την εποχή, τους μαθητές, την χώρα ή και την πόλη, που εξετάζουμε. Οι πιο κλασικές/ παραδοσιακές τεχνικές είναι της εισήγησης ή διάλεξης, της παρουσίασης, του διαλόγου και των ερωτοαποκρίσεων. Όμως οι σημερινοί μαθητές, αποτελούν πρόκληση για τους καθηγητές τους. Από την μία πλευρά οι νεαροί μαθητές που μεγάλωσαν στην ψηφιακή εποχή, έχουν μάθει να επεξεργάζονται με άλλον τρόπο και ρυθμό τις πληροφορίες και από την άλλη οι ενήλικες έχουν κουραστεί από ενημερωτικές παρουσιάσεις και φυλλάδια για την ευαισθητοποίηση και την δια βίου μάθηση σε θέματα του εργασιακού τους περιβάλλοντος. Η ανάγκη υιοθέτησης εναλλακτικών τεχνικών μάθησης που θα τραβάει το ενδιαφέρον και θα αυξάνει τα κίνητρα των μαθητών είναι επιτακτική έτσι ώστε οι μαθησιακοί στόχοι να έχουν επιτυχία και η όλη διαδικασία να έχει νόημα.

Με τον κατάλληλο σχεδιασμό της μεθοδολογίας μάθησης όλες οι τεχνικές, από τις τυπικές αίθουσες διδασκαλίας μέχρι την εξ αποστάσεως μάθηση μπορούν να φέρουν τα επιθυμητά αποτελέσματα. Η ηλεκτρονική μάθηση μπορεί να προσφέρει ευελιξία μέσω της ασύγχρονης πρόσβασης στις μαθησιακές διαδικασίες χωρίς τον περιορισμό του τόπου, του χρόνου και του ρυθμού μάθησης. Η ενεργητική μάθηση στις τυπικές αίθουσες διδασκαλίας με την βοήθεια της τεχνολογίας όπως προσομοιώσεις, συζητήσεις, πειράματα, μελέτες περίπτωσης κ.α ενισχύουν και δίνουν μεγαλύτερο κίνητρο στους εκπαιδευόμενους. Γενικότερα, ο συνδυασμός διάφορων μαθησιακών μοντέλων, μικτές μέθοδοι μάθησης, είναι μια ελκυστική προσέγγιση (Παναγιώταρου, 2020).

Τέτοιες εναλλακτικές προσεγγίσεις χρειάζονται να ληφθούν υπόψη και για την ευαισθητοποίηση των ανθρώπων σε διάφορους τομείς που είναι απαραίτητοι για την ομαλή λειτουργία του κόσμου γενικότερα (περιβαλλοντικά ζητήματα), μιας κοινωνίας, μιας επιχείρησης ή ενός οργανισμού ειδικότερα. Η ευαισθητοποίηση δεν είναι εκπαίδευση, αλλά επικέντρωση της προσοχής σε ένα ζήτημα το οποίο είναι σημαντικό αλλά για ποικίλους λόγους δεν είναι αξιοπρόσεκτο από όλους και χρειάζεται να γίνει (Wilson, 2003). Μια προσέγγιση η οποία έχει συνεχή δράση ενημέρωσης και μάθησης θα δώσει την ευκαιρία στους εκπαιδευόμενους να αναπτύξουν δεξιότητες και ικανότητες ώστε να είναι σε θέση να αντιμετωπίσουν και να λύσουν πιθανά προβλήματα και πρωτόγνωρες καταστάσεις (Katsantonis, 2019).

Έτσι λόγω όλων αυτών των χαρακτηριστικών που απαρτίζουν την παιχνιδοποίηση και κυρίως χάρη στην άμεση αλληλεπίδραση των παικτών και στο στοιχείο της επιβράβευσης καθώς και στην ταχεία ανάπτυξη των βιντεοπαιχνιδιών έχει γίνει μια ευρέως γνωστή στροφή στις μελέτες για την αποτελεσματικότητα της στην τριτοβάθμια εκπαίδευση (Varannai, 2017) και όχι μόνο. Έχουν δημιουργηθεί ήδη πλαίσια, εδώ και αρκετό καιρό, για την καθοδήγηση στην κατασκευή και ανάλυση παιχνιδιών στην εκπαίδευση (Benjamin, 2007) αλλά και για έννοιες όπως το σύστημα ανταμοιβής που μπορεί να εφαρμοστεί σε διαφορετικά πλαίσια, γνωστά ως SAPS (Κατάσταση, Πρόσβαση, Ισχύς και Stuff) για την ανάπτυξη ανταγωνισμού μεταξύ των παικτών έτσι ώστε να παραμείνουν αφοσιωμένοι στο παιχνίδι και συνεχίζουν να διερευνώνται κι άλλα κίνητρα όπως η απολαβή δωρεάν αντικειμένων (Scholefield, 2019). Αποτελέσματα από πειράματα στην δευτεροβάθμια και τριτοβάθμια εκπαίδευση ήταν πολύ θετικά αφού παρατηρήθηκε πως μαθητές μετά την εκμάθησή τους με βιντεοπαιχνίδια είχαν βελτιώσεις στην κατανόηση, επιμέλεια, στα κίνητρα και στην κριτική σκέψη και περνούσαν

πιο ευχάριστα και ενδιαφέρουσα την ώρα τους συνδυάζοντας μάθηση και διασκέδαση (Benjamin, 2007; Fotaris, 2019).

Η μάθηση που βασίζεται σε παιχνίδια (game based learning, GBL) δημιουργεί ένα διασκεδαστικό, διαδραστικό και παρακινητικό περιβάλλον εκμάθησης που προωθεί την βιωματική μάθηση, εκμεταλλεύοντας τις τεχνολογίες και τις τεχνικές των παιχνιδιών. Έχει καθορισμένα μαθησιακά αποτελέσματα και έχει σχεδιαστεί για να εξισορροπεί το αντικείμενο της μάθησης με το παιχνίδι και την ικανότητα του παίκτη να διατηρεί και να εφαρμόζει το εν λόγω αντικείμενο στον πραγματικό κόσμο (Χριστοπούλου, 2021). Ένα ιδιαίτερο χαρακτηριστικό που την ξεχωρίζει από τις διαλέξεις/παραουσιάσεις είναι η δυνατότητα εξισορρόπησης της δυσκολίας ώστε να ταιριάζει με το επίπεδο ικανοτήτων των μαθητών κάνοντας την όλη εμπειρία μάθησης να είναι η βέλτιστη (Fotaris, 2019). Τα σοβαρά παιχνίδια εφαρμόζονται ήδη σε πολλούς τομείς (π.χ. υγειονομική περίθαλψη, άμυνα και διαχείριση) και έχει αποδειχθεί ότι μπορούν να αποτελέσουν αποτελεσματικά εκπαιδευτικά εργαλεία (Katsantonis, 2019).

Το γνωστό εκπαιδευτικό παιχνίδι Duolingo (για την εκμάθηση νέων γλωσσών) όπως και το ClassDojo (για γονείς και εκπαιδευτικούς που βοηθούν στη διδασκαλία των αναπτυξιακών δεξιοτήτων στα παιδιά) χρησιμοποιούν τεχνικές gamification. Ακόμα και σε πανεπιστημιακό επίπεδο έρευνα που έχει διεξαχθεί έβγαλε θετικά αποτελέσματα, παρατηρώντας ότι η «προσέγγισή τους στην gamification είναι αποτελεσματική σε πανεπιστημιακό περιβάλλον» αξιοσημείωτο είναι όμως πως η παιχνιδοποίηση πρέπει να εφαρμοστεί με προσεκτικό σχεδιασμό, για να διασφαλιστεί ότι είναι επωφελής (Scholefield, 2019). Τα δεδομένα δείχνουν πως στους χρήστες αρέσει η «εκμάθηση κατά εμπειρία» περισσότερο από τις εκπαιδεύσεις, παρουσιάσεις ή ακόμη και διαδικτυακά μαθήματα, γιατί έτσι μπορούν να εντοπίσουν τις δικές τους αδυναμίες και να αλλάξουν τις καθημερινές τους πρακτικές (Oroszi, 2019). Βλέποντας όλη αυτή την επιτυχία της παιχνιδοποίησης σε διάφορους τομείς φαίνεται πως έχει τη δυνατότητα να αξιοποιηθεί για να βελτιώσει την ευαισθητοποίηση, την μάθηση και την εκπαίδευση και σε θέματα ασφάλειας στον κυβερνοχώρο (Katsantonis, 2019; Scholefield, 2019).

3.3 Αρχές σχεδιασμού βιντεοπαιχνιδιών

Το παιχνίδι δεν είναι ένα αυθαίρετο κατασκεύασμα, αποτελείται από ένα πλήθος στοιχείων που το καθορίζουν και του δίνουν υπόσταση. Παιχνίδι είναι ένα κλειστό σύστημα με καθορισμένα όρια, κανόνες, στόχους, διαδικασίες και αποτελέσματα (Αναγνώστου, 2009). Τα στοιχεία από τα οποία αποτελείται μπορούν να χωριστούν στα δομικά και τα δραματικά. Τα δομικά καθορίζουν το περιβάλλον μέσα στο οποίο μπορεί να λειτουργήσει ένα παιχνίδι δίκαιο και ψυχαγωγικό και δημιουργούν ένα πρώτο πλαίσιο καθοδήγησης για τον σχεδιαστή που θέλει να αναπτύξει ένα παιχνίδι. Αυτά είναι η συμμετοχή των παικτών, ο στόχος, οι διαδικασίες, οι κανόνες, οι πόροι, η σύγκρουση, τα όρια και το αποτέλεσμα του παιχνιδιού. Οι παίκτες του παιχνιδιού μέσα από τις διαδικασίες που επιτρέπονται και την βοήθεια μέσω των πόρων που προσφέρονται προσπαθούν να εκπληρώσουν τους στόχους του παιχνιδιού. Τα δραματικά στοιχεία όπως η πρόκληση, η αίσθηση του παίξει, το υπόβαθρο/θέμα, ο κεντρικός ήρωας, η ιστορία/ σενάριο, είναι απαραίτητα στοιχεία για να αυξήσουν το ενδιαφέρον και την εμπλοκή του παίκτη στο παιχνίδι. Το πόσο εύκολη και φυσική φαίνεται η διαδικασία παιχνιδιού σε έναν παίκτη καθορίζει την ψυχαγωγική αξία του παιχνιδιού και την εμπειρία που αποκομίζει ο παίκτης από αυτό (Αναγνώστου, 2009).

Τα παιχνίδια μπορούν να ακολουθήσουν διάφορες τεχνικές κατά την δημιουργία τους. Κάποια παιχνίδια χρησιμοποιούν πλήρης και άλλα ημιτελής πληροφορία. Για μία δοκιμασία πλήρους πληροφορίας, στο παιχνίδι παρέχει όλη την απαραίτητη γνώση που απαιτείται για την επίλυση της και το περιβάλλον του παιχνιδιού/ πίστα είναι ορατό ολόκληρο (π.χ. σκάκι rac-man, space invaders). Ο παίκτης γνωρίζει τους κινδύνους ανά πάσα στιγμή. Από την άλλη πλευρά, μια δοκιμασία ημιτελούς πληροφορίας δεν παρέχει όλη την απαραίτητη γνώση για την αντιμετώπισή της έτσι ενισχύεται η αίσθηση του απρόβλεπτου και επιτρέπεται στον παίκτη να σχηματίσει τη δική του εικόνα για τον κόσμο βάσει της οποίας θα κινηθεί μέσα σε αυτόν.

Ακόμη για την επίτευξη του στόχου μπορεί ανάλογα το παιχνίδι να χρειαστούν γνώσεις από τον εξωτερικό κόσμο, που ο παίκτης έχει μάθει από την εκπαίδευσή του και από την εμπειρία του μέχρι να ξεκινήσει να παίζει, όπως η έννοια της βαρύτητας. Αλλιώς μπορεί να υπάρχει εσωτερική γνώση μέσω των προκλήσεων, που θα μάθει πράγματα τα οποία θα χρησιμοποιήσει στην πορεία του παιχνιδιού για την επίλυση επόμενων προκλήσεων και γρίφων, τα οποία ενδεχομένως μπορεί να αξιοποιήσει και στην πραγματική του ζωή.

Μία επιπλέον σχεδιαστική απόφαση είναι η επιλογή προκαθορισμένων ή ανακύπτουσων δοκιμασιών. Μία δοκιμασία μπορεί να προσδιοριστεί εκ των προτέρων από το σχεδιαστή του παιχνιδιού έτσι ώστε να έχει προκαθορισμένα και άμεσα τρόπο αντιμετώπισης (explicit). Σε ορισμένες περιπτώσεις σε δοκιμασίες δεν έχουν καθοριστεί επακριβώς από το σχεδιαστή η λύση του δεν είναι συγκεκριμένη και ακριβής (ανακύπτουσες, emergent). (Αναγνώστου, 2009)

Ένα παιχνίδι το οποίο έχει εξισορροπηθεί σωστά, έχει καθορισμένους στόχους, δεν περιλαμβάνει τίποτα μη σχετικό με την επίτευξη του στόχου που να διασπά την προσοχή, προσφέρει άμεση ανάδραση των ενεργειών και αποτελεί συνεχή πρόκληση μπορεί να εισάγει τον παίκτη σε μία κατάσταση που ονομάζεται ροή (flow). Η επίτευξη της ροής σε ένα παιχνίδι είναι απώτερος στόχος κάθε δημιουργού γιατί επιτυγχάνει έτσι το μέγιστο της ψυχαγωγικής αξίας του παιχνιδιού.

Για να κατορθώσει ένα παιχνίδι να μπλέξει τον παίκτη πρέπει συνεχώς να αποφεύγει να τον οδηγήσει σε κατάσταση ανίας ή σε κατάσταση εκνευρισμού, Πρέπει δηλαδή να τον κάνει να βρίσκεται συνεχώς μέσα στο επανομαζόμενο κανάλι ροής. Η δυσκολία του παιχνιδιού πρέπει να αυξάνεται σταδιακά, ανάλογα με την επιδεξιότητα του χρήστη, ώστε αυτός να βρίσκεται συνεχώς σε κατάσταση ροής και να αποκομίζει την καλύτερη δυνατή εμπειρία από το παιχνίδι (Αναγνώστου, 2009).

Ο Αμερικανός μυθολόγος, συγγραφέας και καθηγητής Τζόζεφ Κάμπελ (1904-1987), υποστήριξε ότι όλες οι αφηγήσεις αποτελούν παραλλαγές ενός ενιαίου μύθου (μονομυθία). Στο βιβλίο του "Ο ήρωας με τα χίλια πρόσωπα (1949)" μελετά μια τέτοια αρχετυπική δομή, η οποία είναι δυνητικά ανιχνεύσιμη σε κάθε ιστορία, ανεξαρτήτως του τόπου και του χρόνου δημιουργίας της. Αυτή η δομική αρχή ονομάστηκε από τον ίδιο «Ταξίδι του ήρωα». Η πρώτη πράξη αρχίζει με τον ήρωα να ζει στην ήσυχη και συνηθισμένη ζωή του και τελειώνει με το πρώτο βήμα του ταξιδιού, με το οποίο αρχίζει ουσιαστικά η περιπέτεια. Κατά τη διάρκεια της δεύτερης πράξης, ο ήρωας πέρνα όλες τις δοκιμασίες, γενικά όλα τα εμπόδια μέχρι να φτάσει στην τελική δοκιμασία και στην κορύφωση του δράματος. Υπερνικώντας και τη δοκιμασία αυτή, μπορεί να συλλέξει το τρόπαιο και να αρχίσει το δρόμο του γυρισμού, που σηματοδοτεί την αρχή της τρίτης και τελευταίας πράξης. Στην τρίτη πράξη το κακό ίσως να

κάνει μια τελευταία επανεμφάνιση ή μπορεί να συμβεί κάποια απρόσμενη τροπή στο σενάριο στο τέλος ο ήρωας επιστρέφει νικητής στον παλιό τρόπο ζωής κλείνοντας τον κύκλο του ταξιδιού. Στα περισσότερα παιχνίδια οι σχεδιαστές δίνουν μικρότερη σημασία στην πρώτη και τελευταία φάση, σε όφελος της δεύτερης στην οποία λαμβάνει χώρα όλη η δράση. Συνήθως κάποιος με εισαγωγικό βίντεο εισάγει τον παίκτη στην ιστορία και στη συνέχεια ο παίκτης καλείται να αναλάβει δράση (Αναγνώστου, 2009). Αυτό το πρότυπο ιστορίας χρησιμοποιείται σε πολλές τέχνες πέρα από τη συγγραφή μυθιστορημάτων, όπως σε ταινίες και μπορεί κάλλιστα να χρησιμοποιηθεί και για την δημιουργία σεναρίου για παιχνίδια.



Εικόνα 3. «Το ταξίδι του Ήρωα» και οι τρεις πράξεις μιας ιστορίας (Αναγνώστου, 2008)

Υπάρχουν πάρα πολλοί παράμετροι που πρέπει να ληφθούν υπόψη και καθορίζουν το στυλ του παιχνιδιού. Μεταξύ άλλων είναι το φύλλο, ηλικία, ο χρόνος που έχει το κοινό στη διάθεσή του για παιχνίδι, η κυρία πλατφόρμα παιχνιδιών που χρησιμοποιεί, καθώς και κουλτούρα και οι συνήθειες του συγκεκριμένου κοινού. Επίσης, η επιτυχία ενός παιχνιδιού κρίνεται από την διαχείριση, τον βαθμό δυσκολίας των προκλήσεων, τα τυχαία γεγονότα, την προβλεψιμότητα και την ποικιλία δοκιμασιών, συνολικά το χειρισμό του παιχνιδιού.

3.3.2 Στάδια παραγωγής ενός videogame

Για τον σχεδιασμό και την παραγωγή ενός ηλεκτρονικού παιχνιδιού απαιτείται συνεχής συνεργασία από πολλά διαφορετικά επιστημονικά πεδία. Τα βασικά στάδια παραγωγής ενός παιχνιδιού είναι τρία, το στάδιο προ της παραγωγής του, η παραγωγή του παιχνιδιού και το στάδιο μετά την παραγωγή (Rolling & Morris, 2004). (Πολύζου, 2019)

Ένα από τα βασικά μοντέλα δόμησης ενός ηλεκτρονικού παιχνιδιού περιλαμβάνει δύο βασικά στοιχεία, την εσωτερική μηχανική και τη διεπαφή του χρήστη. Η εσωτερική μηχανική, είναι οι κανόνες του συστήματος που ενθαρρύνουν τον παίκτη να περιηγηθεί και να εξερευνήσει τις δυνατότητες και τις επιλογές που έχει στο παιχνίδι, χρησιμοποιώντας τους ανατροφοδοτούμενους μηχανισμούς του παιχνιδιού (Koster, 2005). Πρόκειται, λοιπόν, για ένα μαθησιακό μοντέλο πάνω στο οποίο δομείται το λογισμικό του παιχνιδιού και μέσω αυτού καθορίζονται οι κανόνες, οι προκλήσεις και οι ενέργειες του χρήστη. Παράλληλα, η διεπαφή, που αναφέρεται συχνά και ως αναπαραστατικό επίπεδο, είναι το τμήμα μέσω του οποίου ο χρήστης έρχεται σε επαφή με το περιβάλλον του παιχνιδιού και αποτελεί το μέσο σύνδεσης του παίκτη και του παιχνιδιού. Στοχεύει στη ψυχαγωγία του χρήστη και μεσολαβεί

ανάμεσα στην εσωτερική μηχανική και το χρήστη μετατρέποντας τις προκλήσεις από τη μηχανική σε γραφικά οθόνης, ήχο κ.α. (Rollings A. Adams E, 2006). (Πολύζου, 2019)

Σε κάθε παιχνίδι ορισμένοι βασικοί και πιο ειδικοί παράγοντες επηρεάζουν την δομή και την οργάνωση τους. Οι βασικοί παράγοντες κάθε παιχνιδιού:

- έχει σκοπό, έχει κανόνες και επίπεδο δυσκολίας, που εξ' αρχής θα επηρεάσουν την πορεία του παιχνιδιού και θα ορίσουν τις ενέργειες και τους περιορισμούς που επιβάλλονται, όσο ο παίκτης ανταγωνίζεται μια άλλη οντότητα (άλλον παίκτη, υπολογιστή, τον εαυτό του ή τον χρόνο).
- οι παίκτες (ρόλους τους, τον αριθμό ατόμων που μπορούν να συμμετάσχουν, τα ονόματα που οι ίδιοι καθορίζουν και τις ομάδες που σχηματίζουν)
- η φαντασία και το κατά πόσο ο κόσμος του παιχνιδιού μοιάζει με τον πραγματικό, εφόσον τα περισσότερα παιχνίδια βασίζονται σε φανταστικά σενάρια που στοχεύουν να προσομοιάσουν ρεαλιστικές συνθήκες ειδικότεροι παράγοντες
- αφορούν στοιχεία απαραίτητου εξοπλισμού που απαιτούνται, οδηγίες (γενικές ή μέσα στη ροή του παιχνιδιού) που κατευθύνουν
- κυρώσεις ή ποινές που επιβάλλονται
- ρυθμίσεις και προεπιλογές που δύνανται να κάνει ο παίκτης ως προς το επίπεδο, την ταχύτητα, την εμφάνιση του
- καθώς και η ασφάλεια του παίκτη, αφού τα παιχνίδια προσφέρουν ένα ασφαλές περιβάλλον όπου ο παίκτης είναι σε θέση να δοκιμάσει ενέργειες που σε πραγματικό περιβάλλον ενδεχομένως να τον έθεταν σε κίνδυνο (Alessi & Trollip, 2001). (Πολύζου, 2019)

Οι παίκτες, όσο διαρκεί ένα παιχνίδι, καλούνται να βιώσουν τρεις διαφορετικές καταστάσεις τη ροή (flow, περιγράφεται ως μια κορυφαία εμπειρία που αφορά το αίσθημα που νιώθουν οι άνθρωποι κατά την πλήρη συμμετοχή τους σε μια ενέργεια), την εμβύθιση/απορρόφηση (immersion, η εμπειρία κατά την διάρκεια του παιχνιδιού, όπου ο παίκτης χάνει την αίσθηση του χρόνου, ενώ ταυτόχρονα ψυχαγωγείται) και την παρουσία (presence, αφορά το αίσθημα του να είσαι παρών σε ένα παιχνίδι και να εστιάζεις κατά κύριο λόγο στα τεχνολογικά χαρακτηριστικά του) (Πολύζου, 2019).

3.3.3 Κατηγορίες

Η κατηγοριοποίηση των βιντεοπαιχνιδιών συνεχώς μεταβάλλεται λόγω της ανάπτυξης ολοένα και περισσότερων βιντεοπαιχνιδιών με την κατηγοριοποίηση διαρκώς να μεταβάλλεται. Η κατηγοριοποίηση των ηλεκτρονικών παιχνιδιών δε βασίζεται στην αίσθηση και την εμπειρία που προκαλούν, αλλά στη δυναμική και την μηχανική του παιχνιδιού. Τα είδη και ο διαχωρισμός των παιχνιδιών περιγράφουν ένα σύνολο μηχανισμών, χωρίς ωστόσο αυτός ο διαχωρισμός να είναι ακριβής εφόσον οι μηχανισμοί κάθε παιχνιδιού είναι διαφορετικοί, και κάθε φορά δημιουργούν εντελώς διαφορετικές συνθήκες, εμπειρίες και ιστορίες (Πολύζου, 2019). Ενδεικτικά θα αναφέρω κάποιες κατηγοριοποιήσεις.

Υπάρχει κατηγοριοποίηση βάση του περιβάλλοντος του παιχνιδιού (παιχνίδια μάχης, παιχνίδια περιπέτειας, Εκπαιδευτικά παιχνίδια, παιχνίδια Γρίφων, First Person Shooters, παιχνίδια στρατηγικής, MMORPG' S (Massive multiplayer online role playing game), Αθλητικά παιχνίδια, παιχνίδια Προσομοίωσης, Παραδοσιακά παιχνίδια) όπως και κατάταξη με βάση την εξέλιξη του χώρου, με το αν ο χώρος δημιουργείται από τον παίκτη ή παιχνίδια όπου απλά ο παίκτης αλληλεπιδρά σε κάποιον έτοιμο χώρο (Πολύζου, 2019). Οι χώροι του

παιχνιδιού διαμορφώνονται αναλογικά με το τι θέλει να πετύχει ο σχεδιαστής και σύμφωνα με την αίσθηση που θέλει να αποδώσει.

Επιπλέον μπορεί να γίνει διαχωρισμός των παιχνιδιών με βάση την ιστορία και την αφήγηση. «Στα παιχνίδια όπου η ιστορία είναι γραμμική ο παίκτης καλείται να ολοκληρώσει ένα επίπεδο/πίστα έτσι ώστε να έχει νόημα η αφήγηση της ιστορίας που έχει δημιουργηθεί και να προχωρήσει στο επόμενο επίπεδο. Στα παιχνίδια μη γραμμικής ιστορίας υπάρχει ένας βαθμός ελευθερίας στους παίκτες, οι οποίοι μπορούν να κινηθούν προς πολλές διαφορετικές κατευθύνσεις και επιλογές. Η παράλληλη αφήγηση στο παιχνίδι δίνει διάφορες επιλογές και δυνατότητες στον παίκτη, οι οποίες όμως καταλήγουν στα ίδια σημεία που έχουν καθοριστεί από την αρχή σχεδιασμού. Η διακλαδωτή αφήγηση αποτελείται από πολλές γραμμικές αφηγήσεις και προσφέρει στον παίκτη επιλογές και δυνατότητες που διαμορφώνουν εντελώς διαφορετικά τις συνθήκες του παιχνιδιού. Τα open world (ελεύθερου χάρτη) παιχνίδια διαθέτουν ένα μεγάλο σε έκταση κόσμο/χώρο που βασίζεται σε μια ιστορία και άλλες δευτερεύουσες, όπου ο παίκτης δέχεται αποστολές και τις εκπληρώνει με όποια σειρά θελήσει. Ο παίκτης είναι ελεύθερος και οι ιστορίες αυτόνομες η μια από την άλλη με αποτέλεσμα ο χωρικός σχεδιασμός να είναι εκείνος που επηρεάζει και καθοδηγεί τον χρήστη» (Πολύζου, 2019).

3.4 Παιχνιδοποίηση και Ασφάλεια Υπολογιστών

Η εκπαίδευση στον τομέα της ασφάλειας στον κυβερνοχώρο είναι ένας αναπτυσσόμενος κλάδος, πόσο μάλλον και με χρήση τεχνικών παιχνιδοποίησης. Τα σοβαρά παιχνίδια και οι τεχνικές παιχνιδοποίησης αποτελούν μεγάλη ευκαιρία για την ενίσχυση της ευαισθητοποίησης και της εκπαίδευσης σε θέματα ασφάλειας για οποιοδήποτε κοινό (Katsantonis, 2019). Όλοι, με βάση τα σημερινά δεδομένα και το στάδιο που βρίσκεται και εξελίσσεται η τεχνολογία, είτε παιδιά (μαθητές σχολείου), είτε φοιτητές, είτε επιστήμονες, είτε εργαζόμενοι σε διάφορες επιχειρήσεις, εταιρείες ή οργανισμούς κτλ. πρέπει να είναι εφοδιασμένοι με τις κατάλληλες δεξιότητες για την πρόληψη, προστασία και απόκρουση των κινδύνων που εγκυμονούν διαρκώς στον κυβερνοχώρο. Μπορεί να αυξάνεται η αποτελεσματικότητα των μέτρων προστασίας για τα συστήματα και τις ευαίσθητες πληροφορίες που διαφυλάσσονται, όμως το ανθρώπινο στοιχείο εξακολουθεί να είναι ο αδύναμος κρίκος, καθώς οι άνθρωποι παραμένουν επιρρεπείς σε χειρισμούς τρίτων (Mouton, 2016).

Για να έχει ανταπόκριση μια συγκεκριμένη διδασκαλία μάθησης θα πρέπει οι εκπαιδευόμενοι να την αποδεχτούν και να την υιοθετήσουν. Έτσι προτάθηκε ένα ερευνητικό μοντέλο που στηρίζεται στο Μοντέλο Αποδοχής της Τεχνολογίας (TAM, Technology Acceptance Model) έτσι ώστε να εξετάσει τους παράγοντες και την πρόθεση των εκπαιδευομένων να χρησιμοποιήσουν ψηφιακά εργαλεία για την προσωπική ή επαγγελματική τους εξέλιξη. Μέσα από διάφορες μελέτες που χρησιμοποίησαν το TAM φαίνεται ότι υπάρχουν τέσσερις βασικές μεταβλητές οι οποίες δείχνουν την πρόθεση αξιοποίησης της νέας τεχνολογίας, η αντιληπτή χρησιμότητα (PU), ο βαθμός στον οποίο ένα άτομο πιστεύει ότι η χρήση ενός συστήματος θα βελτιώσει την απόδοσή του, η αντιληπτή ευκολία χρήσης (PEOU), ο βαθμός στον οποίο ένα άτομο πιστεύει ότι η χρήση ενός συστήματος θα είναι εύκολη, η πρόθεση χρήσης (IU) και η πραγματική χρήση (AU). Για τον έλεγχο αποδοχής περιβάλλοντος ψηφιακής μάθησης με παιχνίδι έγινε χρήση ενός εκτεταμένου μοντέλου TAM, όπου λήφθηκε επιπλέον υπόψη ο παράγοντας της διασκέδασης. Τα αποτελέσματα είναι πολύ θετικά γεγονός που δείχνει πως η

παιχνιδοποίηση θα μπορούσε να χρησιμεύσει στην βελτίωση της εκπαιδευτικής διαδικασίας αρκεί οι σχεδιαστές να επιλέξουν τους κατάλληλους μηχανισμούς της παιχνιδοποίησης (Παναγιώταρου, 2020).

Η μάθηση είναι μια εξελισσόμενη διαδικασία με στάδια την επίγνωση, την κατάρτιση και την εκπαίδευση. Η ευαισθητοποίηση απλώς τραβάει την προσοχή σε κάποιο συγκεκριμένο θέμα, δεν εκπαιδεύει πάνω σε αυτό (Wilson, 2003). Ο συνδυασμός της μάθησης και της ασφάλειας που είναι δύο θέματα τα οποία βρίσκονται συνεχώς σε μία ροή και δεν είναι στάσιμα συνεπάγονται και τις απαιτούμενες ενέργειες και προγράμματα τα οποία θα ανατροφοδοτούν συνεχώς τους εκπαιδευόμενους, κάτι το οποίο τα εκπαιδευτικά προγράμματα για την ασφάλεια στον κυβερνοχώρο δεν το έχουν πετύχει ακόμη. Όπως προαναφέρθηκε η μάθηση βάσει παιχνιδιών είναι ένα αναπτυσσόμενο πεδίο, και επειδή οι προσεγγίσεις που βασίζονται σε παιχνίδια στον κυβερνοχώρο δεν είχαν ένα κοινό πρότυπο μεθοδολογίας και σχεδιασμού ώστε να παρέχουν χρήσιμες πληροφορίες για τις δυνατότητες τέτοιων προσεγγίσεων δημιουργήθηκε το πλαίσιο COFELET. Αρχικά, μπορεί να βοηθήσει στην ανάπτυξη παιχνιδιών που έχουν ως σκοπό της καλύτερη εκπαίδευση στον κυβερνοχώρο ενσωματώνοντας σύγχρονες προσεγγίσεις μάθησης και εκπαίδευσης και αφετέρου να πραγματοποιήσει έναν βιώσιμο κύκλο ζωής της μάθησης (Katsantonis, 2019).

Ο Oroszi (2019) υιοθέτησε την ιδέα του δωματίου απόδρασης (escape room) στον χώρο της κυβερνοασφάλειας με ασκήσεις πάνω σε λάθος πρακτικές και συνήθειες που παρατήρησε πως κάνουν οι εργαζόμενοι, όταν δούλευε ως σύμβουλος ασφάλειας πληροφοριών, οι οποίες βασίζονται σε βασικές γνώσεις ασφάλειας πληροφοριών όπως για παράδειγμα ασθενείς και ισχυρούς κωδικούς πρόσβασης (passwords). Ισχυρίζεται πως ο καλύτερος τρόπος ευαισθητοποίησης των εργαζομένων είναι όταν βλέπουν τι κάνουν λάθος, (οι ίδιοι ή οι άλλοι) ή τι συμβαίνει όταν δεν έχουν τις απαιτούμενες γνώσεις ασφάλειας. Το δωμάτιο διαφυγής επιλέγεται με βάση το περιβάλλον της επιχείρησης ώστε να είναι πιο οικεία η κατάσταση και συνεπώς καλύτερη και η εμπειρία, μπορεί να είναι το γραφείο ενός βοηθού, προϊσταμένου κτλ. Απαραίτητη στη συγκεκριμένη θεματολογία δωματίου είναι η ύπαρξη και η χρήση υπολογιστή τόσο για απλές ενέργειες όπως το άνοιγμα αρχείων και η αναζήτηση όσο και για την αξιοποίηση εφαρμογών ασφάλειας αν οι εμπλεκόμενοι είναι πιο εξειδικευμένοι. Επίσης ως κίνητρο για περισσότερη συγκέντρωση στην όλη διαδικασία θα μπορούσε να είναι η χρήση ποινών όπου π.χ. εάν ανοιχτεί ένα κακόβουλο μήνυμα ηλεκτρονικού ταχυδρομείου να υπάρξει μείωση του διαθέσιμου χρόνου (Oroszi, 2019).

3.4.1 Προσεγγίσεις/ Υλοποιήσεις Παιχνιδοποίησης

Συνοψίζοντας, η κυβερνοασφάλεια είναι ένα θεμελιώδες θέμα στον σημερινό κόσμο του διαδικτύου. Για την υποστήριξη της ευαισθητοποίησης και της μάθησης στον τομέα αυτό αναγνωρίζεται ευρέως πως τα ηλεκτρονικά παιχνίδια και τεχνικές παιχνιδοποίησης είναι πολύτιμα εργαλεία (Παναγιώταρου, 2020). Έχουν γίνει αρκετές προσεγγίσεις και υλοποιήσεις σοβαρών παιχνιδιών σχετικά με την ασφάλεια στον κυβερνοχώρο που απευθύνονται σε παιδιά, νέους και ενήλικες εξειδικευμένων επαγγελματιών. Σχετίζονται με την ασφάλεια και προστασία της ιδιωτικής και επαγγελματικής ζωής, την χρήση ασφαλών κωδικών πρόσβασης, το ηλεκτρονικό ψάρεμα, κακόβουλο λογισμικό κτλ. Στη συνέχεια αναφέρονται κάποια από αυτά τα παιχνίδια.

Για παιδιά:

- η διαδικτυακή ακαδημία Webonauts, ένα διαδικτυακό παιχνίδι σχεδιασμένο για την εκπαίδευση των παιδιών σχετικά με τη διαδικτυακή εθιμοτυπία (Scholefield, 2019)

για νέους:

- το Cybersecurity Lab, σχεδιασμένο να διδάσκει στους νέους βασικές δεξιότητες στον κυβερνοχώρο μέσα από το ρόλο ενός Chief Technology Officer σε μια εταιρεία κοινωνικών μέσων ενημέρωσης, ο οποίος πρέπει να υπερασπιστεί την εφαρμογή ενάντια σε μια σειρά επιθέσεων.(Scholefield, 2019)
- GenCyber, μια σειρά καλοκαιρινών κατασκηνώσεων για μαθητές λυκείου που χρηματοδοτήθηκε από την Εθνική Υπηρεσία Ασφάλειας και το Εθνικό Science Ίδρυμα Επιστημών και διοργανώθηκαν στις ΗΠΑ για να αυξήσουν την ευαισθητοποίηση σχετικά με την ασφάλεια στον κυβερνοχώρο και να ενθαρρύνουν το ενδιαφέρον για υπολογιστές, καλύπτοντας θέματα όπως η ασφαλής διαδικτυακή συμπεριφορά και κοινωνική μηχανική(Scholefield, 2019).
- Το Be Internet Awesome (Google, 2017) είναι ένα online διαδικτυακό παιχνίδι που εισάγει θέματα που σχετίζονται με τις επιθέσεις ηλεκτρονικού "ψαρέματος" (phishing), την παρενόχληση στο Internet, την ασφάλεια των κωδικών πρόσβασης και άλλα θέματα ασφάλειας

για ενήλικες:

- για αξιωματικούς επιβολής του νόμου που παρακολουθούν ένα τόπο εγκλήματος.
- το Game of Threats, για τα μέλη του Διοικητικού Συμβουλίου οργανώσεων από τη Pwc για τον χειρισμό περιστατικών στον κυβερνοχώρο (Scholefield, 2019).
- Η δημιουργία ενός παιχνιδιού για την εκπαίδευση αστυνομικών στην ασφάλεια του κυβερνοχώρου αναπτύχθηκε από τον Coull N. et al. (2017).

για το ευρύ κοινό:

- NoPhish, εφαρμογή Android για κινητές συσκευές, για να βοηθήσει τους χρήστες στον εντοπισμό συνδέσμων ηλεκτρονικού ψαρέματος (Scholefield, 2019)
- παιχνίδι σε μορφή ερωτηματολογίου (με ερωτήματα τύπου RPG),ως μέρος μιας μελέτης το 2019 από τους Scholefield & Lynsay, για την πλατφόρμα Android για την εκπαίδευση των χρηστών σχετικά με την ασφάλεια του κωδικού πρόσβαση (Scholefield, 2019)
- Το CyberCIEGE, παιχνίδι για τη διδασκαλία εννοιών διασφάλισης πληροφοριών. Μπορεί να εφαρμοστεί σε ένα ευρύ φάσμα κοινών με διαφορετικά επίπεδα τεχνικής πολυπλοκότητας. Έχει τη δική του γλώσσα για τη δημιουργία νέων εκπαιδευτικών σεναρίων και συνοδεύεται από εργαλεία και μαθήματα που βοηθούν τους εκπαιδευτές να αναπτύξουν προσαρμοσμένα σενάρια (Benjamin, 2007)
- Οι Sharevski, Trowbridge & Westbrook το 2018 σχεδίασαν ένα εκπαιδευτικό πρόγραμμα που αφορούσε την ασφάλεια των IoT συσκευών.

3.4.2 Παρατήρηση άλλων παιχνιδιών εκπαίδευσης υπαλλήλων σε θέματα ασφάλειας

Σε προσεγγίσεις και υλοποιήσεις παιχνιδιών που έχουν γίνει για την ευαισθητοποίηση των υπαλλήλων επιχειρήσεων, ο χαρακτήρας που θα ελέγχει ο παίκτης μπορεί να έχει διάφορους ρόλους. Ο κεντρικός χαρακτήρας του παιχνιδιού μπορεί να έχει είτε τον ρόλο του επιτιθέμενου

(https://cybersecurity-escaperoom.nl/index_en.html, <https://one-conference.nl/news/innovation-floor>), είτε να είναι μέλος μιας ομάδας ερευνητών που έχουν ως σκοπό να εντοπίσουν παραβιάσεις ασφάλειας και να εξετάσουν μια πιθανή παραβίαση δεδομένων (<https://livingsecurity.com/products/escape-rooms/>), είτε τον εργαζόμενο μιας εταιρείας (<https://www.infosecure.com/security-awareness-game> , <https://securityintelligence.com/a-fun-and-educational-answer-to-the-security-awareness-pro>

[blem-the-security-escape-room/](#)). Σε κάθε περίπτωση ο παίκτης θα πρέπει να ολοκληρώσει τις απαραίτητες ενέργειες σε ένα δεδομένο περιβάλλον ώστε είτε να δημιουργήσει, κενά ασφαλείας ή να εκτελέσει επιθέσεις εάν είναι ο επιτιθέμενος, είτε να σώσει τον οργανισμό/ επιχείρηση από εσωτερικές ή εξωτερικές απειλές.

4. Μεθοδολογία και Σενάρια Παιχνιδιού

Για την πραγματοποίηση της παρούσας πτυχιακής εργασίας, αρχικά έγινε μια εκτενής μελέτη σε αντίστοιχες έρευνες και συστήματα που αφορούν την κυβερνοασφάλεια. Σε πρώτο στάδιο μελετήθηκαν οι απειλές και οι επιθέσεις που υπάρχουν στον κυβερνοχώρο και η σημασία της ασφάλειας σε αυτόν και σε επόμενο στάδιο ο ρόλος της ασφάλειας συγκεκριμένα σε επιχειρήσεις. Στη συνέχεια σχεδιάστηκαν κάποια ενδεικτικά σενάρια παιχνιδιού όπου το καθένα πραγματεύεται μία από τις πιο συνηθισμένες και συχνές απειλές που πλήττουν μια επιχείρηση. Μετέπειτα, έγινε έρευνα για την καταλληλότερη παιχνιδομηχανή και τέλος υλοποιήθηκε το παιχνίδι SAGE (Security Awareness Game for Employees) το οποίο υλοποιεί το πρώτο σενάριο για την ευαισθητοποίηση των παικτών στο ηλεκτρονικό ψάρεμα (phishing).

4.1.1 Πρόβλημα

Όπως συζητήθηκε στις προηγούμενες ενότητες αυτής της εργασίας, το κύριο πρόβλημα που θα αντιμετωπίσει το προτεινόμενο έργο είναι το ζήτημα ότι το ανθρώπινο σφάλμα εξακολουθεί να είναι η κύρια αιτία στις παραβιάσεις οργανωτικών δεδομένων. Αυτές οι παραβιάσεις μπορούν να μετριαστούν μέσω της σωστής εκτέλεσης της ευαισθητοποίησης και εκπαίδευσης των εργαζομένων αλλά πολλές εταιρείες δεν προσεγγίζουν την εκπαίδευση των εργαζομένων με αποτελεσματικό τρόπο. Η εκπαίδευση συχνά θεωρείται ως ένα συγκεκριμένο χρονικό διάστημα μία φορά τον χρόνο ή και λιγότερο που πρέπει να παρουσιαστούν κάποιες έννοιες. Οι υπάλληλοι δεν το βλέπουν ως κάτι θετικό το οποίο θα τους βοηθήσει να αναπτύξουν παραπάνω δεξιότητες αλλά ως κάτι χρονοβόρο το οποίο τους αποσπά την προσοχή από την καθημερινή εργασία τους που πρέπει να περατωθεί. Υπάρχουν πολλές μορφές προγραμμάτων κατάρτισης που μπορούν να υιοθετήσουν οι οργανισμοί, το καθένα με οφέλη και μειονεκτήματα (Cole, 2019). Η εκπαίδευση με βάση τεχνικές παιχνιδοποίησης φαίνεται να είναι η πιο αποδοτική από πλευράς ενδιαφέροντος, κινήτρου και αποτελεσματικότητας.

4.1.2 Λύση

Η λύση μου στο θέμα που περιγράφηκε παραπάνω είναι η ανάπτυξη ενός παιχνιδιού, το οποίο θα χρησιμοποιηθεί ως πρόγραμμα εκπαίδευσης και ευαισθητοποίησης σχετικά με την ασφάλεια που για τους υπαλλήλους των επιχειρήσεων. Το πρόγραμμα θα διαθέτει διαδραστικό ενότητες που μοιάζουν με παιχνίδια που θέτουν τον εργαζόμενο σε σενάρια που πιθανότατα θα είχαν συναντήσει και θα ξανασυναντήσουν στην πραγματική ζωή, προκειμένου να ενισχυθεί καλύτερα η πιο ασφαλής συμπεριφορά σε αυτές τις καταστάσεις. Για παράδειγμα κάποια θέματα ασφάλειας τα οποία θα επιχειρεί να επέμβει είναι η εξ αποστάσεως εργασία από δωμάτιο ξενοδοχείου ή καφετέρια, ο εντοπισμός και η αναφορά μιας επίθεσης κοινωνικής μηχανικής και η δημιουργία ισχυρού κωδικού πρόσβασης κτλ. Κάθε ενότητα θα έχει διαφορετικές έννοιες διδασκαλίας, παρουσιάζοντας στον εργαζόμενο καταστάσεις που μπορεί να βιώσει στην εργασία του. Το παιχνίδι θα έχει πολλαπλές διαδρομές ακολουθίας και ο εργαζόμενος θα έχει την δυνατότητα να ξεκινήσει ξανά από την αρχή. Αυτό τους επιτρέπει να ξαναζήσουν την κατάσταση, κάνοντας αυτή τη φορά τη σωστή επιλογή (Cole, 2019).

