ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

ΣΧΟΛΗ ΚΟΙΝΩΝΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΟΛΙΤΙΣΜΙΚΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΩΙΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΕΙΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ ΤΗΣ ΙΔΙΩΤΙΚΟΤΗΤΑΣ ΜΕΣΩ ΤΗΣ ΠΑΙΓΝΙΔΟΠΟΙΗΣΗΣ

Προπτυχιακή Φοιτήτρια: Χατζούλα Ελένη

Επιβλέπων Καθηγητής: Αναπληρωτής Καθηγητής, Καλλονιάτης Χρήστος

ΜΥΤΙΛΗΝΗ, ΙΟΥΝΙΟΣ 2018

Περιεχόμενα

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέπων καθηγητή μου, Αναπληρωτή Καθηγητή κ. Καλλονιάτη Χρήστο για την συνεργασία που είχαμε και τη Μαυροειδή Κατερίνα για την πολύτιμη βοήθειά της. Επίσης, θα ήθελα να ευχαριστήσω τους γονείς μου και τους φίλους μου για την υποστήριξή τους.

Περίληψη

Η παρούσα πτυχιακή εργασία ασχολείται με την παιγνιοποίηση και τη χρήση της σε εφαρμογές σχετικά με ζητήματα ασφάλειας και ιδιωτικότητας. Ο στόχος της εργασίας είναι η βιβλιογραφική ανασκόπηση του θέματος αυτού, έτσι ώστε να παρατηρηθούν τυχών κενά που μπορεί να υπάρχουν στη βιβλιογραφία. Αρχικά, δίνεται ο ορισμός της παιγνιοποίησης, καθώς και οδηγίες για το σχεδιασμό παιγνιωδών εφαρμογών. Επίσης, παρουσιάζονται παραδείγματα χρήσης της παιγνιοποίησης σε διάφορους τομείς. Στη συνέχεια, αναλύονται τα ζητήματα σχετικά με την επίγνωση της ασφάλειας και της ιδιωτικότητας στα πληροφοριακά συστήματα. Επιπλέον, δίνονται και κάποια παραδείγματα εφαρμογών που συνδυάζουν την παιγνιοποίηση με την επίγνωση της ασφάλειας και της ιδιωτικότητας. Η εργασία αυτή, ερευνά αρχικά την έννοια της παιγνιοποίησης και στη συνέχεια απαντά σε ερωτήματα, όπως «πώς μπορεί να χρησιμοποιηθεί στις καθημερινές δραστηριότητες και στους τομείς», «γιατί χρειάζεται οι χρήστες να αποκτήσουν επίγνωση σε ζητήματα ασφάλειας και ιδιωτικότητας στο διαδίκτυο» και «πώς μπορεί να συμβάλλει η παιγνιοποίηση στη δημιουργία εφαρμογών για αυτά τα ζητήματα, έτσι ώστε να γίνουν πιο ελκυστικά στο χρήστη».

Abstract

This thesis deals with gamification and its use in applications related to security and privacy issues. The aim of this thesis is to review this topic in order to observe any gaps that may exist in the bibliography. First, of the term “gamification” is defined and instructions for designing gamification applications are described. Also, there are examples of how to use gamification in different areas. Next, the issues of security and privacy awareness in information systems are analyzed. Additionally, there are some examples of applications that combine gamification with security and privacy awareness and training. This work initially investigates the concept of gamification and how it can be used in daily activities, why users need to be aware of online security and privacy issues and how applications can be gamified in order to be more attractive for the users.

Κεφάλαιο 1^{ο}: Εισαγωγή

Στην εποχή μας η καθημερινή χρήση του Διαδικτύου δημιουργεί συνεχώς νέες ανάγκες για την προστασία των χρηστών σε θέματα ασφάλειας και ιδιωτικότητας. Ο χρήστης θα πρέπει να είναι ενημερωμένος και να εκπαιδεύεται σε αυτά τα ζητήματα. Έτσι, θα μπορέσει να προστατέψει την ασφάλεια και την ιδιωτικότητά του κατά τη χρήση των πληροφοριακών συστημάτων. Η εργασία αυτή ασχολείται με την βιβλιογραφική ανασκόπηση σε ό,τι έχει γραφτεί σχετικά με ζητήματα επίγνωσης ασφάλειας και ιδιωτικότητας και πώς μπορεί η παιγνιοποίηση να συμβάλλει στη δημιουργία εφαρμογών που να είναι πιο ενδιαφέρουσες στη χρήση. Στην αρχή, γίνεται μια εισαγωγή στον ορισμό της παιγνιοποίησης. Είναι μια έννοια η οποία χρησιμοποιείται τα τελευταία χρόνια και παρά τις πολλές προσπάθειες των συγγραφέων, δεν υπάρχει κάποιος συγκεκριμένος ορισμός. Οι περισσότεροι συμφωνούν σε έναν ορισμό που συνοψίζει ικανοποιητικά το περιεχόμενο της λέξης. Ο ορισμός αυτός γράφτηκε από τους Deterding et al. [1] και ορίζεται ως εξής: «παιγνιοποίηση» είναι η χρήση στοιχείων σχεδιασμού των παιχνιδιών σε εφαρμογές που δεν αποτελούν παιχνίδια (the use of game design elements in non-game contexts). Μετά την διευκρίνιση της έννοιας, γίνεται μια έρευνα σε ό,τι έχει γραφτεί για τους τρόπους που υπάρχουν σχετικά με το σχεδιασμό παιγνιωδών εφαρμογών. Αρκετοί συγγραφείς έχουν προσπαθήσει να ορίσουν κάποια στάδια σχεδιασμού παιγνιωδών εφαρμογών, οι οποίες κάνουν πιο ελκυστικό το περιεχόμενο τους ως προς το χρήστη. Ταυτόχρονα, τονίζεται η χρησιμότητα της παιγνιοποίησης σε διάφορους τομείς, όπως την εκπαίδευση, το μάρκετινγκ, τους τομείς υγείας, τις επιχειρήσεις, το περιβάλλον και το crowdsourcing. Στη συνέχεια, αναλύονται τα ζητήματα ασφάλειας σε πληροφοριακά συστήματα. Είναι σημαντική η επίγνωση ασφάλειας, έτσι ώστε να προστατευτεί ο χρήστης από διάφορους κινδύνους. Περιγράφονται κάποιες οδηγίες σχεδιασμού για προγράμματα επίγνωσης ασφάλειας και εξάσκησης, τα οποία χρησιμεύουν στις εταιρίες και τους οργανισμούς για να διευκολύνουν τους υπαλλήλους σε θέματα που μπορεί να αντιμετωπίσουν σχετικά με την ασφάλεια των συστημάτων. Μαζί με την επίγνωση ασφάλειας, γίνεται και αναζήτηση στη βιβλιογραφία για ζητήματα ιδιωτικότητας, καθώς η ιδιωτικότητα είναι εξίσου σημαντική με την ασφάλεια. Χρειάζεται λοιπόν ο χρήστης να έχει επίγνωση και ως προς την ιδιωτικότητα. Στο τελευταίο κομμάτι της εργασίας δίνονται παραδείγματα εφαρμογών παιγνιοποίησης πάνω σε θέματα ασφάλειας και ιδιωτικότητας. Παρατηρείται η ανάγκη δημιουργίας περισσότερων εφαρμογών με παιγνιώδη στοιχεία, οι οποίες είναι πιο εύχρηστες και ευχάριστες.