4.2 Σενάρια

Αφού εξετάστηκαν οι μέθοδοι που χρησιμοποιούνται σε υπάρχοντα βιντεοπαιχνίδια και ιστοσελίδες που προσφέρονται για την επιμόρφωση εργαζομένων σε επιχειρήσεις, δημιουργήθηκαν έξι σενάρια που προσομοιώνουν κάποιες από τις πιο συχνές απειλές και κινδύνους που ελλοχεύουν από κυβερνοεγκληματίες εις βάρος επιχειρήσεων. Ο παίκτης σε κάθε σενάριο, διαδραματίζει το ρόλο του υπαλλήλου μιας επιχείρησης και έρχεται αντιμέτωπος με διάφορες απειλές που είναι κρυμμένες στις περισσότερες καθημερινές του ενέργειες στο περιβάλλον εργασίας του. Τα σενάρια ασχολούνται με κάποιες βασικές έννοιες που θεωρώ πως όλοι οι εργαζόμενοι σε μια επιχείρηση και όχι μόνο, είναι απαραίτητο να γνωρίζουν. Καθ'όλη την διάρκεια της ροής του παιχνιδιού οι παίκτες θα ενημερώνονται για τους τρόπους που ενεργούν οι δράστες, τις διαφορετικές τακτικές προστασίας και αντιμετώπισης επικίνδυνων αυτών πράξεων και τον σημαντικό ρόλο που έχουν στην προστασία της επιχείρησής τους, σε όποια θέση κι αν βρίσκονται. Ακόμη στόχος του είναι να δείξει στους παίκτες πως μία επίθεση που μπορεί να λάβει χώρα στα πλαίσια της εργασίας τους δεν έχει συγκεκριμένη ώρα, μέρα, τόπο ή τρόπο. Ένα νέο τηλεφώνημα, ένα νέο μήνυμα ηλεκτρονικού ταχυδρομείου, μια μεταφορά ευαίσθητων δεδομένων από ανοιχτό σημείο πρόσβασης wifi και πολλά ακόμα καθημερινά πράγματα που προσομοιώνονται στο παιχνίδι μπορεί να μην γίνονται με καλές προθέσεις και ενδεχομένως να κρύβεται από πίσω, κάποια απειλή.

4.2.1 Σενάριο - Ηλεκτρονικό ψάρεμα

4.2.1.1 Εισερχόμενο email ηλεκτρονικού ψαρέματος

Το πρώτο σενάριο του παιχνιδιού έρχεται να κινητοποιήσει τον παίκτη ενάντια στην απειλή του ηλεκτρονικού ψαρέματος (phishing) για να τον βοηθήσει να κατανοήσει την έννοια του όρου. Επιλέχθηκε αυτή η απειλή ως το πρώτο σενάριο προσομοίωσης κακόβουλης ενέργειας, γιατί είναι μια από τις πιο γνωστές και συχνες απειλές μιας επιχείρησης ή ενός οργανισμού επειδή έχει να κάνει με τον ανθρώπινο δυναμικό της επιχείρησης. Ο τρόπος με τον οποίο ο κακόβουλος χρήστης έχει στήσει την παγίδα του είναι αρκετά απλός αλλά το μέγεθος των επιπτώσεων που μπορεί να επιφέρει στον υπάλληλο είναι μεγάλο και μπορεί για την επιχείρηση να είναι ακόμη και καταστροφικό. Έτσι, το παιχνίδι προσομοιώνοντας μία οθόνη υπολογιστή και μια πλατφόρμα ηλεκτρονικού ταχυδρομείου καλεί τον παίκτη να επιλέξει τι θα κάνει σε μία νέα πρόκληση, στη παραλαβή ενός νέου μηνύματος ηλεκτρονικού ταχυδρομείου στον επαγγελματικό του λογαριασμό. Φτάνοντας προς το τέλος του σεναρίου τον επιβραβεύει ή τον συμβουλεύει ανάλογα με το τελικό αποτέλεσμα του παιχνιδιού. Υπάρχει ένας μικρός σχολιασμός σχετικά με το πόσο καλά διαχειρίστηκε το νέο αυτό μήνυμα ηλεκτρονικού ταχυδρομείου όπως αν πιάστηκε στα δίκτυα του κακόβουλου αποστολέα ή αν έκανε κάποια ενέργεια αναφοράς στο Τεχνικό Τμήμα της επιχείρησης για να κάνουν κι αυτοί με την σειρά τους τις απαραίτητες ενέργειες. Τέλος συνοψίζει και του υποδεικνύει κάποια σημεία κλειδιά (αποστολέας, κείμενο, υπερσυνδέσμους, συνημμένα αρχεία, απάντηση) στα οποία θα πρέπει να δίνει ιδιαίτερη σημασία κάθε επόμενη φορά που θα δέχεται ένα νέο μήνυμα ηλεκτρονικού ταχυδρομείου. Καθ'όλη τη διαδικασία, ο παίκτης θα μάθει διαισθητικά πως ένας εισβολέας εκμεταλλεύεται την εμπιστοσύνη του, ώστε να μπορέσει να αναπτύξει μια πιο έντονη αίσθηση υπεράσπισης απέναντί τους. Σε κάθε κρίσιμη στιγμή που ο παίκτης πρέπει να κάνει κάποια ενέργεια το παιχνίδι τον ρωτάει ποιο είναι το επόμενο βήμα που κάνει, με την ερώτηση “τι θα κάνεις;”.

Ο παίκτης βρίσκεται στο γραφείο του και κάποια στιγμή βλέπει πως στο επαγγελματικό ηλεκτρονικό ταχυδρομείο έχει έρθει ένα νέο μήνυμα (e-mail) με αποστολέα κάποια εταιρεία/οργανισμό που συνεργάζεται με την εταιρία στην οποία δουλεύει. Στην προκειμένη περίπτωση ο αποστολέας του μηνύματος προσποιείται πως είναι από τον Ελληνικό Όμιλο Επιχειρήσεων, έναν οργανισμό με τον οποίο συνεργάζεται η επιχείρηση του. Ο παίκτης έχει την επιλογή είτε να ανοίξει το νέο μήνυμα και να το διαβάσει είτε να το αγνοήσει. Δεν του δίνεται η επιλογή να το διαγράψει για να δώσει τον χρόνο στον παίκτη, έστω σε επόμενη ερώτηση να το ανοίξει και να μπορέσει έρθει σε οπτική επαφή με ένα καλούπι ενός συνηθισμένου μηνύματος ηλεκτρονικού ψαρέματος. Στην περίπτωση που ο παίκτης επιλέξει να ανοίξει το καινούργιο e-mail που μόλις έλαβε, βλέπει πως του ζητάει να επαληθεύσει τα προσωπικά του στοιχεία πατώντας πάνω στον σύνδεσμο που είναι επισυναπτόμενος μέσα στο e-mail ή στο κουμπί που διαθέτει το μήνυμα, ώστε να συνδεθεί στην αντίστοιχη ιστοσελίδα. Το κίνητρο για να κάνει αυτά τα βήματα ο παίκτης είναι η ανανεωμένη πλατφόρμα στην οποία αν ξανακάνει σύνδεση θα μπορεί να είναι συνέχεια ενημερωμένος με όλα όσα έχουν να κάνουν με την επιχείρηση του (πελάτες, προϊόντα, συνεργάτες, προμηθευτές κ.τλ). Σε αυτό το σημείο ο παίκτης έχει τις εξής επιλογές: να ακολουθήσει τις οδηγίες, να αγνοήσει ή να διαγράψει το email, ή να πάρει λίγο ακόμα χρόνο να το σκεφτεί. Στην περίπτωση που επιλέξει τον περισσότερο χρόνο, οι επιλογές που έχει είναι οι ίδιες με πριν με επιπλέον επιλογή να μπορέσει να απευθυνθεί στο τεχνικό γραφείο της επιχείρησης (IT) προωθώντας το και τέλος, η επιλογή να επισκεφθεί την ιστοσελίδα που του ζητάνε στο email αλλά όχι πατώντας απευθείας πάνω στο σύνδεσμο που τον προτρέπουν, αλλά αντιγράφοντας τον σύνδεσμο σε ένα καινούργιο παράθυρο στον περιηγητή. Αν ο παίκτης αποφασίσει να πατήσει τον σύνδεσμο, οδηγείτε σε μία πλαστική ιστοσελίδα η οποία μοιάζει πολύ με την αυθεντική του αντίστοιχου οργανισμού τον οποίο προσποιείται. Έτσι αν ο παίκτης επιλέξει να συμπληρώσει τα προσωπικά του στοιχεία στην φόρμα που του παρουσιάζεται στην πλαστική ιστοσελίδα τότε ουσιαστικά παραχωρεί τα στοιχεία του στους κυβερνοεγκληματίες οι οποίοι μπορούν πλέον να τα χρησιμοποιήσουν για να αποσπάσουν χρηματικά πόσα, στοιχεία της εταιρείας ή τα προσωπικά του, ή και να εκδώσουν πιστωτικές κάρτες με το όνομά του.

4.2.1.2 Διάκριση μηνυμάτων ηλεκτρονικού ψαρέματος

Ένα ακόμη σενάριο εκπαίδευσης πάνω στην αναγνώριση επιθέσεων ηλεκτρονικού ψαρέματος έχει σχεδιαστεί, ώστε να μπορεί να γίνεται διάκριση μεταξύ ηλεκτρονικών μηνυμάτων ηλεκτρονικού ψαρέματος και συνηθισμένων επικοινωνιών μέσω ηλεκτρονικού ταχυδρομείου. Η ιδέα είναι ο παίκτης να εξετάσει τα μηνύματα ηλεκτρονικού ταχυδρομείου και να προσδιορίσει εάν είναι πραγματικά ή παραπλανητικά κάνοντας κλικ στις περιοχές που θεωρεί ύποπτες. Έτσι θα μάθει να αναγνωρίζει τα αναγνωριστικά ηλεκτρονικού ψαρέματος σε μηνύματα ηλεκτρονικού ταχυδρομείου όπως: επείγοντα περιστατικά, κακόβουλοι σύνδεσμοι, κακόβουλα συνημμένα, πλαστογραφία. Θα έχει ο παίκτης ως εργασία, μέσα από αρκετά εισερχόμενα email να ανιχνεύσει ποιά είναι phishing emails και ποιά είναι γνήσια. Κάθε email θα έχει έναν αριθμό. Θα πρέπει να διαχωρίσει τα μηνύματα ηλεκτρονικού ταχυδρομείου, ώστε να απομείνουν μόνο τα μηνύματα ηλεκτρονικού "ψαρέματος" και ένα σύνολο αντίστοιχων αριθμών. Για εκπαιδευτικούς σκοπούς, αυτοί οι αριθμοί μπορεί να είναι ο αριθμός τηλεφώνου της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος 11188 ή του εκάστοτε γραφείου τεχνικής υποστήριξης υπολογιστών της κάθε εταιρείας.

4.2.2 Σενάριο - Κωδικός πρόσβασης

4.2.2.1 Αφορμή επιλογής σεναρίου “Κωδικός πρόσβασης”

Το δεύτερο σενάριο αναφέρεται στον ασφαλή κωδικό πρόσβασης. Ο κωδικός πρόσβασης είναι μια από τις πιο γνωστές μορφές προστασίας και τον χρησιμοποιούμε όταν θέλουμε να κρατήσουμε ασφαλή κάτι σημαντικό για το οποίο δεν θέλουμε κάποιος τρίτος να έχει πρόσβαση για να το διαβάσει, να το τροποποιήσει ή να το εκτελέσει. Το γεγονός όμως ότι αυτή η τεχνική χρησιμοποιείται από πολύ παλιά, έχει δώσει την ευκαιρία σε κακόβουλος χρήστες να εντρυφήσουν πάνω στην λογική που χρησιμοποιεί ένας μέσος χρήστης για την δημιουργία ενός κωδικού. Μπορεί στις μέρες μας να χρησιμοποιείται συνδυασμός μεθόδων ταυτοποίησης, με κάτι που έχεις, είσαι ή ξέρεις, για την σύνδεση σε μία υπηρεσία ή προϊόν (two factor authentication, three factor authentication) όμως δεν παύει ο κωδικός πρόσβασης (κάτι που ξέρεις μόνο εσύ) να είναι ένα τα συστατικά αυτού του συνδυασμού τις περισσότερες αν όχι όλες τις φορές. Από τη μία πλευρά θέλουμε να έχουμε έναν σύνθετο κωδικό με συνδυασμό χαρακτήρων, αριθμών, σημειών στίξης κτλ. από την άλλη όμως θέλουμε έναν ξεχωριστό κωδικό για κάθε υπηρεσία κτλ. που να τον θυμόμαστε εύκολα ώστε να μην χρειάζεται να τον έχουμε κάπου γραμμένο και άθελά μας να πέσει στα χέρια τρίτων. Η σημασία της χρήσης διαφορετικών κωδικών θέλουμε να γίνει απόλυτα κατανοητή. Στην περίπτωση που χρησιμοποιούνται τα ίδια στοιχεία σύνδεσης (κωδικός, όνομα χρήστη ή email) σε πολλούς ή όλους τους λογαριασμούς που διαθέτει ένα άτομο μπορεί εύκολα κάποιος κακόβουλος χρήστης να εντοπίσει και να εκμεταλλευτεί κάποια ευπάθεια, σε μια από τις ιστοσελίδες που έχει λογαριασμό, και να την χρησιμοποιήσει για να υποκλέψει τα στοιχεία των χρηστών της. Έτσι αν χτυπήσει μια απλή ιστοσελίδα ή μπλοκ, θα αποκτήσει τα στοιχεία και για πιο σημαντικές, που εμπλέκουν ίσως και την επιχείρηση στην οποία εργάζεται. Συνεπώς, θεωρώ πως είναι απαραίτητη η αφιέρωση ενός σεναρίου για αυτό το θέμα, αφού ο καθένας μας, χρησιμοποιεί κωδικό πρόσβασης για να συνδέεται καθημερινά πια, στα κοινωνικά δίκτυα, για συναλλαγές με την τράπεζα, σε επαγγελματικές πλατφόρμες και πολλά ακόμη. Σκοπός του είναι η εκμάθηση του παίκτη στο να δημιουργεί έξυπνο και ισχυρό κωδικό (δύσκολα προβλέψιμο, εύκολα μνημονικό) μέσα από μια σειρά βημάτων, να αναδείξει την ανάγκη ανανέωσης του μετά από κάποιο χρονικό διάστημα και την σωστή διασφάλιση του για να μην διαρρεύσει. Αρχικά θα γίνει εκπαίδευση του χρήστη για την δημιουργία και χρήση ισχυρών κωδικών πρόσβασης.

4.2.2.2 Σενάριο

Ο παίκτης θα χρειαστεί να ανοίξει ένα σημειωματάριο (*notepad*) στον υπολογιστή του ώστε μέσα σε αυτό βήμα- βήμα να συνθέσει έναν ισχυρό κωδικό πρόσβασης.

Αρχικά, θα επισημαίνονται λέξεις οι οποίες καλό είναι να τις αποφεύγει, όπως αυτές που περιγράφουν προσωπικές πληροφορίες (το όνομά του, όνομα κατοικίδιου, ημερομηνίες γενεθλίων, αριθμοί τηλεφώνων) και πολύ συχνές λέξεις-φράσεις όπως *password1234*, *mom*, *dad*, *sunshine* κτλ. Η διαδικασία αυτή θα γίνει με οπτικοποιημένο τρόπο, παρουσιάζοντας κάποια εικονίδια που θα καλείται να επιλέξει και θα αντιπροσωπεύουν μία λέξη και στη συνέχεια θα επισημαίνεται το εικονίδιο αν είναι καλή επιλογή ή όχι. Τελικά, θα του προτείνεται να χρησιμοποιήσει για κωδικό πρόσβασης μία φράση, αντί για μία λέξη, της επιλογής του με τέσσερις-πέντε λέξεις για παράδειγμα (π.χ. στίχοι από το αγαπημένο του τραγούδι ώστε να μπορεί να το θυμάται), και αυτόματα και σταδιακά θα μετατρέπεται η φράση σε κωδικό.

- π.χ. το πρώτο γράμμα της κάθε λέξης θα γίνεται κεφάλαιο και θα αφαιρούνται τα κενά ανάμεσα στις λέξεις (Συντομογραφία που αποτελείται από τους πρώτους χαρακτήρες της φράσης / πρότασης)
- Θα αντικαθίστανται κάποια γράμματα με ειδικούς χαρακτήρες ή και αριθμούς, όπως το α με το παπάκι(@) ή το ς με το δολάριο (\$) και το ι με τον αριθμό ένα (1) (ή και με πιο σπάνιες αντικαταστάσεις)

Στη συνέχεια θα προστίθενται ενδιάμεσα δύο γράμματα παραδείγματος χάρη, που θα σχετίζονται με την ιστοσελίδα στην οποία θα αναφέρεται ο κωδικός έτσι ώστε να μάθει να χρησιμοποιεί ο παίκτης κάθε φορά ξεχωριστό κωδικό για διαφορετική υπηρεσία/εφαρμογή και ας έχουν παρεμφερή λειτουργία. Συνολικά το τελικό password θα πρέπει να έχει τουλάχιστον 8 χαρακτήρες/σύμβολα.

Επίσης θα επισημαίνεται πως αυτός ο κωδικός που δημιουργήθηκε, όσο καλός και αν είναι, δεν μπορεί να μείνει ο ίδιος για πάντα, θα πρέπει ο χρήστης να αλλάζει τον κωδικό πρόσβασης ανά τακτά χρονικά διαστήματα, (το λιγότερο μία φορά τον χρόνο).

Επόμενο ζήτημα εκπαίδευσης τη δημιουργία κωδικού, είναι ο τρόπος και το μέρος φυλάξης του. Ο παίκτης θα ερωτηθεί εάν θέλει να φυλάξει το νέο του κωδικό κάπου π.χ. στο γραφείο του με ένα Post it, σε μία ατζέντα, να το πει σε έναν φίλο ή συγγενή, ώστε τελικά να καταλάβει πως θα πρέπει απλά να το θυμάται από μόνος του εάν θέλει να είναι ασφαλής.

Ανάλογα με το τρόπο που θα επιλέξει ο παίκτης να αποθηκεύσει τον κωδικό αν συνεπάγεται μια πιθανή επίθεση θα πραγματοποιείται εκείνη την στιγμή, έτσι ώστε να αναγνωρίσει τους κινδύνους που εγκυμονούν από αυτή την απόφαση του. Για παράδειγμα αν επιλέξει να κρατήσει τον κωδικό του σε ένα χαρτάκι (post it) πάνω στην οθόνη του υπολογιστή του, τότε θα εμφανιστεί είτε ένας συναδελφος του είτε ένας πολίτης που έχει έρθει για να εξυπηρετηθεί από τον παίκτη, και θα κλέψει τον κωδικό πρόσβασης του απλά και μόνο διαβάζοντας το κομμάτι χαρτί με τον κωδικό πρόσβασης (looking over the user's shoulder). Αν βρεθεί τρόπος, θα αναπαρασταθούν κι άλλες επιθέσεις εκτός από το να τον κλέψουν, όπως brute force attack, dictionary attack, and hybrid method.

Επίσης θα τονιστεί, πως δεν θα πρέπει να ξεχνά να κάνει αποσύνδεση όταν τελειώνει την εργασία που κάνει σε μία διαδικτυακή υπηρεσία (ιδιαίτερα όταν βρίσκεται σε έναν “ξένο” υπολογιστή) και να βάζει σε λειτουργία ύπνου τον υπολογιστή την ώρα που κάνει διάλειμμα ή απομακρύνεται από αυτόν (clean desk πολιτική). Επιπλέον θα επισημανθεί πως καλό είναι να αποφεύγει την λειτουργία <<Remember me>>, όπου ο περιηγητής θυμάται τον κωδικό πρόσβασης μαζί με το username του λογαριασμού του χρήστη, στις ιστοσελίδες που επισκέπτεται. Τέλος, θα επισημανθεί πως όπου υπάρχει δυνατότητα 2-Step Authentication/ 2 factor να επιλέγεται γιατί προσφέρει επιπλέον επίπεδο προστασίας.

4.2.3 Σενάριο - Δημόσιο WiFi

4.2.3.1 Αφορμή επιλογής σεναρίου “Δημόσιο WiFi”

Εκπαίδευση του χρήστη για ασφαλή wifi σύνδεση. Το επόμενο σενάριο που σχεδιάστηκε, αφορά τα free hotspot και τις συνδέσεις WiFi σε δημόσιους χώρους. Είναι σύνηθες φαινόμενο στην εποχή μας να χρησιμοποιούμε τις φορητές συσκευές μας (smartphone, laptop, tablet) σε δημόσιους χώρους για επαγγελματικούς λόγους πέρα από επικοινωνιακούς και ψυχαγωγικούς, αφού μπορούμε να έχουμε πρόσβαση στο διαδίκτυο από οποιοδήποτε σημείο κι αν βρισκόμαστε είτε μέσω κινητής τηλεφωνίας (2G, 3G, 4G, 5G,...) είτε μέσω

ασύρματου δικτύου. Όμως όσον αφορά το κομμάτι του δωρεάν ασύρματου δικτύου είτε με κάποιον κωδικό πρόσβασης είτε χωρίς, κανείς δεν μπορεί να είναι σίγουρος για το ποιος το έχει στήσει ανεξαρτήτως του ονόματος του δικτύου που αναγράφεται. Σκοπός του σεναρίου αυτού είναι να βάλει τον παίκτη να δει κι άλλα πράγματα πίσω από μια δωρεάν και φαινομενικά ασφαλή σύνδεση δικτύου σε δημόσιο χώρο και ταυτόχρονα να αναδείξει τους κινδύνους που απειλούν την συσκευή του αν έχει δεν λάβει τα κατάλληλα μέτρα προστασίας.

4.2.3.2 Σενάριο

Το σενάριο έχει ως εξής: *Ήρθε η ώρα ο παίκτης να κάνει το διάλειμμα του κι έτσι πηγαίνει στο κυλικείο/ καφετέρια. Εκεί ανοίγει το wi-fi από το κινητό του για να σερφάρει στο Internet και να δει τις ειδοποιήσεις του από τα social media. Εκείνη την ώρα του τηλεφωνεί ο συνάδελφός του από το διπλανό γραφείο και του ζητά να προωθήσει ένα σημαντικό email της δουλειάς, για μία ενέργεια που έκαναν νωρίτερα μαζί. Οι επιλογές που έχει είναι να προωθήσει το email είτε χρησιμοποιώντας το προσωπικό του κινητό τηλέφωνο, είτε να επιστρέψει στο γραφείο του πριν ολοκληρώσει το διάλειμμα του, για να χρησιμοποιήσει τον σταθερό υπολογιστή. Τελικά αν του απαντήσει πως θα του το προωθήσει αμέσως αφού μπορεί να σκέφτεται πως μπορεί να μπει γρήγορα από το κινητό του εκείνη τη στιγμή. Έτσι κοιτάζει τα διαθέσιμα δίκτυα με τα οποία μπορεί να πραγματοποιήσει σύνδεση μέσω wi-fi. Ανάμεσα στα διαθέσιμα δίκτυα υπάρχει το όνομα της καφετέριας δύο φορές, μία με πεζά και μία με κεφαλαία γράμματα και τα δύο δίκτυα wi-fi δεν απαιτούν κωδικό πρόσβασης. Θα πρέπει ο παίκτης να αποφασίσει εάν θα επιλέξει ένα από τα δύο δίκτυα wi-fi στην τύχη για να συνδεθεί ή αν θα ρωτήσει τον υπάλληλο του μαγαζιού για το ποιο είναι το σωστό. Το ένα δίκτυο WiFi έχει κλωνοποιήσει το πραγματικό και αξιόπιστο δίκτυο της καφετέριας και ενώ φαίνεται νόμιμο έχει δημιουργηθεί από κάποιον επιτιθέμενο/χάκερ. Ο εισβολέας μπορεί να υποκλέψει τα δεδομένα που μεταφέρονται μεταξύ των δύο συστημάτων. Αυτή η επίθεση ονομάζεται Man In The Middle, και τα δεδομένα που αποστέλλονται από τον παίκτη στον συνάδελφο του μέσω του μη ασφαλούς δικτύου πλέον μπορούν να κλαπούν από τον χάκερ ο οποίος είναι ο ιδιοκτήτης του δικτύου απλά και μόνο παρακολουθώντας τα πακέτα - δεδομένα που μεταδίδονται μέσα από αυτό το δίκτυο. Έτσι ο χάκερ έχει πλέον πρόσβαση σε προσωπικά δεδομένα της εταιρείας και μπορεί να τα εκμεταλλευτεί είτε άμεσα είτε στο μέλλον αφού συλλέξει κι άλλες πληροφορίες και στοιχεία για μεγαλύτερο δικό του όφελος που συνεπάγεται μεγαλύτερο κίνδυνο για την εταιρεία.*

Πέρα από την παρακολούθηση και καταγραφή των δεδομένων που κινούνται στο διαδίκτυο από κάποιον τρίτο, μπορεί να μολυνθεί και η συσκευή που χρησιμοποιήθηκε για την σύνδεση σε αυτό το δίκτυο, πιο ευκολα σε δίκτυα κάτω από αυτές τις συνθήκες μέσω διάφορων κακόβουλων προγραμμάτων, αρχείων λήψης και ψεύτικων διαφημίσεων, ειδικά εάν δεν έχει και η συσκευή εγκατεστημένα προγράμματα προστασίας όπως antivirus, firewall, antimalware κτλ.

4.2.4 Σενάριο - Κοινωνική Μηχανική

4.2.4.1 Αφορμή επιλογής σεναρίου “Κοινωνική Μηχανική”

Το τέταρτο σενάριο θέλει να ενημερώσει τον παίκτη σχετικά με την κοινωνική μηχανική (social engineering). Η κοινωνική μηχανική βασίζεται στο γεγονός πως τις περισσότερες φορές τον υπολογιστή τον χειρίζεται ο άνθρωπος. Κακόβουλοι χρήστες έχουν μελετήσει την ανθρώπινη ψυχολογία και συμπεριφορά για να εκμεταλλευτούν τις ανθρώπινες αδυναμίες

και συναισθήματα (εξυπηρέτηση, εμπιστοσύνη, απειρία, περιέργεια, ανάγκη, φόβος κ.α.) με απώτερο σκοπό να “ψαρέψουν” πληροφορίες των ίδιων αλλά και της επιχείρησης στην οποία εργάζονται. Υπάρχουν πολλές τεχνικές για την εφαρμογή της κοινωνικής μηχανικής από χάκερ με πιο γνωστή αυτή του ηλεκτρονικού ψαρέματος που είδαμε και στο πρώτο σενάριο. Μπορούν να επιτύχουν τον σκοπό τους όχι μόνο χρησιμοποιώντας έναν υπολογιστή ασύγχρονα αλλά και άμεσα, όπως μέσω τηλεφώνου. Στόχος αυτού του σεναρίου, είναι η ανάδειξη του φαινομένου αυτού και τα στάδια από τα οποία αποτελείται (έρευνα για το θύμα, ανάπτυξη σχέσεων και εμπιστοσύνης, εκμετάλλευση εμπιστοσύνης και χρήση πληροφοριών). Πολύ σημαντικός στόχος ο οποίος θα βοηθήσει να ενημερωθούν οι υπάλληλοι μιας επιχείρησης έτσι ώστε να μπορέσει και η ίδια η επιχείρηση να μετριάσει τους εσωτερικούς κινδύνους από το ανθρώπινο δυναμικό της, αφού όπως έχουμε ξαναφέρει η ευαισθητοποίηση, η ενημέρωση και η εκπαίδευση των υπαλλήλων είναι από τα πρώτα μέτρα προστασίας που πρέπει να εφαρμόζονται σε κάθε επιχείρηση.

4.2.4.2 Σενάριο

Το σενάριο εξελίσσεται ως εξής: ο παίκτης κάθεται στο γραφείο του και κάποια στιγμή χτυπάει το σταθερό τηλέφωνο. Στο τηλέφωνο είναι ένας επιτιθέμενος χρήστης που υποδύεται εκπρόσωπο από κάποιον οργανισμό και χρησιμοποιώντας πλαστές ειδήσεις προσπαθεί να παραπλανήσει τον παίκτη για να κερδίσει την εμπιστοσύνη του και να πάρει στοιχεία που υπο κανονικές συνθήκες δεν δικαιούται. Σηκώνει το τηλέφωνο και ο επιτιθέμενος ισχυρίζεται πως καλεί από το “Κεντρικό Τμήμα Ασφάλειας Ηλεκτρολογικών Υπολογιστών” και λόγω του τελευταίου περιστατικού κυβερνοεπίθεσης που έδειξαν υποτίθεται και οι ειδήσεις, χρειάζονται την βοήθεια του ώστε να δουν αν ο υπολογιστής του, έχει κάποια συγκεκριμένα χαρακτηριστικά παρόμοια με των υπολογιστών που δέχτηκαν την επίθεση. Αρχίζουν να τον ρωτάνε για διάφορα πράγματα ώστε να αποκτήσουν πληροφορίες που δεν θα έπρεπε να έχουν, προσπαθώντας να του δείξουν πως τον εμπιστεύονται και πως μόνο αυτός μπορεί να τους βοηθήσει να εκτελέσουν το έργο τους. Επιπλέον, τον καθοδηγούν σε διάφορα μονοπάτια (path) μέσα στον υπολογιστή ώστε τελικά να τους αποκαλύψει έμπιστες πληροφορίες και δεδομένα. Προτού κάνουν το τηλεφώνημα έχουν κάνει βαθιά έρευνα κυρίως για την επιχείρηση στην οποία εργάζεται αλλά και ειδικότερα για αυτόν από τα προσωπικά του προφίλ στα κοινωνικά δίκτυα κτλ. ώστε να κάνουν πιο στοχευμένες ερωτήσεις και να αντλήσουν πιο γρήγορα χωρίς να τους αντιληφθεί, τα δεδομένα που αναζητούν. Τελικά μέσα από τις κινήσεις που θα κάνει ο παίκτης θα φανεί αν τα κατάφερε ο επιτιθέμενος να έχει πρόσβαση σε ευαίσθητα δεδομένα της εταιρείας.

4.2.5 Σενάριο - Ransomware μέσω USB

4.2.5.1 Αφορμή επιλογής σεναρίου “Ransomware μέσω USB”

Αυτό το σενάριο έχει στόχο να ενημερώσει τον χρήστη για τα κακόβουλα λογισμικά. Συγκεκριμένα για το ransomware με μέσο μετάδοσης usb flash drive (usb stick). Το ransomware είναι ένα είδος κακόβουλου λογισμικού ηλεκτρονικών υπολογιστών, που κρυπτογραφεί τα αρχεία ή/και μπλοκάρει την πρόσβαση στο σκληρό δίσκο, ζητώντας χρήματα (λύτρα) για να τα ελευθερώσει. Ορισμένοι τύποι κακόβουλου λογισμικού - όπως ransomware και worms - μπορούν να διαδώσουν και να μολύνουν όλους τους υπολογιστές που είναι συνδεδεμένοι στο ίδιο δίκτυο. Η καλύτερη άμυνα απέναντι σε αυτή την απειλή, αφενός είναι να δημιουργούνται αντίγραφα ασφαλείας, σε κάποιο εξωτερικό δίσκο, που δεν

είναι μόνιμα συνδεδεμένος στον υπολογιστή και αφετέρου ο στόχος αυτού του σεναρίου. Δηλαδή, η ενημέρωση των χρηστών ώστε να μην φτάσουν τα λογισμικά αυτά καν στον υπολογιστή τους για να χρειαστούν τα αντίγραφα ασφαλείας. Το σενάριο αναπαριστά την εύρεση άγνωστης προέλευσης usb flash drive κοντά στον χώρο εργασίας του υπαλλήλου και την επιπόλαια εισαγωγή του σε συσκευή της επιχείρησης του με αποτέλεσμα το κλείδωμα πολύτιμων αρχείων και την απαίτηση λύτρων για την αποκρυπτογράφηση των αρχείων και την ανεμπόδιστη πρόσβαση σε αυτά.

4.2.5.2 Σενάριο

Καθώς φτάνει το πρωί στη δουλειά, λίγο έξω από την εξωτερική κεντρική πόρτα του κτιρίου της επιχείρησης, παρατηρεί πως είναι πεσμένο ένα usb stick χωρίς κάποια ετικέτα ή κάποιο άλλο διακριτικό. Η πρώτη σκέψη που του έρχεται είναι μήπως ανήκει σε κάποιον συνάδελφο του, αλλά δεν ξέρει σε ποιον να απευθυνθεί. Αντί να το πάει στο τεχνικό τμήμα και να το αφήσει εκεί διαλέγει να το πάρει μαζί του στο γραφείο και να το βάλει στον υπολογιστή του, έτσι ώστε να το διαβάσει και να αναγνωρίσει αν ανήκει σε κάποιον συνάδελφο του ή όχι. Μόλις ο παίκτης/θύμα τοποθετήσει το άγνωστο USB stick σε ένα μηχάνημα, το κακόβουλο λογισμικό που υπάρχει σε αυτό θα εγκατασταθεί αυτόματα. Κάποια από τα συμπτώματα που προκύπτουν και θα φανούν στην οθόνη του παίκτη, είναι η διπλή επέκταση σε αρχεία (.jpg.vbs ή *.gif.exe), η αργή λειτουργία κατά την εκκίνηση του υπολογιστή, η έλλειψη ανταπόκρισης της διαχείρισης εργασιών των Windows, η διακοπή της λειτουργίας προγραμμάτων ακόμα και μετά την διαγραφή τους και την επανεγκατάστασή τους, η εμφάνιση ενοχλητικών μηνυμάτων και διαφημίσεων που δεν τα επέλεξε ο χρήστης, η αλλοίωση των δεδομένων, εφαρμογών και αρχείων του συστήματος ή η διαγραφή αυτών, η έλλειψη διαθεσιμότητας πόρων χωρίς λογική αιτία και η αναστολή ή δυσλειτουργία του συστήματος, κ.α. Πλέον, δεν έχει πρόσβαση στα αρχεία του, τα οποία λόγω της θέσης του στην επιχείρηση, είναι σημαντικά για την λειτουργία της. Οι υπεύθυνοι για αυτή την επίθεση “εμφανίζονται” τώρα, για να ικανοποιήσουν τον απώτερο σκοπό τους που είναι η απόσπαση χρημάτων από το θύμα/θύματα και όχι η καταστροφή του υποκείμενου λειτουργικού συστήματος ή η αποθήκευση των δεδομένων. Έτσι, ως αντάλλαγμα, ώστε να αντιστρέψουν την διαδικασία και να επαναφέρουν το σύστημα στην κατάσταση που βρισκόταν πριν την εισαγωγή του μολυσμένου usb stick, ζητάνε λύτρα από την επιχείρηση και ο παίκτης βρίσκεται σε πολύ δύσκολη θέση.*

4.2.6 Σενάριο - Ιδιωτικότητα και GDPR

4.2.6.1 Αφορμή επιλογής σεναρίου “Ιδιωτικότητα και GDPR”

Σενάριο για εκπαίδευση του χρήστη σε θέματα ιδιωτικότητας με έμφαση σε μερικά σενάρια εφαρμογής του Γενικού Κανονισμού για την Προστασία των Δεδομένων 2016/679 ο οποίος είναι στην νομοθεσία της ΕΕ για την προστασία των δεδομένων και την ιδιωτικότητα στην Ευρωπαϊκή Ένωση και στον Ευρωπαϊκό Οικονομικό Χώρο. Κάθε επιχείρηση είναι υπεύθυνη για την ασφάλεια των δεδομένων των πελατών αλλά και των εργαζομένων της. Δεδομένα όπως το όνομα, το email, την ip διεύθυνση, την ηλικία κτλ.. Το Gdpr ειδικότερα προστατεύει ευαίσθητα προσωπικά δεδομένα όπως ιατρικά αρχεία, εισοδήματα, πολιτικές και θρησκευτικές πεποιθήσεις κτλ. Κύριος σκοπός του σεναρίου είναι η αναγνώριση του είδους των δεδομένων που διαχειρίζεται η επιχείρηση προσομοίωσης, η μεταβίβαση δεδομένων σε τρίτους και η σωστή μεταφορά τους.

4.2.6.2 Σενάριο

Η επιχείρησή του παίκτη ελέγχει όλα αυτά τα δεδομένα (είναι data Controller) των υποκειμένων (data subject) που ανήκουν τα δεδομένα. Αρχικά, θα πρέπει να κατηγοριοποιήσει δεδομένα (data categorization) που θα του εμφανιστούν, σε προσωπικά και ευαίσθητα προσωπικά δεδομένα με βάση τον ορισμό στον Γενικό Κανονισμό Προστασίας Δεδομένων. Στη συνέχεια για να γίνει πλήρως αντιληπτό το ότι ευαίσθητες και προσωπικές πληροφορίες/δεδομένα δεν πρέπει να δίνονται σε τρίτους οι οποίοι δεν έχουν την δικαιοδοσία, θα έρχεται ένα χαρακτήρας ο οποίος είτε θα είναι συνάδελφος είτε θα είναι κάποια τρίτη οντότητα, ξένη για την επιχείρηση και θα ζητάει βοήθεια αναζητώντας πληροφορίες είτε για κάποιο συγκεκριμένο πελάτη είτε για ένα σύνολο αυτών. Εάν δεν έχει εξακριβωθεί η ταυτότητα του παραλήπτη δεν πρέπει ο παίκτης να μεταβιβάσει τα δεδομένα αλλά ταυτόχρονα πρέπει να ζητήσει και τον συγκεκριμένο λόγο για τον οποίο του ζητάει τα δεδομένα για επεξεργασία. Έστω, πως έγινε αυθεντικοποίηση του προσώπου που ζητάει την πληροφορία, δεν μπορεί να του αποστείλει τα δεδομένα με οποιονδήποτε τρόπο. Ο παίκτης θα πρέπει να διαλέξει το κατάλληλο μέσο μεταφοράς. Υψηλού κινδύνου πληροφορίες δεν πρέπει να μεταφέρονται με fax, ακόμα και αν υπάρχει κάποιος νόμιμος λόγος για τη μεταφορά τους. Ακόμη, θα πρέπει να μεταφέρονται με ιδιαίτερη προσοχή μόνο οι σχετικές πληροφορίες και όχι ένα σύνολο που μέσα σε αυτές είναι οι σχετικές. Επίσης, το USB δεν είναι και τόσο ασφαλές όποτε δεν θα πρέπει να το επιλέξει, ειδικά όταν είναι μη κρυπτογραφημένο και μπορεί να χαθεί ή να χαθούν τα δεδομένα που είναι αποθηκευμένα σε αυτό εάν δεν χρησιμοποιηθεί με ιδιαίτερη προσοχή.

Στη συνέχεια θα επισημανθεί μέσα από το σενάριο, πως δεν θα πρέπει να αποσπάται η προσοχή του παίκτη/υπαλλήλου από την εργασία του, όπως και ότι πρέπει να είναι κάθε στιγμή σε ετοιμότητα αφού δεν μπορεί να γνωρίζει με βεβαιότητα ποιον έχει απέναντί του και τον απώτερο σκοπό αυτού.

Την ώρα που έρχεται ένας υποτιθέμενος πελάτης για εξυπηρέτηση (με κακόβουλο σκοπό), τηλεφωνεί στον παίκτη ένα κοντινό του πρόσωπο π.χ. το παιδί του, και αφού το χαιρετήσει και μιλήσουν για ότι χρειαζόταν κλείνει το τηλέφωνο και συνεχίζει τη δουλειά του. Κατά τη διάρκεια της κλήσης όμως μπορεί είτε άθελά του να διέρευσε δικές του προσωπικές πληροφορίες που μπορεί να βοηθήσουν στην αποκάλυψη π.χ. κάποιου κωδικού πρόσβασης, είτε ο πελάτης κρυφοκοίταξε την οθόνη του υπολογιστή του την ώρα που είχε υπό επεξεργασία ευαίσθητα προσωπικά δεδομένα.

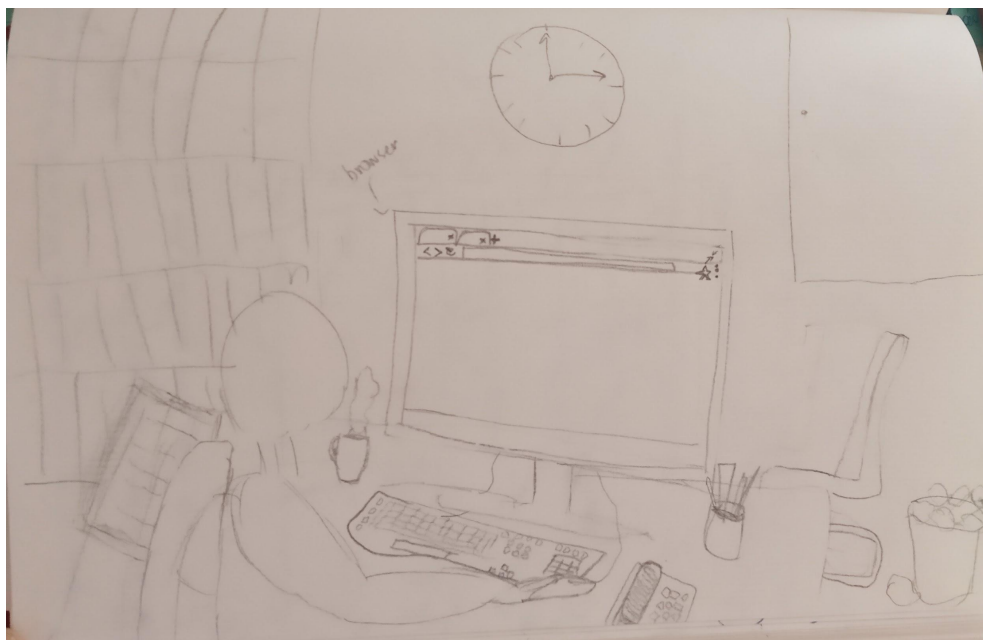
Τέλος ανάδειξη της σημασίας πλήρους διαγραφής όλων των στοιχείων που υπάρχουν σε μια επαγγελματική συσκευή πριν την απόσυρση της. Το σενάριο τελειώνει ως εξής: σε επόμενη στιγμή ο υπολογιστής του παίκτη κρασάρει για άλλη μία φορά, είναι ώρα να τον αντικαταστήσει με έναν καινούργιο. Τον βγάζει έξω από το γραφείο του ώστε να γίνει πλήρως αντιληπτό ότι χρειάζεται εδώ και τώρα έναν καινούργιο υπολογιστή για να συνεχίσει να εργάζεται και ότι δεν μπορεί να πάρει άλλο παράταση. Πριν τον αποχωριστεί, μεταφέρει όλα τα δεδομένα που χρειάζεται σε ένα USB stick, σβήνει όλα τα υπόλοιπα και τον απομακρύνει από το γραφείο του. Με αυτό τον τρόπο πιστεύει ότι ο υπολογιστής είναι έτοιμος για τον κάδο της ανακύκλωσης όμως στην πραγματικότητα με τη διαγραφή που έκανε στα αρχεία δεν σημαίνει πως τα αρχεία αυτά δεν είναι προσβάσιμα πλέον από τρίτους αν το επιθυμούν.

5. Security Awareness Game for Employees (SAGE)

Το όνομα που επιλέχθηκε για το παιχνίδι είναι «Security Awareness Game for Employees» το οποίο για λόγους ευκολίας θα αναφέρεται ως SAGE. Η γενική ιδέα του παιχνιδιού είναι ότι ο παίκτης είναι ο πρωταγωνιστής και βρίσκεται στο γραφείο που εργάζεται και πρέπει να διαχειριστεί διάφορες προκλήσεις. Το παιχνίδι είναι click-based ή point & click και απευθύνεται σε επιχειρήσεις οι οποίες αναζητούν έναν εναλλακτικό, ενδιαφέρον και αποτελεσματικό τρόπο για να ευαισθητοποιήσουν κυρίως, αλλά και για να ενημερώσουν και να εκπαιδεύσουν τους υπαλλήλους τους σε θέματα ασφάλειας στον κυβερνοχώρο ώστε να ελαχιστοποιήσουν τους κινδύνους που προέρχονται από τον ανθρώπινο παράγοντα. Σχεδιάστηκε χρησιμοποιώντας τη παιχνιδομηχανή ανοιχτού κώδικα, Godot 3 και το πρόγραμμα σχεδιασμού διανυσματικών γραφικών, Inkscape. Ο παίκτης στη πορεία του παιχνιδιού, χρειάζεται να κάνει τις κατάλληλες στρατηγικές επιλογές ώστε να αντιμετωπίσει μια ενδεχόμενη επίθεση. Το σενάριο είναι ημιτελούς πληροφορίας για να επιτρέψει στον παίκτη να σχηματίσει τη δική του εικόνα για το περιβάλλον βάσει της οποίας θα κινηθεί και αναλόγως.

5.1.1 Αρχικές Σκέψεις

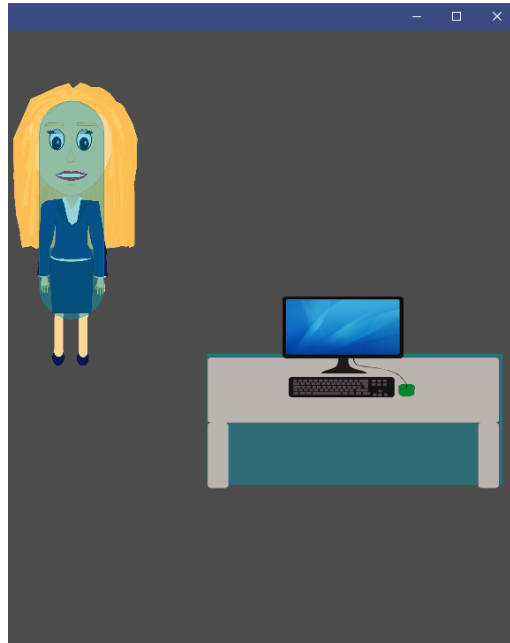
Στην αρχή σχεδιάστηκαν με χαρτί και μολύβι κάποιες πρώτες ενδεικτικές σκηνές για το περιβάλλον του παιχνιδιού. Η αρχική ιδέα ήταν να γίνει ένα παιχνίδι τύπου escape room όπου ο παίκτης θα μπορούσε να βλέπει και να χειρίζεται τον κεντρικό χαρακτήρα (πρωταγωνιστή) του παιχνιδιού.



Εικόνα 4. Πρώτη ενδεικτική σκηνή του παιχνιδιού (σχέδιο στο χαρτί)

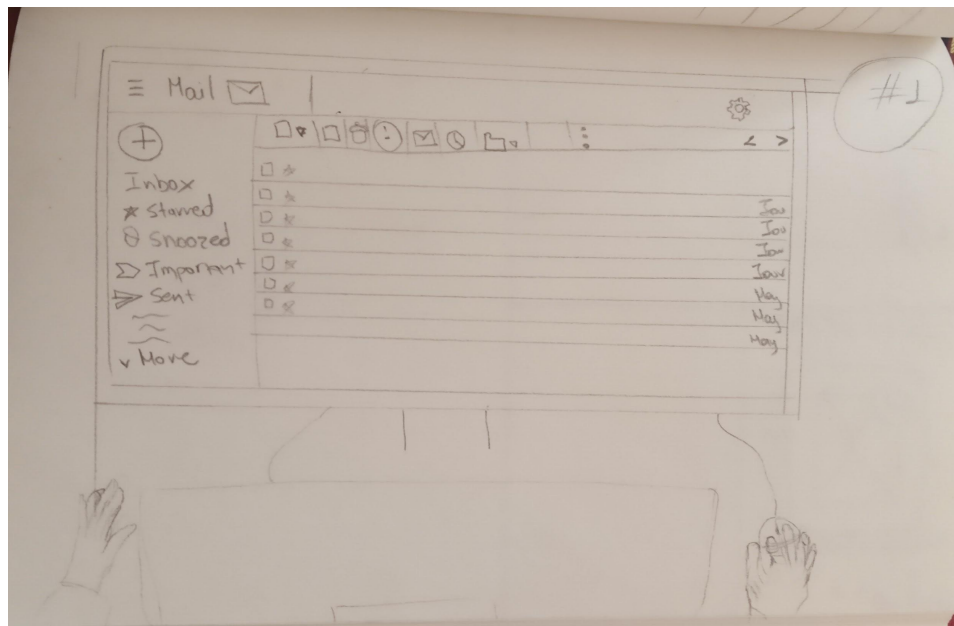
Ο παίκτης μπορεί να περιηγηθεί στο χώρο, ο οποίος θα προσομοίωνε ένα γραφείο στο οποίο είτε θα ήταν μόνος του ο κεντρικός χαρακτήρας είτε θα υπήρχαν και άλλοι χαρακτήρες όπως συνάδελφοι, εξωτερικοί συνεργάτες ή και πελάτες μαζί του. Επίσης θα υπήρχε αλληλεπίδραση με τον χώρο στον οποίο θα βρισκόταν και με την καθοδήγηση του αφηγητή

του παιχνιδιού θα άρχιζαν οι προκλήσεις του παιχνιδιού μέσα από τις οποίες θα γινόταν η εκπαίδευση του χρήστη.



Εικόνα 5. Χαρακτήρας σε αλληλεπίδραση με το γραφείο του

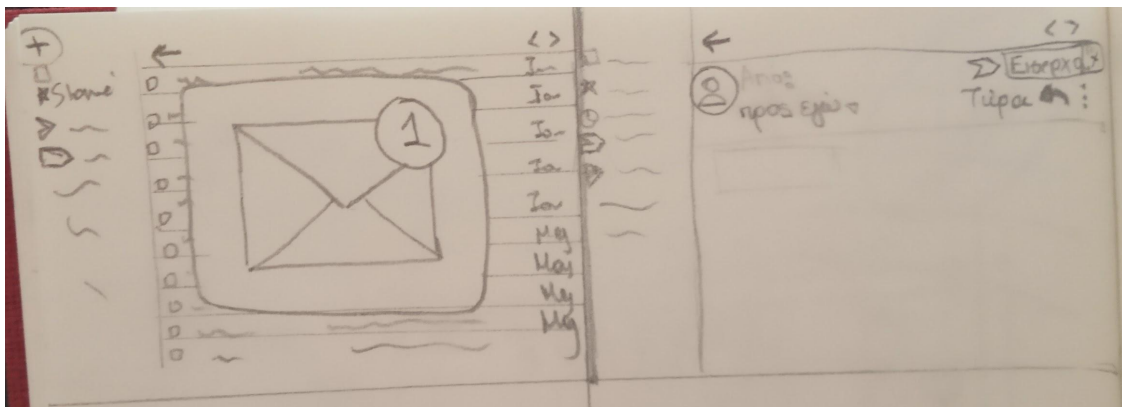
Για παράδειγμα, αν ο παίκτης ήταν όρθιος και πλησίαζε το γραφείο του, αυτόματα θα ήταν σαν να κάθεται ο ίδιος και θα του εμφανιζόταν η οθόνη του υπολογιστή με το task του επιπέδου αυτού. Σε περίπτωση που δεν πλησίαζε καθόλου το γραφείο ο καθηγητής αφηγητής θα του έδινε οδηγίες ώστε να προχωρήσει το παιχνίδι και να μην μείνει στάσιμος.



Εικόνα 6. Ο εικονικός υπολογιστής (σχέδιο στο χαρτί)

5.1.2 Τελικός Σχεδιασμός

Τελικά όμως αποφάσισα το παιχνίδι να επικεντρωθεί στο κύριο ζήτημα της εκπαίδευσης του παίκτη για γίνει πιο απλό και να προλάβει να υλοποιηθεί. Έτσι δημιουργήθηκε ένα παιχνίδι καθαρά διεπαφής και όχι τύπου escape room ή 2d που ήταν κι αυτό μια σκέψη, στο οποίο ο παίκτης δεν θα βλέπει τον κεντρικό χαρακτήρα τον οποίο θα υποδυόταν και θα χειριζόταν, αλλά μόνο την οθόνη του υπολογιστή. Η επιλογή αυτή πάρθηκε για να είναι το παιχνίδι και πιο εύκολο στη χρήση για τους συμμετέχοντες αφού δεν έχουν όλοι οι υπάλληλοι μιας επιχείρησης, την ίδια ευχέρεια με τον χειρισμό διδιάστατων και τριδιάστατων παιχνιδιών. Στο μέλλον μπορεί να γίνει επέκταση και να γίνει συνδυασμός αυτών των δύο. Η αισθητική του παιχνιδιού έχει ως σκοπό να υποβάλλει τον παίκτη στην αίσθηση ότι χειρίζεται ένα ηλεκτρονικό υπολογιστή σαν αυτό που χρησιμοποιεί στην εργασία του.



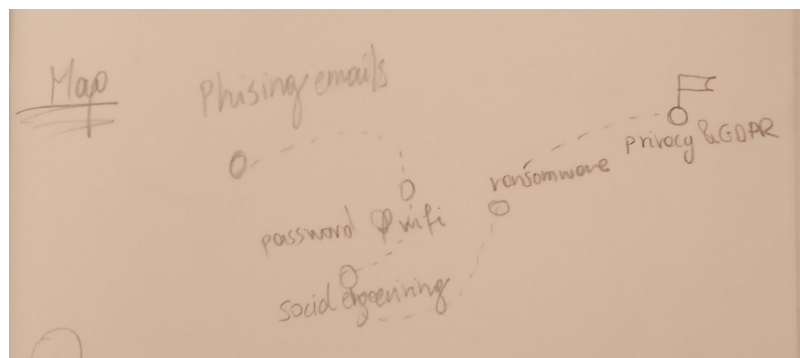
Εικόνα 7. Οθόνες ηλεκτρονικού ταχυδρομείου (σχέδιο στο χαρτί)

Θα χρησιμοποιούνται έντονα αλλά συγχρόνως και ξεκούραστα χρώματα παρόμοια με αυτά που συναντάμε στους περιηγητές του διαδικτύου αλλά και στα ηλεκτρονικά ταχυδρομεία. Η συνολική εμφάνιση είναι ένα σύνολο εικονιδίων και το παιχνίδι έχει συνεχή κάλυψη ηχητικής επένδυσης για να δώσει το αίσθημα απομόνωσης και εμβύθισης στον παίκτη.

Η αλληλεπίδραση του παίκτη με το παιχνίδι γίνεται μέσω του κέρσορα εάν τρέχει το παιχνίδι με την βοήθεια ποντικιού ή απλά με τα σημεία επαφής των δακτύλων του χεριού του με την οθόνη αφής.

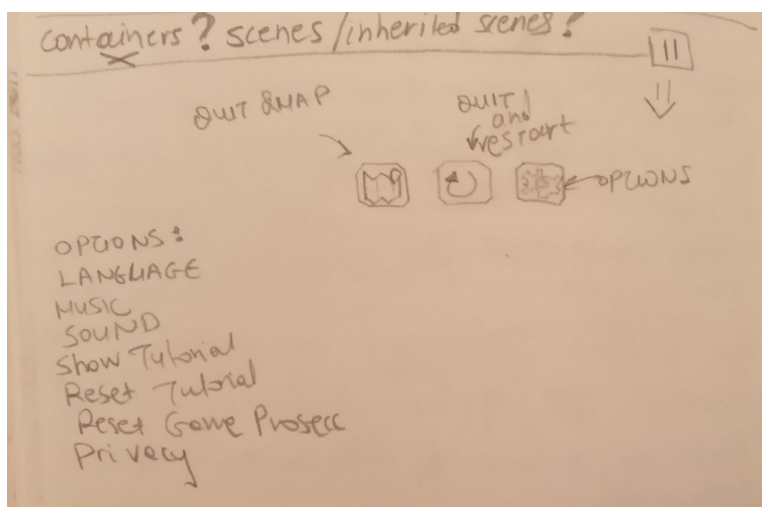
Με βάση την θεωρία μελετήθηκε η χρήση κάποιων χαρακτηριστικών παιχνιδιού. Στο SAGE δεν υπάρχει πρόβλεψη για την ύπαρξη κάποιου είδους οικονομικού συστήματος το οποίο θα δίνει την δυνατότητα στον παίκτη να αγοράζει προϊόντα από κάποιο shop στην αρχική οθόνη, ανταλλάσσοντας κάποια αντικείμενα που μαζεύει ή κερδίζει. Υπήρχε η προοπτική όμως με βάση την αρχική ιδέα, για την επιλογή της εμφάνισης (customization) του κεντρικού χαρακτήρα στην αρχική οθόνη του παιχνιδιού. Από το φύλο του χαρακτήρα, μέχρι τα χρώματα στα μαλλιά και την ενδυμασία.

Επιπλέον σχεδιάστηκε μία πρώτη μορφή ενός χάρτη του παιχνιδιού. Ο χάρτης αυτός δείχνει στο παίκτη σε ποιο επίπεδο ή σενάριο του παιχνιδιού βρίσκεται, σε ποιο θα πάει και πόσα έχει ακόμη μέχρι το τέλος του παιχνιδιού. Συνολικά υπάρχουν έξι κόμβοι/επίπεδα, όσα και τα σενάρια που έχουν σχεδιαστεί. Ο παίκτης έχει πρόσβαση στον χάρτη αυτό κατά την εκκίνηση του παιχνιδιού με το πάτημα κουμπιού για έναρξη νέου παιχνιδιού, με το πάτημα κουμπιού για συνέχιση του παιχνιδιού από το επίπεδο που είχε σταματήσει και κατά την διάρκεια του παιχνιδιού πατώντας το κουμπί της παύσης.



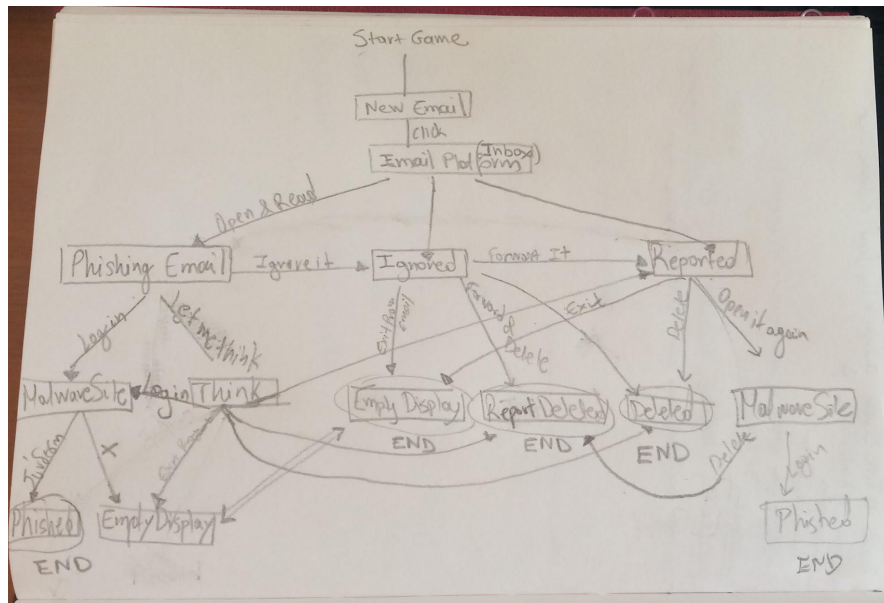
Εικόνα 8. Χάρτης παιχνιδιού (σχέδιο στο χαρτί)

Η ύπαρξη επιλογής παύσης ήταν κάτι το επιθυμητό. Πέρα από την παύση του παιχνιδιού, σχεδιάστηκε να εμφανίζεται και ένα μικρό menu, το οποίο θα προσφέρει διάφορες ρυθμίσεις και επιλογές. Οι ρυθμίσεις θα προσφέρονται και στην αρχική οθόνη και θα έχουν να κάνουν με την αλλαγή γλώσσας, την αλλαγή στην ένταση ή στην ύπαρξη ήχου και μουσικής αλλά και πιθανόν και άλλων πρόσθετων ρυθμίσεων. Οι επιλογές που θα έχει διαθέσιμες ο χρήστης, είναι αυτές της εγκατάλειψης από το συγκεκριμένο επίπεδο και η επιστροφή στον χάρτη, της επανέναρξης του επιπέδου στο οποίο βρίσκεται ο παίκτης και η συνέχιση του παιχνιδιού.



Εικόνα 9. Σκηνή παύσης με τις διαθέσιμες επιλογές (σχέδιο στο χαρτί)

Για αυτό το σενάριο έχουν επιλεγεί προκαθορισμένη δοκιμασία. Έχει προσδιοριστεί εκ των προτέρων έτσι ώστε να έχει προκαθορισμένο και άμεσα τρόπο αντιμετώπισης (explicit) της κάθε κίνησης του παίκτη. Στην Εικόνα , φαίνεται ένα πρωτότυπο διάγραμμα των προκαθορισμένων καταστάσεων το οποίο βοηθάει στον έλεγχο της ροής του παιχνιδιού.



Εικόνα 10. Διάγραμμα ροής παιχνιδιού, σε στάδιο μελέτης (σχέδιο στο χαρτί)

6. Στάδια Υλοποίησης Παιχνιδιού

6.1.1 Έρευνα υπαρχουσών παιχνιδομηχανών

Ο σχεδιασμός και η ανάπτυξη ενός παιχνιδιού (game development) υποστηρίζεται από ποικίλες πλατφόρμες (game engines) δημιουργίας ψηφιακού υλικού, οι οποίες επιλέγονται με διαφορετικά κριτήρια από τους εκάστοτε σχεδιαστές ή προγραμματιστές developers/programmers), προς υλοποίηση των στόχων (Κατσαράκη, 2020). Η επιλογή της κατάλληλης πλατφόρμας εξαρτάται από τον τύπο του παιχνιδιού (2d, 3d...), από την γλώσσα προγραμματισμού ή τον εικονικό προγραμματισμό (visual programming) αλλά και από την συσκευή με την οποία αναπτύσσεται το παιχνίδι. Δύο από τις πιο δημοφιλείς παιχνιδομηχανές είναι η Unity¹ και η Unreal Engine².

Η Unity είναι μια πανίσχυρη μηχανή παιχνιδιών με την οποία μπορείς να δημιουργήσεις όποιον τύπο παιχνιδιού θες, από 2D μέχρι εικονικής (virtual reality-VR) και επαυξημένης πραγματικότητας (augmented reality-AR) αλλά επεκτείνεται και στη βιομηχανική και αυτοκινητοβιομηχανία (industrial and automotive design), αρχιτεκτονική οπτικοποίηση (architectural visualization) και κινηματογραφική βιομηχανία (film industry). Έχει τεσσάρων ειδών άδειες χρησιμοποιήσεις με την πρώτη να είναι εντελώς δωρεάν για παιχνίδια με έσοδα λιγότερα από 100.000 δολάρια (USD) τον χρόνο.

Η Unreal Engine 5 είναι γνωστή για 2d και 3d παιχνίδια με λεπτομερείς γραφικά, γραμμένη κι αυτή σε C++ γλώσσα προγραμματισμού ή με την επιλογή χρήσης σχεδιαγραμμάτων (Unreal Blueprints) με drag-and-drop λειτουργία για πιο γρήγορη υλοποίηση. Προσφέρεται από την Epic Games και είναι δωρεάν. Η μόνη αμοιβή που πρέπει να δώσεις είναι το 5% των εσόδων σου, αν το παιχνίδι που δημιουργήσες και πούλησες ξεπερνά τα 1.000.000 δολάρια (USD) σε έσοδα.

Μία ακόμη δημοφιλής είναι η Game Maker³. Η Game Maker 2 είναι μια πολύ δυνατή πλατφόρμα για 2D παιχνίδια που παρέχει και την δυνατότητα προγραμματισμού μέσω visual scripting programming, όπως και την δυνατότητα να δεις τον κώδικα πίσω από τη visual scripting για πιο προχωρημένους προγραμματιστές. Έχει ετήσια συνδρομή η οποία κυμαίνεται ανάλογα με τις πλατφόρμες τις οποίες θες να εξάγεις το τελικό παιχνίδι εκτός αν θες απλώς να δεις πως δουλεύει η game maker που είναι δωρεάν. Είναι πολύ δημοφιλής σε indie developers, προγραμματιστές που αποτελούν μια μικρή ομάδα ή και εντελώς μόνοι τους που θέλουν να αναπτύξουν παιχνίδια.

Η Construct⁴ είναι πολύ δημοφιλής για Html παιχνίδια, για τα οποία έχεις πρόσβαση από τον περιηγητή, από αρχάριους developers χωρίς γνώσεις προγραμματισμού για την ανάπτυξη 2d παιχνιδιών και προτύπων σε μικρο χρονικό διάστημα. Είναι δωρεάν με περιορισμένα χαρακτηριστικά και για την πλήρη χρήση του χρειάζεται μηνιαία ή ετήσια συνδρομή, χωρίς επιπλέον χρέωση για την εξαγωγή του παιχνιδιού ή την πώληση του.

¹ <https://unity.com/>

² <https://www.unrealengine.com/en-US/>

³ <https://www.yovogames.com/en/gamemaker>

⁴ <https://www.construct.net/en>

Άλλες game engines που ακολουθούν είναι η GDevelop⁵, η Phaser⁶, η Godot⁷ και η Adventure Game Studio⁸ κάποιες από αυτές επί πληρωμή και άλλες εντελώς δωρεάν.

Η Godot εμφανίστηκε το 2001 με αλλαγές πολλών ονομάτων μέχρι να φτάσει σε αυτό. Το 2020 βραβεύτηκε με το Epic Mega Grant με το ποσό των 200.000 δολαρίων στην κατηγορία λογισμικό γραφικών ανοιχτού κώδικα. Τα γραφικά του είναι πολύ καλά για 2d αλλά και για 3d παιχνίδια και κάθε τύπου προγραμματιστή. Ως γλώσσα σεναρίων (scripting) για τη συγγραφή του κώδικα μπορεί να χρησιμοποιηθεί C#, C++, visual scripting και μια γλώσσα που μοιάζει με την Python, η GDScript (GoDot Script). Η GDScript είναι μία domain specific γλώσσα προγραμματισμού, που σημαίνει ότι μπορεί να χρησιμοποιηθεί μόνο από κάποια εφαρμογή και σε αυτή την περίπτωση η GDScript μπορεί να λειτουργήσει μόνο στην εφαρμογή Godot. Η Godot προσφέρει δύο κυρίως τρόπους δημιουργίας τύπων: Σκηνές (Scenes) και Σενάρια (Scripts). Και τα δύο αντιπροσωπεύουν κλάσεις αφού η Godot προσανατολίζεται στον αντικειμενοστραφή προγραμματισμό. Αυτό μπορεί να μην είναι προφανές στον αρχάριο ή ενδιάμεσης εμπειρίας χρήστη[Ταφραλίδης]. Λειτουργεί σε Windows, Mac, Linux και BSD και μπορεί να αναπτύξει παιχνίδια σε Windows, Mac, Linux, BSD, Universal Windows Platform, Android, iOS, HTML5, WebAssembly και ενώ δεν υποστηρίζει επίσημα για consoles, μέλη της κοινότητας έχουν βρει τρόπους για να εξάγουν σε PS4, Xbox One και Nintendo Switch. Η εγκατάσταση και η χρήση είναι δωρεάν, είναι και ανοιχτού κώδικα και έχει δημοσιευτεί με άδεια του MIT.

Για την δημιουργία παιχνιδιών δεν είναι απαραίτητο να χρησιμοποιηθούν μηχανές παιχνιδιών που απαιτούν εγκατάσταση. Ανάλογα με τις απαιτήσεις του παιχνιδιού καταλήγει ο προγραμματιστής και στο κατάλληλο εργαλείο ανάπτυξής του. Για την δημιουργία εκπαιδευτικών escape rooms για παράδειγμα μπορούν να χρησιμοποιηθούν online προγράμματα που προσφέρουν έτοιμες δομές για να γίνει εισαγωγή του περιεχομένου και να προσαρμοστεί το περιβάλλον στις ανάγκες του κάθε παιχνιδιού. Κάποια από αυτά τα εργαλεία είναι το Create Online Escape Rooms⁹ από τη Google και το Room Escape Maker¹⁰. Από τη μια αυτά τα εργαλεία έχουν περιορισμένες δυνατότητες σε σχέση με την μηχανές παιχνιδιών που προανανέφερα αλλά από την άλλη είναι εύκολα στη χρήση και ότι πρέπει για κάποιον που ψάχνει ένα έτοιμο καλούπι για να κάνει μικρές αλλαγές ώστε να φτιάξει γρήγορα ένα παιχνίδι.

6.1.2 Έρευνα υπαρχουσών εργαλείων σχεδιασμού

Ένα υποσύνολο της ανάπτυξης παιχνιδιών είναι ο καλλιτεχνικός σχεδιασμός του παιχνιδιού που ξεκινάει από τα πρώτα στάδια της ανάπτυξής του. Οι χαρακτήρες, τα αντικείμενα, το περιβάλλον και η διεπαφή του παιχνιδιού μπορούν είτε να σχεδιαστούν από την αρχή είτε να χρησιμοποιηθούν έτοιμα συστατικά (assets) μέσω ειδικών ιστοσελίδων.

Όσον αφορά την σχεδίαση των συστατικών του παιχνιδιού από την αρχή, υπάρχουν πολλά σχεδιαστικά εργαλεία είτε δωρεάν είτε επί πληρωμή που μπορούν να βοηθήσουν και τον πιο αρχάριο σχεδιαστή. Στη διδιάστατη σχεδίαση, το πρώτο πράγμα που πρέπει να επιλεγεί είναι αν τα γραφικά θα είναι τύπου «Raster» ή «Διανύσματος» (Vector). Οι ψηφιακές

⁵ <https://gdevelop-app.com/>

⁶ <https://phaser.io/>

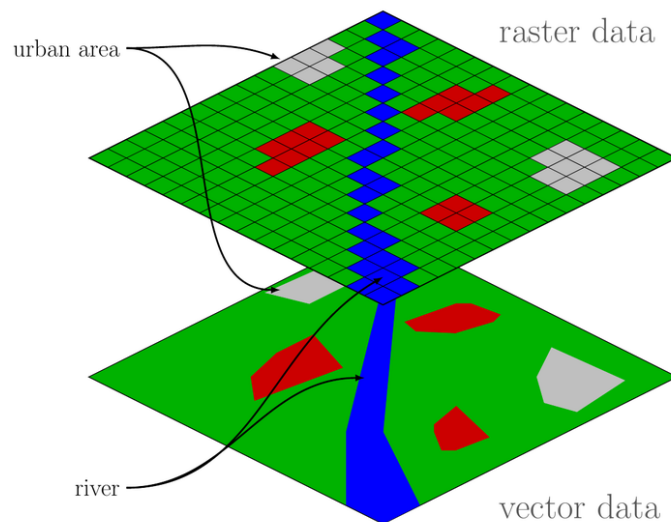
⁷ <https://godotengine.org/>

⁸ <https://www.adventuregamestudio.co.uk/>

⁹ <https://sites.google.com/view/creatingonlineers/create-your-own>

¹⁰ <https://roomescapemaker.com/>

εικόνες raster που αποτελούνται από εικονοστοιχεία (pixel), χρησιμοποιούν χάρτες bit για την αποθήκευση πληροφοριών και δεν είναι πλήρως κλιμακούμενες σε πολλαπλές αναλύσεις. Για να επεξεργαστούμε τέτοιες εικόνες χρησιμοποιούμε Photoshop, δηλαδή επεξεργαστή εικόνας που βασίζεται σε ραστερ, ενώ για να επεξεργαστούμε διανύσματα χρησιμοποιούμε επεξεργαστή «Illustrator». Τα διανυσματικά γραφικά, από την άλλη πλευρά, χρησιμοποιούν μαθηματικές εξισώσεις για να τοποθετήσουν γραμμές σε σχήμα 2D/ 3D. Το διάνυσμα έχει μέγεθος και κατεύθυνση. Όταν κλιμακώνεται η εικόνα υπάρχει μηδενική απώλεια λεπτομέρειας επειδή η κατεύθυνση είναι προκαθορισμένη και το μόνο που αλλάζει είναι το μέγεθος. Δεν είναι απαραίτητο να χρησιμοποιηθεί ή ο ένας ή ο άλλος τρόπος απεικόνισης, μπορούν και οι δύο σε ένα παιχνίδι.



Εικόνα 11. Διαφορά μεταξύ raster και vector γραφικών

Το πιο γνωστό δωρεάν εργαλείο photoshop για σχεδιασμό παιχνιδιών είναι το GIMP¹¹ (GNU Image Manipulation Program). Είναι ανοικτού κώδικα διαθέτει μαθήματα χρήσης (tutorials) της εφαρμογής και έχει μεγάλη κοινότητα για επιπλέον βοήθεια. Είναι ένα εργαλείο πολλαπλών χρήσεων και μπορεί να χρησιμοποιηθεί για τα πάντα, από την τέχνη του παιχνιδιού μέχρι το ρετουσάρισμα φωτογραφιών. Το GIMP υποστηρίζεται σχεδόν σε όλες τις πλατφόρμες υπολογιστών και υπάρχουν πολλά πρόσθετα (add-ons) που μπορούν να κατέβουν στο GIMP για να βελτιωθεί η εμπειρία. Για τα εικόνες διανυσμάτων, οι περισσότεροι developers χρησιμοποιούν το Inkscape¹². Είναι και αυτο ανοικτού κώδικα και δωρεάν λογισμικό, προσφέρει ένα πλούσιο σύνολο χαρακτηριστικών, χρησιμοποιείται ευρέως τόσο για καλλιτεχνικές όσο και για τεχνικές εικονογραφήσεις και χρησιμοποιεί την τυποποιημένη μορφή αρχείου SVG ως κύρια μορφή. Διαθέτει ένα ολοκληρωμένο σύνολο δυνατοτήτων, μια απλή διεπαφή, πολυγλωσσική υποστήριξη και έχει σχεδιαστεί ώστε να μπορεί να επεκταθεί με πρόσθετα. Όπως και με το GIMP, υπάρχει κοινότητα η οποία παρέχει βοήθεια και υπάρχουν πολλά εκπαιδευτικά υλικά για να βοηθήσουν τους νέους χρήστες να ξεκινήσουν να δημιουργούν.

¹¹ <https://www.gimp.org/>

¹² <https://inkscape.org/>

Η τριδιάστατη μοντελοποίηση είναι η διαδικασία δημιουργίας μιας μαθηματικής αναπαράστασης της επιφάνειας ενός αντικειμένου σε τρισδιάστατο χώρο μέσω εξειδικευμένου λογισμικού. Ένα πολύ ισχυρό και δωρεάν εργαλείο είναι το Blender¹³. Το Blender είναι μια δωρεάν και ανοιχτού κώδικα σουίτα δημιουργίας 3D. Υποστηρίζει το σύνολο του αγωγού 3D - μοντελοποίηση, κινούμενα σχέδια, προσομοίωση, απόδοση, σύνθεση και παρακολούθηση κίνησης, ακόμη και επεξεργασία βίντεο και δημιουργία παιχνιδιών. Οι προχωρημένοι χρήστες χρησιμοποιούν το API του Blender για σενάρια Python για να προσαρμόσουν την εφαρμογή και να γράψουν εξειδικευμένα εργαλεία, συχνά αυτά περιλαμβάνονται στις μελλοντικές κυκλοφορίες του Blender. Ως έργο βασισμένο στην κοινότητα βάσει της GNU General Public License (GPL), το κοινό εξουσιοδοτείται να κάνει μικρές και μεγάλες αλλαγές στη βάση κώδικα, γεγονός που οδηγεί σε νέες δυνατότητες, αποκριτικές διορθώσεις σφαλμάτων και καλύτερη χρηστικότητα.

Από την άλλη μεριά υπάρχει μεγάλη ποικιλία έτοιμων assets δωρεάν ή επι πληρωμή. Στα δωρεάν κυριαρχούν κυρίως 2D assets. Υπάρχουν έτοιμα αντικείμενα, χαρακτήρες ηχητικά εφέ, sprites (διδιάστατος χάρτης bit που ενσωματώνεται σε μια μεγαλύτερη σκηνή, συχνότερα σε ένα 2D παιχνίδι) και πολλά άλλα τα οποία μπορείς να κατεβάσεις και να χρησιμοποιήσεις. Φυσικά να φτιάξεις κι εσύ τα δικά σου μπορείς να τα ανεβάσεις σε αυτές τις σελίδες για να μπορέσουν να τα χρησιμοποιήσουν και άλλοι developers. Το OpenGameArt¹⁴, itch.io¹⁵, sketchfab¹⁶ είναι μόνο τρία από τα πολλά σημεία από όπου μπορείς να προμηθευτείς έτοιμα συστατικά παιχνιδιού.

6.2. Υλοποίηση

Το πρώτο σενάριο από αυτά που αναφέρθηκαν προηγουμένως έχει υλοποιηθεί το οποίο αφορά το ηλεκτρονικό ψάρεμα (phishing). Για την υλοποίηση του SAGE χρησιμοποιήθηκε η παιχνιδομηχανή Godot και το εργαλείο σχεδιασμού Inkscape. Αρχικά έγινε δοκιμή υλοποίησης μέσω της Unreal Engine 4 όμως ο φορητός υπολογιστής που διέθετα για την ανάπτυξη του παιχνιδιού, δεν μπόρεσε να την υποστηρίξει λόγω της προαπαιτήσης στον ρυθμό των κύκλων ρολογιού του επεξεργαστή (2.5 GHz ενώ εγώ είχα 1.60 GHz).

6.2.1. Δημιουργία νέου έργου με την Godot

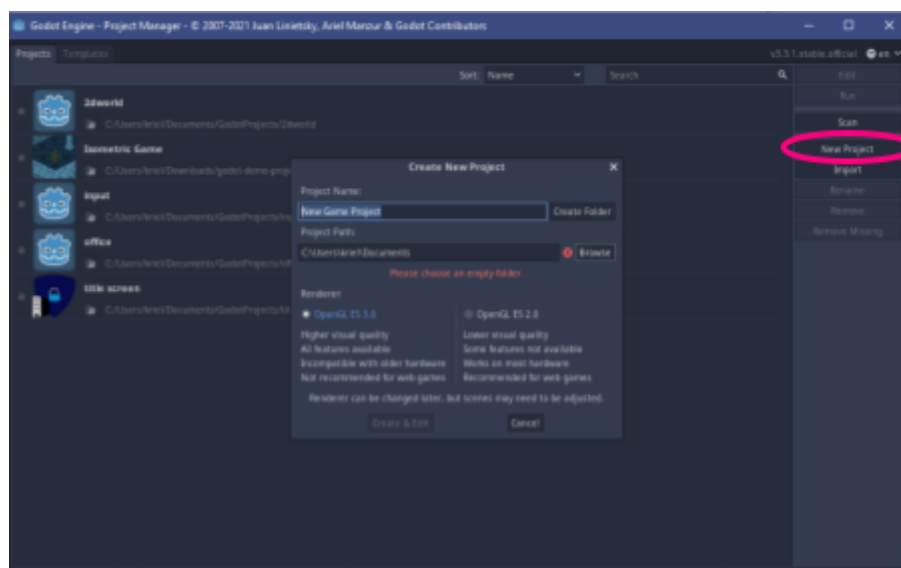
Για να ξεκινήσει η υλοποίηση του παιχνιδιού με το Godot, το πρώτο πράγμα που χρειάζεται να γίνει είναι η δημιουργία ενός νέου «project». Με το που ξεκινήσουμε την μηχανή Godot, το πρώτο παράθυρο που θα δούμε είναι το «Project Manager», μέσω του οποίου μπορούμε να δημιουργήσουμε, να αφαιρέσουμε, να εισάγουμε ή να παίξουμε έργα παιχνιδιών. Πατώντας το κουμπί «Νέο έργο» στα δεξιά δημιουργούμε ένα νέο έργο δίνοντας ένα όνομα και επιλέγοντας έναν κενό φάκελο στον υπολογιστή για αποθήκευση.

¹³ <https://www.blender.org/>

¹⁴ <https://opengameart.org/>

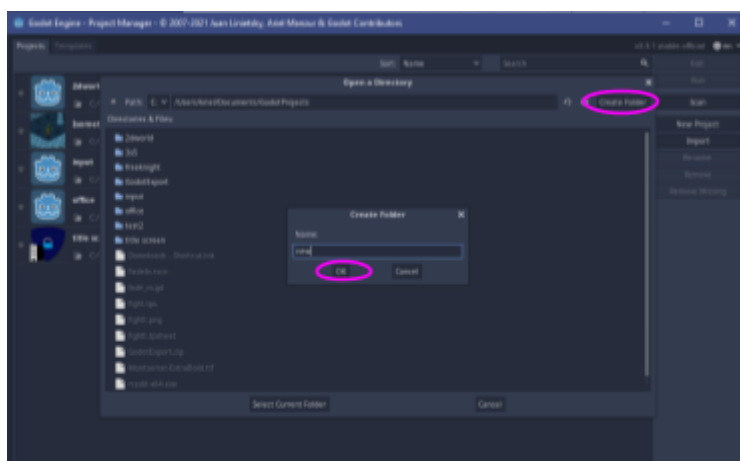
¹⁵ <https://itch.io/game-assets>

¹⁶ <https://sketchfab.com/>



Εικόνα 12. Νέο έργο (New Project) στη Godot

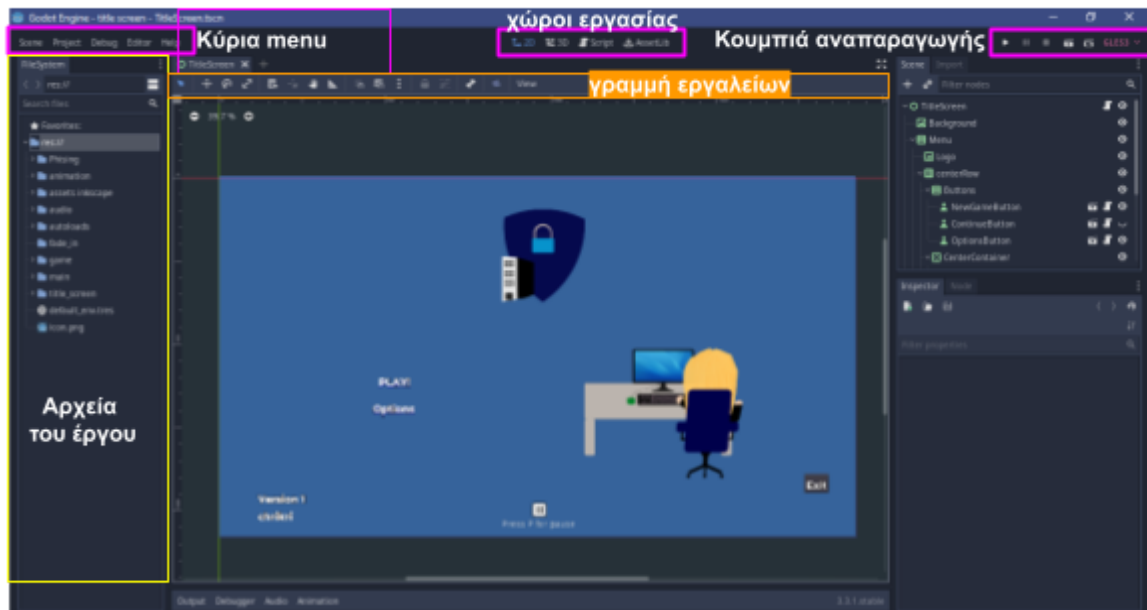
Εάν δεν έχουμε κάποιο κενό φάκελο μπορούμε να δημιουργήσουμε έναν πατώντας το κουμπί «Browse» (εξερεύνηση). Στο νέο παράθυρο πατάμε «New folder» επιλέγουμε το μονοπάτι που θέλουμε να έχουμε το έργο μας, εισάγουμε το όνομά του και πατάμε «OK».



Εικόνα 13. Δημιουργία νέου φακέλου (Create Folder)

Τέλος βλέποντας το πράσινο σημάδι σημαίνει ότι υπάρχει άδειος φάκελος και ότι είμαστε έτοιμοι να δημιουργήσουμε το έργο μας σε αυτόν.

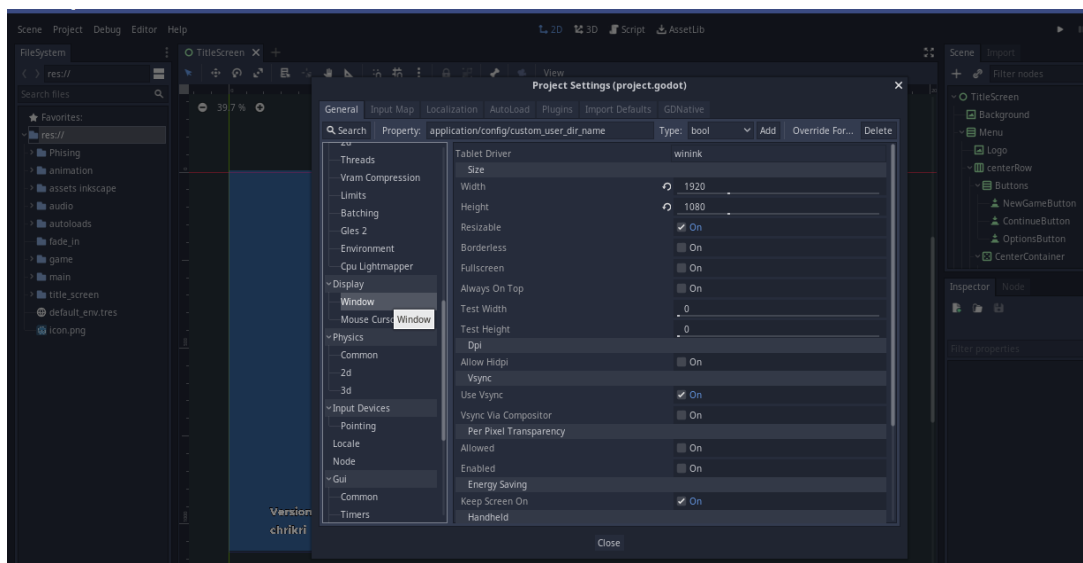
Στο επάνω μέρος, από αριστερά προς τα δεξιά, είναι τα κύρια μενού (Scene, Project, Debug, Editor, Help), οι χώροι εργασίας (2D, 3D, Script, AssetLib) και τα κουμπιά δοκιμής αναπαραγωγής. Το «FileSystem» είναι η θέση όπου διαχειριζόμαστε τα αρχεία και τα στοιχεία του έργου.