Ως προς τη μεθοδολογία που χρησιμοποιήθηκε, αρχικά έγινε μια έρευνα των όρων «gamification», «security awareness», «privacy awareness», για να βρεθεί η σχετική βιβλιογραφία. Η αναζήτηση των όρων έγινε στις πλατφόρμες Google Scholar, Scopus, JSTOR και στη βιβλιοθήκη του πανεπιστημίου. Επίσης αναζητήθηκαν και οι όροι «security with gamification», «privacy with gamification» και «gamified programs», καθώς και οι ελληνικοί όροι «παιγνιοποίηση», «επίγνωση ασφάλειας», «επίγνωση ιδιωτικότητας», «παιγνιώδεις εφαρμογές». Μέσα από αρκετά αποτελέσματα, ερευνήθηκε η βιβλιογραφία, η οποία κατέληξε στα κείμενα και στις ιστοσελίδες που χρησιμοποιήθηκαν και βρίσκονται στο τέλος της εργασίας. Παρατηρήθηκε ότι υπάρχει ελάχιστη βιβλιογραφία στα ελληνικά, οπότε τα περισσότερα κείμενα προέρχονται από ξένους συγγραφείς. Στη συνέχεια, έγινε ένας διαχωρισμός της παιγνιοποίησης από την επίγνωση ασφάλειας και ιδιωτικότητας, έτσι ώστε κάποιος που διαβάζει το κείμενο να είναι σε θέση να αποσαφηνίσει τους όρους και να τους συνδέσει μεταξύ τους. Μετά την εύρεση της βιβλιογραφίας, έγινε η καταγραφή και ο εντοπισμός ελλείψεων στον κάθε ορισμό ξεχωριστά. Παρατηρήθηκε ότι δεν έχει δοθεί ιδιαίτερη σημασία στον τομέα της ιδιωτικότητας. Τέλος, μετά την καταγραφή σημειώθηκαν τα συμπεράσματα αυτής της βιβλιογραφικής ανασκόπησης.

Κεφάλαιο 2ο:Παιγνιοποίηση (Gamification)

Στο κεφάλαιο αυτό αναφέρονται οι διάφορες προσεγγίσεις αναφορικά με τον ορισμό της έννοιας «παγνιοποίηση» (gamification), περιγράφονται οι οδηγίες σχεδιασμού παιγνιωδών εφαρμογών και τέλος, παρουσιάζονται κάποια παραδείγματα εφαρμογής αυτής της μεθόδου σε διάφορους τομείς, όπως εκπαίδευση, υγεία κλπ.

2.1 Ορισμός

Η παιγνιοποίηση (gamification) σαν έννοια είναι ένα ζήτημα που έχει απασχολήσει αρκετούς ερευνητές. Μολονότι πολλοί έχουν προσπαθήσει να δώσουν ένα σαφή ορισμό, διαπιστώνεται ότι υπάρχει μία δυσκολία στην αποτύπωση της έννοιας. Στη βιβλιογραφία, οι περισσότεροι αρχικά ορίζουν την έννοια του παιχνιδιού που είναι και το πρώτο σύνθετο της λέξης.

Από τους πρώτους που ασχολήθηκαν με τον ορισμό του παιχνιδιού ήταν οι Avedon και Sutton-Smith (1971) [1], οι οποίοι υποστηρίζουν ότι το παιχνίδι είναι μια εθελοντική δραστηριότητα που οριοθετείται από κανόνες. Ο Crawford (1984) [1] αργότερα αναφέρει, πως τα παιχνίδια πρέπει να αντιπροσωπεύουν κάποια πραγματικότητα, δηλαδή να εξαρτώνται από την αλληλεπίδραση μεταξύ του συστήματος και του χρήστη, δίνοντας στο χρήστη τη δυνατότητα να έρθει σε «σύγκρουση» με το παρεχόμενο εικονικό περιβάλλον. Για τον Huizinga (2000) [1] το παιχνίδι είναι μία μη σοβαρή αλλά έντονα εθελοντική δραστηριότητα, η οποία βασίζεται σε κανόνες και κοινωνικά όρια. Οι σχεδιαστές παιχνιδιών, Salen και Zimmerman (2004) [1], ορίζουν το παιχνίδι ως ένα σύστημα που προσδιορίζεται από κανόνες. Κατά τη διάδρασή με το σύστημα, οι παίκτες εμπλέκονται σε μια τεχνητή «σύγκρουση», της οποίας το αποτέλεσμα μπορεί να ποσοτικοποιηθεί. Ο Juul (2003) [1] προτείνει ότι όλα τα παιχνίδια έχουν έξι βασικά χαρακτηριστικά: α) κανόνες, β) ποικιλία, γ) μετρήσιμα αποτελέσματα, δ) αποτέλεσμα με αξία, ε) προσπάθεια του παίκτη, στ) επένδυση του παίκτη και διαπραγματεύσιμες συνέπειες, με σεβασμό στην πραγματική ζωή.