Εικόνα 14. Περιβάλλον Godot 3

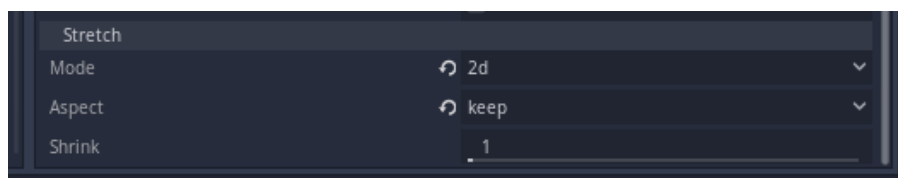
6.2.2 Ρυθμίσεις

Στις γενικές (General) ρυθμίσεις του έργου (Project → Project Manager) στην κατηγορία Display, ρύθμισα την εμφάνιση του παιχνιδιού σε Width 1920 και Height 1080 pixels τα οποία αφορούν τη φυσική ανάλυση στην οποία γίνεται το αρχικό rendering του παιχνιδιού από τη μηχανή. Η ανάλυση είναι προσαρμόσιμη (resizable) στο σύστημα που θα επιλεγεί για να παίξει κάποιος το παιχνίδι σε πλήρη οθόνη. Το «Vsync» είναι ενεργοποιημένο για να επιτρέπει το συγχρονισμό του παιχνιδιού με τον αριθμό του καρέ ανά δευτερόλεπτο της οθόνης του υπολογιστή. Η λειτουργία «Keep Screen On» αποτρέπει τα χαρακτηριστικά οικονομίας ενέργειας να δράσουν κατά τη διάρκεια του παιχνιδιού, όπως για παράδειγμα την αδράνεια που μπορεί να έχει ρυθμιστεί για την συσκευή μετά από λίγα λεπτά να ενεργοποιείται. Ο προσανατολισμός της οθόνης είναι οριζόντια σε «landscape».



Εικόνα 15. Γενικές ρυθμίσεις οθόνης (Display)

Οι επιλογές του «Stretch Mode» καθορίζουν πως η βασική ανάλυση του παιχνιδιού θα προσαρμοστεί σε διάφορες οθόνες και παράθυρα. Έχω επιλέξει την επιλογή 2D όπου το παιχνίδι θα «Απλωθεί» σε όλη την οθόνη οποιαδήποτε συσκευής και στις επιλογές «Aspect» την επιλογή «Keep» για να κρατηθεί σταθερός ο λόγος πλάτους προς ύψος.



Εικόνα 16. Stretch options

Τέλος η τελευταία αλλαγή στη διαμόρφωση του project είναι στο χρώμα που έχει το φόντο του παιχνιδιού στην καρτέλα «Rendering» στην επιλογή περιβάλλον (Environment) από το προκαθορισμένο «4c4c4c» σε χρώμα «263138» για να γίνει γκρι-μπλε.

6.2.3 Input Map

Οι ενέργειες και τα συμβάντα από συσκευές εισόδων μπορούν να οριστούν στην καρτέλα Εισαγωγή χάρτη (Input Map) δεξιά από τις Γενικές ρυθμίσεις. Αυτό περιλαμβάνει πατήματα πλήκτρων, κουμπιά και κίνηση του ποντικιού, «joypads» και ενέργειες εισαγωγής. Στο SAGE πρόσθεσα να ενεργοποιείται η δράση «Pause» κάθε φορά που θα πατιέται το κουμπί «P».

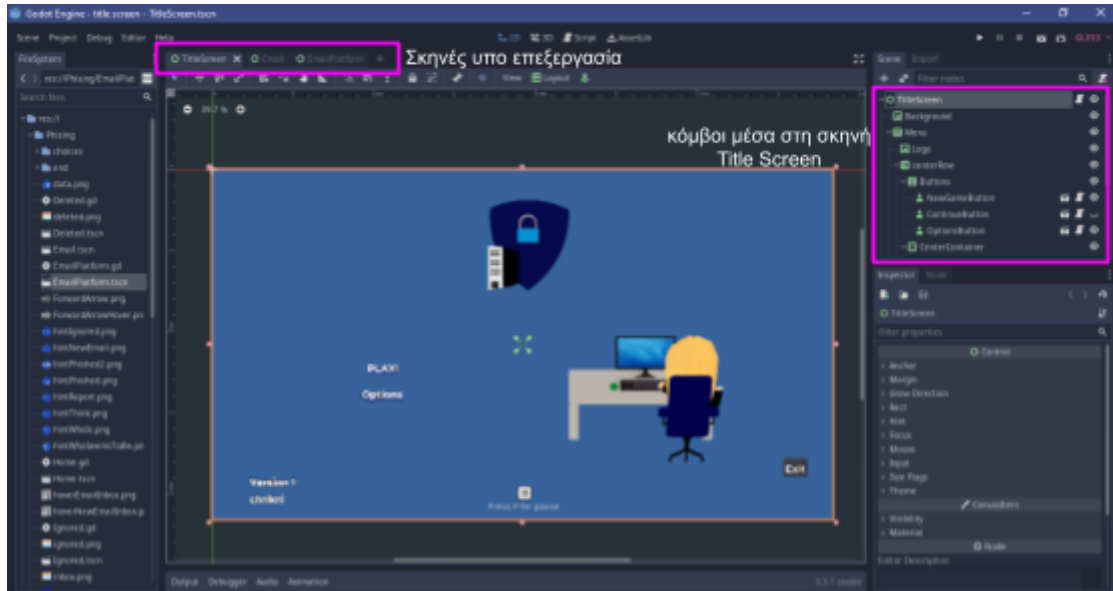


Εικόνα 17. Input Map, προσθήκη της παύσης

6.2.4 Σκηνές

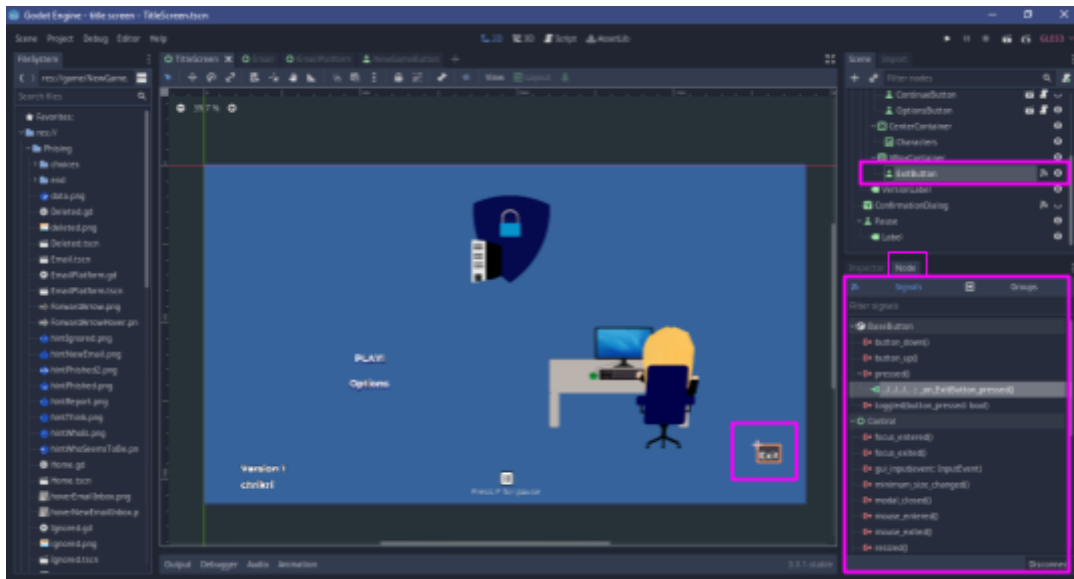
Στη Godot κάθε παιχνίδι είναι δέντρα από κόμβους (nodes) ομαδοποιημένα σε σκηνές (scenes). Αυτοί οι κόμβοι μπορούν να “δεθούν” ώστε να μπορούν να επικοινωνούν μεταξύ

τους μέσω των σημάτων (signals). Οι σκηνές έχουν την δυνατότητα να επαναχρησιμοποιούνται κατά την ανάπτυξη του παιχνιδιού. Μια σκηνή μπορεί να είναι χαρακτήρας, αντικείμενο, μενού στη διεπαφή με τον χρήστη, ολόκληρο επίπεδο (level) κτλ. Είναι δηλαδή ευέλικτες, μπορούν να χρησιμοποιηθούν σαν ένα πρότυπο (prefab) αλλά και να εμφωλευτούν η μία μέσα στην άλλη δημιουργώντας και στιγμιότυπα (instancing). Κάθε σκηνή αποτελείται από έναν ή περισσότερους κόμβους. Οι κόμβοι είναι τα μικρότερα δομικά στοιχεία του παιχνιδιού που τακτοποιούνται σε μορφή δέντρων.

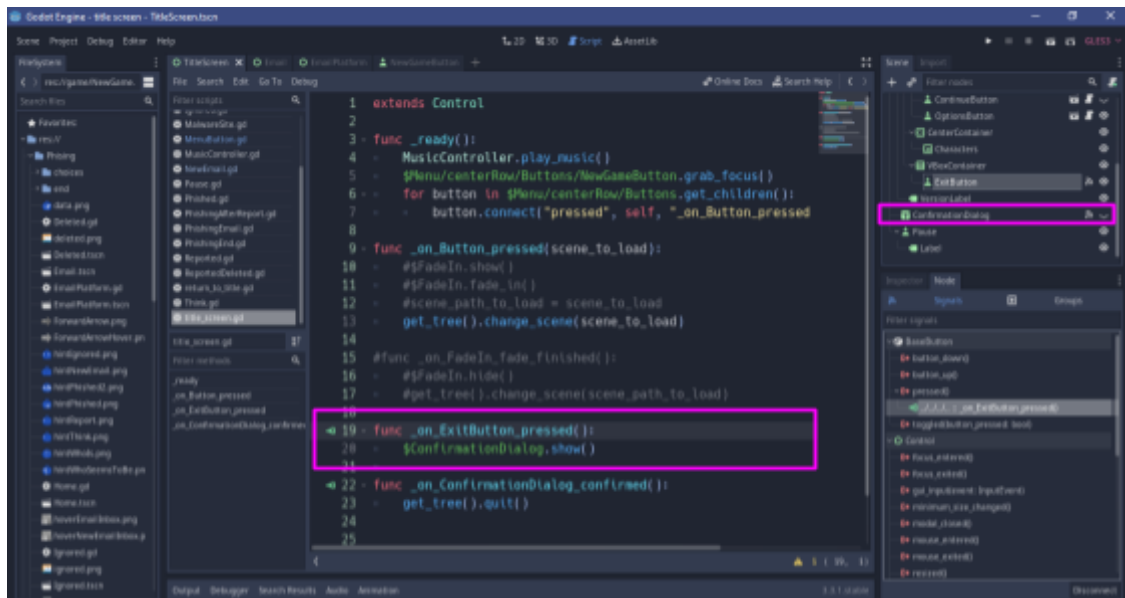


Εικόνα 18. Περιβάλλον σκηνών

Οι κόμβοι εκπέμπουν σήματα όταν συμβαίνει κάποιο συμβάν. Μέσω των σημάτων μπορούμε να κάνουμε τους κόμβους να επικοινωνούν χωρίς να τους συνδέσουμε με κώδικα, κι έτσι έχουμε μεγαλύτερη ευελιξία στο πως είναι δομημένες οι σκηνές. Τα σήματα είναι η έκδοση του Godot για το μοτίβο παρατηρητή (observer) μια τεχνική που χρησιμοποιείται σε πολλές γλώσσες προγραμματισμού. Επιτρέπουν σε έναν κόμβο να στέλνει ένα μήνυμα στο οποίο οι άλλοι κόμβοι μπορούν να ακούσουν και να απαντήσουν. Για παράδειγμα, αντί να γίνεται συνεχώς έλεγχος σε ένα κουμπί για να δούμε αν πιέζεται, το κουμπί μπορεί να εκπέμπει ένα σήμα όταν πιέζεται και έτσι μπορούμε να γράψουμε κώδικα ο οποίος θα ενεργοποιηθεί όταν λάβει το σήμα. Στο SAGE αν πατηθεί το κουμπί «Exit» έξοδος στην αρχική οθόνη του παιχνιδιού τότε εκτελείται κώδικας ο οποίος κάνει ορατό τον κρυμμένο κόμβο «Confirmation Dialog» που και αυτός ο κόμβος έχει συνδεθεί με σήμα και καλεί με την σειρά του ,να εκτελεστεί άλλο κομμάτι κώδικα.

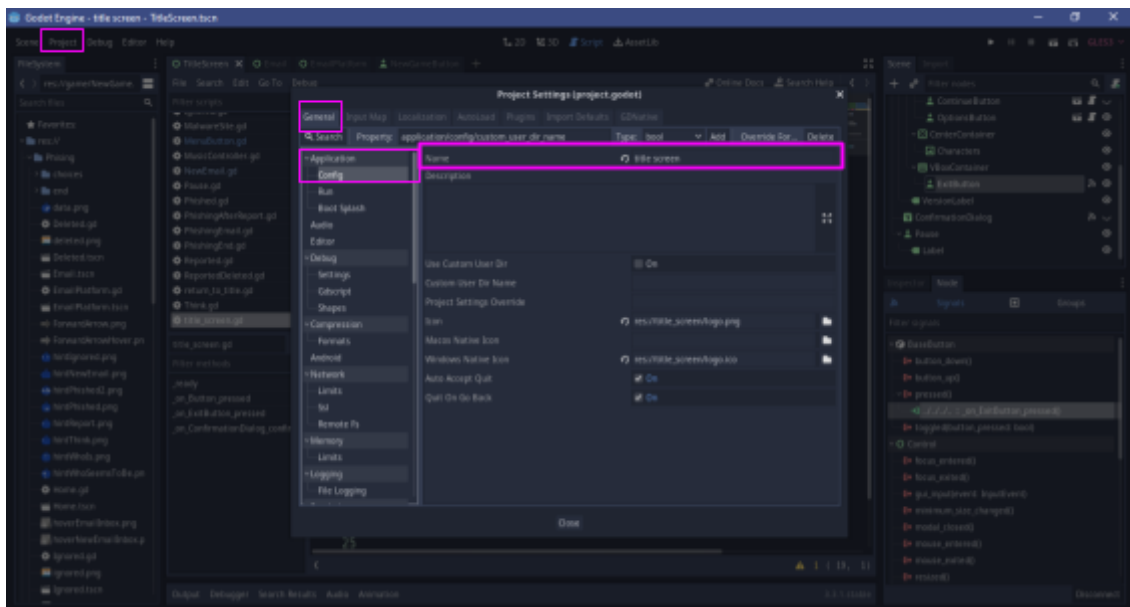


Εικόνα 19. Σήματα (signals) κουμπιού «Exit»



Εικόνα 20. Συνάρτηση εκκίνησης διαδικασιών με το πάτημα του κουμπιού

Το να τρέχεις ένα παιχνίδι σημαίνει να τρέχεις μια σκηνή. Ένα έργο μπορεί να περιέχει αρκετές σκηνές, αλλά για να ξεκινήσει το παιχνίδι, μία από αυτές πρέπει να επιλεγεί ως η κύρια σκηνή. Ως κύρια σκηνή έχω ορίσει την «TitleScreen» η οποία είναι η αρχική οθόνη που εμφανίζεται κατά την εκκίνηση του παιχνιδιού και περιέχει και το αρχικό μενου.

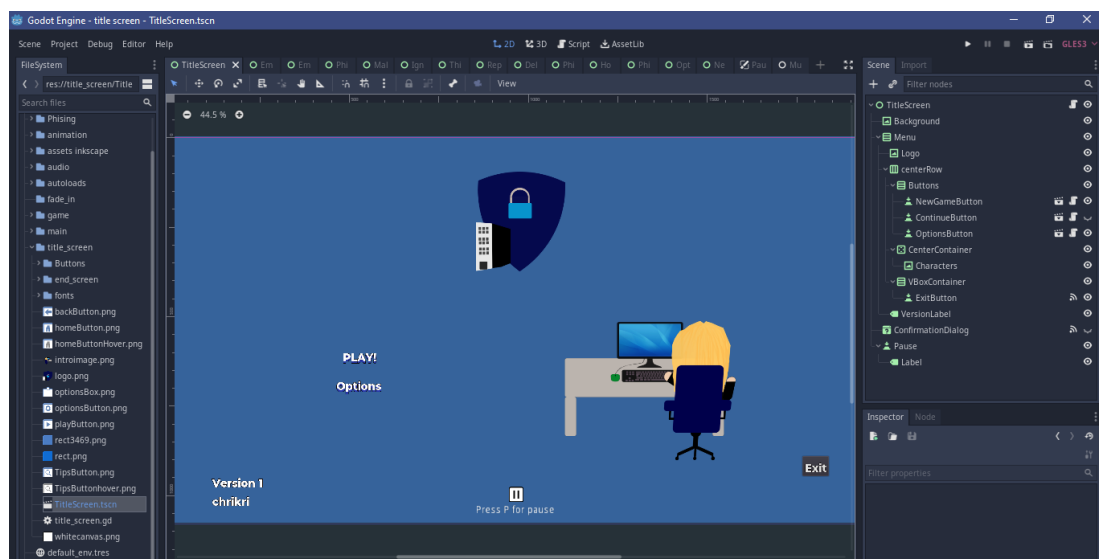


Εικόνα 21. Καθορισμός κύριας σκηνής (main scene)

6.2.5 Σχεδιασμός Πρώτου Σεναρίου

Συνολικά για την υλοποίηση του SAGE, στο οποίο αναπτύχθηκε μόνο το σενάριο της επίθεσης ηλεκτρονικού ψαρέματος, δημιουργήθηκαν δεκαέξι σκηνές. Από αυτές μία είναι η αρχική οθόνη με το μενού που προανέφερα, η «Title Screen.tscn», εξι είναι οι σκηνές/επίπεδα του σεναρίου (*Email.tscn*, *EmailPlatform.tscn*, *PhishingEmail.tscn*, *MalwareSite.tscn*, *Ignored.tscn*, *Think.tscn*), τέσσερις οι σκηνές για τις τέσσερις διαφορετικές τελικές καταστάσεις ανάλογα με τις επιλογές του παίκτη (*ReportedDeleted.tscn*, *Deleted.tscn*, *Phished.tscn*, *Home.tscn*), μία είναι η τελική οθόνη του παιχνιδιού (*PhishingEnd.tscn*) και οι υπόλοιπες πέντε για διάφορες λειτουργίες όπως κουμπιά, ήχο, παύση (*Options.tscn*, *MenuButton.tscn*, *Pause.tscn*, *MusicController.tscn*).

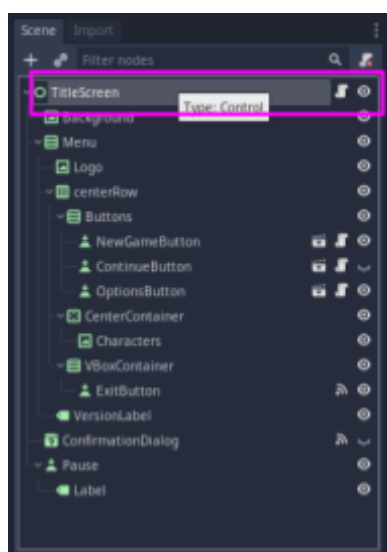
6.2.5.1 Αρχική οθόνη (Title Screen)



Εικόνα 22. TitleScreen.tscn

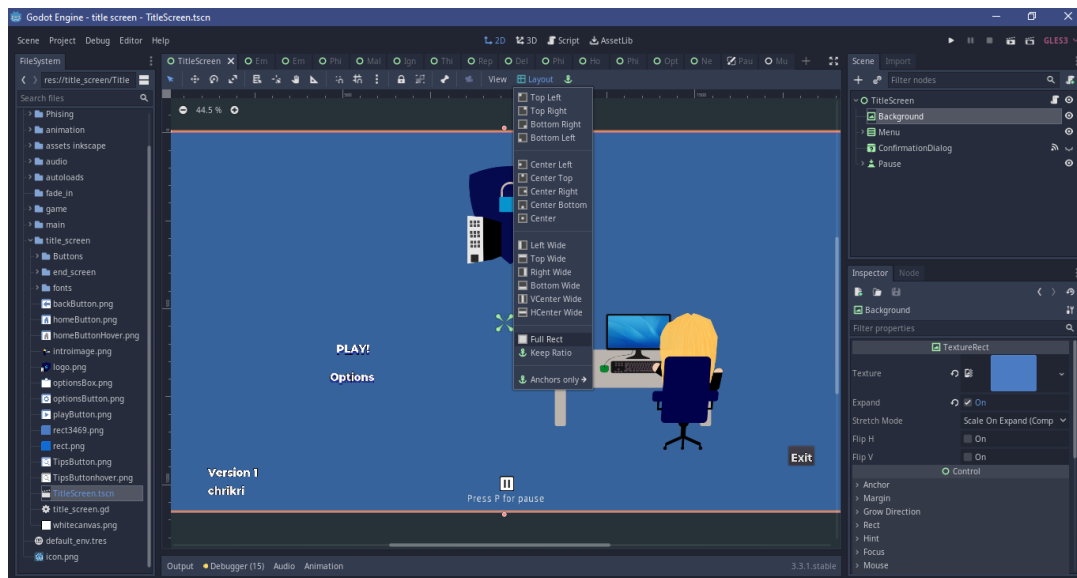
Η αρχική διεπαφή του παίκτη με το παιχνίδι είναι η «TitleScreen». Αποτελείται από τους κόμβους που φαίνονται στην δεξιά πλευρά της εικόνας. Οι δυνατότητες που έχει ο παίκτης σε αυτή τη σκηνή είναι να ξεκινήσει το παιχνίδι πατώντας το κουμπί «PLAY!», να μεταβεί στη σκηνή των ρυθμίσεων πατώντας το κουμπί «Options» και να βγει από το παιχνίδι πατώντας το κουμπί «Exit» στην κάτω δεξιά γωνία. Επιπλέον πληροφορείται για την έκδοση του παιχνιδιού (Version 1), τον δημιουργό (chrikri) και την δυνατότητα να κάνει παύση το παιχνίδι πατώντας το πλήκτρο «P» αν έχει συνδεδεμένο πληκτρολόγιο η συσκευή του. Τέλος στην σκηνή υπάρχει στο πάνω μέρος το logo του SAGE, και ένα εικονίδιο που αναπαριστά μια υπάλληλο σε ένα γραφείο με υπολογιστή για να βάλει στο πνεύμα του παιχνιδιού τον παίκτη.

Για την δημιουργία μια σκηνής τύπου user interface όπως η παραπάνω, χρειάζεται ο πρώτος κόμβος να είναι «Control» κόμβος. Συνήθως παίρνει το όνομα της σκηνής στην οποία ανήκει.



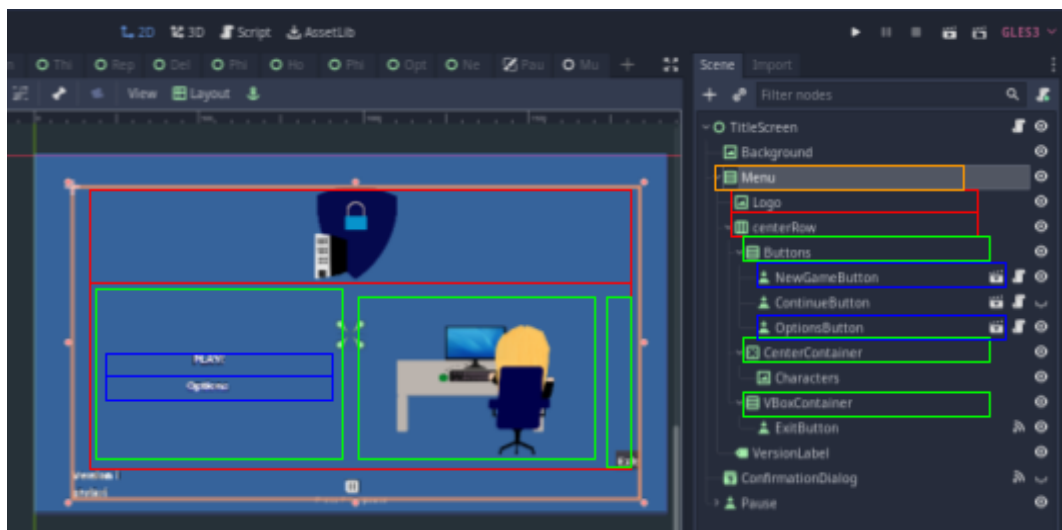
Εικόνα 23. κόμβος Control → *TitleScreen.tscn*

Ως πρώτο παιδί έχω βάλει το «Background» το οποίο είναι τύπου «TextureRect». Χρησιμοποιείται για τη σχεδίαση εικονιδίων και «sprites» σε μια διεπαφή χρήστη. Η τοποθέτηση της υφής μπορεί να ελεγχθεί με την ιδιότητα «stretch_mode». Μπορεί να κλιμακωθεί, να πλακαριστεί ή να παραμείνει κεντραρισμένη μέσα στο οριοθέτη του. Το «Background» όπως και ο γονικός του κόμβος έχουν επιλεγεί με layout «Full rect» ώστε να πιάνουν όλο το «viewport», δηλαδή την οθόνη, όπως έχει επιλεγεί και η επέκταση «Expand».



Εικόνα 24. κόμβος Background→ *TitleScreen.tscn*

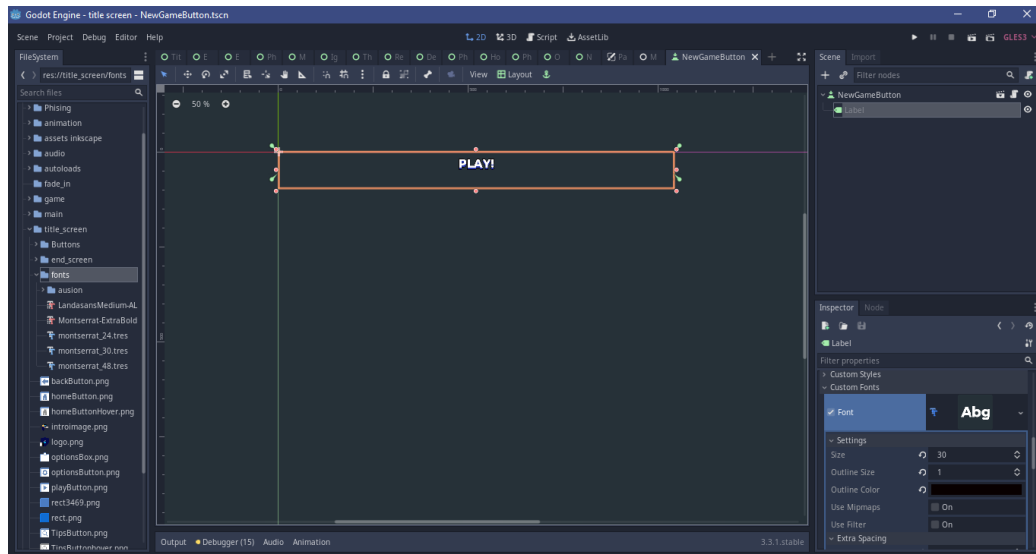
Δεύτερο παιδί κόμβος είναι ένα κατακόρυφο κουτί (VBoxContainer) με όνομα «Menu» με περιθώριο στα άκρα. Τα «containers» βάζουν αυτόματα τα παιδιά τους ταξινομημένα, σε σειρές αν είναι «VBoxContainer» και σε στήλες αν είναι «HBoxContainer». Έτσι μπορεί να χωριστεί το viewport σε επιμέρους κομμάτια για να υπάρχει καλύτερος έλεγχος των στοιχείων που απαρτίζουν την σκηνή. Μέσα στο μενού υπάρχει το «Logo» και ένα «HBoxContainer» το οποίο με την σειρά του περιλαμβάνει τα κουμπιά των επιλογών σε «VBoxContainer», την εικόνα και το κουμπί «Exit». Η εικόνα με τον χαρακτήρα είναι μέσα σε κεντρικό κουτί (CenterContainer) μέχρι κόμβου «TextuteRect».



Εικόνα 25. Containers (*TitleScreen.tscn*)

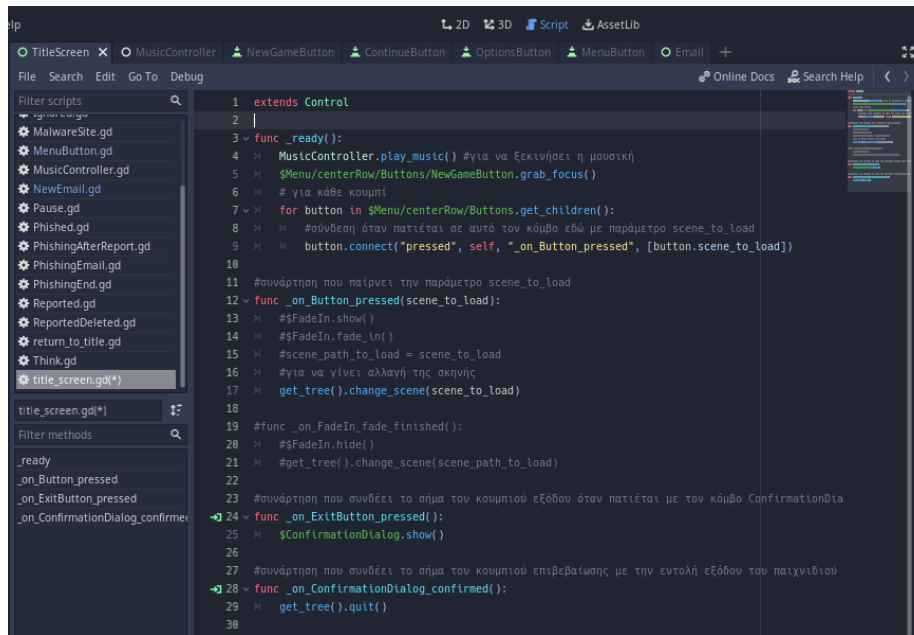
Τα κουμπιά επιλογών (PLAY!, Options) είναι στιγμιότυπα της σκηνής «GameButton.tscn» για αυτο έχουν και τα αντίστοιχα εικονίδια δεξιά από το όνομά τους και έτσι φτιάχνεις μια φορά το πρότυπο των κουμπιών και μετά μπορείς να τα ξαναχρησιμοποιήσεις αλλάζοντας το περιεχόμενο. Για να μπει κείμενο πάνω στα κουμπιά πρόσθεσα κόμβο label και στη συνέχεια για να μεγαλώσω τα γράμματα, έγινε προσαρμογή

γραμματοσειράς (Custom Fonts) με εισαγωγή δυναμικής γραμματοσειράς (DynamicFont) από τον Inspector στο κάτω δεξί πλαίσιο του Godot.

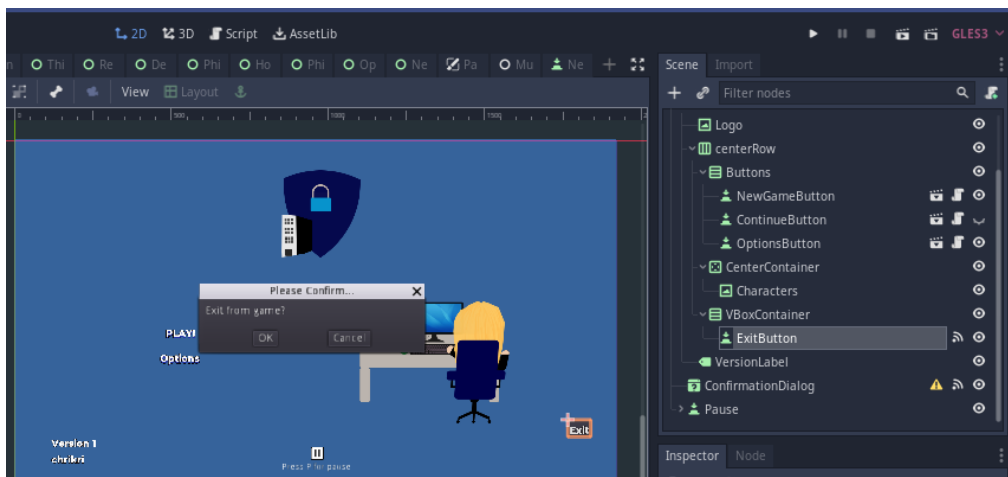


Εικόνα 26. *GameButton.tscn*

Όσον αφορά τον κώδικα, η συγκεκριμένη σκηνή απαρτίζεται από το κύριο script που είναι επισυναπτόμενο στον πατέρα κόμβο «TitleScreen» και τα «script» των στιγμιότυπων κουμπιών. Το «script» της «TitleScreen», περιέχει την συνάρτηση «_ready», η οποία εκτελείται όταν ο κόμβος και τα παιδιά του έχουν μπει στο δέντρο και είναι έτοιμα. Περιέχει εντολή για να ξεκινήσει το ηχητικό κομμάτι (`MusicController.play_music()`) και για χρήση πληκτρολογίου για επιλογή των κουμπιών πέρα από το ποντίκι (`$Menu/.../NewGameButton.grab_focus()`). Ακόμη έχει δύο συναρτήσεις που είναι συνδεδεμένες με σήματα για την έξοδο του χρήστη από το παιχνίδι με τη χρήση κουτιού διαλόγου επιβεβαίωσης της επιλογής (`ConfirmationDialog`). Η μία, η `_on_ExitButton_pressed()`, ενεργοποιείται μόλις πατήσει ο χρήστης το κουμπί «Exit» ζητώντας να εμφανιστεί το κουτί επιβεβαίωσης και η άλλη, η `_on_ConfirmationDialog_confirmed()`, ενεργοποιείται μόλις πατήσει ο χρήστης το κουμπί «OK» όπου επιβεβαιώνεται πως θέλει να αποχωρήσει από το παιχνίδι και λέμε με το `get_tree().quit()` να σταματήσει να τρέχει το παιχνίδι.

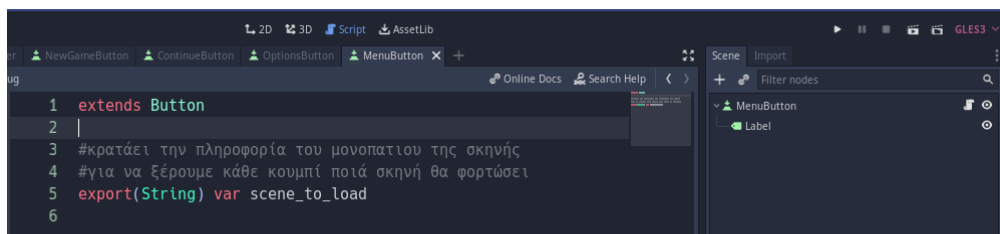


Εικόνα 27. TitleScreen.gd



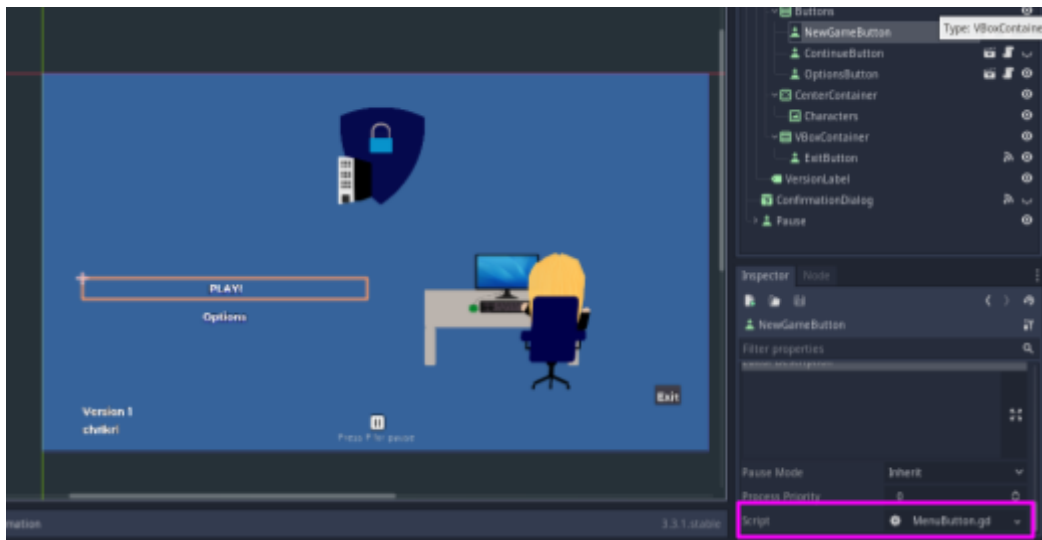
Εικόνα 28. ExitButton

Τα κουμπιά χρησιμοποιούν τον κώδικα που είναι γραμμένος στο «MenuButton» ο οποίος κρατάει πληροφορία για το μονοπάτι της σκηνής που θα πρέπει να φορτώσει το κάθε κουμπί επιλογής.



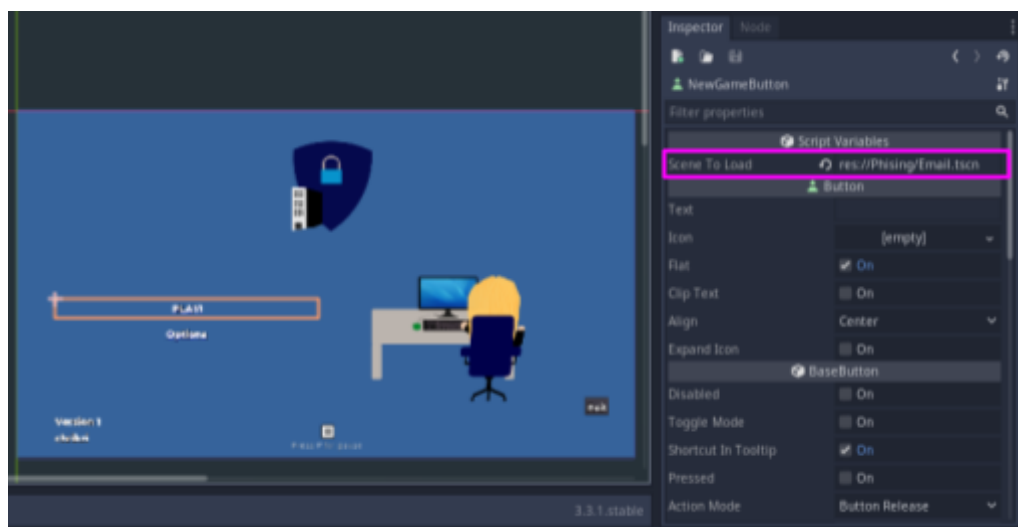
Εικόνα 29. MenuButton.gd

Στη συνέχεια για κάθε κουμπί που έχουμε βάλει στη σκηνή μας, πάμε στο κάτω μέρος του Inspector στο Node και κάνουμε reload το script.



Εικόνα 30. *NewGameButton* (Inspector load script)

Μετά πάμε στη σκηνή του κάθε κουμπιού και βάζουμε το σωστό μονοπάτι για τη σκηνή που πρέπει να φορτώνει, κάθε φορά που πατιέται. Το play κουμπί κάθε φορά που πατιέται φορτώνει την σκηνή «PhisingEmail.tscn». Αυτό γίνεται από το πάνω μέρος του Inspector που μας εμφανίζει τις μεταβλητές που έχουμε προσθέσει στο script μας και σε αυτή την περίπτωση είναι η μεταβλητή «Scene To Load» και το μονοπάτι που έβαλα το «res://Phising/Email.tscn».

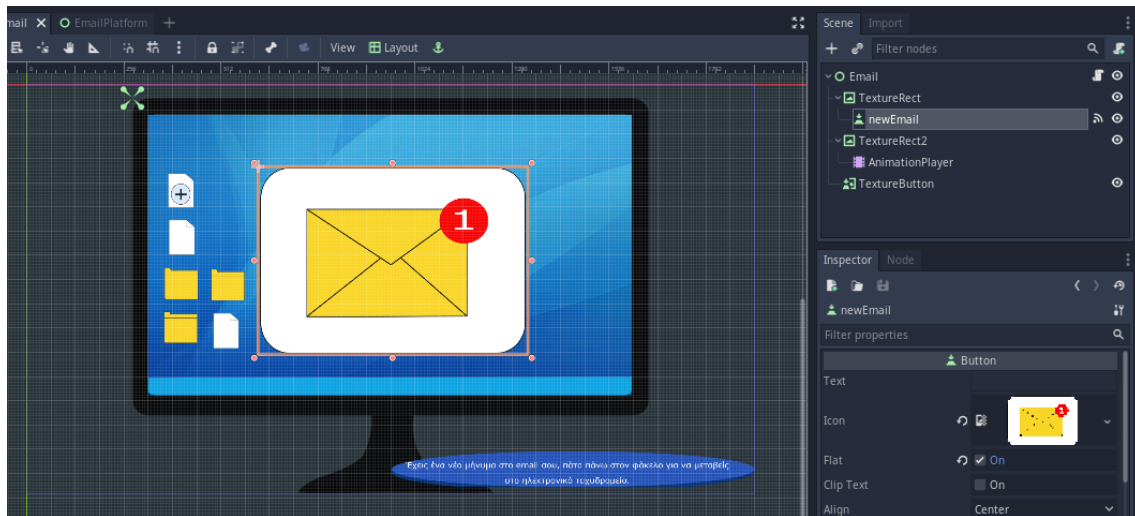


Εικόνα 31. *NewGameButton* (Inspector Script Variables)

6.2.5.2 Σκηνή *Email.tscn*

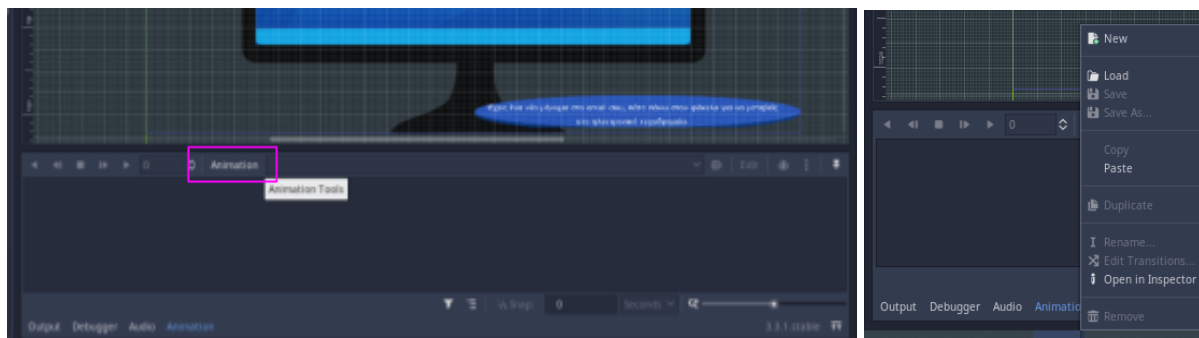
Η πρώτη σκηνή του σεναρίου είναι απλή και αρχίζει να βάζει τον παίκτη στο πνεύμα του παιχνιδιού. Αποτελείται από δύο κόμβους *TextureRect*. Ο ένας κόμβος είναι για το εικονίδιο που αναπαριστά την οθόνη του υπολογιστή, που είναι το μέσο της απειλής και έχει ως παιδί κόμβο ένα κουμπί (*Button*) με όνομα «newEmail» και εικονίδιο (*icon*) έναν κίτρινο φάκελο για να δείξει ένα νέο εισερχόμενο μήνυμα. Ο άλλος κόμβος είναι για το οβαλ σχήμα στο κάτω δεξιά μέρος της οθόνης το οποίο λειτουργεί σαν επεξήγηση της εικόνας που βλέπει μπροστά του ο παίκτης και σαν καθοδήγηση για να πει στον

παίκτη πως έχει την δυνατότητα να πατήσει πάνω στο μήνυμα για να συνεχίσει το παιχνίδι. Το οβάλ αυτό σχήμα υπάρχει και στις υπόλοιπες σκηνές που χρειάζεται ο παίκτης να κάνει κάποια ενέργεια.