Η εξέλιξη της τεχνολογίας έχει οδηγήσει στην αλλαγή του τρόπου με τον οποίο παίζονται τα παιχνίδια. Πλέον από το κλασσικό παιχνίδι έχει γίνει μετάβαση στο βιντεοπαιχνίδι, στο οποίο έχουν αλλάξει τα σημεία εμπλοκής του χρήστη, καθώς και ο τρόπος διασκέδασής του κατά τη διάδρασή του με αυτό (Brumels et al., 2008) [2]. Επίσης, λόγω της αυξανόμενης χρήσης των μέσων κοινωνικής δικτύωσης αλλά και γενικά του Διαδικτύου, στην κοινωνία

του 21ου αιώνα η διασκέδαση μέσω των παιχνιδιών είναι μια συνηθισμένη δραστηριότητα [2]. Ο σχεδιαστής παιχνιδιών Jesse Schell (2010) [2] παρουσιάζει ένα μέλλον, στο οποίο τα βιντεοπαιχνίδια αποτελούν μέρος της πραγματικότητας. Οι Mora, Riera et al. (2015) [2], εξηγούν ότι λόγω της παρουσίας των παιχνιδιών στην καθημερινότητα της σύγχρονης κοινωνίας, η παιγνιοποίηση αναδύεται σχεδόν αυτόματα, ως ένας τρόπος εξαγωγής χαρακτηριστικών των παιχνιδιών και ενσωμάτωσής τους σε άλλα περιβάλλοντα.

Όπως αναφέρθηκε, η «παιγνιοποίηση» ως έννοια δεν έχει κάποιο συγκεκριμένο ορισμό. Μία πρώτη προσέγγιση έγινε από τον Nick Pelling (2002) [2], ο οποίος όρισε την παιγνιοποίηση ως μια εφαρμογή που παρέχει στο χρήστη μια διεπαφή, η οποία θυμίζει παιχνίδι για να κάνει τις ηλεκτρονικές συναλλαγές τόσο εύχρηστες όσο και γρήγορες. Από τότε βέβαια, ο ορισμός έχει διαμορφωθεί και έχει αλλάξει αρκετά, συνδυάζοντας τα στοιχεία των παιχνιδιών και του σχεδιασμού.

Οι Seaborn και Fels (2014) [1] στην έρευνά τους, βρήκαν ότι πολύ πριν δοθεί ο όρος παιγνιοποίηση, είχαν χρησιμοποιηθεί διαφορετικοί όροι για αυτή τη μέθοδο. Στη βιβλιογραφία παρατηρείται ένας μεγάλος αριθμός λέξεων που προτάθηκαν ως πιθανές ορολογίες, όπως για παράδειγμα οι λέξεις *«funware»* (Azadegan and Riedel, 2012), *«funology»* (Malone, 1982), *«productivity games», «surveillance entertainment», «behavioral games», «game layers», «applied gaming»* και *«serious games»* [1]. Ο McGonigal's (2011) [1] πρότεινε, επίσης, κάποιες άλλες εκφράσεις, όπως *«alternate reality games»*, *«games with a purpose»* και *«παιχνίδια επαυξημένης πραγματικότητας» (augmented reality games)*, φέρνοντας την πραγματικότητα στον τυπικά φανταστικό και αντιπροσωπευτικό κόσμο των παραδοσιακών παιχνιδιών. Παρ' όλα αυτά η λέξη *«παιγνιοποίηση»* (gamification) έχει επικρατήσει τα τελευταία χρόνια και είναι αποδεκτή από όλους όσους ασχολούνται με τη συγκεκριμένη μέθοδο.

Αν και η χρήση της λέξης «παιγνιοποίηση» είναι σχετικά καινούρια, η μέθοδος αυτή χρησιμοποιείται πολύ τις τελευταίες δεκαετίες σε διάφορα συστήματα, όπως σε προγράμματα ανάγνωσης θερινών βιβλιοθηκών. Οι Zichermann και Linder (2010) [1] προσδιορίζουν την παιγνιοποίηση ως ένα εργαλείο που χρησιμοποιείται για τη συμπλήρωση των πρωτοβουλιών branding μέσω της εφαρμογής των στοιχείων του παιχνιδιού και της μηχανικής. Το 2011 ορίστηκε από τους Deterding et al. [1,3] η μέθοδος της «παιγνιοποίησης». Πρόκειται για τον πιο δημοφιλή ορισμός και χρησιμοποιείται αρκετά σε διάφορες έρευνες σχετικές με τη συγκεκριμένη μέθοδο. Με βάση τους Deterding et al. [1,3] «παιγνιοποίηση» είναι *«η χρήση στοιχείων σχεδιασμού των παιχνιδιών σε εφαρμογές*

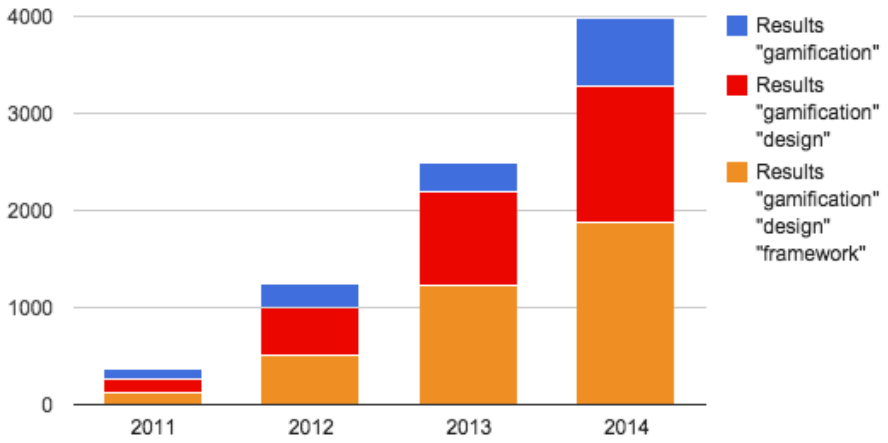
που δεν αποτελούν παιχνίδια» (the use of game design elements in non-game contexts). Στο άρθρο τους αναλύουν ξεχωριστά την κάθε λέξη που χρησιμοποίησαν στον ορισμό τους.

Ταυτόχρονα, οι Huotari και Hamari (2012) [1] βασισμένοι στον ορισμό των Deterding et al., πιστεύουν ότι πρέπει να δοθεί βάση στην εμπειρία του χρήστη και όχι τόσο στο τελικό αποτέλεσμα. Γι' αυτό προτείνουν ότι η παιγνιοποίηση είναι η διαδικασία ενίσχυσης μιας υπηρεσίας με προοπτικές εμπειρίας παιχνιδιού, προκειμένου να υποστηρίξει την εμπειρία του χρήστη. Από την οπτική της επιχειρηματικής στρατηγικής, οι Werbach και Hunter (2012) [1] βλέπουν την παιγνιοποίηση ως τη χρήση των στοιχείων των παιχνιδιών και της τεχνικής της σχεδίασης των παιχνιδιών στο πλαίσιο μη-παιχνιδιού. Γενικά λοιπόν, όπως συμφωνούν και οι συγγραφείς Seaborn και Fels (2014) [1], με βάση όλους αυτούς τους ορισμούς καταλήγουμε στο συμπέρασμα ότι η παιγνιοποίηση είναι η διεθνής χρήση των στοιχείων των παιχνιδιών για μια εμπειρία παιχνιδιού σε διαδικασίες και πλαίσια μη-παιχνιδιού.

2.2 Σχεδιασμός παιγνιωδών εφαρμογών

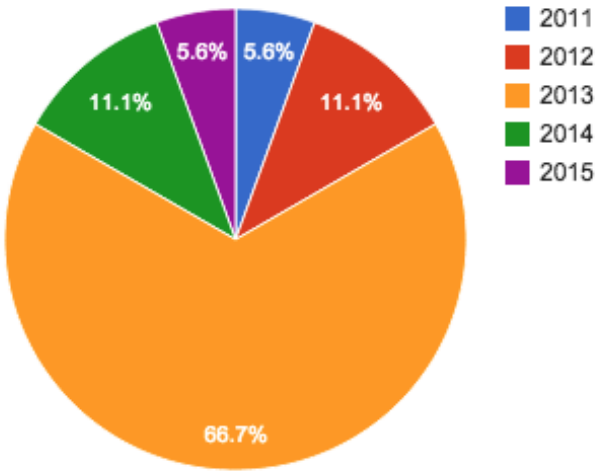
Σε αυτό το υποκεφάλαιο παρουσιάζεται η βιβλιογραφία που υπάρχει σχετικά με το σχεδιασμό παιγνιωδών εφαρμογών. Οι Mora A., Riera D. Gonzalez C. και Arnedo-Moreno J. [2] έκαναν μια βιβλιογραφική ανασκόπηση των κειμένων που έχουν γραφτεί σχετικά με τη σχεδίαση.

Αρχικά, οι συγγραφείς παρουσιάζουν ένα γράφημα, στο οποίο φαίνονται τα συγκεντρωτικά αποτελέσματα του Μελετητή της Google ανά έτος και οι λέξεις – κλειδιά που χρησιμοποιήθηκαν στις αναζητήσεις. Μέσω του γραφήματος είναι εμφανές ότι το ενδιαφέρον της κοινότητας βρίσκεται στο σχεδιασμό παιγνιωδών εφαρμογών και της βιβλιογραφίας. Αυτή η δημοτικότητα περιλαμβάνει όλα τα είδη των περικειμένων: εξάσκηση και εκπαίδευση, ανθρώπινοι πόροι, μάρκετινγκ, πωλήσεις, υγεία, κλπ.



Εικόνα1. «Results of academical searches about gamification», Mora A., Riera D., Gonzalez C. & Arnedo-Moreno J. (2015), A literature review of gamification design frameworks, Spain

Ταυτόχρονα σε άλλο γράφημα, σημειώνουν ότι οι ημερομηνίες δημοσίευσης κειμένων που σχετίζονται με την παιγνιοποίηση είναι αρκετά πρόσφατες. Όπως φαίνεται και στο γράφημα, το 2013 δημοσιεύτηκαν τα περισσότερα άρθρα με ποσοστό 66,7%.



Εικόνα.2 «Gamification design framework publish date», Mora A., Riera D., Gonzalez C. & Arnedo-Moreno J. (2015), A literature review of gamification design frameworks, Spain

Ο σκοπός των στοιχείων του σχεδιασμού παιγνιωδών εφαρμογών είναι αρκετά διαφορετικός από το σχεδιασμό του παιχνιδιού, καθώς το πρώτο χρησιμοποιείται για την ενίσχυση της εμπλοκής σε διαφορετικά πλαίσια, ενώ το δεύτερο στοχεύει στη διασκέδαση. Ο Marczewski (2014) [2] κάνει μια ξεκάθαρη διάκριση ανάμεσα στο παιχνίδι και στο

σχεδιασμό παιγνιωδών εφαρμογών. Αρχικά, το πιο κοινό ξεκίνημα για το σχεδιασμό του παιχνιδιού είναι η ιδέα της διασκέδασης, ενώ η παιγνιοποίηση έχει έναν επιχειρηματικό στόχο. Δεύτερον, ο ορισμός των μετρήσεων ή των γραμμών παιχνιδιών πρέπει να συμβαίνει σε διαφορετικά στάδια της διαδικασίας σχεδιασμού.

Ο σχεδιασμός ενός συστήματος που θυμίζει παιχνίδι με το σχεδιασμό ενός παιχνιδιού είναι τελείως διαφορετική διαδικασία, παρόλο που υπάρχει μα λεπτή γραμμή που τα ενώνει. Αυτή η λεπτή γραμμή είναι ουσιαστικά τα στοιχεία παιχνιδιού. Οι βασικές αρχές της παιγνιοποίησης όμως βασίζονται σε αυτές των παιχνιδιών.

Ο σχεδιασμός παιχνιδιού μπορεί αρχικά να αναφερθεί ως *«η δράση της κατανόησης των πραγμάτων που σχετίζονται με το παιχνίδι».* Αυτός ο ορισμός δεν έχει μεγάλη διαφορά από τον ορισμό του Schell (2008) [2], ο οποίος αναφέρει τα στοιχεία του παιχνιδιού ως *«την προσπάθεια να αποφασίσουμε τι θα περιέχει ένα παιχνίδι»*. Αντίθετα, οι Salen και Zimmerman (2004) [2] έδωσαν ένα σύνολο βασικών αρχών σχεδιασμού παιχνιδιού, οι οποίες είναι:

1. κατανόηση της σχεδίασης, του συστήματος και της διαδραστικότητας, όσο και της επιλογής του παίκτη, της δράσης και του αποτελέσματος,

2. μελέτη των κανόνων του παιχνιδιού και το ‘’σπάσιμό’’ τους, την πολυπλοκότητα και την εμφάνιση, την εμπειρία του παιχνιδιού, την αναπαραγωγή του και την αλληλεπίδρασή του με το κοινωνικό σύνολο και

3. προσθέτοντας την ισχυρή σύνδεση μεταξύ των κανόνων ενός παιχνιδιού και το παιχνίδι που δημιουργούν οι κανόνες, τη διασκέδαση που παρέχουν τα παιχνίδια, τις έννοιες που κατασκευάζουν, τις ιδεολογίες που ενσωματώνουν και τις ιστορίες που λένε.