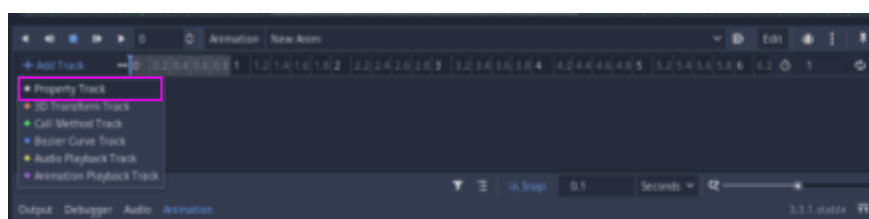


Εικόνα 32. *Email.tscn*

Για να υπάρχει μια μικρή διάδραση, το `TextureRect2` δεν εμφανίζεται απευθείας μαζί με την οθόνη του υπολογιστή, αλλά ένα δευτερόλεπτο αργότερα ως αναδυόμενο παράθυρο (pop up). Η εμφάνιση αυτή γίνεται με τη βοήθεια του κομβίου `AnimationPlayer` που είναι παιδί αυτού του κόμβου που θέλουμε να έχει το συγκεκριμένο εφέ, δηλαδή του `TextureRect2`. Ένας γενικής χρήσης κόμβος για την αναπαραγωγή πηγών κινούμενων εικόνων (Animations). Αφού το εισάγουμε στο δέντρο μας, εμφανίζεται στο κάτω μέρος η καρτέλα Animation. Πατώντας πάνω στα εργαλεία animation (Animation Tools) επιλέγουμε την επιλογή νέο (new) για να φτιάξουμε μια καινούργια κίνηση. Στο αναδυόμενο παράθυρο προσθέτουμε το όνομα του animation (porup) και στη συνέχεια κάνουμε προσθήκη ένα κομμάτι για να επεξεργαστούμε (add track), είδους property.

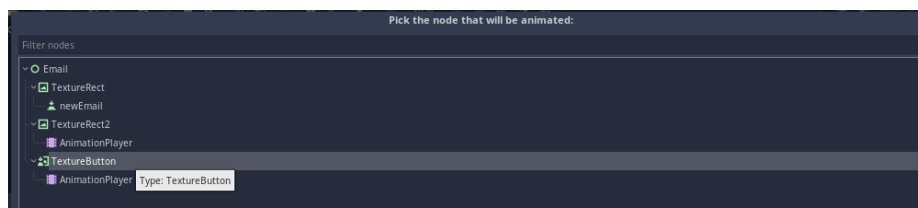


Εικόνα 33. *AnimationPlayer (Email.tscn)*

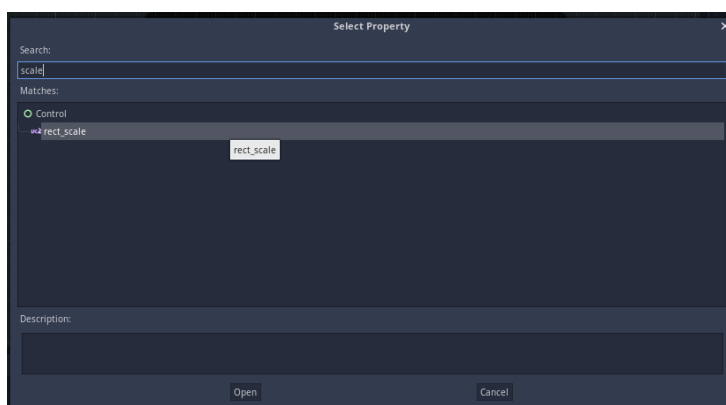


Εικόνα 34. *Property Track (AnimationPlayer)*

Στο αναδυόμενο παράθυρο επιλέγουμε τον κόμβο που θέλουμε να κινείται, και την ιδιότητα που θέλουμε να έχει. Για την popup κίνηση επιλέγουμε την κλιμάκωση (rect_scale). Κλιμακώνεται ο κόμβος, σε σχέση με το rect_size του.

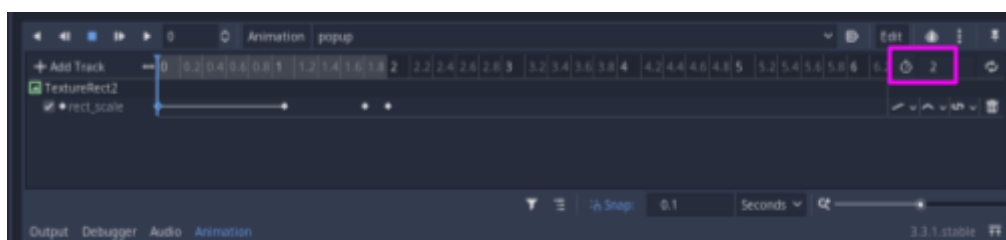


Εικόνα 35. Animated node (AnimationPlayer)



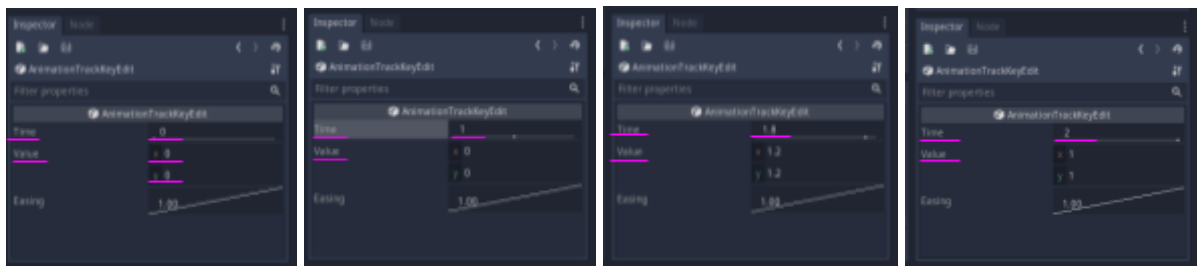
Εικόνα 36. rect_scale (AnimationPlayer)

Στη συνέχεια εισάγουμε σημεία κλειδιά στο πάνω στο χρονοδιάγραμμα. Επέλεξα ο κόμβος μου να εμφανίζεται ένα δευτερόλεπτο αφού μπει η σκηνή και η κίνηση του να διαρκεί για άλλο ένα δευτερόλεπτο, άρα συνολικά όλο το animation διαρκεί δύο δευτερόλεπτα.



Εικόνα 37. popup (AnimationPlayer)

Τα πρώτα δύο σημεία κλειδιά είναι στη χρονική στιγμή 0 και 1 και έχουν τιμές 0 για τα x και y επειδή δεν θέλουμε να φαίνεται το πρώτο δευτερόλεπτο. Από την χρονική στιγμή 1 μέχρι 1.8 το σχήμα κλιμακώνεται με τιμή 1.2 και στις δύο διαστάσεις, όπου τελικά την χρονική στιγμή 2 σταθεροποιείται με την τιμή ένα και στις δύο διαστάσεις.



(α) t=0

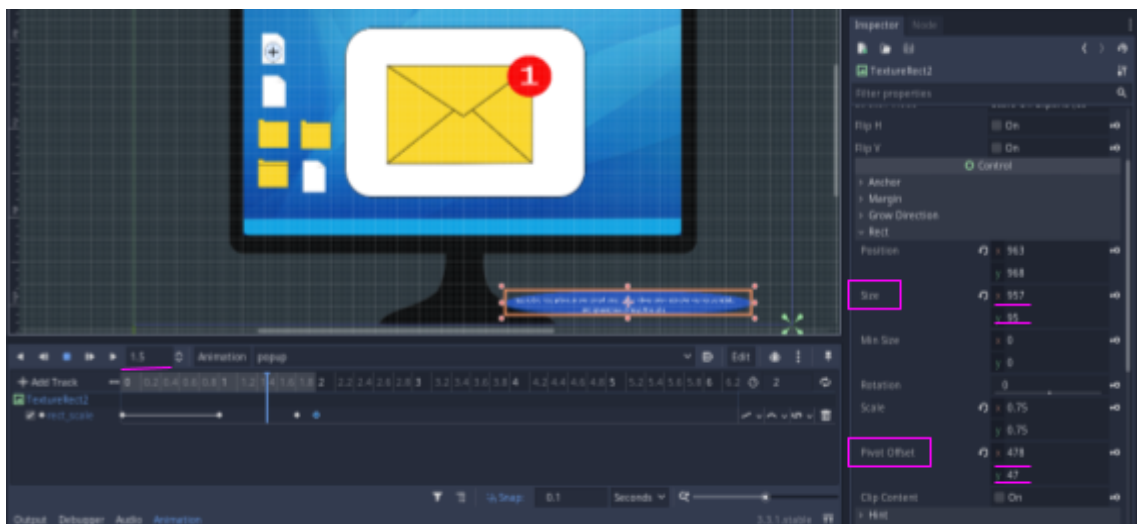
(β) t=1

(γ) t=1.8

(δ) t=2

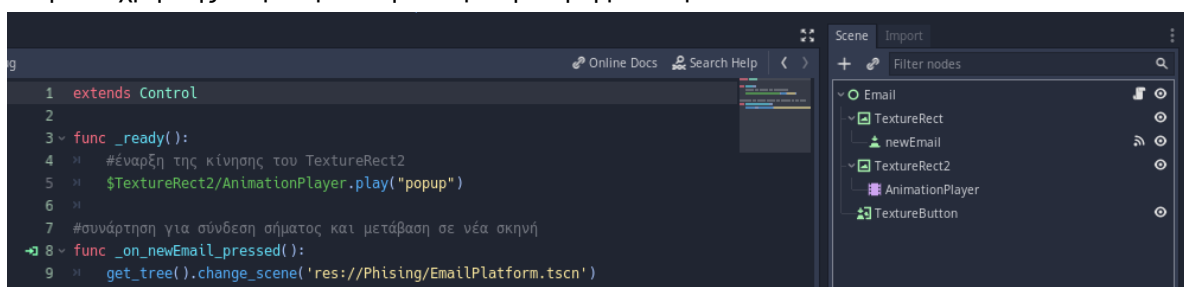
Εικόνα 38. popup timetable (AnimationPlayer)

Αλλάζοντας τη τιμή το `rect_scale`, κλιμακώνεται ο κόμβος γύρω από τον άξονα περιστροφής του κόμβου `rect` (`rect_pivot_offset`). Από προεπιλογή, ο άξονας περιστροφής είναι η επάνω αριστερή γωνία του, άρα θα κλιμακωθεί γύρω από αυτόν τον άξονα περιστροφής. Για να κεντράρουμε τον άξονα στο ορθογώνιο του κόμβου, επιλέγουμε τον χρόνο στα μισά δευτερόλεπτα της κίνησης (η κίνηση είναι από το πρώτο δευτερόλεπτο μέχρι το δεύτερο, άρα 1.5s) και ορίζουμε την ιδιότητα μετατόπισης περιστροφής (`pivot offset`) σε `rect_size / 2`. Το μέγεθος του x είναι 957 και του y:95, άρα η μετατόπιση περιστροφής για x θα είναι 478 και για y:47.



Εικόνα 39. popup pivot_offset (AnimationPlayer)

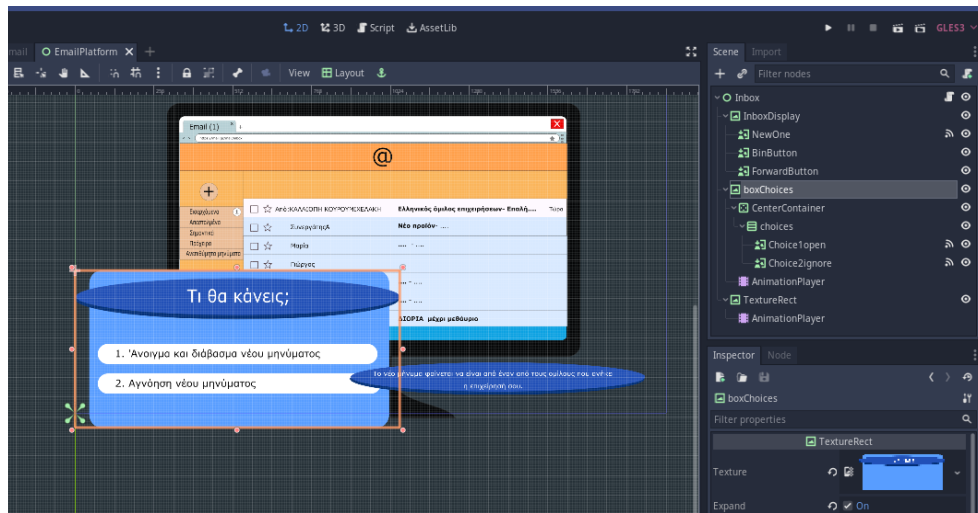
Γράφοντας στο script της σκηνής, «Email.tscn», μέσα στην συνάρτηση `_ready`, την εντολή της γραμμής 3 με το που θα τρέξει η σκηνή θα ξεκινήσει η αναπαραγωγή και την κίνησης. Τέλος, στη γραμμή 6 φαίνεται το συνδεδεμένο σήμα για το κουμπί με εικονίδιο το νέο μήνυμα, το οποίο όταν πατηθεί ο χρήστης θα μεταβεί στην επόμενη σκηνή με όνομα «EmailPlatform».



Εικόνα 40. Email.gd

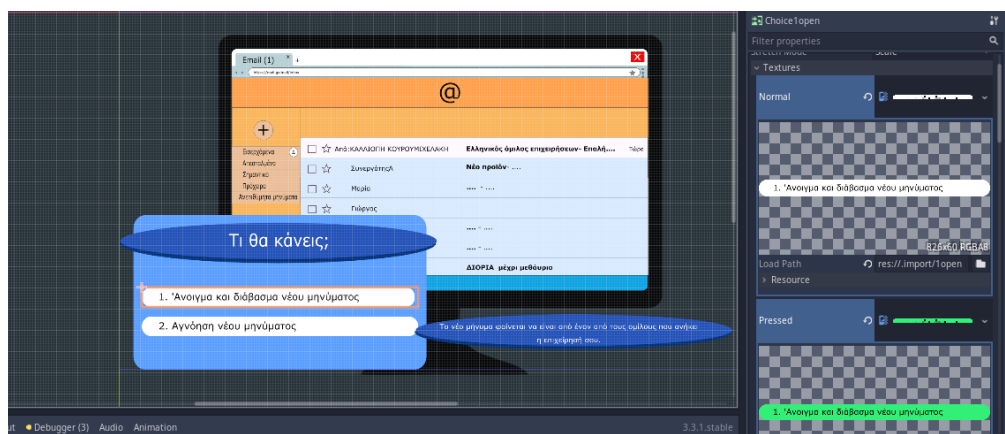
6.2.5.3. Σκηνή «EmailPlatform.tscn»

Η δεύτερη σκηνή του σεναρίου είναι η «EmailPlatform.tscn». Σε αυτή τη σκηνή εκτός από την οθόνη του υπολογιστή και την αφήγηση έχει προστεθεί ένα κουτί επιλογών με κόμβο TextureRect, το οποίο ρωτάει τον χρήστη τι κίνηση θα επιλέξει να κάνει και του δίνει 2 επιλογές ώστε να διαλέξει. Τις επιλογές που τελικά θα κάνει ο χρήστης, μπορεί να τις δηλώσει είτε πατώντας πάνω στα δύο πλαίσια/κουμπιά, μέσα στο κουτί επιλογών, είτε πατώντας τα κουμπιά πάνω στην οθόνη του υπολογιστή.

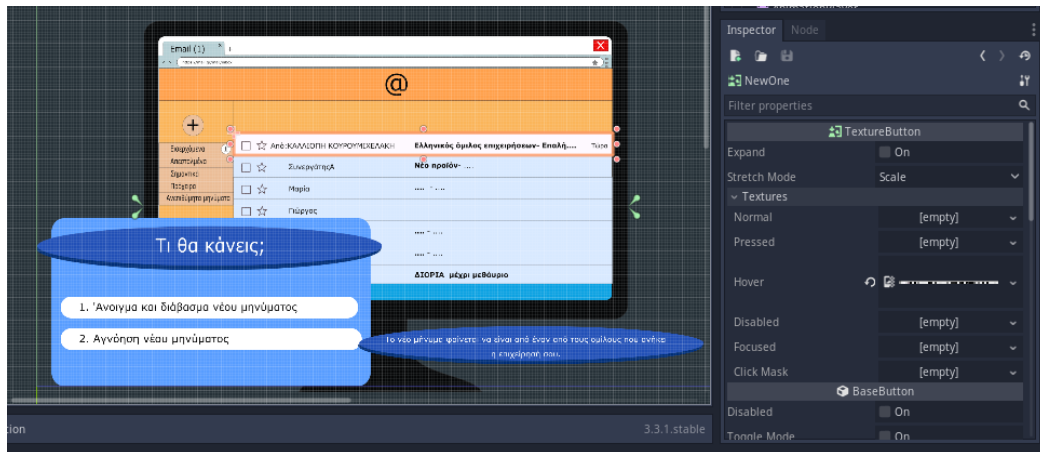


Εικόνα 41. EmailPlatform.tscn

Τα κουμπιά της οθόνης του υπολογιστή προσομοιώνουν δυνατότητες που θα μπορούσε να κάνει ο χρήστης και στον πραγματικό του υπολογιστή. Για παράδειγμα για να ανοίξει το μήνυμα μπορεί είτε να πατήσει την «Επιλογή1» στο κουτί επιλογών η οποία είναι κόμβος TextueButton και όταν πατηθεί γίνεται πράσινη, όπως και η «Επιλογή2», (Εικόνα), είτε το κουμπί «NewOne» πάλι κόμβου TextueButton, το οποίο όταν περνάει από πάνω του το ποντίκι αλλάζει χρώμα για να καταλάβει ο χρήστης πως αυτή η περιοχή είναι κουμπί και μπορεί να την επιλέξει (Εικόνα).

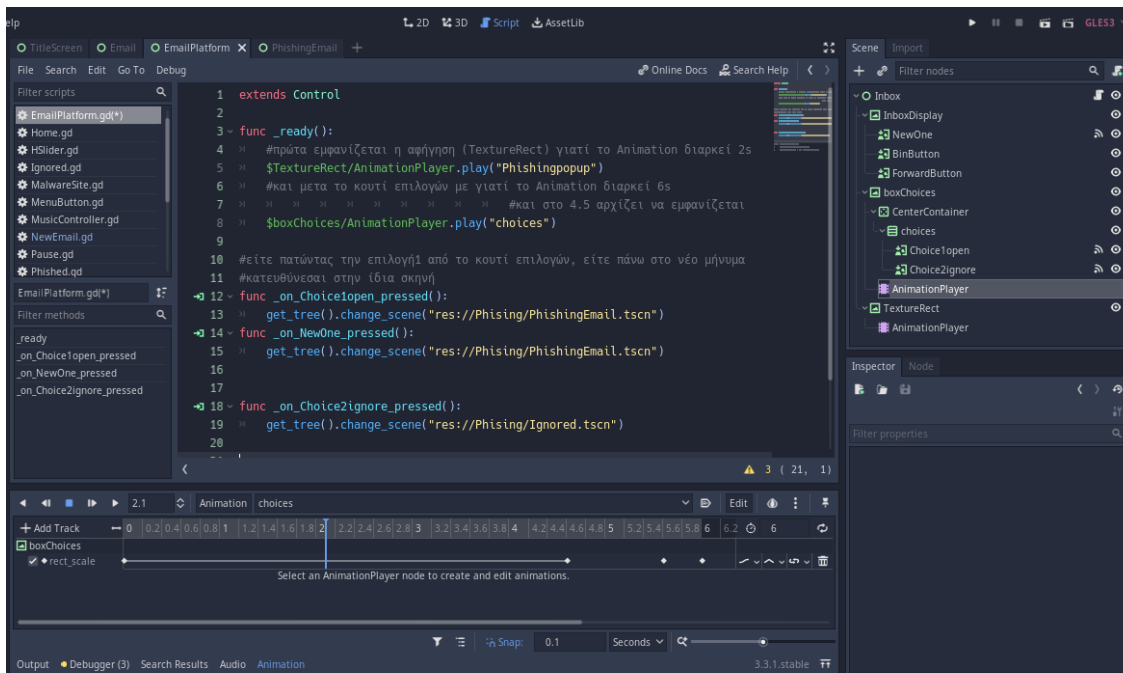


Εικόνα 42. Choice1open button (EmailPlatform)



Εικόνα 43. NewOne button (*EmailPlatform*)

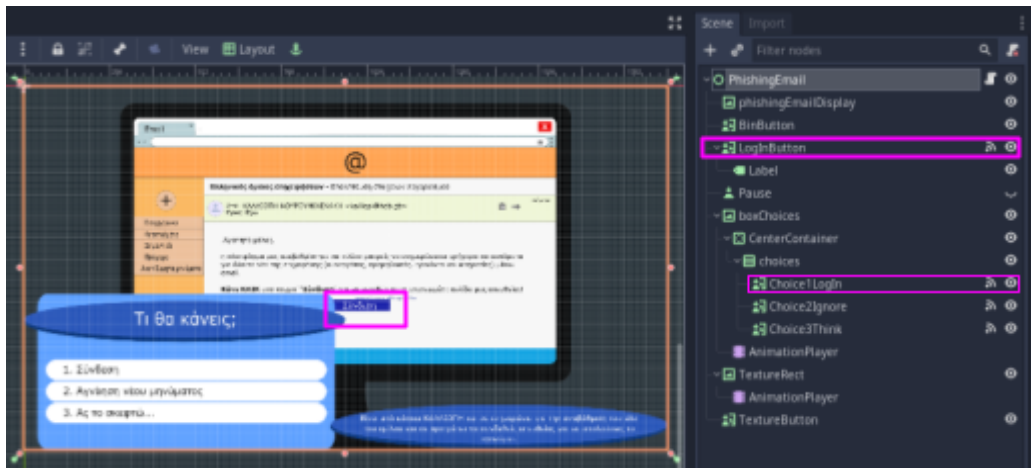
Όποια κίνηση κι αν επιλέξει να κάνει και με οποιονδήποτε από τους δύο τρόπους, ο παίκτης θα φύγει από αυτή τη σκηνή και θα πάει σε άλλη.



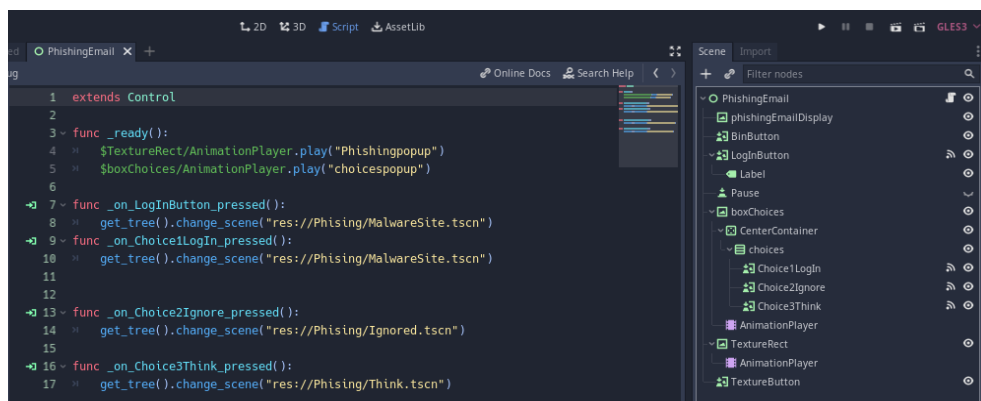
Εικόνα 44. *EmailPlatform.gd*

6.2.5.4 Σκηνή «PhishingEmail.tscn»

Η σκηνή «PhishingEmail» προσφέρει τρεις διαφορετικές επιλογές στο κουτί επιλογών και η «Επιλογή1» μπορεί να υλοποιηθεί και πατώντας το κουμπί «Σύνδεση» (LoginButton).



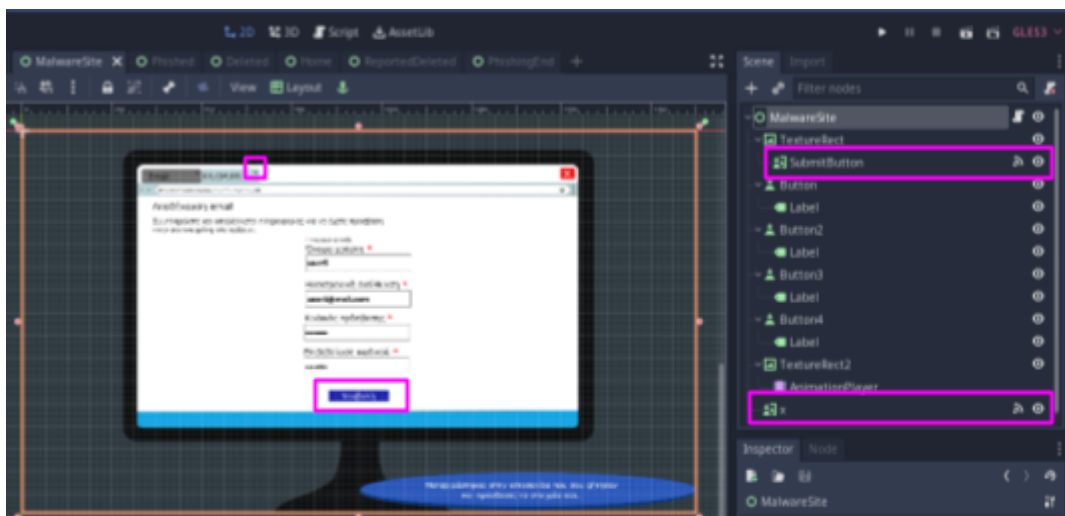
Εικόνα 45. *PhishingEmail.tscn*



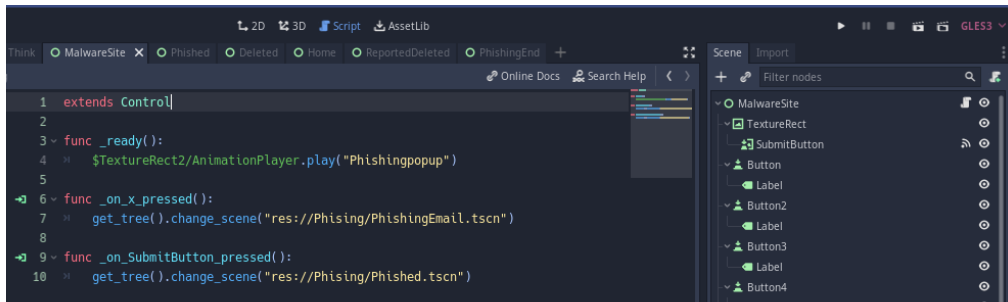
Εικόνα 46. *PhishingEmail.gd*

6.2.5.5 Σκηνή «MalwareSite.tscn»

Στη σκηνή «MalwareSite» υπάρχει η οθόνη του υπολογιστή και η αφήγηση χωρίς το κουτί επιλογών. Διαθέσιμα κουμπιά είναι αυτό της υποβολής (SubmitButton) και της εξόδου από την κακόβουλη ιστοσελίδα με το κουμπί «X» στην καρτέλα του περιηγητή.

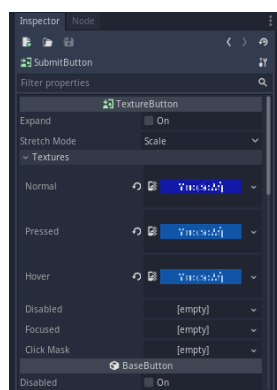


Εικόνα 47. *MalwareSite.tscn*

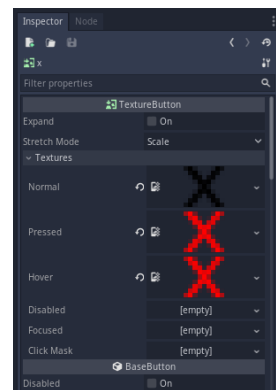


Εικόνα 48. *MalwareSite.gd*

Όταν τα κουμπιά υποβολής (SubmitButton) και εξόδου (κουμπί “X”) πατηθούν ή περάσει ο κέρσορας από πάνω τους τότε αντικαθίστανται με τα ίδια εικονίδια αλλά σε άλλο χρώμα (Εικόνα).



(α) SubmitButton

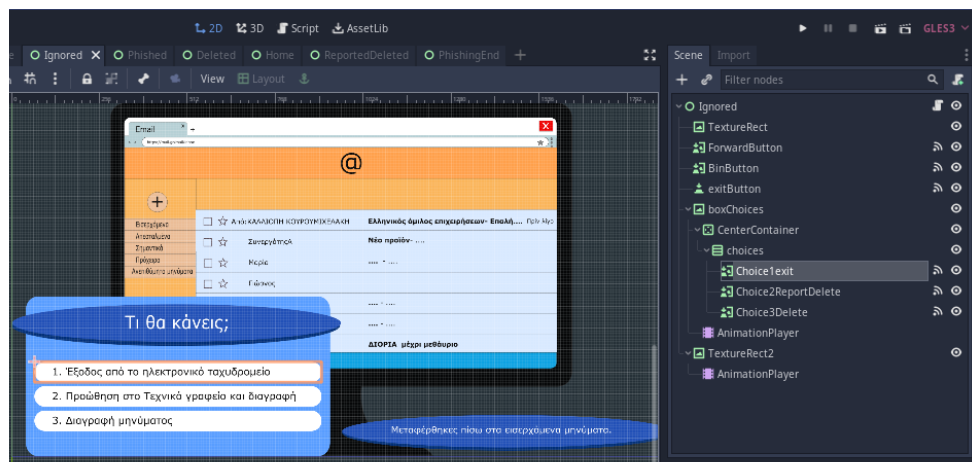


(β) “X”

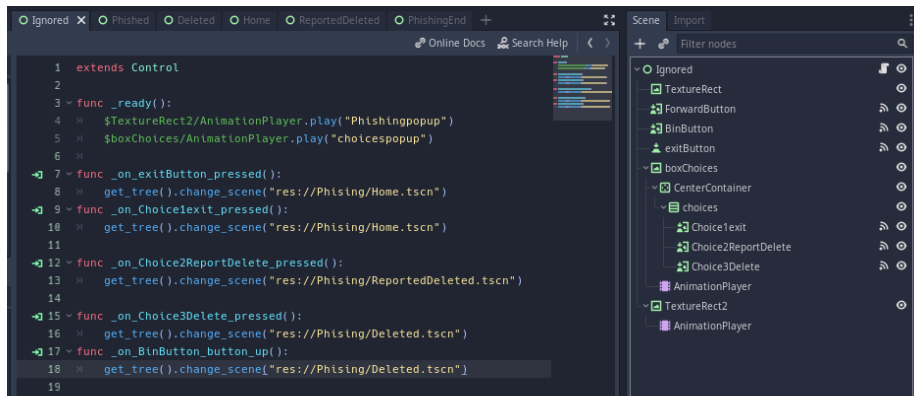
Εικόνα 49. Buttons (*MalwareSite*)

6.2.5.6 Σκηνή «Ignored.tscn»

Η σκηνή «Ignored» ακολουθεί την ίδια λογική με τη σκηνή «EmailPlatform».



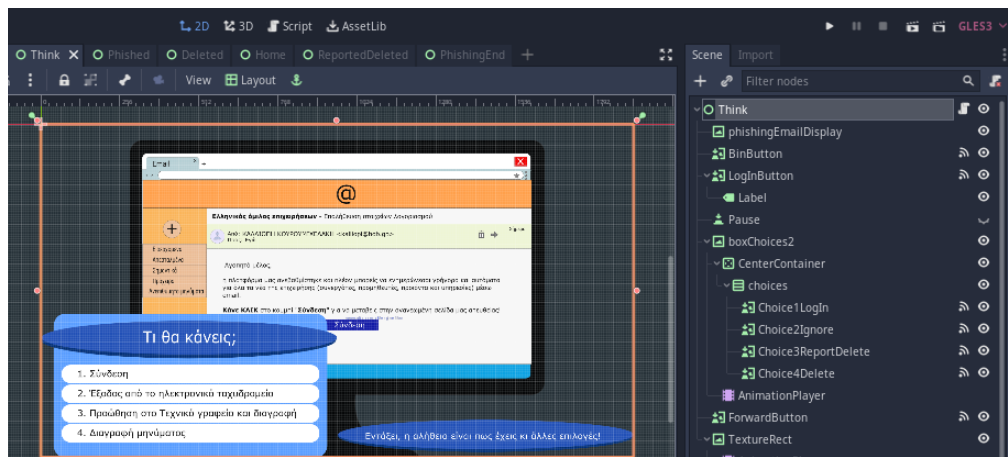
Εικόνα 50. *Ignored.tscn*



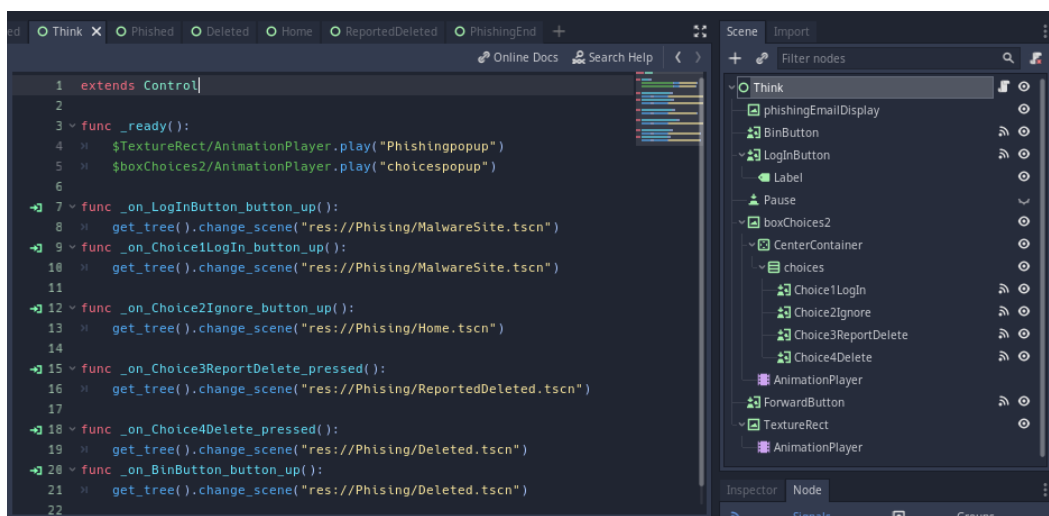
Εικόνα 51. Ignored.gd

6.2.5.7 Σκηνή «Think.tscn»

Όπως και η σκηνή «Think» ακολουθεί την ίδια λογική με τη σκηνή «EmailPlatform».



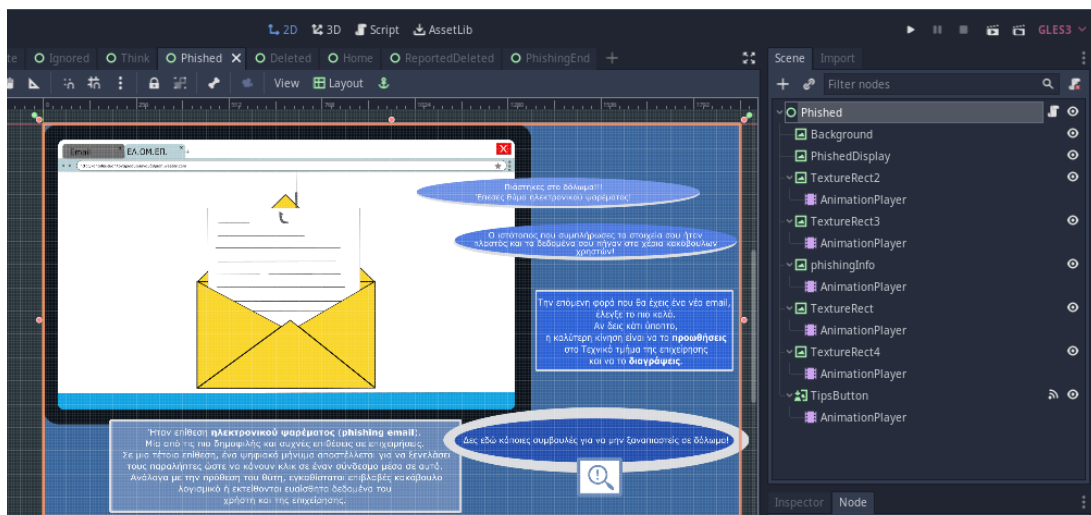
Εικόνα 52. Think.tscn



Εικόνα 53. Think.gd

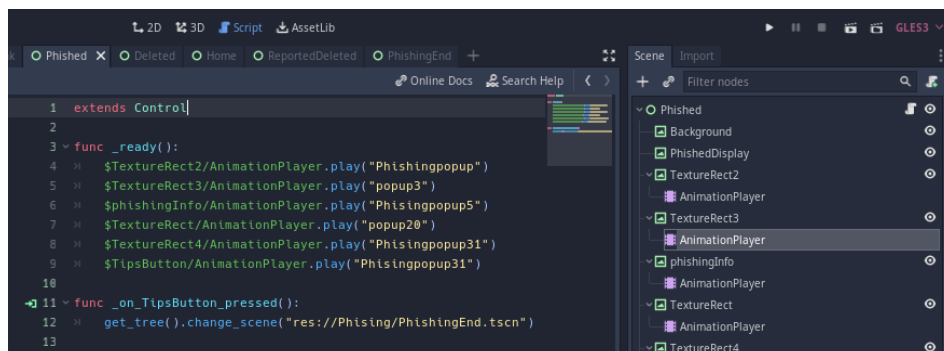
6.2.5.8 Σκηνή «Phished.tscn»

Η σκηνή αυτή, είναι μία από τις τελικές σκηνές όπου φαίνεται το αποτέλεσμα τις επιθέσεις του ηλεκτρονικού ψαρέματος αν πέτυχε ή όχι. Στη σκηνή αυτή έχουμε την οθόνη του υπολογιστή με ένα εικονίδιο που σηματοδοτεί ότι ο παίκτης έπεσε στην παγίδα του κακόβουλου χρήστη και κάποια πλαίσια τα οποία ανακοινώνουν το αποτέλεσμα του παιχνιδιού και ενημερώνουν τον παίκτη για το τι είναι ακριβώς αυτή η απειλή στην οποία έπεσε θύμα και στο τέλος τον συμβουλεύουν να πατήσει το κουμπί των συμβουλών, ώστε να ενημερωθεί κατάλληλα για τα σημεία κλειδιά που θα πρέπει να προσέχει κάθε επόμενη φορά που θα του έρθει ένα νέο μήνυμα ηλεκτρονικού ταχυδρομείου.



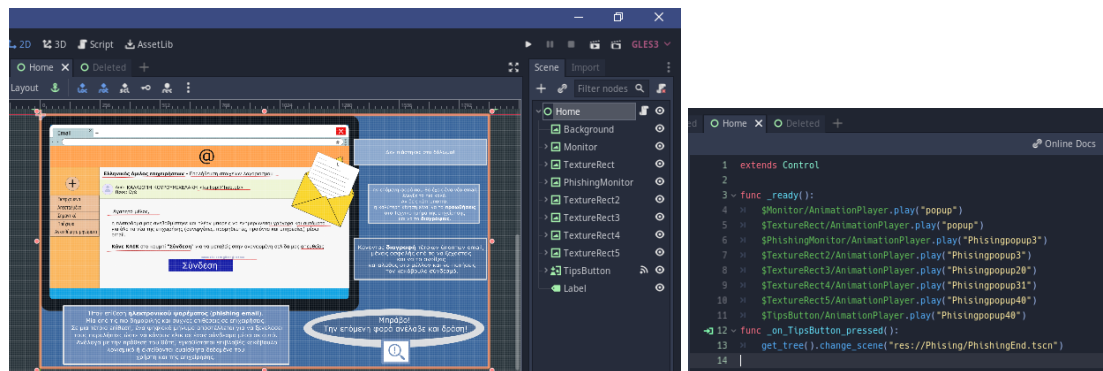
Εικόνα 54. *Phished.tscn*

Κάθε πλαίσιο έχει διαφορετικό animation player επειδή έχει διαφορετική διάρκεια κίνησης. Τα πλαίσια εμφανίζονται ένα-ένα ώστε να προλάβει ο χρήστης να τα διαβάσει. Δεν υπάρχει δυνατότητα να προσπεράσει ή να αυξήσει την ταχύτητα που εμφανίζονται τα πλαίσια διότι σκοπός αυτής της σκηνής, είναι ο παίκτης να τα διαβάσει όλα.

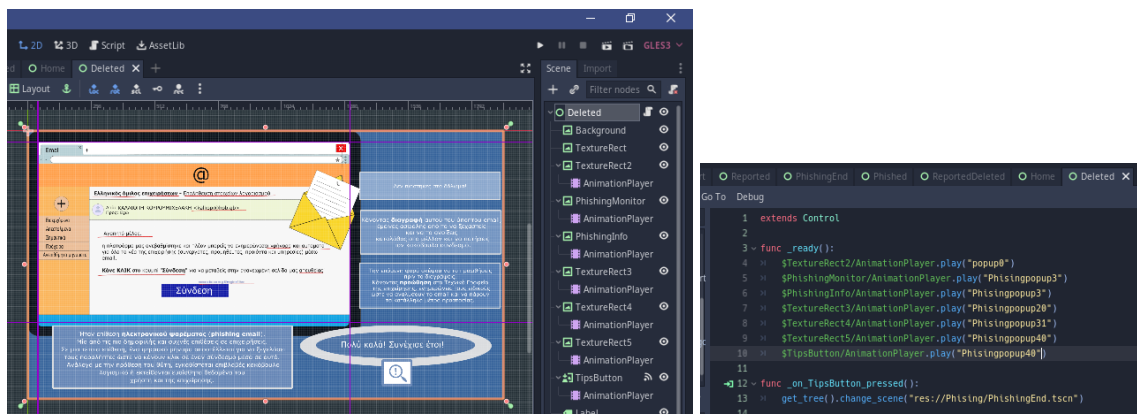


Εικόνα 55. *Phished.gd*

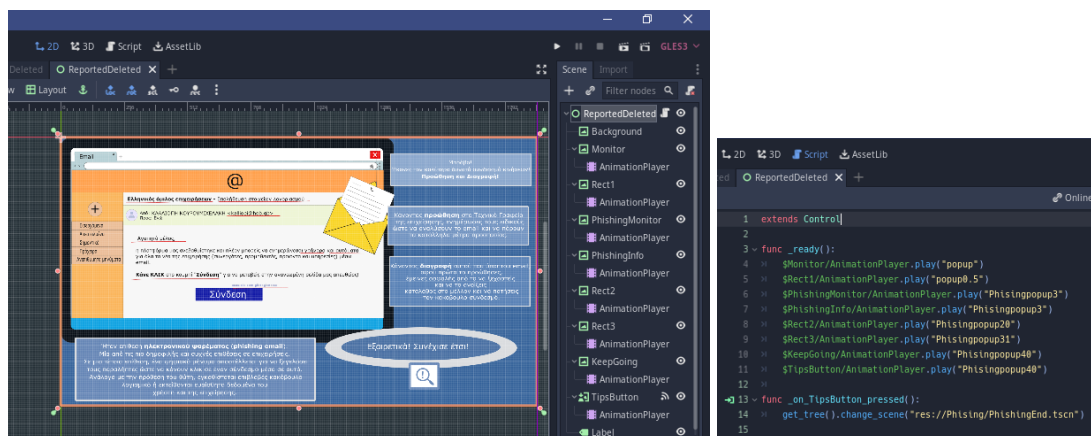
Η ίδια λογική χρησιμοποιήθηκε στη δημιουργία των σκηνών «Home» (Εικόνα), «Deleted» (Εικόνα) και «ReportedDeleted» (Εικόνα).