Οι Brathwaite και Schreiber (2009) [2], μελετώντας αυτές τις αρχές, δήλωσαν ότι μόλις αναγνωριστούν τα διαφορετικά στοιχεία των παιχνιδιών, είναι απαραίτητο να διερευνηθεί ο τρόπος αλληλοσυσχέτισής τους και εφαρμογής τους. Χρησιμοποίησαν όρους από την επιστήμη της χημείας για να τα διευκρινίσουν, ορίζοντας τα άτομα του παιχνιδιού ως *«τα μικρότερα μέρη ενός παιχνιδιού που μπορούν να απομονωθούν και να μελετηθούν ξεχωριστά»*. Με βάση αυτή την προσέγγιση, η διαδικασία της σχεδίασης ενός παιχνιδιού με τη χρήση πολλών ατόμων γίνεται πιο ξεκάθαρη. Αυτή η ιδέα χρησιμοποιήθηκε από τους Reeves και Red (2013) [2], οι οποίοι παρουσίασαν τα δέκα συστατικά για τη σχεδίαση παιχνιδιού:

- Αυτό-αναπαράσταση (Self-representation)
- Τρισδιάστατο περιβάλλον (three-dimensional environment)
- Αφήγηση (narrative)

- Ανατροφοδότηση (feedback)
- Φήμη γύρων και επιπέδων (reputations ranks and levels)
- Αγορές και οικονομία (marketplaces and economies)
- Ανταγωνισμός σύμφωνα με ορισμένους κανόνες (competition under rules)
- Ομάδες (teams)
- Επικοινωνία (communication)
- Πίεση χρόνου (time pressure)

Οι Hunicke et al το 2004 [2] ανέπτυξαν μια δομή για το περιεχόμενο των στοιχείων του παιχνιδιού, την οποία ονόμασαν «MDA» (Mechanics, Dynamics and Aesthetics). Είναι μια προσέγγιση, η οποία προσπαθεί να καλύψει το κενό ανάμεσα στο σχεδιασμό και την ανάπτυξη των παιχνιδιών, την κριτική του παιχνιδιού και την τεχνική έρευνά παιχνιδιών. Σύμφωνα με αυτή την προσέγγιση, τα παιχνίδια αποτελούνται από τρία στοιχεία: κανόνες, σύστημα και διασκέδαση. Αυτά τα στοιχεία μεταφράζονται απευθείας στα ακόλουθα συστατικά στοιχεία σχεδιασμού, τα οποία πρέπει να ορίζονται κατά το σχεδιασμό ενός παιχνιδιού με την ίδια σειρά:

1. Μηχανισμοί, οι οποίοι περιγράφουν τα στοιχεία του παιχνιδιού σε επίπεδο παρουσίασης δεδομένων και αλγορίθμων
2. Δυναμική, η οποία περιγράφει τη συμπεριφορά εκτέλεσης των μηχανικών, ενεργώντας στις εισόδους των παικτών και στις εξόδους των άλλων στο πέρασμα του χρόνου και
3. Αισθητική, η οποία περιγράφει την επιθυμητή ψυχολογική αντίδραση του παίχτη όταν έρχεται σε επαφή με το σύστημα του παιχνιδιού.

Έτσι, από την προοπτική της εμπειρίας του παιχνιδιού, ένα μοντέλο είναι μόνο ένα μέρος του συνόλου, όπως προτείνει και ο Cavillo-Gamez (2010) [2] στην θεωρία του «Core Elements of the Gaming Experience (CEGE)». Προτείνει μια σειρά από απαραίτητες αλλά όχι επαρκείς συνθήκες για την παροχή μιας θετικής εμπειρίας κατά τη διάρκεια του παιξίματος, οι οποίες πρέπει να συμπεριληφθούν στη διαδικασία σχεδίασης: interface design pattern, design patter and dynamics, design principles and heuristics, models. Έτσι, οι Zichermann και Cunnigham (2011) [2] συμφώνησαν ότι το παιχνίδι και οι σχεδιαστές της εμπειρίας του χρήστη χρησιμοποιούν αυτές τις τεχνικές εδώ και δεκαετίες για να δημιουργήσουν εθιστικά παιχνίδια και να βελτιώσουν την εμπειρία του παίχτη. Ο Globally, ο Deterding και άλλοι συγγραφείς [2] περιγράφουν τις απαραίτητες δράσεις σχεδιασμού παιχνιδιών για διασκέδαση σε επίπεδα: πρότυπα σχεδιασμού διεπαφών παιχνιδιού(game interface design patterns),πρότυπα σχεδιασμού παιχνιδιού και μηχανισμών (game design patterns and

mechanics),αρχές σχεδιασμού παιχνιδιού και ευρετικών (game design principles and heuristics), μοντέλων παιχνιδιού(game model) και μεθόδους σχεδιασμού παιχνιδιού (game design methods).

Η παιγνιοποίηση έχει απασχολήσει άτομα από διαφορετικούς κλάδους συμπεριλαμβανομένων και των σχεδιαστών παιχνιδιών, UX/UI σχεδιαστών, ψυχολόγους, κοινωνιολόγους, μηχανικούς υπολογιστών και άλλων. Το ενδιαφέρον είναι επικεντρωμένο στη διαδικασία σχεδιασμού, υπενθυμίζοντας το ρόλο που έχει ο κάθε επαγγελματίας σε αυτή τη διαδικασία.

Ο Di Tomasso (2011) [2] περιγράφει μια δομή για μια πετυχημένη σχεδίαση βασισμένη στη θεωρία του Self-Determination των Ryan και Deci (2000) [2], γνωστή και ως SDT. Από τη γνώση των διαφορών των παικτών και των κοινωνικών επιρροών, προτείνει τα ακόλουθα βήματα:

- Ανακάλυψη αιτιών για παιγνιοποίηση (ενδιαφερόμενα μέρη και επιχειρηματικοί στόχοι)
- Αναγνώριση του προφίλ των παιχτών και των κινητήριων οδηγών
- Ορισμός στόχων
- Περιγραφή δεξιοτήτων
- Παρακολούθηση και μέτρηση
- Ορισμός θεμάτων ενδιαφέροντος
- Επιθυμητά αποτελέσματα (με βάση την ανάδραση και την καθιέρωση της κατάστασης ‘’κέρδισες’’)
- Δοκιμές παιχνιδιού
- Τελειοποίηση

Ωστόσο, η πιο γνωστή δομή σχεδίασης παρουσιάστηκε από τους Werbach και Hunter (2012) [2] που περιλαμβάνει έξι βήματα (Six Steps to Gamification, 6D). Αυτό το πλαίσιο ξεκινά από έναν ορισμό των επιχειρηματικών στόχων και έπειτα, προχωρά στη στόχευση των αναμενόμενων συμπεριφορών, περιγράφει τους παίκτες, επινοεί τους βρόχους δραστηριότητας χωρίς να ξεχνά τη διασκέδαση και τελικά αναπτύσσει το σύστημα παιγνιοποίησης με τα κατάλληλα εργαλεία. Η θεωρία αυτή επηρεάζεται επίσης, από την έρευνα της σχεδίασης παιχνιδιών των Hunicke και άλλων [2], MDA. Αυτό φαίνεται και στην πυραμίδα των στοιχείων της παιγνιοποίησης (Pyramid of Gamification Elements), η οποία προτείνει τα εξής στοιχεία: Μηχανική (mechanics), Δυναμική (dynamics) και Σύνθεση (components). Η πυραμίδα αυτή είναι η βάση πολλών άλλων θεωριών για τη σχεδίαση της παιγνιοποίησης.

Ταυτόχρονα, το 2012 ο Marczewski [2] προτείνει μια θεωρία που την ονόμασε GAME και βασίζεται σε δύο φάσεις. Αρχικά, στην οργάνωση και σχεδίαση, οι οποίες περιλαμβάνουν τη συγκέντρωση των βασικών πληροφοριών, όπως πχ τους τύπους χρηστών της παιγνιοποίησης. Έπειτα, η καλύτερη λύση για την επίτευξη των στόχων είναι η μέτρηση της δραστηριότητας των χρηστών και των αποτελεσμάτων. Προτείνει , επίσης, μια άλλη θεωρία που την ονομάζει RAMP (Relatedness, Autonomy, Mastery, Purpose). Ο σχεδιασμός πρέπει να εμπλουτίζεται συνέχεια.

Οι Marache-Francisco και Brangier το 2013 [2], παρουσίασαν μια διαδικασία σχεδιασμού παιγνιοποίησης, η οποία είναι βασισμένη στις αρχές της διεπαφής Ανθρώπου-Υπολογιστή (Human-Computer Interaction HCI). Αναγνωρίζουν κάποιες διαστάσεις πέρα από τις αρχές της παιγνιοποίησης, οι οποίες μπορούν να χρησιμοποιηθούν για να οριστεί μια θεωρία/δομή. Περιγράφουν τρείς διαστάσεις: τη διάσταση sensory-motor, τη διάσταση της κινητήριας συγκίνησης και δέσμευσης και τη γνωστική διάσταση της αλληλεπίδρασης. Με βάση αυτές τις διαστάσεις η διαδικασία σχεδίασης αποτελείται από δύο μεγάλα επαναλαμβανόμενα βήματα: την ανάλυση του περιεχομένου (User-Centered Design) και την επαναλαμβανόμενη αντίληψη της εμπειρίας της παιγνιοποίησης. Παράλληλα, αναφέρεται μια εργαλειοθήκη για την βοήθεια των σχεδιαστών στη διαδικασία της παιγνιοποίησης που ονομάζεται «Core Principles»..

Ο De Paz (2013) [2] προτείνει μια σειρά από βήματα ή γενικές οδηγίες για την παιγνιοποίηση, τα οποία μπορούν να χρησιμοποιηθούν σε οποιοδήποτε έργο. Η θεωρία αυτή φαίνεται να έχει επηρεαστεί από τα 6 βήματα των Werbach και Hunter [2]. Οι οδηγίες της πρότασής του είναι χωρισμένες σε τρείς φάσεις: στην οργάνωση των επιχειρηματικών στόχων (προετοιμασία), στον καθορισμό του βασικού σχεδιασμού και στην χρήση των στοιχείων του παιχνιδιού (game elements). Η εφαρμογή και η συντήρησή τους συνιστάται στο να χτίσει κάποιος το σύστημα και να το τρέξει. Η προσέγγιση αυτή, επίσης, προτείνει τη χρήση μετρήσεων.

Οι Robinson και Bellotti (2013) [2], ισχυρίζονται ότι τα διαφορετικά κείμενα στη βιβλιογραφία , μπορούν να βοηθήσουν στο σχεδιασμό παιγνιωδών εφαρμογών αλλά δε συμπίπτουν με τις απόψεις τους. Όπως εξηγούν και οι ίδιοι, δεν παρέχουν μια συνοπτική αλλά μια περιεκτική παρουσίαση των κοινών στοιχείων παιγνιοποίησης από την άποψη των διαφόρων πτυχών της εμπειρίας των χρηστών που υποστηρίζουν. Παρουσιάζουν επίσης, έξι κατηγορίες στοιχείων της παιγνιοποίησης βασισμένες σε ποικιλία πηγών από τη βιβλιογραφία. Αυτές οι κατηγορίες είναι γενικά πλαίσια (frames), γενικοί κανόνες και

πλαίσια επιδόσεων, κοινωνικά χαρακτηριστικά, κίνητρα, πόροι και περιορισμοί και τέλος πληροφορίες ανάδρασης και κατάστασης.

Σε αυτό το σημείο, η προσέγγιση των Francisco-Aparicio et al. (2013) [2] επιτρέπει από τη μια πλευρά τον καθορισμό του είδους των δραστηριοτήτων μηχανικής παιχνιδιών που θα πρέπει να ενσωματωθούν για να ανταποκριθούν στις ψυχολογικές και κοινωνικές ανάγκες των ανθρώπινων κινήτρων (SDT). Από την άλλη πλευρά, έχει στόχο την αξιολόγηση της αποτελεσματικότητας της διαδικασίας της παιγνιοποίησης, με βάση το κριτήριο της διασκέδασης. Οι ιδιότητές της χαρακτηρίζουν τη δυνατότητα αναπαραγωγής και το βαθμό βελτίωσης για την επίτευξη ικανοποιητικών αποτελεσμάτων, χρησιμοποιώντας έναν ποιοτικό τρόπο λειτουργίας. Σε αυτό το κείμενο τα παιχνίδια είναι χωρισμένα σε τρία μέρη: στον πυρήνα του παιχνιδιού (game core), τη μηχανή (engine) και τη διεπαφή (interface). Οι απαραίτητες δραστηριότητες που προτείνονται είναι: ανάλυση του τελικού χρήστη (end-user analysis), προσδιορισμός των βασικών στόχων και των επικαλυπτόμενων (main objectives and cross-cutting identification), εφαρμογή (implementation) και ανάλυση της αποτελεσματικότητας (analysis of the effectiveness).