Εικόνα 56. Home.tscn και Home.gd



Εικόνα 57. Deleted.tscn και Deleted.gd

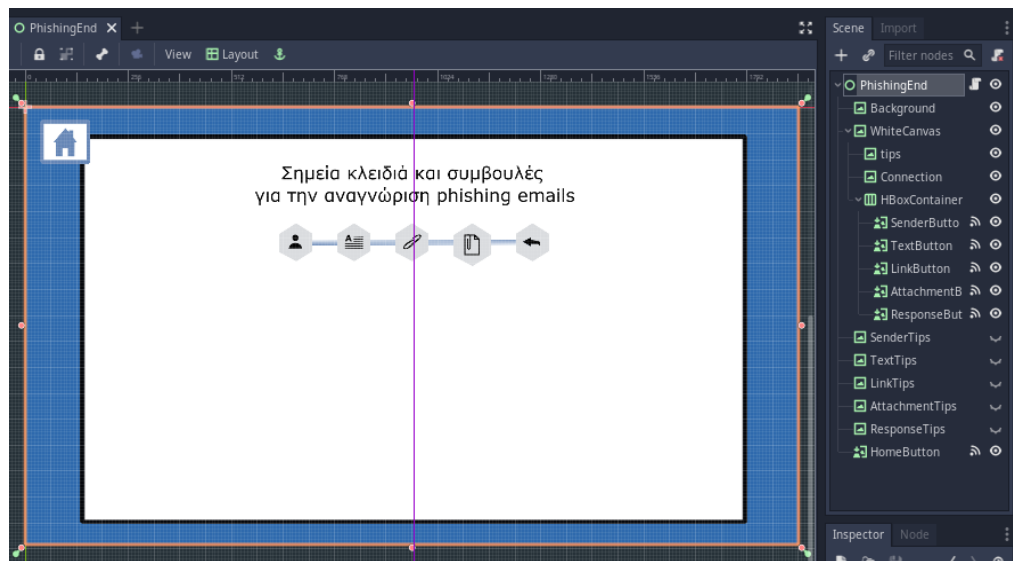


Εικόνα 58. ReportedDeleted.tscn και ReportedDeleted.gd

6.2.5.9 Σκηνή «PhishingEnd.tscn»

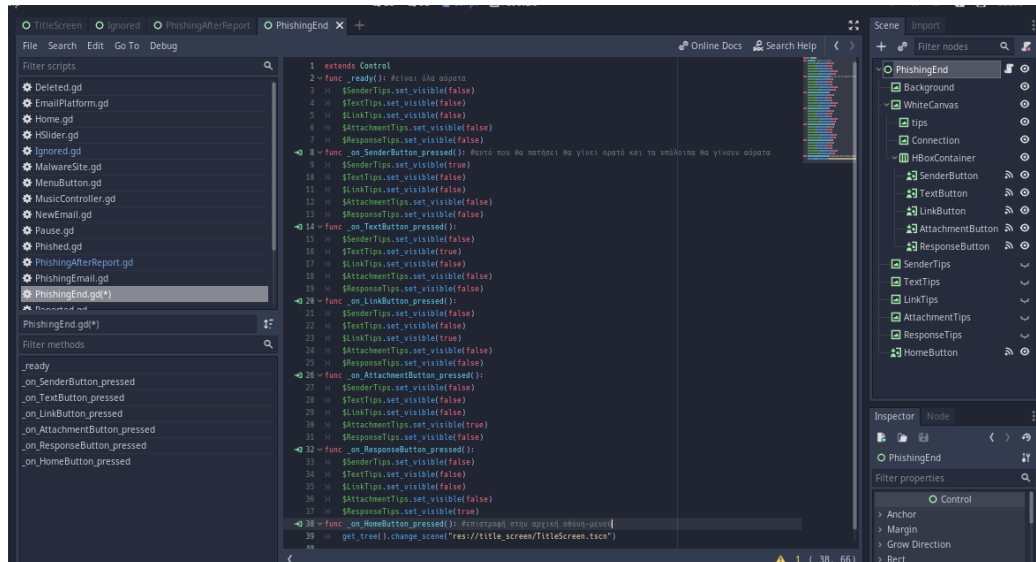
Η τελική σκηνή του σεναρίου είναι σαν οδηγός για αποφυγή εξαπάτησης από ηλεκτρονικό ψάρεμα. Έχει πέντε κουμπιά που το καθένα αντιπροσωπεύει κάποιο “κομμάτι” στην διαδικασία παραλαβής ενός νέου εισερχομένου μηνύματος στο ηλεκτρονικό ταχυδρομείο που χρήζει ιδιαίτερης προσοχής. SenderButton για τον αποστολέα, TextButton για το σώμα του μηνύματος «LinkButton» για τους υπερσυνδέσμους και τα κουμπιά μέσα στο μήνυμα,

«AttachmentButton» για συνημμένα αρχεία και «ResponseButton» για απάντηση σε μηνύματα.



Εικόνα 59. *PhishingEnd.tscn*

Όλα τα κουμπιά είναι κόμβοι `TextureButton` και μόλις πατηθούν εμφανίζεται το αντίστοιχο κείμενο που είναι `TextureRect`. Πατώντας το κουμπί στη γωνιά πάνω αριστερά με το σπίτι, επιστρέφει ο παίκτης στην αρχική σκηνή με το μενού («TitleScreen»).



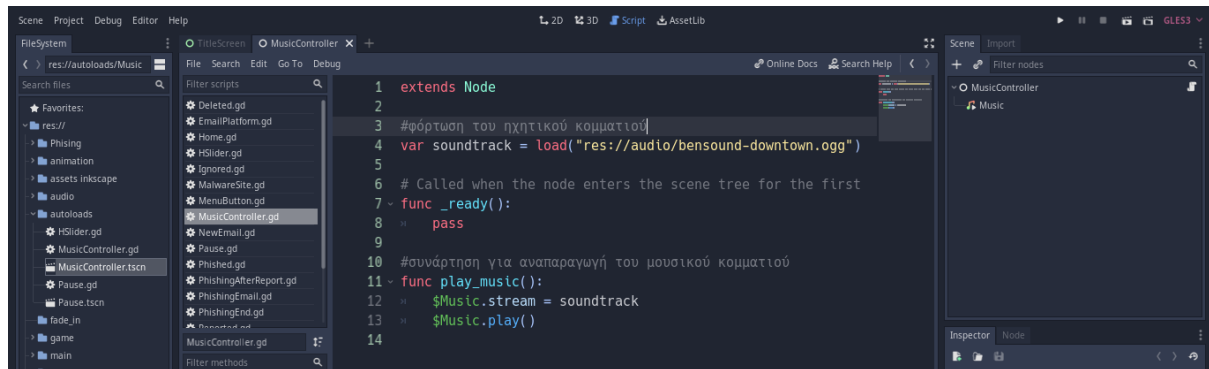
Εικόνα 60. *PhishingEnd.gd*

6.2.5.10 autoloads

Η Godot προσφέρει μια δυνατότητα αυτόματης φόρτωσης κόμβων στη ρίζα του έργου, επιτρέποντάς να έχουμε πρόσβαση σε αυτούς παγκοσμίως. Αυτοί οι αυτόματα φορτωμένοι κόμβοι δεν απελευθερώνονται όταν αλλάζει η σκηνή από κώδικα με το `SceneTree.change_scene`. Η παύση και η μουσική προστέθηκαν ως νέες σκηνές και

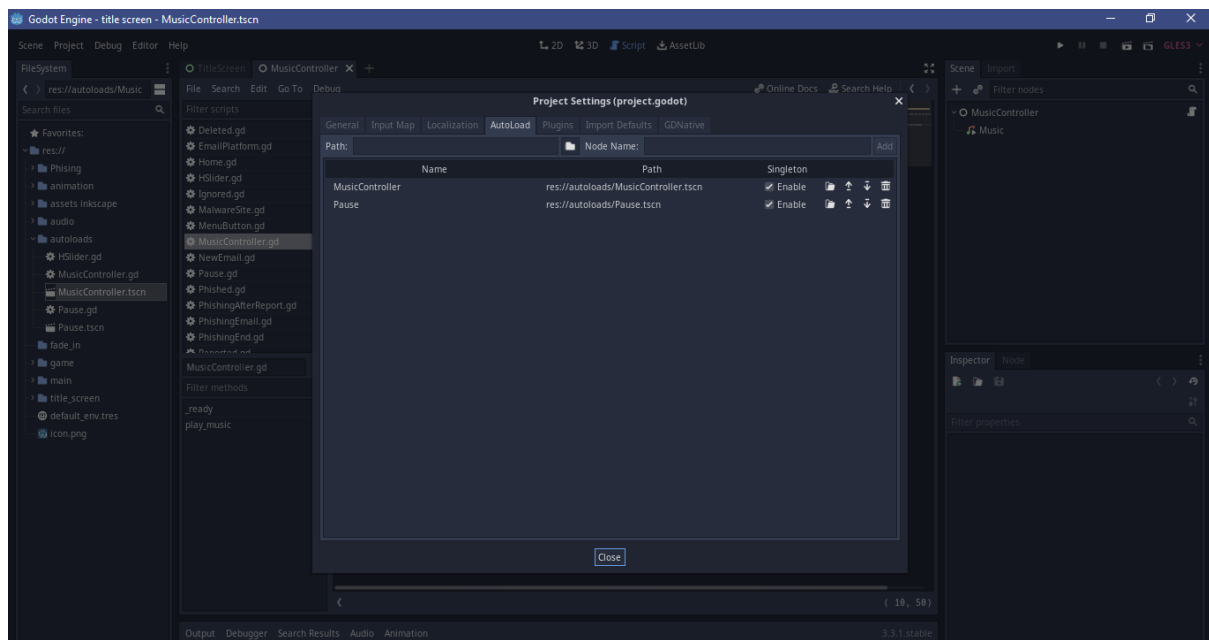
χρησιμοποίησαν την λειτουργία autoload (αυτόματη φόρτωση) ώστε να μπορούν να αξιοποιηθούν από όλες τις σκηνές χωρίς κάποια διακοπή ή επανεκκίνηση.

Δημιουργήθηκε ένας φάκελος με όνομα «autoloads». Αρχικά για την μουσική προστέθηκε μια νέα σκηνή με όνομα «MusicController.tscn» όπου σε αυτή δημιουργήθηκε ένας βασικός κόμβος (MusicController) και παιδί αυτού, ένας κόμβος AudioStreamPlayer (Music) για να γίνει η αναπαραγωγή της μουσικής.



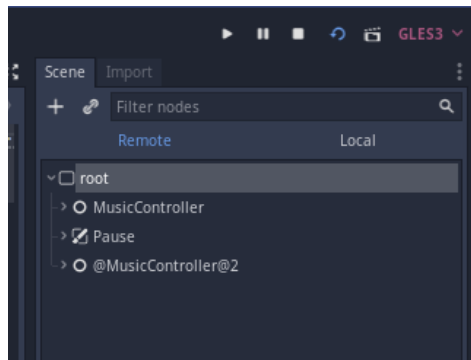
Εικόνα 61. MusicController.gd

Αφου δημιουργήθηκε και ο κώδικας για να φορτωθεί και να αναπαραχθεί όταν χρειαστεί το ηχητικό κομμάτι, προστέθηκε η σκηνή στα autoloads του συστήματος (Project→ Project Settings → Autoloads).



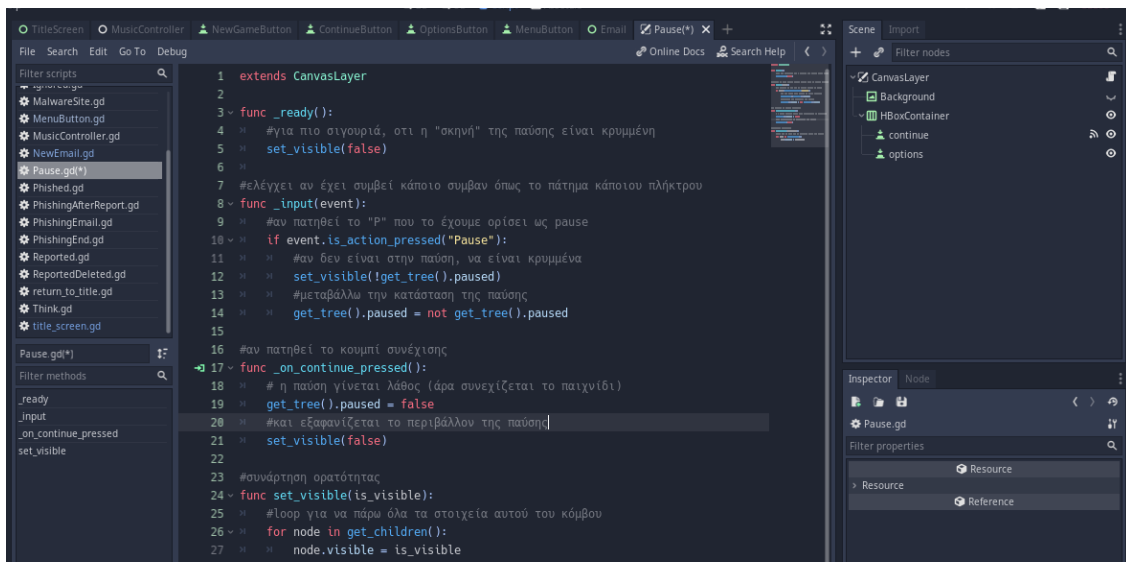
Εικόνα 62. Autoload settings

Με αυτό τον τρόπο μπορούμε να δούμε από το remote panel, που είναι η ζωντανή αναπαράσταση του κεντρικού δέντρου, δηλαδή του παιχνιδιού, πως ο MusicController έχει φορτωθεί.



Εικόνα 63. Remote panel

Παρόμοια διαδικασία έγινε και για την λειτουργία παύσης του παιχνιδιού. Μέσα στον φάκελο autoloads δημιουργήθηκε η σκηνή «Pause.tscn» με CanvasLayer κόμβο και προστέθηκε script με όνομα «Pause.gd». Στη συνάρτηση _input η οποία περιμένει ένα συμβάν (event) να συμβεί, πιάνω το πλήκτρο «P». Οπότε αν πατηθεί το «P» που το έχουμε ορίσει στο input map ως παύση (pause) μεταβάλλεται η κατάσταση της παύσης από False (Ψευδής) σε True (Αληθής) και αντίστροφα.



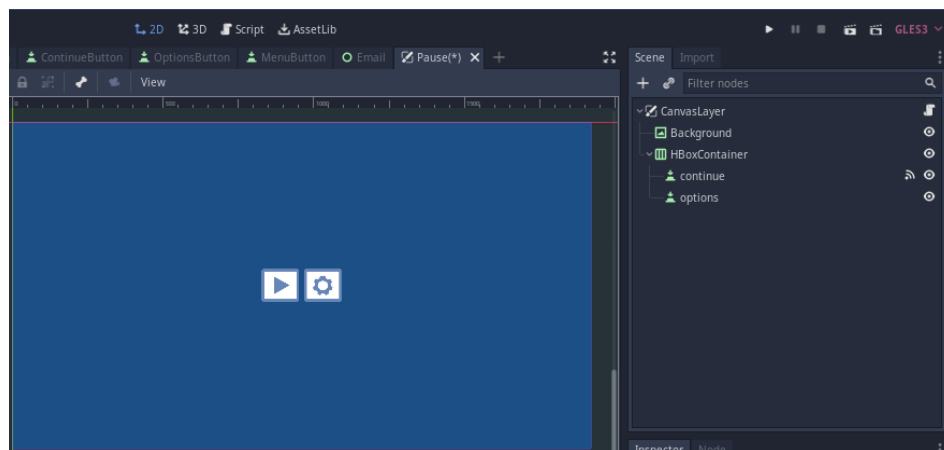
Εικόνα 64. Pause.gd

Έγινε προσθήκη και αυτής της σκηνής στους autoloads πόρους του έργου. Στη Godot όλοι οι κόμβοι έχουν τη δυνατότητα pause και όταν είναι ενεργή αυτή η κατάσταση, όλες οι διαδικασίες 2D ή 3D, όπως rendering, πιάσιμο σημάτων, και άλλοι υπολογισμοί σταματάνε, όπως και τα δεδομένα εισαγωγής από αυτούς τους κόμβους. Από προεπιλογή όλα τα στοιχεία κληρονομούν αυτή την κατάσταση δηλαδή χρησιμοποιούν την κατάσταση παύσης του γονικού τους κόμβου. Αλλάζοντας λοιπόν την κατάσταση της παύσης αλλάζει παντού, σε όλα τα στοιχεία, ακόμα και στην σκηνή της παύσης, όμως χρειάζεται να έχουμε την δυνατότητα να επιστρέψουμε στην κατάσταση λειτουργίας του παιχνιδιού, κάνοντας την κατάσταση της παύσης False. Για αυτό τον λόγο, έγινε αλλαγή του τρόπου παύσης για την σκηνή «Pause.tscn» από Inherit (κληρονομιά) σε Process (διαδικασία), επειδή όταν πατάει ο χρήστης παύση, θέλουμε να δουλεύει η σκηνή της παύσης, ανεξάρτητα με το τι κάνουν τα

υπολοιπα στοιχεία του παιχνιδιού. Όταν ο χρήστης πατήσει το «P» σταματούν όλα στο παιχνίδι, εκτός της σκηνής της παύσης, με τις λειτουργίες που προσφέρει.

Μια από τις λειτουργίες που προσφέρει είναι το κουμπί συνέχισης του παιχνιδιού, ώστε ο παίκτης να μπορεί να συνεχίσει το παιχνίδι μετά την παύση του.

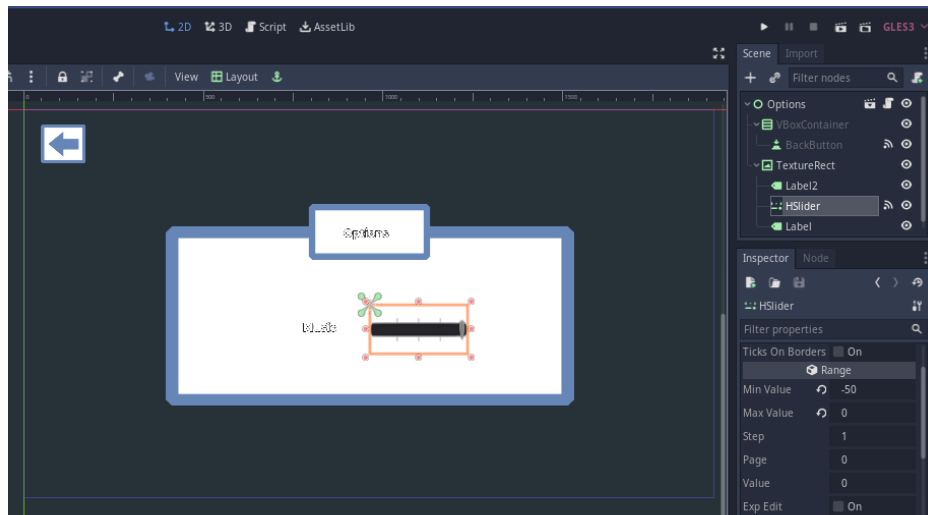
Για την εμφάνιση της σκηνής παύσης επιλέχθηκε ένα TextureRect με μπλε εικονίδιο και ορατότητα στο 50%, ως Background, μέσα στο CanvasLayer. Το CanvasLayer είναι ένας κόμβος που προσθέτει ένα ξεχωριστό επίπεδο απόδοσης 2D για όλα τα παιδιά και τα εγγόνια του. Τα παιδιά του Viewport θα σχεδιάσουν από προεπιλογή στο επίπεδο "0", ενώ ένα CanvasLayer θα σχεδιάσει σε οποιοδήποτε αριθμητικό επίπεδο. Εδώ ρυθμίστηκε στο επίπεδο (layer) 1. Τα στρώματα με μεγαλύτερο αριθμό θα τραβηχτούν πάνω από αυτά που έχουν μικρότερο αριθμό.



Εικόνα 65. *Pause.tscn*

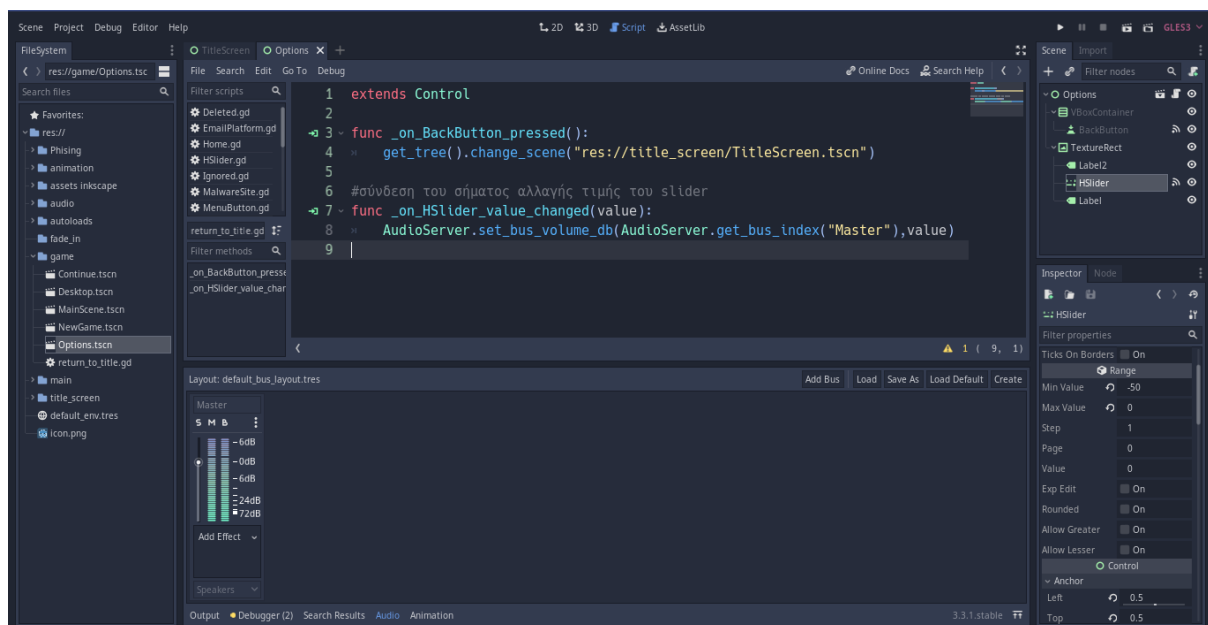
6.2.5.10. Σκηνή «Options.tscn»

Η σκηνή «Options», είναι οι ρυθμίσεις του παιχνιδιού και εμφανίζεται όταν ο χρήστης πατάει το κουμπί options από την αρχική οθόνη του παιχνιδιού. Η σκηνή αυτή στην κατάσταση που είναι τώρα προσφέρει μόνο ρύθμιση για τον ήχο μέσω ενός slider, ο οποίος επηρεάζει την ένταση του ήχου στο παιχνίδι (Εικόνα). Ο κώδικας επεξεργασίας ήχου του Godot έχει γραφτεί με γνώμονα τα παιχνίδια, με στόχο να επιτευχθεί η βέλτιστη ισορροπία μεταξύ απόδοσης και ποιότητας ήχου. Το περιβάλλον ήχου του Godot έχει σχεδιαστεί για να ανταποκρίνεται στις προσδοκίες των επαγγελματιών σχεδιασμού ήχου. Για το σκοπό αυτό, χρησιμοποιεί κυρίως την κλίμακα decibel. Τα 0 dB είναι το μέγιστο δυνατό πλάτος σε ένα ψηφιακό ηχοσύστημα. Ο ήχος με πολύ μεγάλα πλάτη για να παρασταθεί σωστά κάτω από 0 dB δημιουργεί ένα είδος παραμόρφωσης που ονομάζεται αποκοπή. Για να αποφευχθεί η αποκοπή, η μίξη ήχου πρέπει να είναι διατεταγμένη έτσι ώστε η έξοδος του κύριου διαύλου να μην υπερβαίνει τα 0 dB. Κάθε 6 dB κάτω από το όριο των 0 dB, η ηχητική ενέργεια μειώνεται στο μισό. Αυτό σημαίνει πως η ένταση του ήχου στα -6 dB είναι μισή πιο δυνατή από τα 0dB. Στα -12 dB είναι το μισό πιο δυνατό από -6 dB και ούτω καθεξής. Ο ήχος θεωρείται ότι δεν ακούγεται μεταξύ -60 dB και -80 dB όταν χρησιμοποιούμε decibels. Οπότε το εύρος του slider ορίστηκε σε μέγιστη τιμή 0 dB και ελάχιστη τιμή - 60 decibels, όπου δεν υπάρχει καθόλου ήχος στην ελάχιστη τιμή.



Εικόνα 66. Options.tscn

Τέλος συνδέθηκε το σήμα αλλαγής τιμής του slider στο script του μενού. Χρησιμοποιήθηκε audio service που είναι μία διεπαφή διακομιστή χαμηλού επιπέδου για πρόσβαση στον ήχο έτσι ώστε κάθε φορά που θα αλλάζει η τιμή μέσω του slider, να ρυθμίζεται η ένταση του διαύλου, με όνομα «Master», στην αντίστοιχη τιμή (Εικόνα).



Εικόνα 67. Options.gd

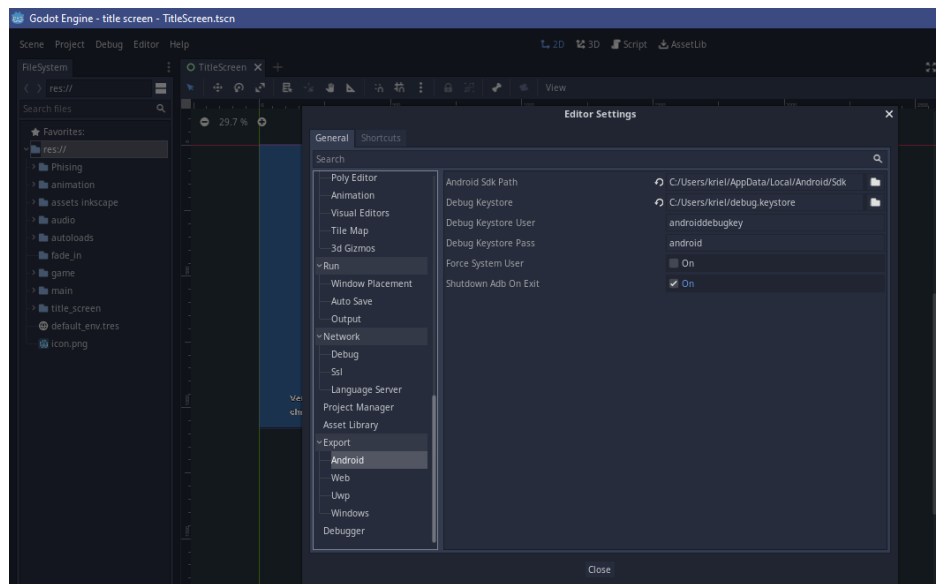
6.2.6 Πλατφόρμες έκδοσης

Η μηχανή Godot διαθέτει export menu με λίστα πλατφορμών (Android, IOS, HTML5, Mac OSX, Windows Universal, Windows Desktop, Linux/X11) όπου μπορείς να επιλέξεις την επιθυμητή πλατφόρμα εξαγωγής για το project σου.

Ένα θετικό με την χρήση της μηχανής Godot είναι ότι με λίγες μόνο τροποποιήσεις μπορεί να υπάρξουν εκδόσεις του παιχνιδιού για όλες τις παραπάνω πλατφόρμες. Το SAGE εξάχθηκε στην πλατφόρμα των Windows (στις εκδόσεις 7,8,10), Mac OSX, Android.

Για την εξαγωγή σε κάποιες πλατφόρμες όπως των Windows και Android, απαιτούνται πρόσθετα εργαλεία (SDK) για εγκατάσταση. Η εξαγωγή σε Android χρειάζεται και η εγκατάσταση του λογισμικού Android Studio. Στη συνέχεια στις ρυθμίσεις του Godot, στο editor settings→export → Android, πρέπει να εισαχθούν τα κατάλληλα μονοπάτια (Android SDK Path, Debug keystroke) επειδή θέλουμε αυτά τα εργαλεία να υπογράψουν και να εξαγάγουν το Android package. Στην έκδοση 3.3.1 του Godot που χρησιμοποίησα,

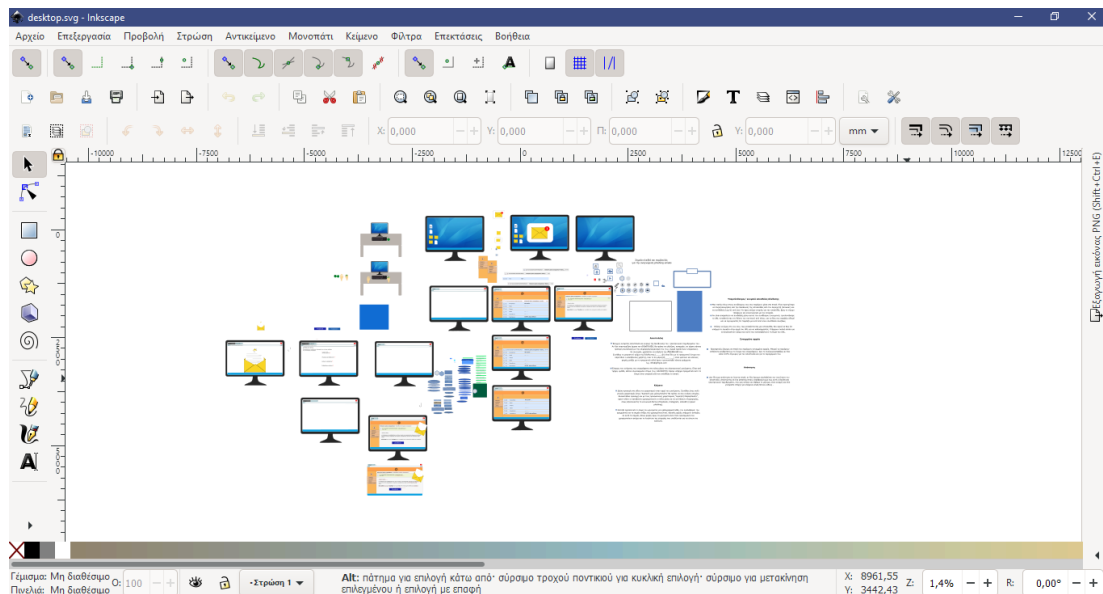
- το πρώτο μονοπάτι που χρειάζεται να προσθέσουμε είναι εκείνο που περιέχει το Android Sdk (C:\Users\kriel\AppData\Local\Android\Sdk)
- το δεύτερο μονοπάτι είναι για το Debug keystroke, επειδή δεν είχε δημιουργηθεί από το JDK ούτε από το Android Studio χρησιμοποίησα το βασικό εργαλείο του JDK μέσω της γραμμής εντολών για να το δημιουργήσω με την εντολή «keytool -keyalg RSA -genkeypair -alias androiddebugkey -keypass android -keystore debug.keystore -storepass android -dname "CN=Android Debug,O=Android,C=US" -validity 9999 -deststoretype pkcs12».



Εικόνα 68. Γενικές ρυθμίσεις για εξαγωγή σε πλατφόρμα android

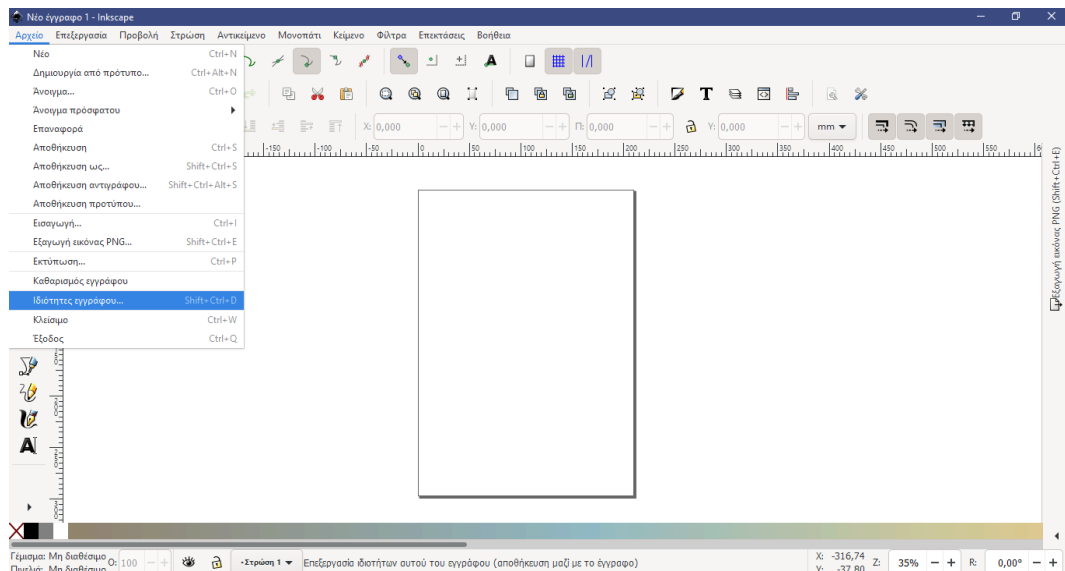
6.2.7 η Διεπαφή του Παιχνιδιού

Όλα τα εικονίδια σχεδιάστηκαν από την αρχή με τη βοήθεια του εργαλείου Inkscape. Είναι ένα δυνατό εργαλείο, κατάλληλο και για αρχάριους στο design, όπως εμένα, και χρειάζεται λίγο χρόνο για εξοικείωση με το περιβάλλον του.

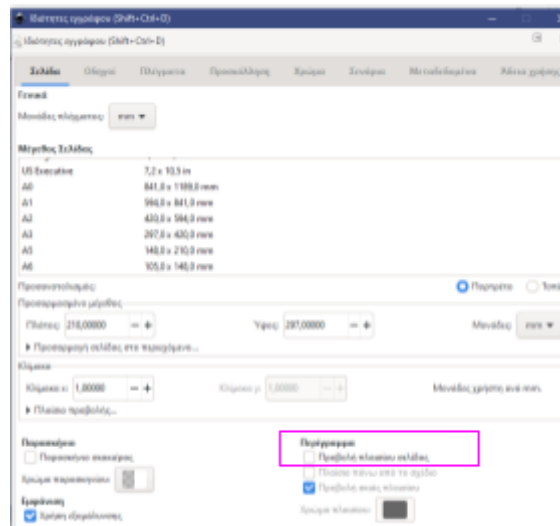


Εικόνα 69. Περιβάλλον του Inkscape

Τα περισσότερα στοιχεία του παιχνιδιού τα δημιούργησα σε ένα έργο του Inkscape. Με το που το ανοίγουμε, εμφανίζει αυτή την σελίδα στο κέντρο που φαίνεται στην Εικόνα 70. Για να μην με περιορίζει το αφάιρεσα, ακολουθώντας το μονοπάτι Αρχείο → Ιδιότητες εγγράφου → Περίγραμμα, και έβγαλα από την επιλογή την λειτουργία “Προβολή πλαισίου σελίδας” (Εικόνα 71).



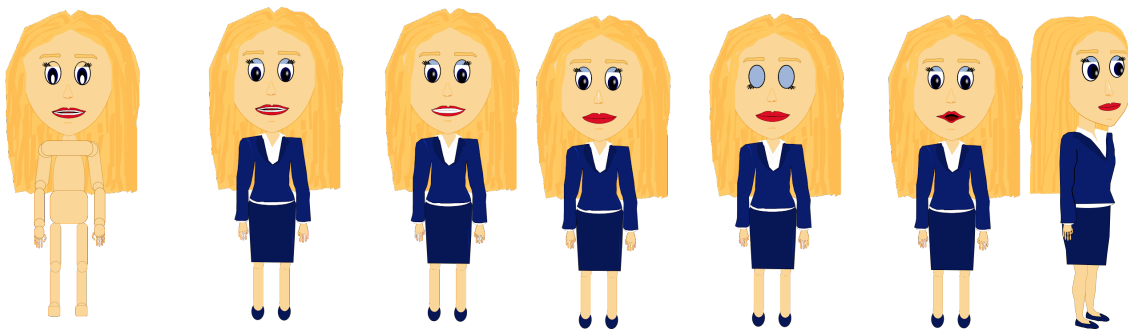
Εικόνα 70. Νέο έργο στο Inkscape



Εικόνα 71. Ιδιότητες εγγράφου (Inkscape)

Μπορεί να υπάρχει μεγάλη ποικιλία εργαλείων αλλά δεν χρειάζεται η εκμάθηση όλων για την δημιουργία σχεδίων. Γενικά, όλα τα σχέδια πραγματοποιήθηκαν με την βοήθεια γεωμετρικών σχημάτων και περισσότερο με την χρήση κύκλων. Τα γεωμετρικά σχήματα, παρά την απλή τους εμφάνιση, είναι χρήσιμα για πολλές τεχνικές σχεδίασης.

Αρχικά σχεδιάστηκε ένας πιθανός χαρακτήρας ο οποίος τελικά δεν χρησιμοποιήθηκε, με μικρές αλλαγές στο πρόσωπο για να φτιαχτεί ένα sprite για την διαδικασία της ομιλίας (lip sync). Ένας πρότυπος χαρακτήρας θα έμοιαζε κάπως όπως στην εικόνα:



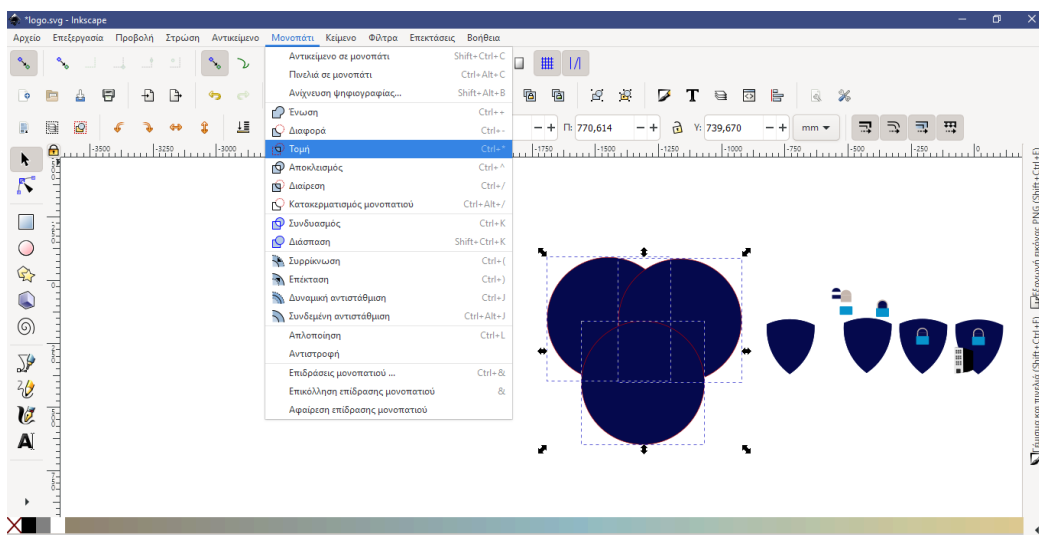
Εικόνα 72. Εικονογραφίες συγχρονισμού χειλιών (Inkscape)

Χρησιμοποιήθηκε βέβαια για την αρχική οθόνη ο χαρακτήρας αυτός, καθιστός, σε ένα γραφείο με έναν υπολογιστή για να προετοιμάσει ελάχιστα τον παίκτη για το κλίμα του παιχνιδιού.



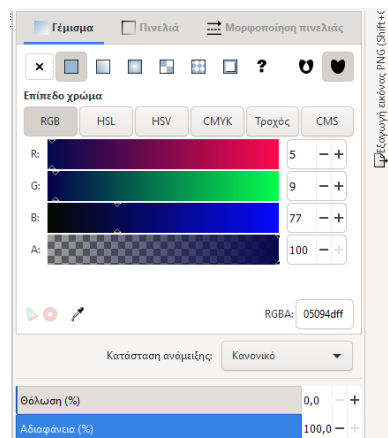
Εικόνα 73. Χαράκτηρας - γραφείο (Inkscape)

Κάποιες από τις λειτουργίες που προσφέρει και είναι πολύ χρήσιμες, είναι οι λειτουργίες «Διαδρομής». Με τις λειτουργίες «Ένωσης», «Διαφοράς», «Τομής», επιλέγοντας δύο ή περισσότερα σχήματα που έχουν σχεδιαστεί, μπορούν να δημιουργηθούν γρήγορα, εκπληκτικά αποτελέσματα από κάποια στοιχειώδη σχήματα. Χρησιμοποιώντας στη συνέχεια τα εργαλεία διαδρομής μπορεί το αποτέλεσμα να βελτιωθεί ακόμα περισσότερο. Για παράδειγμα, για την δημιουργία του λογότυπου (logo) του SAGE (Εικόνα 74), χρησιμοποιήθηκε η Τομή.

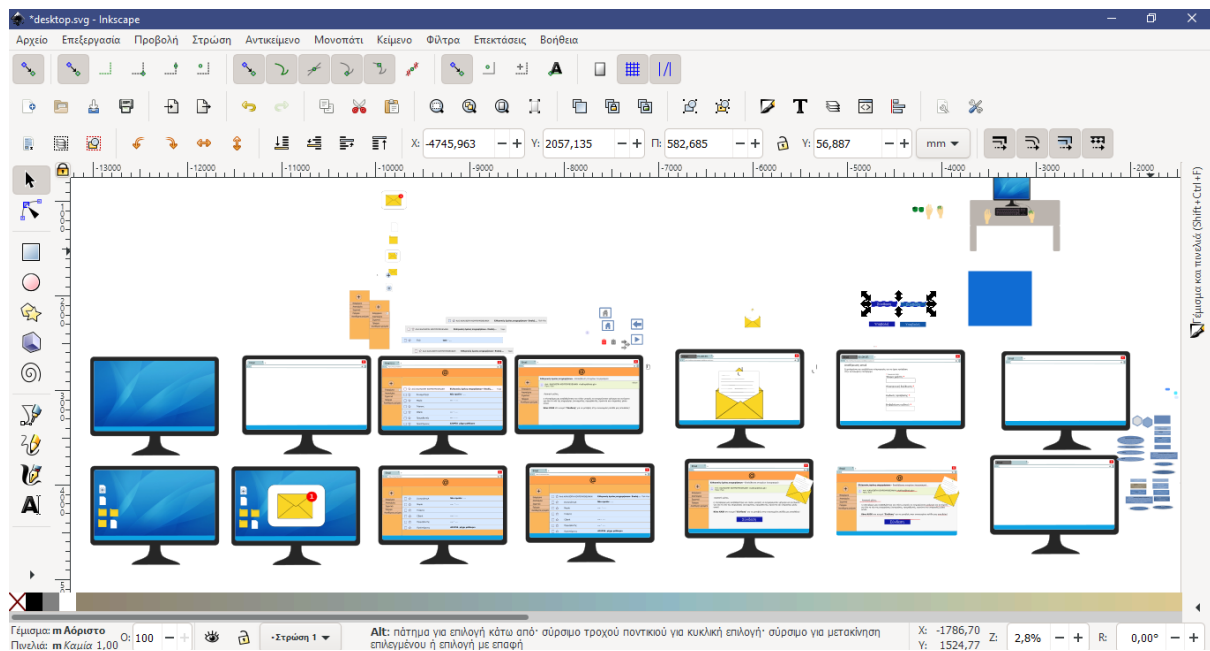


Εικόνα 74. Λειτουργίες διαδρομής και λογότυπο (Inkscape)

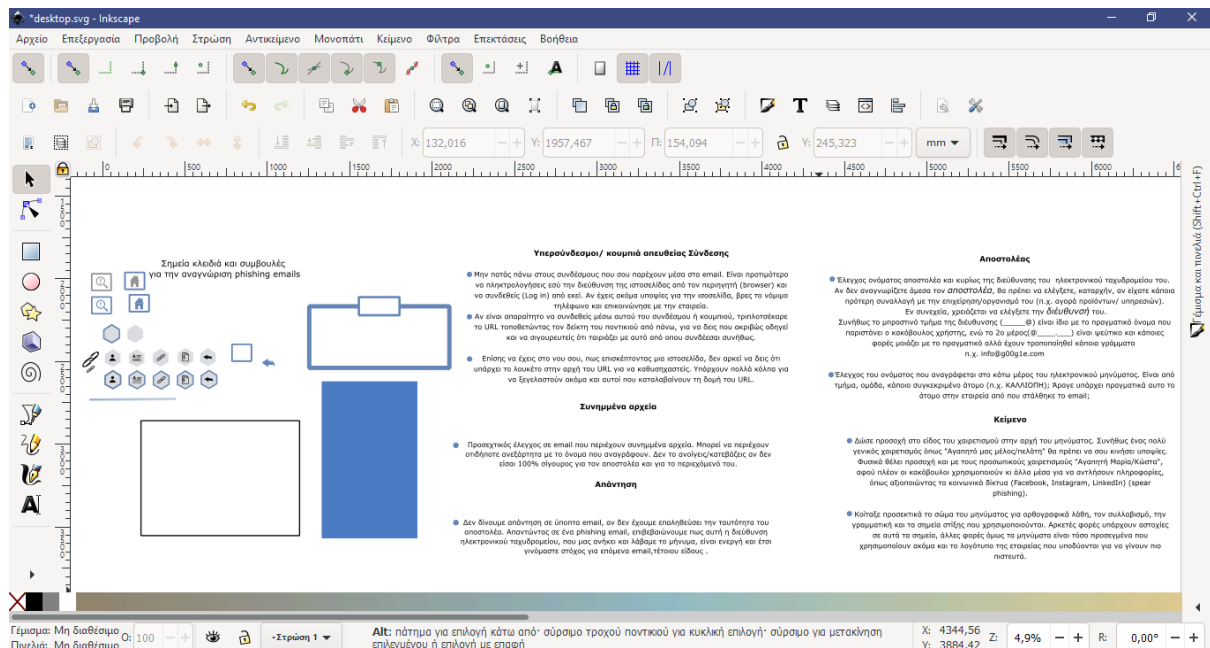
Άλλες χρήσιμες λειτουργίες που αξιοποίησα ήταν η ομαδοποίηση και απομαδοποίηση αντικειμένων, ο επιλογέας χρωμάτων (color picker), τα εργαλεία καλλιγραφική πινελιά και σχεδίαση μονοπατιού με κουκίδες....