Με βάση την ηθική προοπτική του θέματος, ο Versteeg (2013) [2] δημιουργεί ένα απλούστερο κείμενο για την ηθική πειστικότητα της σχεδίασης της παιγνιοποίησης. Συνδυάζει ένα κανονιστικό ορθολογικό πλαίσιο (ηθικός σχεδιασμός) με τα πιο συναφή θέματα των ακόλουθων μεθοδολογιών. Είναι βασισμένο στο κείμενο των Bardichevsky και Erik Neuenschwander (1999) [2] για τον ηθικό σχεδιασμό και τους ηθικούς χρυσούς κανόνες που πρέπει να ακολουθεί ο σχεδιαστής. Επιπλέον, συνδυάζει τη μεθοδολογία της ανάλυσης της ηθικής των τεχνολογιών όπως πρότεινε ο Fogg (2002) [2]. Τα βήματα λοιπόν είναι: ορισμός των ηθικών αρχών και αξιών, εννοιολογική έρευνα με τη συμμετοχή των ενδιαφερόντων και αξιολόγηση και επανάληψη.

Επιπρόσθετα, μια ολοκληρωμένη μεθοδολογία που αφορά στην παιγνιοποίηση ονομάζεται Octalysis (2013) [2] προτείνεται από τον Yu-kai Chou. Με βάση αυτή την προσέγγιση, η παιγνιοποίηση είναι ο σχεδιασμός που δίνει περισσότερη έμφαση στα ανθρώπινα κίνητρα στη διαδικασία. Στην ουσία, προσθέτει έναν ανθρωποκεντρικό σχεδιασμό βασισμένος σε ένα οκτάγωνο σχήμα με οχτώ ‘’πυρήνες οδήγησης’’ (core drivers). Κάθε «πυρήνας» αφορά σε μια πλευρά του οκτάγωνου σχήματος. Συγκεκριμένα:

- Επική έννοια και κάλεσμα (epic meaning and calling)
- Ανάπτυξη και επίτευγμα (development and accomplishment)
- Δημιουργικότητα και ανατροφοδότηση (creativity and feedback)
- Ιδιοκτησία και κατοχή (ownership and possession)

- Κοινωνική επιρροή και συσχέτιση (social influence and relatedness)
- Σπανιότητα και ανυπομονησία (scarcity and impatience)
- Έλλειψη προγνωσιμότητας και περιέργειας (unpredictability and curiosity)
- Απώλεια και αποφυγή (loss and avoidance)

Τέλος, οι Mora A., Riera D. Gonzalez C. και Arnedo-Moreno J. [2], προσθέτουν μια τελευταία έρευνα των Al Marshedi et al. (2015) [2] με τίτλο «A framework for sustainable gamification impact». Η προσέγγισή τους θέλει να αυξήσει τη βιωσιμότητα των επιθυμητών επιπτώσεων των παιγνιωδών εφαρμογών. Είναι βασισμένη κυρίως σε τρείς θεωρίες: στη θεωρία διάστασης ροής (Flow Dimension Theory) του Csikszentmihaly (1990) [2], στα καθοδηγούμενα στοιχεία κινήτρου (drive motivation elements) του Pink (2011) [2] και στην θεωρία του Αυτοκαθορισμού (Self-determination theory). Επίσης, επικεντρώνεται στο σχεδιασμό με κέντρο τον χρήστη (User-Centered Design, UCD). Όπως υποστηρίζουν και οι συγγραφείς, είναι ένας τρόπος για να ενσωματωθεί ο σκοπός, η μαεστρία, η συσχέτιση και η ροή με την αρμοδιότητα και το χρόνο. Το κείμενό τους πρέπει να χρησιμοποιείται ως οδηγός για τους σχεδιαστές που θέλουν να δημιουργήσουν σχετικές εμπειρίες με τις οποίες οι άνθρωποι θα έχουν μακροχρόνια διάδρασή.

Οι Seaborn και Fels το 2014 [1] έγραψαν ένα άρθρο με τίτλο «Gamification in theory and action: A survey», στο οποίο, επίσης, συγκέντρωσαν βιβλιογραφία που σχετίζεται με την παιγνιοποίηση.

Ο Zichermann (2010) [1] χωρίζει το κίνητρο (motivation), από την πλευρά της ψυχολογίας, σε ενδογενή (intrinsic) και εξωγενή (extrinsic). Εξηγεί ότι στο ενδογενή κίνητρο η συμπεριφορά είναι θεσπισμένη ή μια δραστηριότητα αναλαμβάνεται, επειδή ταιριάζει με τις εσωτερικές αξίες του ατόμου, ενώ στο εξωγενή κίνητρο προσφέρονται κάποιες εξωγενείς ανταμοιβές, όπως χρήματα, για να δεσμευτεί το άτομο σε συγκεκριμένες δραστηριότητες και έχοντας την ανάλογη συμπεριφορά. Σύμφωνα, λοιπόν, με τον Zichermann, το ενδογενές κίνητρο είναι αναξιόπιστο και μεταβλητό και επομένως, η τροφοδοσία των βασικών εγγενών αξιών μπορεί να μην είναι εφικτή και χρήσιμη. Μια στρατηγική που προτείνει είναι να δημιουργούνται εξωγενή κίνητρα με τέτοιο τρόπο ώστε να δίνουν την αίσθηση ότι είναι ενδογενή. Επίσης, τονίζει ότι τα χρήματα ως ένα παραδοσιακό εξωγενές κίνητρο, μπορούν να μειώσουν το κίνητρο ενώ όμως ταυτόχρονα βελτιώνουν την απόδοση. Γι' αυτό προτείνει ότι οι σχεδιαστές πρέπει να λαμβάνουν υπόψη και τα δύο είδη κινήτρων και να χρησιμοποιούν νομισματικά και μη-νομισματικά κίνητρα [1]. Τα γενικά ενδογενή κίνητρα μπορεί να είναι πιο αποτελεσματικά από τα ειδικευμένα ενδογενή κίνητρα, δίνοντας στο χρήστη να καταλάβει τι έχει κίνητρο. Παρόλο που κάποιοι

(Deci et al., 1999; Ryan, 2012) [1] υποστηρίζουν ότι τα περιορισμένα ενδογενή κίνητρα παράγουν καλύτερη ικανοποίηση, πρέπει να γίνουν κι άλλες έρευνες πάνω στο θέμα των ενδογενή και εξωγενή κινήτρων.