Εικόνα 75. επιλογέας χρωμάτων (color picker, Inkscape)

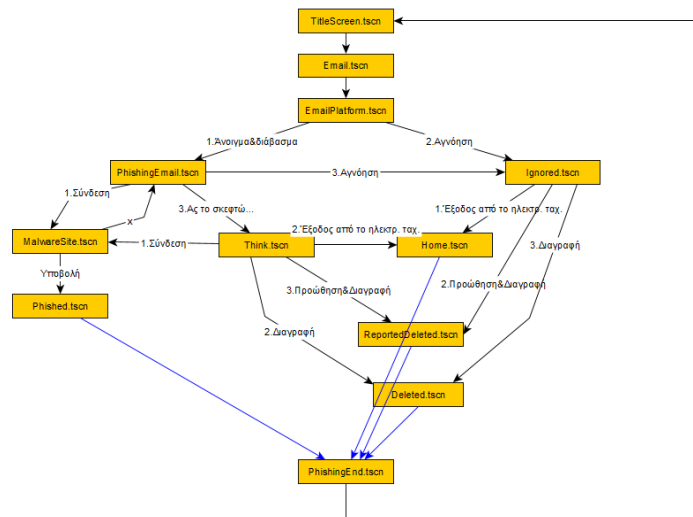


Εικόνα 76. Σχέδια παιχνιδιού (α) (Inkscape)



Εικόνα 77. Σχέδια παιχνιδιού (β) (Inkscape)

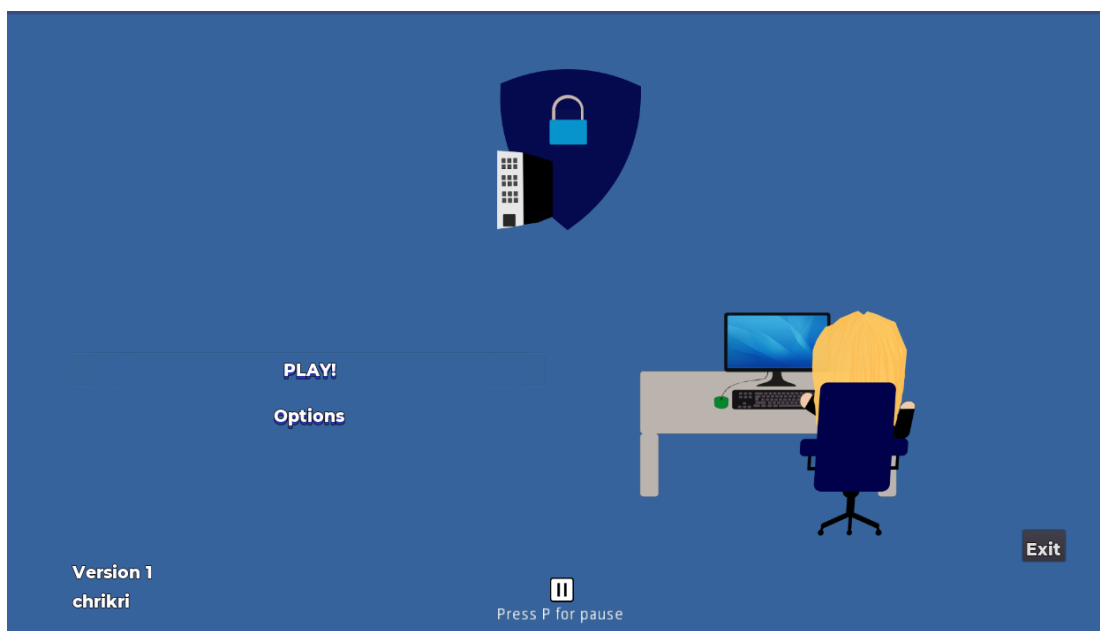
6.2.8 Πρωτότυπο



Εικόνα 78. Διάγραμμα σκηνών

6.2.8.1 Εισαγωγική οθόνη

Με την έναρξη του παιχνιδιού θα υπάρχει μια εισαγωγική οθόνη που θα έχει γαλάζιο υπόβαθρο, στο πάνω μέρος το εικονίδιο (logo) του παιχνιδιού και από κάτω επιλογές, για έναρξη παιχνιδιού «Play!», ρυθμίσεις «Options», και έξοδο «Exit» κάτω δεξιά με την οποία θα τερματίζεται το παιχνίδι. Το μουσικό υπόβαθρο θα ξεκινάει από το μενού.

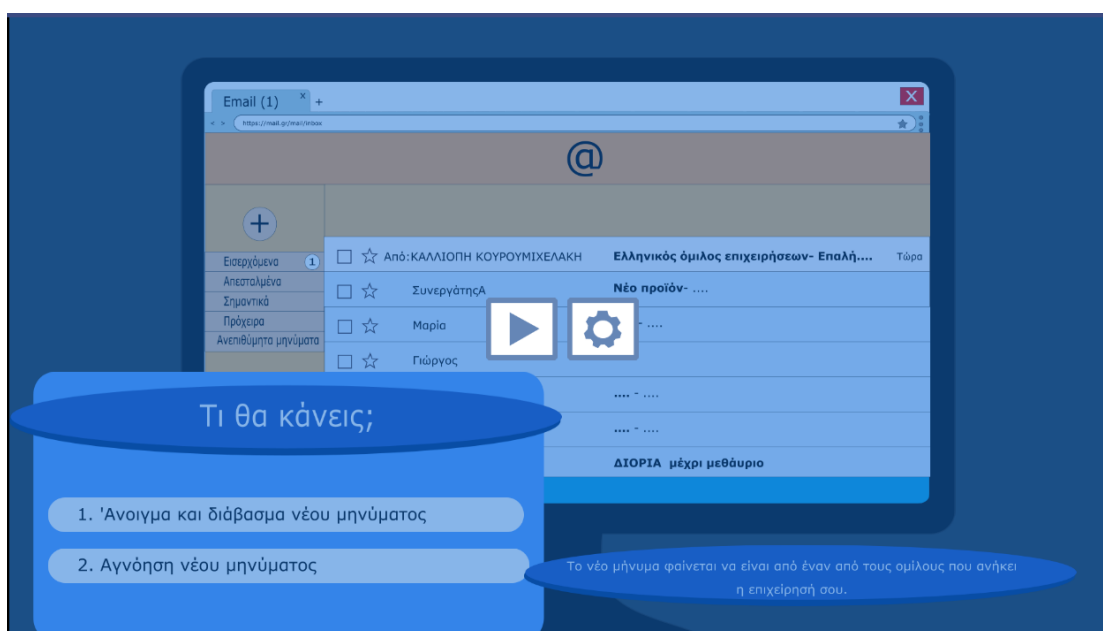


Εικόνα 79. Πρώτη οθόνη διεπαφής χρήστη - SAGE

Κατά τη διάρκεια του παιχνιδιού θα υπάρχει μια οθόνη παύσης του παιχνιδιού, θα εμφανίζεται αν πατήσει ο παίκτης το πλήκτρο «Ρ», που θα έχει τις επιλογές «Συνέχεια» και «Ρυθμίσεις» με τη μορφή εικονιδίων. Σε αυτή την φάση του παιχνιδιού το κουμπί «Ρυθμίσεις» δεν είναι λειτουργικό.

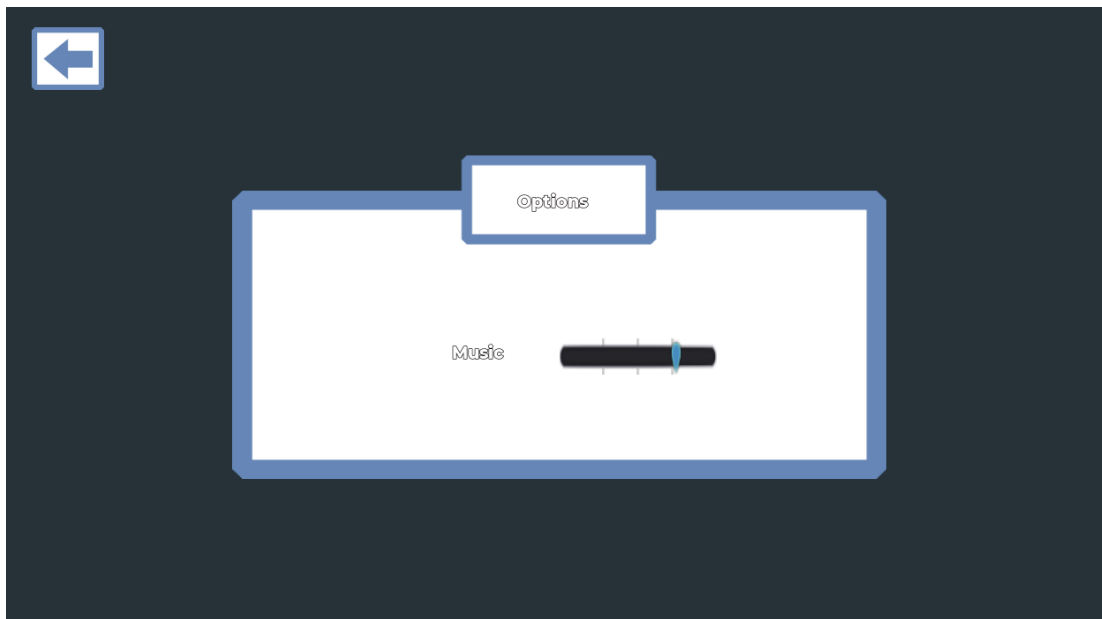
6.2.8.2 Επιλογές του παιχνιδιού

Κατά τη διάρκεια του παιχνιδιού υπάρχει η δυνατότητα παύσης και συνέχειας αλλά όχι η δυνατότητα προσωρινής αποθήκευσης και συνέχειας αργότερα από την αρχική οθόνη. επειδή το παιχνίδι είναι σύντομο σε διάρκεια.



Εικόνα 80. Οθόνη παύσης παιχνιδιού

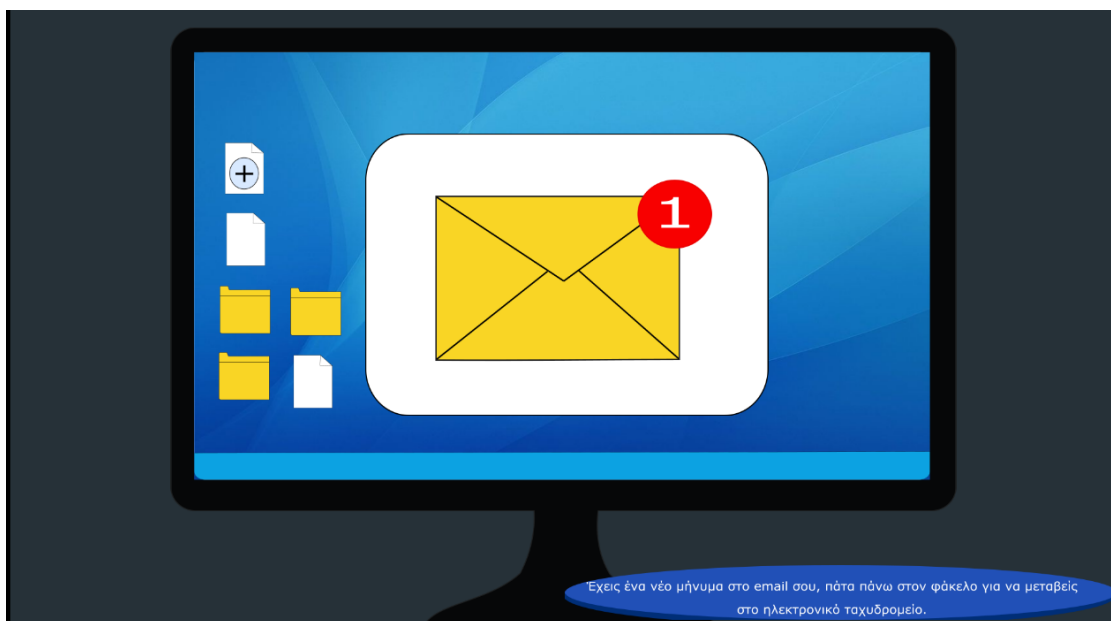
Στην αρχή του παιχνιδιού υπάρχει και η δυνατότητα ρύθμισης της έντασης του ήχου πατώντας το κουμπί «Options». Σέρνοντας τον slider προς τα αριστερά χαμηλώνει η ένταση της μουσικής υπόκρουσης του παιχνιδιού και σέρνοντας τον δεξιά αυξάνει αντίστοιχα.



Εικόνα 81. Οθόνη Ρυθμίσεων

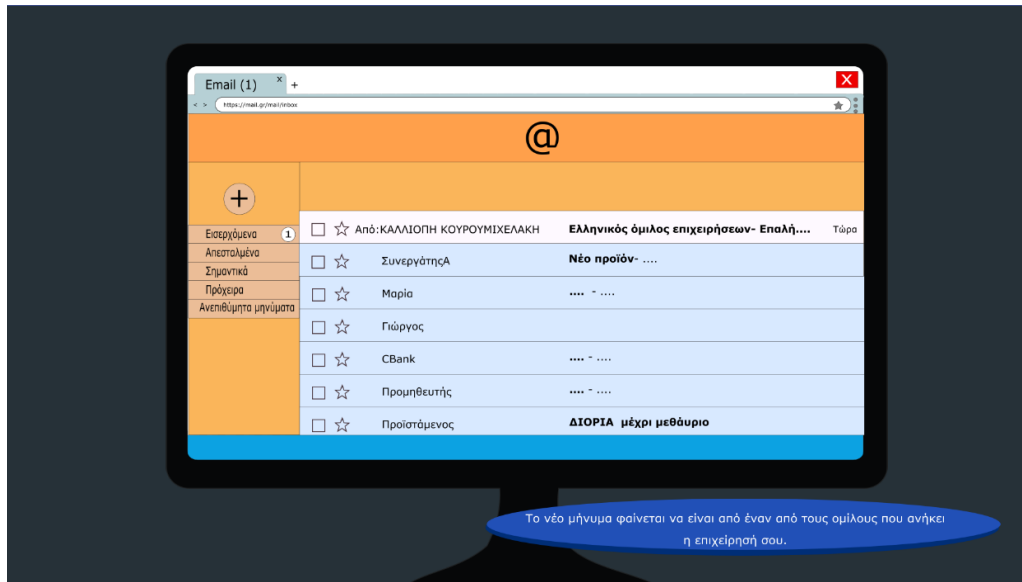
6.2.8.3 Η πρόοδος στο Παιχνίδι

Με το ξεκίνημα του παιχνιδιού εμφανίζεται μια εικονική οθόνη υπολογιστή και στη κάτω δεξιά γωνία ένα οβάλ πλαίσιο. Η οθόνη είναι το βασικό αντικείμενο του παιχνιδιού και υπάρχει σε όλες τις σκηνές. Το οβάλ μπλε πλαίσιο είναι η αφήγηση του παιχνιδιού η οποία υπάρχει για να μπορέσει να καθοδηγήσει τον παίκτη στο τι βλέπει και τι πρέπει να κάνει.



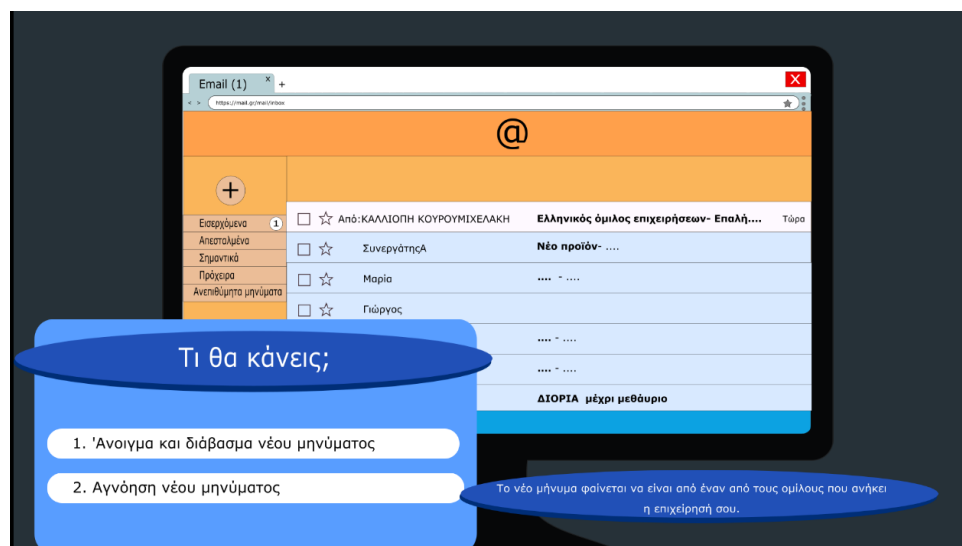
Εικόνα 82. Πρώτη οθόνη σεναρίου Phishing

Σε κάθε σκηνή (εκτός την πρώτη και την τελευταία) του παιχνιδιού, ο παίκτης θα πρέπει να επιλέξει μία από τις διαθέσιμες κινήσεις που υπάρχουν μέσα στο κουτί επιλογών με τίτλο «Τι θα κάνεις;». Το κουτί επιλογών εμφανίζεται λίγα δευτερόλεπτα αφού μπει η νέα σκηνή στη κάτω αριστερή γωνία. Δεν εμφανίζεται αμέσως για να έχει ο παίκτης τον χρόνο να διαβάσει την αφήγηση και να δει ολόκληρη την οθόνη προτού μπει στην διαδικασία να σκεφτεί πως θα δράσει, με βάση τα δεδομένα που έχει μπροστά του.



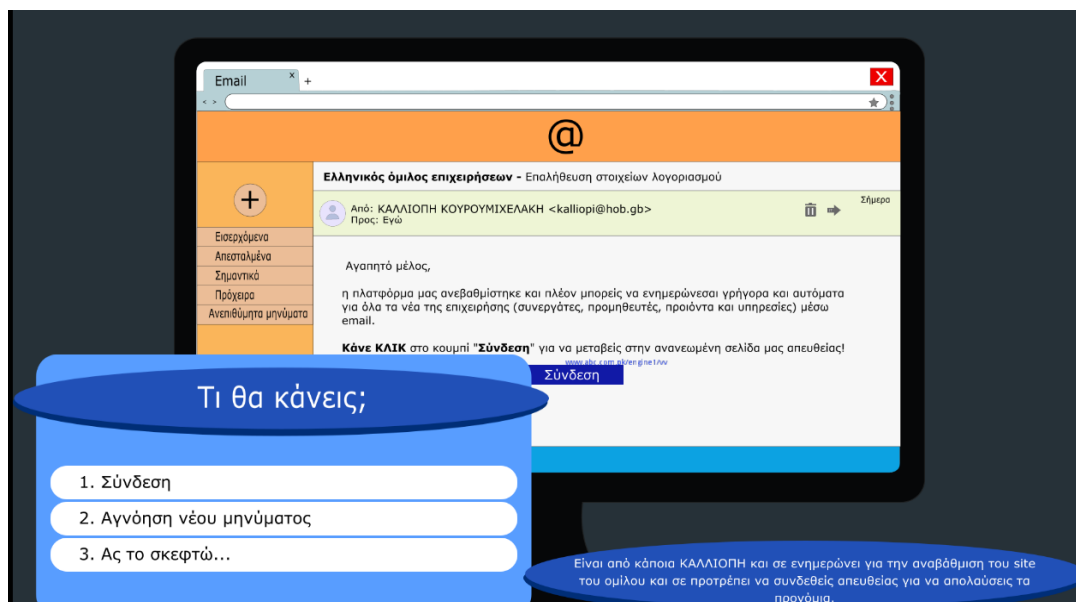
Εικόνα 83. Δεύτερη οθόνη σεναρίου Phishing (μόνο “αφήγηση”)

Για να πραγματοποιήσει την ενέργεια που τελικά θα επιλέξει μπορεί να πατήσει είτε πάνω στην επιλογή μέσα στο κουτί των επιλογών είτε απευθείας πάνω στην οθόνη υπολογιστή, του παιχνιδιού. Για παράδειγμα αν θέλει να επιλέξει την επιλογή «1. Άνοιγμα και διαβάσμα του νέου μηνύματος» μπορεί να πατήσει είτε στο κουτί επιλογών την πρώτη επιλογή είτε να πατήσει πάνω στο καινούργιο μήνυμα ηλεκτρονικού ταχυδρομείου όπως θα πάταγε στο κανονικό του υπολογιστή.



Εικόνα 84. Δεύτερη οθόνη σεναρίου Phishing (ολοκληρωμένη)

Ανάλογα με την επιλογή που θα κάνει ο παίκτης θα μεταβεί και στην κατάλληλη σκηνή, όπου θα αλλάξει το περιεχόμενο που δείχνει η εικονική οθόνη υπολογιστή. Αν πατήσει την επιλογή 1., που έφερα ως παράδειγμα θα του εμφανιστεί η οθόνη με το νέο μήνυμα. Σε κάθε σκηνή, εκτός από την πρώτη, υπάρχουν τουλάχιστον δύο σκηνές εξόδου.



Εικόνα 85. Οθόνη επιλογής “1.Άνοιγμα και διάβασμα” (Phishing)

Ο σκοπός του παιχνιδιού είναι να αποφασίσει ποιές επιλογές θα κάνει για να διαχειριστεί αυτή τη νέα πρόκληση.

7. Αξιολόγηση

7.1 Ποσοτική έρευνα

Για την ολοκλήρωση της πτυχιακής εργασίας με μία πρώτη αξιολόγηση του παιχνιδιού SAGE, στο τωρινό στάδιο ανάπτυξης του, διεξήχθη μια ποσοτική έρευνα που πραγματοποιήθηκε με τη δημιουργία ενός ερωτηματολογίου μέσω Google Forms. Το ερωτηματολόγιο αποτελείται από 20 ερωτήσεις και την δυνατότητα κατάθεσης επιπλέον σχολίων στο τέλος. Το ερωτηματολόγιο χωρίζεται σε πέντε ενότητες. Η πρώτη είναι μια εισαγωγική ενότητα με ερωτήσεις σχετικές με στοιχεία του ερωτώμενου, η δεύτερη περιλαμβάνει ερωτήσεις σχετικές με την Βιβλιογραφία της εργασίας, η τρίτη σχετικά με το παιχνίδι γενικά. Η τέταρτη περιλαμβάνει ερωτήσεις σχετικές με την χρηστικότητα και η πέμπτη με τον ρόλο της ευαισθητοποίησης μέσω του παιχνιδιού. Οι ερωτήσεις διαμοιράστηκαν μέσω ηλεκτρονικού ταχυδρομείου σε γνωστούς.

7.2 Δημογραφικά στοιχεία των συμμετεχόντων

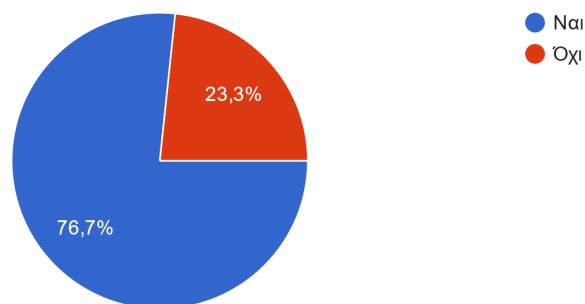
Το συγκεκριμένο ερωτηματολόγιο απευθύνεται σε άτομα κάθε ηλικίας και επαγγελματικού προσανατολισμού. Παρ' όλα αυτά, έστρεψα εσκεμμένα την έρευνα σε εργαζόμενους ενήλικες για να απαντηθούν όσο το δυνατόν καλύτερα τα ερευνητικά ερωτήματα που τέθηκαν. Συνολικά ερωτήθηκαν 30 άτομα από τα οποία 1 είχε ηλικία μεταξύ 12-18 ετών, 10 είχαν ηλικία μεταξύ 19-25 από τους οποίους τρεις εργάζονται και όλοι οι υπόλοιποι εργάζονταν και 2 είχαν ηλικία μεταξύ 26-35, 11 είχαν ηλικία μεταξύ 36-50 και 6 είχαν ηλικία 51+.

7.3 Αποτελέσματα της έρευνας

Τα αποτελέσματα της ποσοτικής έρευνας βοήθησαν αρκετά σε ένα πρώτο feedback (ανατροφοδότηση) για να δω, το τι περίπου γνωρίζουν οι ερωτηθέντες σχετικά με το ηλεκτρονικό ψάρεμα, το πως βλέπουν γενικά την ιδέα της εκπαίδευσης με τεχνικές παιχνοδοποίησης αλλά και το πως τους φαίνεται το συγκεκριμένο παιχνίδι.

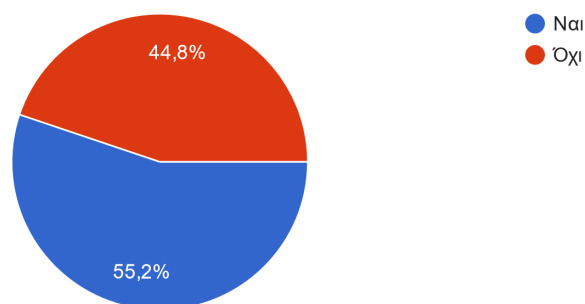
Από τους ερωτηθέντες, οι 23 απάντησαν πως έχουν συναντήσει παρόμοιο περιστατικό με αυτό του παιχνιδιού στην πραγματική τους ζωή και 16 από τους 29 στον χώρο εργασίας τους.

Έχετε συναντήσει παρόμοιο περιστατικό με αυτό το παιχνιδιού στην πραγματική σας ζωή;
30 απαντήσεις



Εικόνα 86. Ερώτηση 8

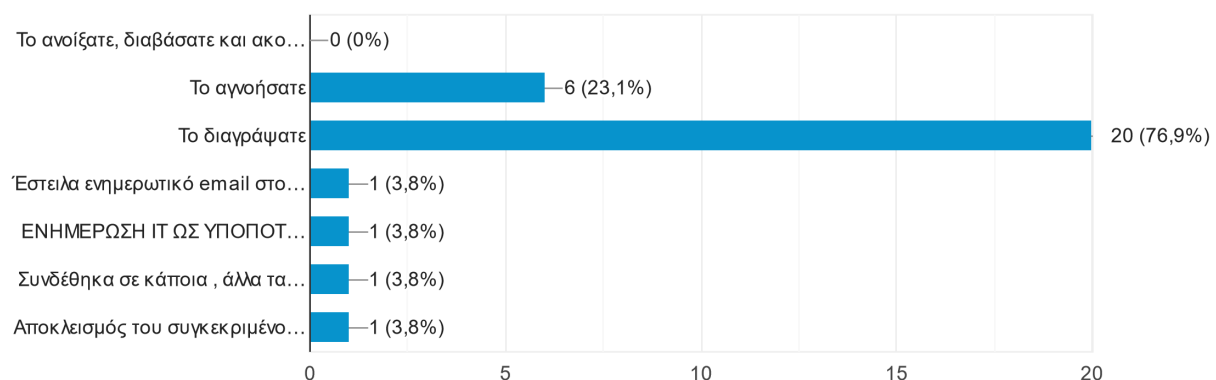
Έχετε συναντήσει παρόμοιο περιστατικό με αυτό το παιχνιδιού στην εργασία σας;
29 απαντήσεις



Εικόνα 87. Ερώτηση 9

Οι περισσότεροι, 20 από τους ερωτηθέντες, επέλεξαν να διαγράψουν το ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου ενώ κάποιοι το αγνόησαν, το προώθησαν ή το απέκλεισαν.

Εαν ναι, πως διαχειριστήκατε αυτό το νέο μήνυμα ηλεκτρονικού ταχυδρομείου;
26 απαντήσεις

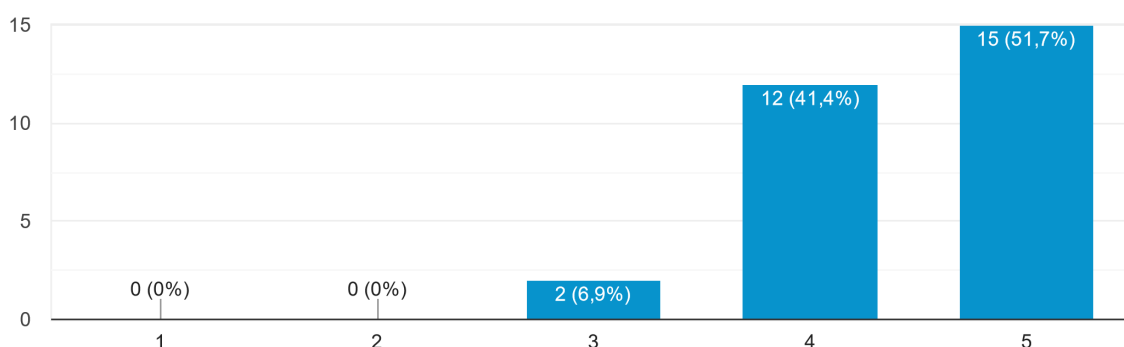


Εικόνα 88. Ερώτηση 10

Δύο από τους ερωτηθέντες δεν βρήκαν το παιχνίδι ελκυστικό οι οποίοι δήλωσαν και πως το περιβάλλον του SAGE (τα γραφικά, η μουσική, οι μεταβάσεις κτλ.) τους άρεσε λίγο (Ερώτηση 11,12).

Οι ερωτηθέντες στη πλειοψηφία τους δήλωσαν πως ήταν εύκολος ο χειρισμός του παιχνιδιού εκτός από ένα άτομο το οποίο είχε δηλώσει και πως το περιβάλλον του παιχνιδιού του άρεσε λίγο (Ερώτηση 13). Οι οδηγίες/ αφήγηση του παιχνιδιού ήταν σαφείς και κατανοητές σχεδόν σε όλους (Ερώτηση 14). 5 άτομα δήλωσαν πως οι διαθέσιμες κινήσεις/επιλογές ήταν μέτρια επαρκείς, ενώ οι υπόλοιποι πως ήταν ικανοποιητικά έως πολύ επαρκείς (Ερώτηση 15).

Θα προτείνατε να αξιοποιηθεί/ ενταχθεί η ολοκληρωμένη έκδοση του παιχνιδιού για την επιμόρφωση όλων των εργαζομένων πάνω σε θέματα ασφάλειας, στην εργασία σας;
29 απαντήσεις



Εικόνα 89. Ερώτηση 20

Η τελική εικόνα από αυτή την έρευνα/ αξιολόγηση είναι πως η εκπαίδευση μέσω τεχνικών παιχνιδοποίησης φαίνεται να είναι μια αποδεκτή μέθοδος από το κοινό. Ακόμα και το συγκεκριμένο παιχνίδι φάνηκε μια ικανοποιητική προσπάθεια από πολλούς και θα το προτείνανε να αξιοποιηθεί/ ενταχθεί η ολοκληρωμένη έκδοση του παιχνιδιού για την επιμόρφωση όλων των εργαζομένων πάνω σε θέματα ασφάλειας, στην εργασία τους. Όμως χρειάζεται βελτιώσεις και ιδιαίτερα στο περιβάλλον του όπως φάνηκε από τα σχόλια των συμμετεχόντων, για να γίνει ακόμα πιο ελκυστικό στους χρήστες του.

Οι επίσημοι μηχανισμοί αξιολόγησης και ανατροφοδότησης είναι κρίσιμα συστατικά κάθε προγράμματος ευαισθητοποίησης, κατάρτισης και εκπαίδευσης σχετικά με την ασφάλεια. Η συνεχής βελτίωση δεν μπορεί να συμβεί χωρίς καλή αίσθηση του τρόπου λειτουργίας του υπάρχοντος προγράμματος (Wilson, 2003). Έτσι, ανα τακτά χρονικά διαστήματα μετά από κάποια αναβάθμιση του παιχνιδιού και όχι μόνο, καλό είναι να πραγματοποιούνται αξιολογήσεις.

8. Συμπεράσματα-μελλοντικές προεκτάσεις

8.1 Συμπεράσματα

Σε αυτή την εργασία πραγματοποιήθηκε σημαντική μελέτη σε υπάρχουσα συστήματα που αξιοποιούν τεχνικές παιχνιδοποίησης ως μέσο μάθησης για προγράμματα ευαισθητοποίησης και εκπαίδευσης σχετικά με θέματα ασφάλειας στον κυβερνοχώρο. Μετέπειτα, μελετήθηκαν οι πιο χαρακτηριστικές επιθέσεις που πραγματοποιούνται εις βάρος επιχειρήσεων και δημιουργήθηκε μια σειρά από σενάρια, τα οποία καλούν τον παίκτη να κατανοήσει τις απειλές της κυβερνοασφάλειας και τις συνέπειες των κυβερνοεπιθέσεων και να αναπτύξει νέες δεξιότητες ώστε να προφυλαχτεί από αυτές και συγχρόνως να προστατέψει την επιχείρηση στην οποία εργάζεται. Αναπτύχθηκε ένα παιχνίδι, το SAGE (Security Awareness Game for Employees) που ως demo έχει υλοποιηθεί το ένα σενάριο, με θέμα το ηλεκτρονικό ψάρεμα και εύκολα μπορούν να προστεθούν και τα υπόλοιπα σενάρια στο παιχνίδι. Ο πηγαίος κώδικας του παιχνιδιού είναι διαθέσιμος σε αποθετήριο στο Github¹⁷. Τέλος, πραγματοποιήθηκε μία πρώτη αξιολόγηση του παιχνιδιού με ποσοτική έρευνα χρησιμοποιώντας ερωτηματολόγιο το οποίο απαντήθηκε από 30 άτομα.

8.2 Μελλοντικές προεκτάσεις

Προγραμματίζεται να συνεχιστεί η ανάπτυξη του παιχνιδιού και μετά το πέρας της παρούσας εργασίας, εμπλουτίζοντας το και με τα υπόλοιπα σενάρια ώστε γίνει μια πλήρη εφαρμογή ευαισθητοποίησης υπαλλήλων επιχειρήσεων, για την ασφάλεια στον κυβερνοχώρο και στη συνέχεια να πραγματοποιηθεί και μια δεύτερη αξιολόγηση. Με αυτό τον τρόπο θα εκτιμηθεί το επίπεδο ευαισθητοποίησης σχετικά με την ασφάλεια των συμμετεχόντων αλλά και το ενδιαφέρον και η ανταπόκριση για αυτόν τον όχι τόσο γνωστό τρόπο κατάρτισης αλλά και αν καταφέρνει το SAGE να τραβήξει το ενδιαφέρον των χρηστών του και να πετύχει τον στόχο του.

Όσον αφορά το παιχνίδι καθ'αυτό μπορούν να γίνουν κάποιες βελτιώσεις όπως:

- να είναι προσδιορισμένο με μεγαλύτερη σαφήνεια τι είναι δυνατό να κάνει κλικ, ο παίκτης στο πλαίσιο του παιχνιδιού, και τι όχι.
- η υλοποίηση της αναβάθμισης των χαρακτηριστικών του κεντρικού χαρακτήρα (customization)
- εξέταση για προσφορά ρυθμιζόμενων επιπέδων δυσκολίας
- εισαγωγή συστήματος αξιολόγησης του παίκτη που θα τον κατατάσσει σε ένα πίνακα με τις καλύτερες επιδόσεις του σε χρόνο και πόντους
- επιβράβευση του παίκτη, για παράδειγμα με τη χρήση εικονικών αντικειμένων
- αναβάθμιση της αφήγησης σε μορφή ιστορίας
- κατεύθυνση ανακλύπτουσας αφήγησης (emergent storytelling), δυναμική αφήγηση, με τη σύνθεση δομικών στοιχείων και τεχνητής νοημοσύνης των χαρακτήρων, υποστηρίζοντας τη δημιουργία ποικίλων συμπεριφορών, ως απόκριση στις επιλογές του παίκτη, αντί της κλασικής και τρέχουσας προσέγγισης της δημιουργίας μιας ιστορίας με δενδρική δομή, όπου κάθε απόφαση του παίκτη καθορίζει ποια διακλάδωση θα ακολουθήσει και είναι αρκετά περιοριστική λόγω του περιορισμένου αριθμού διακλαδώσεων που μπορεί να υπάρξουν.

¹⁷ <https://github.com/chrikri/SAGE>

- χρήση του κόμβου «Timer» για την ενεργοποίηση ενός νέου γεγονότος μετά από καθορισμένο διάστημα μέσω εκπομπής σήματος λήξης
- περισσότερες ρυθμίσεις για τον ήχο κτλ. με δυνατότητα πρόσβασης σε αυτές από την οθόνη παύσης.
- να μην μπορεί ο παίκτης να αλληλεπιδράσει με το παιχνίδι, να μην μπορεί να πατήσει τα κουμπιά, μέχρι να εμφανιστεί το πλαίσιο «Τι θα κάνεις;» έτσι ώστε να μην μπορεί να προσπεράσει τις ερωτήσεις πατώντας απλά πάνω στην οθόνη σε τυχαία σημεία.
- εφόσον έχει παίξει μία φορά το σενάριο ο παίκτης, δημιουργία δυνατότητας πρόσβασης στην τελευταία οθόνη με τα σημεία κλειδιά και τις συμβουλές, από την αρχική οθόνη για να μην αναγκάζεται ο παίκτης κάθε φορά που θα θέλει να τα μελετήσει να παίξει από την αρχή το ίδιο επίπεδο.

9. Βιβλιογραφία

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. NIST Special publication, 800(50), 1-39.

Karakasiliotis, A., Furnell, S. M., & Papadaki, M. (2006). Assessing end-user awareness of social engineering and phishing. *Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia*. <https://doi.org/10.4225/75/57a80e47aa0cb>

Cazier, J. A., & Medlin, B. D. (2006). Password security: An empirical investigation into e-commerce passwords and their crack times. *Information Systems Security*, 15(6), 45-55.

Cone, B. D., Irvine, C. E., Thompson, M. F., & Nguyen, T. D. (2007). A video game for cyber security training and awareness. *computers & security*, 26(1), 63-72.
<https://doi.org/10.1016/j.cose.2006.10.005>

Zhang, J., Luo, X., Akkaladevi, S., & Ziegelmayer, J. (2009). Improving multiple-password recall: an empirical study. *European Journal of Information Systems*, 18(2), 165-176.

Αναγνώστου, Κ. (2009). Βιντεοπαιχνίδια-Βιομηχανία και Ανάπτυξη. *Αθήνα: Κλειδάριθμος*.

Kato, K., & Klyuev, V. (2013, September). Strong passwords: Practical issues. In *2013 IEEE 7th International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS)* (Vol. 2, pp. 608-613). IEEE.

Le Compte, A., Elizondo, D., & Watson, T. (2015). A renewed approach to serious games for cyber security. In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace* (pp. 203-216). IEEE. <https://doi.org/10.1109/CYCON.2015.7158478>

Πασπαλάς, Γεώργιος, Αλέξανδρος. (2015). Διαχείριση Κινδύνων από κυβερνοεπιθέσεις, μελέτες περιπτώσεων απο AOL και SONY. Πως επηρεάζει το Cloud Computing. Πανεπιστήμιο Μακεδονίας. Διατμηματικό πρόγραμμα μεταπτυχιακών σπουδών στη διοίκηση επιχειρήσεων. Διπλωματική Εργασία.

Arnab, S., Lim, T., Carvalho, M. B., Bellotti, F., De Freitas, S., Louchart, S., ... & De Gloria, A. (2015). Mapping learning and game mechanics for serious games analysis. *British Journal of Educational Technology*, 46(2), 391-411. <https://doi.org/10.1109/EDUCON.2019.8725061>.

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).

Watts, S. (2016). Secure authentication is the only solution for vulnerable public wifi. *Computer Fraud & Security*, 2016(1), 18-20. ISSN 1361-3723,
[https://doi.org/10.1016/S1361-3723\(16\)30009-4](https://doi.org/10.1016/S1361-3723(16)30009-4)

Κουτσοδόντης, Κ. (2016). Ηλεκτρονικές επιθέσεις σε ελληνικές επιχειρήσεις. Πτυχιακή Εργασία. Πανεπιστήμιο Αιγαίου. Σχολή Επιστημών Διοίκησης Τμήμα Διοίκησης Επιχειρήσεων.

Qader, N. N. (2016). Boosting Authentication Security by Building Strong Password and Individualizing Easy to Remember Techniques. *Journal of University of Human Development*, 2(3), 520-527.

Cook, A., Smith, R., Maglaras, L., & Janicke, H. (2016). Using gamification to raise awareness of cyber threats to critical national infrastructure. In *4th International Symposium for ICS & SCADA Cyber Security Research 2016 4* (pp. 84-94).
<https://doi.org/10.14236/ewic/ICS2016.10>.

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers & Security*, 59, 186-209.
<https://doi.org/10.1016/j.cose.2016.03.004>

Sabillon, R., Cano, J. J., Cavaller Reyes, V., & Serra Ruiz, J. (2016). Cybercrime and cybercriminals: A comprehensive study. *International Journal of Computer Networks and Communications Security*, 2016, 4 (6).

Epps, C. (2017). Best practices to deal with top cybercrime activities. *Computer Fraud & Security*, 2017(4), 13-15. doi:[10.1016/S1361-3723\(17\)30032-5](https://doi.org/10.1016/S1361-3723(17)30032-5)

Μπασδαράς, Π. (2017). Εκτιμώντας τις συνέπειες των κυβερνοεπιθέσεων σε μια εταιρεία και την προστασία της. Διπλωματική εργασία. Σχολή Επιστημών Διοίκησης Επιχειρήσεων. Τμήμα Λογιστικής και Χρηματοοικονομικής. Πανεπιστήμιο Μακεδονίας

Tioh, J. N., Mina, M., & Jacobson, D. W. (2017). Cyber security training a survey of serious games in cyber security. In *2017 IEEE Frontiers in Education Conference (FIE)* (pp. 1-5). IEEE. <https://doi.org/10.1109/FIE.2017.8190712>

Varannai, I., Sasvári, P. L., & Urbanovics, A. (2017). The use of gamification in higher education: an empirical study. *International Journal of Advanced Computer Science and Applications*, 8(10), 1-6. <https://doi.org/10.14569/IJACSA.2017.081001>

Puspitaningrum, E. A., Devani, F. T., Putri, V. Q., Hidayanto, A. N., & Hapsari, I. C. (2018, October). Measurement of Employee Information Security Awareness: Case Study at A Government Institution. In *2018 Third International Conference on Informatics and Computing (ICIC)* (pp. 1-6). IEEE.

Schütz, A. E. (2018). Information security awareness: it's time to change minds. In *Proceedings of International Conference on Applied Informatics Imagination, Creativity, Design, Development-ICDD*.

Karageorgiou Z., Mavrommati E., Christopoulou E., Fotaris P. "Escape Room as learning environment: combining technology, theater and creative writing in education". *2nd International Conference on "Digital Culture & AudioVisual Challenges - Interdisciplinary Creativity in Arts and Technology"*, Corfu, Greece, May 10-11, 2019.

Calabrò, A., Daoudagh, S., & Marchetti, E. (2019). Integrating access control and business process for GDPR compliance: A preliminary study. In *ITASEC*.

Κουτρώσιος, Αντώνιος. (2019). Ετοιμότητα για την Ασφάλεια στον Κυβερνοχώρο στις Μικρές και Μεσαίες Επιχειρήσεις στη Κύπρο. Μεταπτυχιακή Διατριβή. Ανοικτό Πανεπιστήμιο Κύπρου. Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Ταφραλίδης, Ν. (2019). Ανάπτυξη Παιχνιδιού με τη Χρήση της Μηχανής Godot. Πτυχιακή εργασία

Bhandari, I. P. S. (2019). *Designing a virtual environment in VR space using memory enhancement techniques: Introducing a VR approach to GDPR awareness training* (Master's thesis).

Scholefield, S., & Shepherd, L. A. (2019). Gamification techniques for raising cyber security awareness. In *International Conference on Human-Computer Interaction* (pp. 191-203). Springer, Cham. https://doi.org/10.1007/978-3-030-22351-9_13

Cole, J. R., Pence, T., Cummings, J., Baker, E. (2019) Gamifying Security Awareness: A New Prototype. In: Moallem A. (eds) HCI for Cybersecurity, Privacy and Trust. HCII 2019. Lecture Notes in Computer Science, vol 11594. Springer, Cham. https://doi.org/10.1007/978-3-030-22351-9_8

Καραδούκας, Ε., & Κολλάτου, Ε. (2019). Η γνωστοποίηση πληροφοριών στο διαδίκτυο. Ευκαιρίες και απειλές για τις ελληνικές επιχειρήσεις. Πτυχιακή εργασία. Σχολή Οικονομικών και Διοικητικών Επιστημών. Τμήμα Λογιστικής και Χρηματοοικονομικής.

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, 11(3), 73. <https://doi.org/10.3390/fi11030073>

Rastenis, J., Ramanauskaitė, S., Janulevičius, J., & Čenys, A. (2019). Credulity to Phishing Attacks: A Real-World Study of Personnel with Higher Education. In *2019 Open conference of electrical, electronic and information sciences (eStream)* (pp. 1-5). IEEE. <https://doi.org/10.1109/eStream.2019.8732169>

Πολύζου, Δήμητρα. (2019). Game Design: από τα videogames του '90 στα escape rooms. Ελληνικό Ανοικτό Πανεπιστήμιο. Σχολή Εφαρμοσμένων Τεχνών. Γραφικές Τέχνες – Πολυμέσα ΜΑ.Διπλωματική Εργασία.

Oroszi, E. D. (2019, June). Security awareness escape room-a possible new method in improving security awareness of users. In *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)* (pp. 1-4). IEEE. <https://doi.org/10.1109/CyberSA.2019.8899715>

Hassan, N. A. (2019). *Ransomware revealed: a beginner's guide to protecting and recovering from ransomware attacks*. Apress. <https://doi.org/10.1007/978-1-4842-4255-1>

Scholefield, S., & Shepherd, L. A. (2019). Gamification techniques for raising cyber security awareness. In *International Conference on Human-Computer Interaction* (pp. 191-203). Springer, Cham. https://doi.org/10.1007/978-3-030-22351-9_13

Moallem, A. (Ed.). (2019). *HCI for Cybersecurity, Privacy and Trust: First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings* (Vol. 11594). Springer.

Μπουρής, Φ. Μάλλιος, Σ. (2019). Μοντελοποίηση των ενεργειών εξαπάτησης χρηστών διαδικτύου μέσω της υπηρεσίας email και δημιουργία ιστοτόπου αντιμετώπισης του φαινομένου. Πτυχιακή εργασία. Πανεπιστήμιο Πατρών. Σχολή Οικονομικών Επιστημών και Διοίκησης Επιχειρήσεων. Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας.

(2019, November 28). RevengeHotels: cybercrime targeting hotel front desks worldwide. SecureList. <https://securelist.com/revengehotels/95229/>

Fotaris, P., & Mastoras, T. (2019, October). Escape rooms for learning: A systematic review. In *Proceedings of the European Conference on Games Based Learning* (pp. 235-243).

Katsantonis, M., Kotini, I., Fouliras, P., Mavridis, Ioannis. (2019). Conceptual Framework for Developing Cyber Security Serious Games. 872-881. doi:10.1109/EDUCON.2019.8725061.

Karageorgiou Z., Fotaris P., Christopoulou E., Mavrommati E. "Escape room in education: Evaluating using Experience Pyramid Model", *5th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM 2020)*, Corfu, Greece, September 25-27, 2020.

Hill, Winston Anthony Jr., Fanuel, Mesafint, Yuan, Xiaohong, Zhang, Jinghua, Sajad, Sajad. (2020). A Survey of Serious Games for Cybersecurity Education and Training. *KSU Proceedings on Cybersecurity Education. Research and Practice*. 7.

Γιουφτσιάδης, Ιωάννης. (2020). Καταπολέμηση ηλεκτρονικής απάτης στην εποχή του Open Banking. Διπλωματική Εργασία. Ελληνικό Ανοικτό Πανεπιστήμιο.

Podgórski, G. (2020) Analysis of the internet Activity of employees in the context of threats and their activity in the network - a case study. Silesian University of technology publishing house. Scientific papers of Silesian University of technology. *Zeszyty Naukowe. Organizacja i Zarządzanie/Politechnika Śląska*, (149), 507-519. <http://dx.doi.org/10.29119/1641-3466.2020.149.42>

Παναγιώταρου, Α. (2020). Ποσοτική και ποιοτική διερεύνηση της αποτελεσματικότητας των εκπαιδευτικών προγραμμάτων σε ψηφιακές δεξιότητες στην Ελλάδα και προτάσεις για βελτιώσεις σύμφωνα με τα πρότυπα της ΕΕ. Διδακτορική Διατριβή. Πανεπιστήμιο Πατρών. Τμήμα Διοίκησης Επιχειρήσεων.

Hart, S., Margheri, A., Paci, F., & Sassone, V. (2020). Riskio: A serious game for cyber security awareness and education. *Computers & Security*, 95, 101827. <https://doi.org/10.1016/j.cose.2020.101827>

Hill Jr, W. A., Fanuel, M., Yuan, X., Zhang, J., & Sajad, S. (2020). A Survey of Serious Games for Cybersecurity Education and Training. *KSU Proceedings on Cybersecurity Education, Research and Practice*. 7. <https://digitalcommons.kennesaw.edu/ccerp/2020/Research/7>

Kourtis, A. (2020). Raising Information Security Awareness: the role of Gamification. Master Thesis. University of the Aegean. School of Engineering. Dpt. of Information and Communication Systems Engineering.

Κατσαράκη, Γ. (2020). Τα εκπαιδευτικά παιχνίδια περιπέτειας πολλών χρηστών σε τρισδιάστατους εικονικούς κόσμους. Μεταπτυχιακή εργασία.

Andreasson, A., Artman, H., Brynielsson, J., & Franke, U. (2020, December). A Census of Swedish Government Administrative Authority Employee Communications on Cybersecurity during the COVID-19 Pandemic. In *2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* (pp. 727-733). IEEE

Tsohou, A., Magkos, E., Mouratidis, H., Chrysoloras, G., Piras, L., Pavlidis, M., ... & Crespo, B. G. N. (2020). Privacy, security, legal and technology acceptance elicited and consolidated requirements for a GDPR compliance platform. *Information & Computer Security*.

Security Magazine. 2020. First ransomware-related death reported in Germany. <https://www.securitymagazine.com/articles/93409-first-ransomware-related-death-reported-in-germany>. [Online; accessed 3-September-2021].

Poojary, P. S. (2021). Safety Measures to be Maintained while Using Public Wi-Fi. *Journal homepage: www.ijrpr.com ISSN, 2582, 7421*.

Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2021). A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. *arXiv preprint arXiv:2102.06249*.

Wade, M. (2021). Digital hostages: Leveraging ransomware attacks in cyberspace. *Business Horizons*.

Omar, N. S., Foozy, C. F. M., Hamid, I. R. A., Hafit, H., Arbain, A. F., & Shamala, P. (2021, May). Malware Awareness Tool for Internet Safety using Gamification Techniques. In *Journal of Physics: Conference Series* (Vol. 1874, No. 1, p. 012023). IOP Publishing.

Χριστοπούλου Ε., “Η παιχνιδιοποίηση της μάθησης – Δημιουργία εκπαιδευτικών παιχνιδιών και η αξιοποίησή τους στην εκπαίδευση”, *Πρακτικά της Επιστημονικής Τηλε- Διημερίδας Η Μετάβαση της Εκπαιδευτικής Κοινότητας στη Ψηφιακή Εποχή και η Αξιοποίηση της Εξ Αποστάσεως Εκπαίδευσης: Από τη Θεωρία στην Πράξη*, 20-21 Φεβρουαρίου, 2021

Παράρτημα (ερωτηματολόγιο αξιολόγησης)

Ερωτήσεις

Ενότητα 1

1.

Ποια είναι η ηλικία σας; *

- 1. 12-18
- 2. 19-25
- 3. 26-35
- 4. 36-50
- 5. 51+

2.

Εργάζεστε; *

- ☐ Ναι
- ☐ Όχι

3.

Χρησιμοποιείτε κάποια ηλεκτρονική συσκευή (υπολογιστή) κατά την εργασία σας; *

- ☐ Ναι
- ☐ Όχι

4.

Εάν ναι,

	καθόλου	λίγο	μέτρια	πολύ	πάρα πολύ
είναι υποχρεω...	☐	☐	☐	☐	☐
συνδέεστε στο ...	☐	☐	☐	☐	☐

5.

Ποιος είναι ο βαθμός εξοικείωσής σας αναφορικά με την χρήση νέων τεχνολογιών (σύμφωνα με * την κρίση σας) ;

	1	2	3	4	5	
πολύ μικρή	☐	☐	☐	☐	☐	άριστη

Ενότητα 2 (Βιβλιογραφία)

6.

Ποιές από τις παρακάτω έννοιες έχετε ακουστά; *

- ☐ Phishing (ηλεκτρονικό ψάρεμα)
- ☐ Password (κωδικός πρόσβασης)
- ☐ Social engineering (κοινωνική μηχανική)
- ☐ Έλεγχος πρόσβασης και μη εξουσιοδοτημένη πρόσβαση
- ☐ Wi-fi hotspots (ασύρματα σημεία σύνδεσης στο διαδίκτυο)
- ☐ ransomware (ransom + malware)
- ☐ GDPR (General Data Protection Regulation/ Γενικός Κανονισμός Προστασίας Δεδομένων)

7.

Τι γνωρίζετε για το Phishing (ηλεκτρονικό ψάρεμα); *

Κείμενο μακροσκελούς απάντησης

Ενότητα 3 (SAGE)

SAGE (Security Awareness Game for Employees)

Το παιχνίδι SAGE είναι διαθέσιμο στην διεύθυνση: <https://ionio-kryelesi.itch.io/sage>

8.

Έχετε συναντήσει παρόμοιο περιστατικό με αυτό το παιχνιδιού στην πραγματική σας ζωή; *

- ☐ Ναι
- ☐ Όχι

9.

Έχετε συναντήσει παρόμοιο περιστατικό με αυτό το παιχνιδιού στην εργασία σας; *

- ☐ Ναι
- ☐ Όχι

10.

Εαν ναι, πως διαχειριστήκατε αυτό το νέο μήνυμα ηλεκτρονικού ταχυδρομείου;

- ☐ Το ανοίξατε, διαβάσατε και ακολουθήσατε τις οδηγίες
- ☐ Το αγνοήσατε
- ☐ Το διαγράψατε
- ☐ Άλλο...

Ενότητα 4 (Χρηστικότητα)

11.

Θεωρείτε το παιχνίδι ελκυστικό; *

	1	2	3	4	5	
καθόλου	☐	☐	☐	☐	☐	πάρα πολύ

12

Σας άρεσε το περιβάλλον του SAGE (τα γραφικά, η μουσική, οι μεταβάσεις κτλ.) ; *

	1	2	3	4	5	
καθόλου	☐	☐	☐	☐	☐	πάρα πολύ

13.

Πόσο εύκολος ήταν ο χειρισμός του παιχνιδιού; *

	1	2	3	4	5	
καθόλου	☐	☐	☐	☐	☐	πάρα πολύ

14.

Οι οδηγίες/ αφήγηση του παιχνιδιού ήταν σαφείς και κατανοητές; *

	1	2	3	4	5	
καθόλου	☐	☐	☐	☐	☐	πάρα πολύ

15.

Οι διαθέσιμες κινήσεις/επιλογές ήταν επαρκείς;

	1	2	3	4	5	
καθόλου	☐	☐	☐	☐	☐	πάρα πολύ

Ενότητα 5 (Ευαισθητοποίηση)

16.

Σας άρεσε το εκπαιδευτικό κομμάτι του παιχνιδιού; *

	1	2	3	4	5	
καθόλου	☐	☐	☐	☐	☐	πάρα πολύ

17.

Πιστεύετε πως το SAGE σας προετοίμασε κατάλληλα για μια παρόμοια, πιθανή μελλοντική επίθεση ηλεκτρονικού ψαρέματος; *

	1	2	3	4	5	
καθόλου	☐	☐	☐	☐	☐	πάρα πολύ

18.

Ποιο κομμάτι σχετικά με την επίθεση, σας τράβηξε το ενδιαφέρον και το θυμάστε ακόμη; *

- ☐ ο τίτλος
- ☐ ο αποστολέας
- ☐ το σώμα του μηνύματος
- ☐ η πλαστή ιστοσελίδα
- ☐ Άλλο...

19.

Έχετε συναντήσει/ παίξει ξανά παρόμοιο παιχνίδι ευαισθητοποίησης και εκπαίδευσης στα πλαίσια επιμόρφωσης, στην εργασία σας; *

- ☐ Ναι
- ☐ Όχι

20.

Θα προτείνατε να αξιοποιηθεί/ ενταχθεί η ολοκληρωμένη έκδοση του παιχνιδιού για την επιμόρφωση όλων των εργαζομένων πάνω σε θέματα ασφάλειας, στην εργασία σας; *

	1	2	3	4	5	
καθόλου	☐	☐	☐	☐	☐	πάρα πολύ

Σχόλια

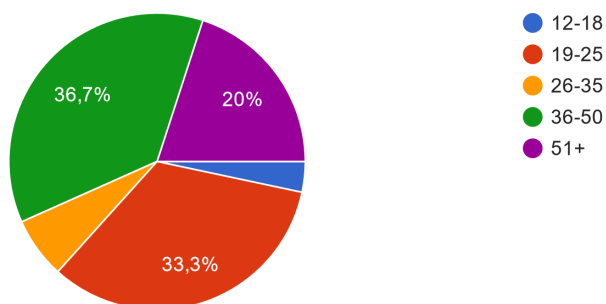
Κείμενο μακροσκελούς απάντησης

Σας ευχαριστώ για τον χρόνο σας!

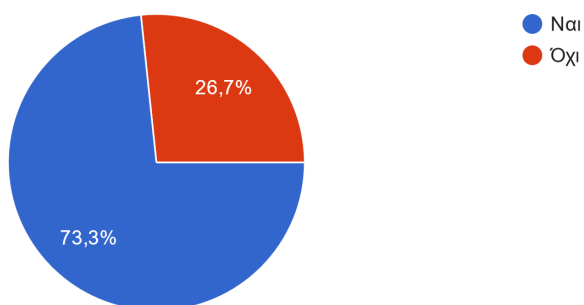
Περιγραφή (προαιρετικό)

Απαντήσεις

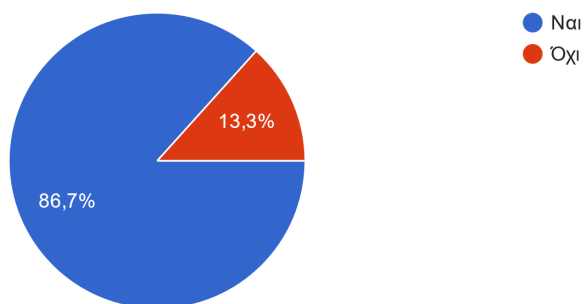
Ποια είναι η ηλικία σας;
30 απαντήσεις



Εργάζεστε;
30 απαντήσεις



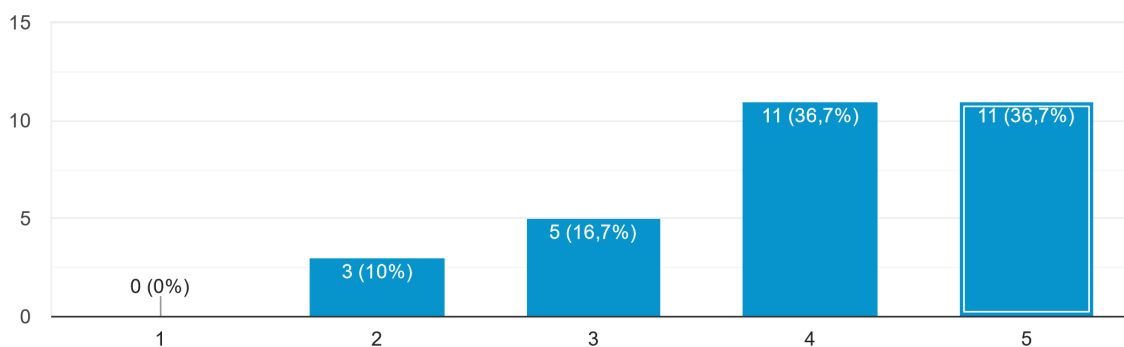
Χρησιμοποιείτε κάποια ηλεκτρονική συσκευή (υπολογιστή) κατά την εργασία σας;
30 απαντήσεις



Εάν ναι,



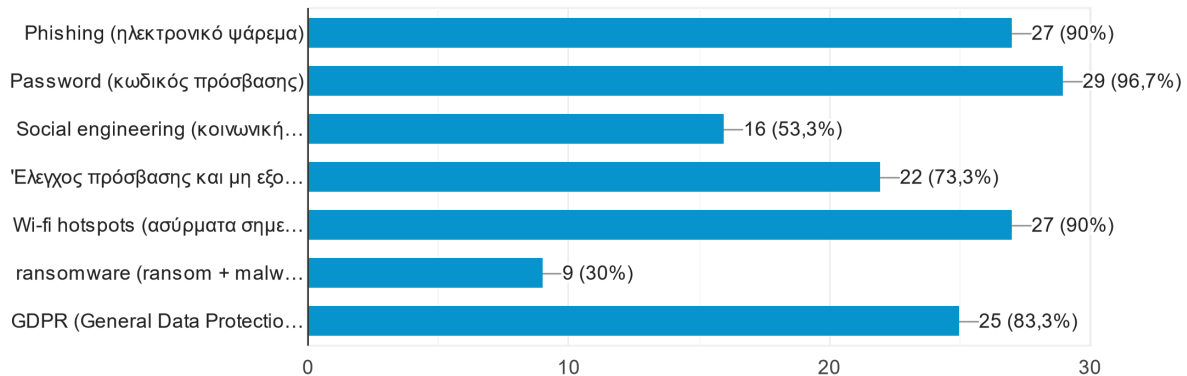
Ποιος είναι ο βαθμός εξοικείωσης σας αναφορικά με την χρήση νέων τεχνολογιών (σύμφωνα με την κρίση σας);
30 απαντήσεις



Βιβλιογραφία

Ποιές από τις παρακάτω έννοιες έχετε ακουστά;

30 απαντήσεις



Τι γνωρίζετε για το Phishing (ηλεκτρονικό ψάρεμα);

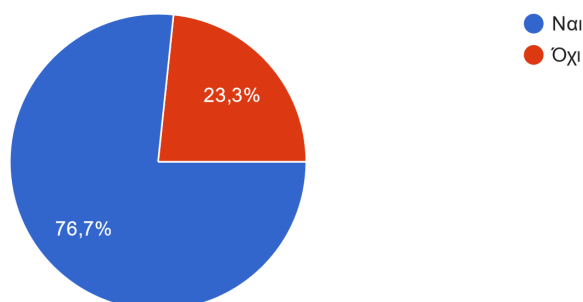
29 απαντήσεις

Ελάχιστα
Απαιτεί να είμαστε ιδιαίτερα προσεκτικοί, διότι μπορεί να πέσουμε θύμα χωρίς καν να το καταλάβουμε
Είναι μια επίθεση που γίνεται στο διαδίκτυο κατά την οποία ένα άτομο υποδύεται μία αξιόπιστη οντότητα και στόχο έχει να κλέψει προσωπικά δεδομένα.
προσπάθεια κλοπής δεδομένων
απάτη για την απόκτηση πληροφοριών μέσω email
Την προσπάθεια που καταβάλει κάποιος όταν με διάφορους τρόπους προσπαθεί να σου αποσπάσει από εσένα προσωπικά στοιχεία στο διαδίκτυο.
Η προσπάθεια που καταβάλλει κάποιος όταν με διάφορους τρόπους προσπαθεί να αποσπάσει από προσωπικά στοιχεία στο διαδίκτυο
Πρόκειται για μέθοδο ηλεκτρονικής εξαπάτησης και υποκλοπής δεδομένων
Μια επίθεση ηλεκτρονικού ψαρέματος (phishing) επιχειρείται όταν κάποιος προσπαθεί να ξεγελάσει κάποιον ,μέσω μηνυμάτων ηλ. ταχυδρομείου, διαφημίσεων ή ιστοτόπων που μοιάζουν με εκείνους που ήδη χρησιμοποιεί, ώστε να κοινοποιήσει προσωπικά στοιχεία στο διαδίκτυο κ.ά.
Η ενέργεια όπου σε εξαπατούν υποδυόμενοι την αξιόπιστη πηγή για να κλέψουν τα προσωπικά σου δεδομένα
Προσπάθεια ηλεκτρονικής εξαπάτησης μέσω του email
Είναι επίθεση με κακόβουλο λογισμικό με σκοπό την πρόσβαση σε προσωπικά δεδομένα
Κακόβουλο λογισμικό, για ψάρεμα στα προσωπικά δεδομένα μας

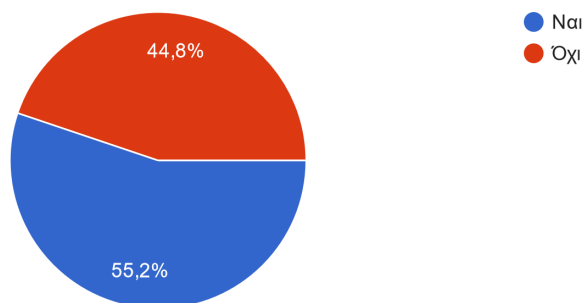
Μήνυμα ηλεκτρονικού ταχυδρομείου, κείμενο ή άλλη μορφή ηλεκτρονικής επικοινωνίας που φαίνεται να προέρχεται από τράπεζα ή κάποια άλλη δημοφιλή ηλεκτρονική υπηρεσία που μας ζητά τα διαπιστευτήρια μας, έναν αριθμό πιστωτικής κάρτας ή άλλες ευαίσθητες πληροφορίες; Αυτή η τεχνική που χρησιμοποιείται για την απόκτηση πληροφοριών οι οποίες κατόπιν θα πουληθούν ή θα αξιοποιηθούν από τους επιτιθέμενους για εκβιασμό, κλοπή χρημάτων, ή υποκλοπή ταυτότητας. είναι το ηλεκτρονικό ψάρεμα οι λεγόμενες ηλεκτρονικές επιθέσεις (phishing).
ΣΥΝΔΕΣΜΟΣ ΠΟΥ "ΨΑΡΕΥΕΙ" ΚΡΙΣΙΜΕΣ ΠΛΗΡΟΦΟΡΙΕΣ
Εκμείευση πληροφοριών κάποιου χρήστη
Είναι μια κυβερνοεπιθεση μέσω της οποίας ο attacker "ψαρεύει" το θύμα προσποιούμενος κάποιο έμπιστο πρόσωπο για να αποκτήσει πρόσβαση σε προσωπικά δεδομένα
Τίποτα
Ηλεκτρονική απάτη
παραπλανητικό μήνυμα για κλοπή προσωπικών στοιχείων
ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ ΠΟΥ ΠΡΟΣΠΑΘΕΙ ΝΑ ΨΑΡΕΥΕΙ ΠΡΟΣΩΠΙΚΑ ΔΕΔΟΜΕΝΑ
ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ ΠΟΥ ΠΡΟΣΠΑΘΕΙ ΝΑ ΥΠΟΚΛΕΨΕΙ
ΠΡΟΣΠΑΘΕΙΑ ΗΛΕΚΤΡΟΝΙΚΗΣ ΥΠΟΚΛΟΠΗΣ
Συνήθως ο χρήστης λαμβάνει κάποιο email από κακόβουλο χρήστη ο οποίος με παραπλανητικούς τρόπους προσπαθεί να αποσπάσει προσωπικά δεδομένα/στοιχεία από την χρήστη.
Βασικά μου το εξήγησες εσύ Χριστιάνα μου αχαχα απ' ο,τι κατάλαβα, είναι κακόβουλα αρχεία σε μορφή Email που στέλνονται σε διάφορους χρήστες με απώτερο στόχο την αποκόμιση χρημάτων από τον αποστολέα, δηλαδή προσπαθούν να τον ψαρέψουν με ηχηρά μηνύματα όπως για παράδειγμα ότι κάποιος οικείος του τραυματίστηκε ώστε να αποστείλουν χρήματα στον αποστολέα του Email για αν βοηθήσουν κ.ο.κ.
είναι η κλοπή προσωπικών δεδομένων
Αλίευση στοιχείων για κακόβουλη χρήση
ΗΛΕΚΤΡΟΝΙΚΗ ΑΠΑΤΗ ΜΕΣΩ EMAIL

SAGE (Security Awareness Game for Employees)

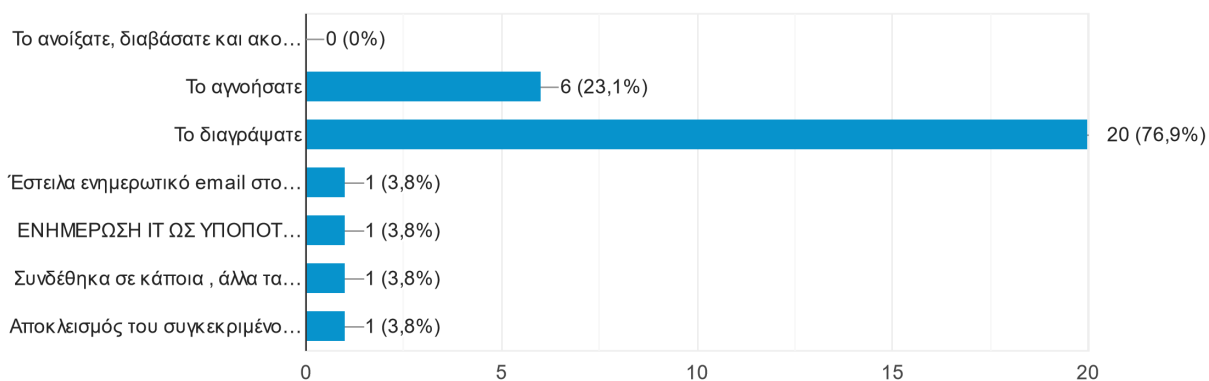
Έχετε συναντήσει παρόμοιο περιστατικό με αυτό το παιχνίδι στην πραγματική σας ζωή;
30 απαντήσεις



Έχετε συναντήσει παρόμοιο περιστατικό με αυτό το παιχνιδιού στην εργασία σας;
29 απαντήσεις

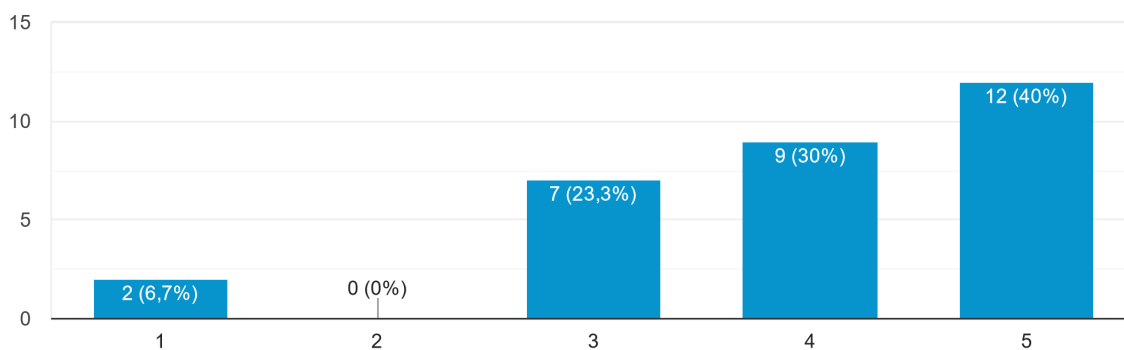


Εαν ναι, πως διαχειριστήκατε αυτό το νέο μήνυμα ηλεκτρονικού ταχυδρομείου;
26 απαντήσεις



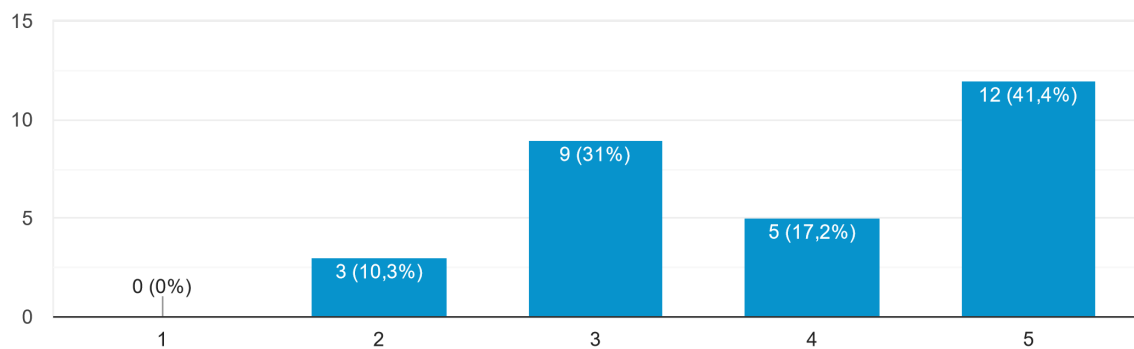
Χρηστικότητα

Θεωρείτε το παιχνίδι ελκυστικό;
30 απαντήσεις



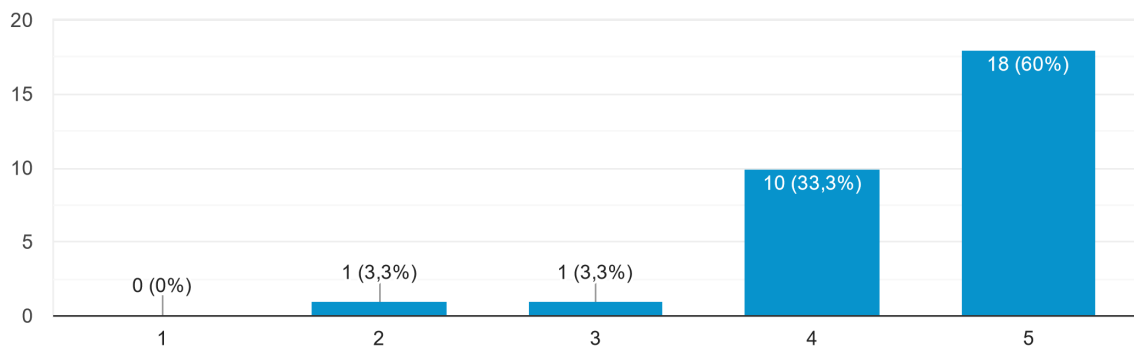
Σας άρεσε το περιβάλλον του SAGE (τα γραφικά, η μουσική, οι μεταβάσεις κτλ.) ;

29 απαντήσεις



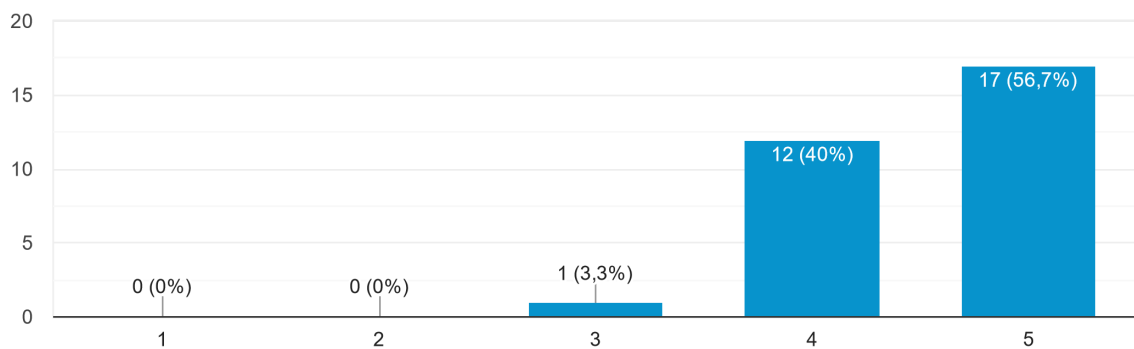
Πόσο εύκολος ήταν ο χειρισμός του παιχνιδιού;

30 απαντήσεις



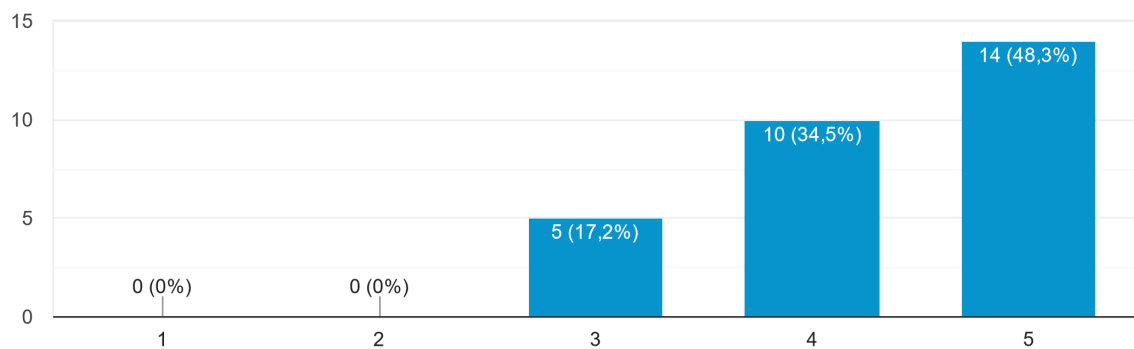
Οι οδηγίες/ αφήγηση του παιχνιδιού ήταν σαφείς και κατανοητές;

30 απαντήσεις



Οι διαθέσιμες κινήσεις/επιλογές ήταν επαρκείς;

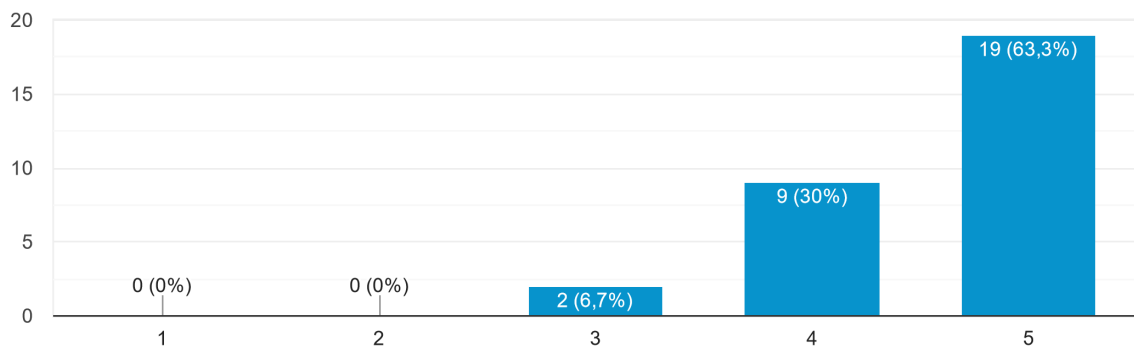
29 απαντήσεις



Ευαισθητοποίηση

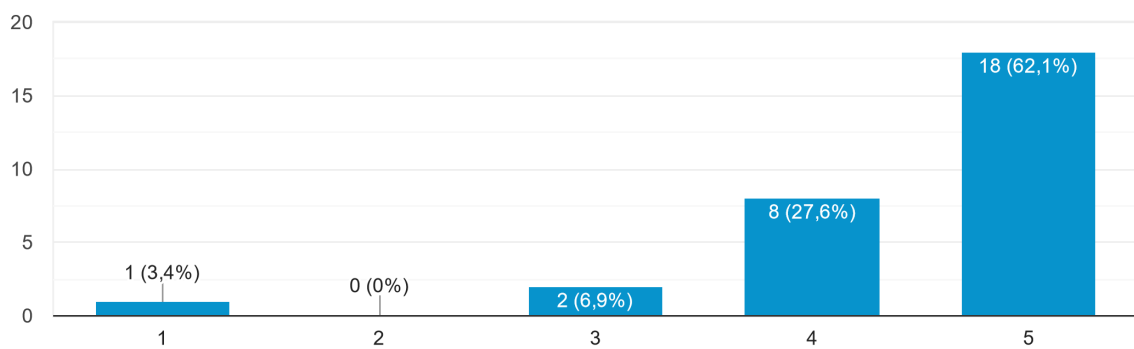
Σας άρεσε το εκπαιδευτικό κομμάτι του παιχνιδιού;

30 απαντήσεις

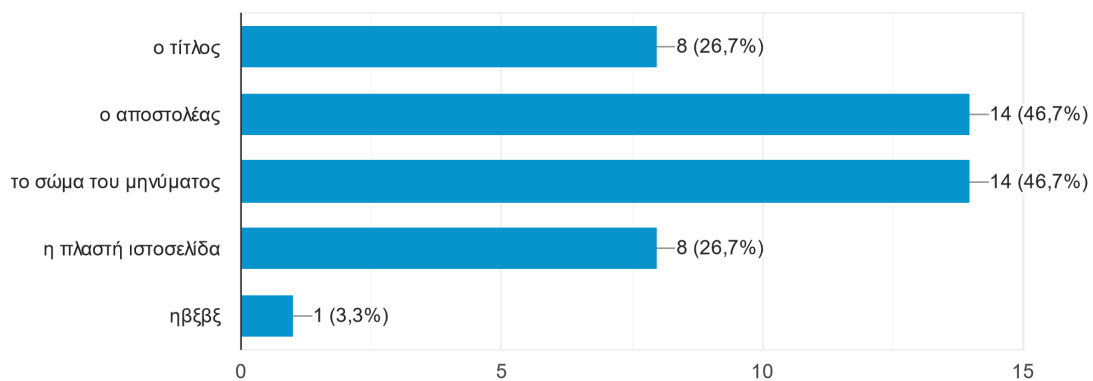


Πιστεύετε πως το SAGE σας προετοίμασε κατάλληλα για μια παρόμοια, πιθανή μελλοντική επίθεση ηλεκτρονικού ψαρέματος;

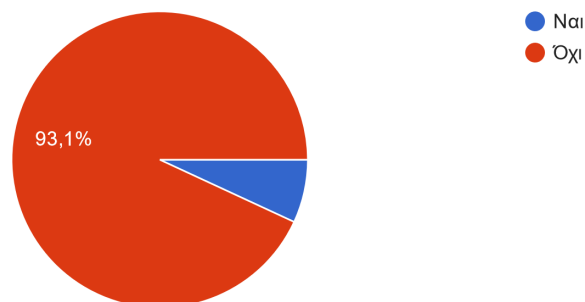
29 απαντήσεις



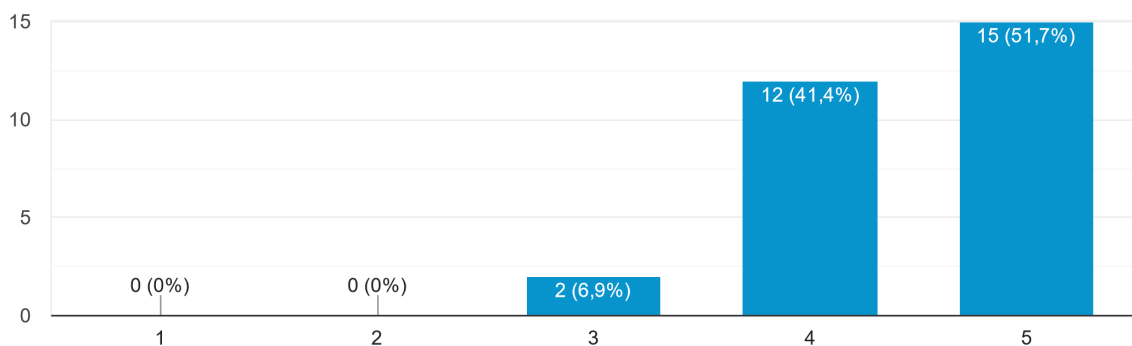
Ποιο κομμάτι σχετικά με την επίθεση, σας τράβηξε το ενδιαφέρον και το θυμάστε ακόμη;
30 απαντήσεις



Έχετε συναντήσει/ παίξει ξανά παρόμοιο παιχνίδι ευαισθητοποίησης και εκπαίδευσης στα πλαίσια επιμόρφωσης, στην εργασία σας;
29 απαντήσεις



Θα προτείνετε να αξιοποιηθεί/ ενταχθεί η ολοκληρωμένη έκδοση του παιχνιδιού για την επιμόρφωση όλων των εργαζομένων πάνω σε θέματα ασφάλειας, στην εργασία σας;
29 απαντήσεις



Σχόλια

8 απαντήσεις

Αρκετοί χρήστες ηλεκτρονικών υπολογιστών είναι ανυποψίαστοι σε τέτοιες μεθόδους όπως το phishing και απαιτείται περαιτέρω ενημέρωση ακόμα και από τους εκπαιδευτικούς στα σχολεία.
Προσοχή με τα γράμματα. Δεν φαίνονται καθόλου καλά και αυτό δυσκολεύει πολύ στην ανάγνωση και μειώνει την ελκυστικότητα του παιχνιδιού. Επίσης, υπάρχουν μικρά ορθογραφικά λάθη που πρέπει να διορθωθούν. Είναι ωραίο σαν παιχνίδι απλά θέλει λίγη παραπάνω δουλειά στα γραφικά και την εμφάνιση.
Πολύ καλή δουλειά!!!
Ενδιαφέρον. Καλό θα ήταν να ενταχθεί σε κάθε εργασιακό περιβάλλον
ΠΟΛΥ ΩΡΑΙΑ ΕΡΓΑΣΙΑ - ΜΠΡΑΒΟ ΚΑΛΗ ΕΠΙΤΥΧΙΑ
ΩΡΑΙΟ ΕΡΩΤΗΜΑΤΟΛΟΓΙΟ
Είναι ένα πολύ έξυπνο παιχνίδι που γρήγορα και εύκολα κάνει αυτό για το οποίο κατασκευάστηκε: ευαισθητοποιεί τον χρήστη για τους κινδύνους του φαινομένου
ΕΞΥΠΝΟ VIDEO , ΟΜΟΡΦΑ ΓΡΑΦΙΚΑ ΚΑΙ ΠΟΛΥ ΣΩΣΤΑ ΔΟΜΗΜΕΝΟ! ΣΥΓΧΑΡΗΤΗΡΙΑ ΣΤΟΝ ΔΗΜΙΟΥΡΓΟ