Ο Cunningham μαζί με τον Zichermann (2011) [1] δημιούργησαν μια λίστα με τα στοιχεία του παιχνιδιού και τους μηχανισμούς βασισμένοι σε παραδείγματα. Η εκτίμηση του σχεδίου περιλαμβάνει τον καθορισμό του είδους παίχτη που θα υποστηρίζει το σύστημα, το πώς θα επιτευχθεί η γνώση, τις μεθόδους ‘’επιβίβασης’’ νέων χρηστών στο σύστημα και τον ρόλο του κοινωνικού βρόχου δέσμευσης. Οι απαραίτητοι μηχανισμοί παιχνιδιού είναι:

- Ανατροφοδότηση και ενίσχυση (feedback and reinforcement)
- Αναγνώριση μοτίβων (pattern recognition)
- Συλλογή (collecting)
- Οργάνωση (organizing)
- Έκπληξη και απρόσμενη απόλαυση (surprise and unexpected delight)
- Δώρα (gifting)
- Στοιχεία ρομαντισμού (flirtation and romance)
- Αναγνώριση επιτευγμάτων (recognition for achievement)
- Ηγεσία άλλων (leading others)
- Φήμη και απόκτηση προσοχής (fame and getting attention)
- Ηρωισμός (being a hero)
- Απόκτηση κοινωνικού στάτους (gaining status)
- Καλλιέργεια και ανάπτυξη (nurturing and growing)

Οι συγγραφείς προτείνουν πολλά παραδείγματα με βάση αυτούς τους μηχανισμούς. Παράλληλα, όμως, πολλοί σχεδιαστές παιχνιδιών όπως ο Bogost (2011) και ο Robertson (2010) [1] έκριναν τους συγγραφείς υποστηρίζοντας ότι αυτοί οι μηχανισμοί είναι απαραίτητοι και αμφισβήτησαν το κατά πόσο αυτά τα στοιχεία παρέχουν ή συμβάλλουν μια εμπειρία παιχνιδιού.

Οι Huotari και Hamari (2012) [1,4], τόνισαν ότι η εστίαση πρέπει να λαμβάνεται υπόψη στην εμπειρία του χρήστη, ασχέτως το αποτέλεσμα του τελικού προϊόντος. Επιπλέον, δίνεται έμφαση στην ιδέα ότι οι εμπειρίες μπορούν να σχεδιαστούν χωρίς να είναι σίγουρο το αποτέλεσμα για τον κάθε χρήστη. Επίσης, υποστηρίζουν ότι κάποια στοιχεία των παιχνιδιών, όπως ο εθελοντισμός έχουν χαθεί από την παιγνιοποίηση και παραδέχονται ότι δεν είναι απαραίτητο να ισχύουν όλα τα κριτήρια που προτείνουν για να θεωρείται ένα παιχνίδι ότι είναι παιχνίδι

Οι Werbach και Hunter (2012) [1] ορίζουν τα στοιχεία του παιχνιδιού ως τμήματα που αποτελούν το παιχνίδι, Δυναμική, Μηχανική και Σύνθεση, όπως δηλαδή και των Deterding et al. (2011) [1,3]. Παρόλα αυτά πιστεύουν ότι τα παιγνιοποιημένα συστήματα δεν είναι απαραίτητα παιχνίδια. Σχεδιάζουν για να εκμεταλλευτούν την ανθρώπινη ψυχολογία με τον ίδιο τρόπο που το κάνουν τα παιχνίδια. Επιβεβαιώνουν ότι η παιγνιοποίηση μπορεί να γίνει πιο αποτελεσματική και να επιβραβεύει διαφορετικά από τις παραδοσιακές δομές κινήτρου στις επιχειρήσεις, όπως την νομισματική επιβράβευση, επειδή το ίδιο το στοιχείο του παιχνιδιού επιβραβεύει. Συμφωνούν πάντως στο ότι η παιγνιοποίηση είναι ένας τρόπος να κάνεις υπάρχοντα ψυχαγωγικά παιχνίδια, τα οποία έχουν ελλιπή σχεδιασμό, να είναι πιο διαδραστικά και ουσιώδη, με αποδεδειγμένα θετικά στοιχεία.

Βασισμένοι στη Self-determination theory, οι Aparicio et al. (2012) [1], έκαναν μια έρευνα, η οποία ήταν χωρισμένη σε τέσσερα μέρη. Το πρώτο μέρος σχετίζεται με την αναγνώριση του κυρίως θέματος, την υπογράμμιση δηλαδή των λόγων για τους οποίους χρησιμοποιείται η παιγνιοποίηση. Στο δεύτερο μέρος παρουσιάζεται η αναγνώριση του εγκάρσιου στόχου, δηλαδή τα κίνητρα που θέλει να παρέχει το σύστημα. Το τρίτο μέρος προσδιορίζει ποιους μηχανισμούς θα χρησιμοποιήσει το παιχνίδι, με βάση το πόσο σχετίζονται με την θεωρία του «Αυτό-καθορισμού» και το τέταρτο μέρος ασχολείται με την αξιολόγηση της έρευνας σε εφαρμοσμένα συστήματα.

Οι Blohm και Leimeister (2013) [1] συγκέντρωσαν έναν αριθμό πηγών σε σχέση με την ανάπτυξη μιας στρατηγικής βασισμένης σε υπηρεσίες παιγνιοποίησης. Αυτές οι δέσμες υπηρεσιών παιγνιοποίησης αποτελούνται από μια βασική προσφορά βασισμένη στην επιθυμητή χρήση στόχων και στα επίπεδα παιγνιοποίησης που είναι φτιαγμένα με βάση συγκεκριμένα στοιχεία παιχνιδιών που θα αναφερθούν στη συνέχεια. Η έρευνά τους αυτή έχει ως στόχο να διαφωτίσει το πώς η παιγνιοποίηση μπορεί να λειτουργήσει με τη χρήση ενδογενών και εξωγενών κινήτρων, έτσι ώστε να φέρει αλλαγή στη συμπεριφορά και να επαναπροσδιορίσει δραστηριότητες όπως η μάθηση.

Ο Nicholson (2012) [1,5] έκανε μια έρευνα με επίκεντρο τον χρήστη στην παιγνιοποίηση, με την παιγνιοποίηση να βασίζεται στα ενδογενή κίνητρα και όχι στα εξωγενή. Υπογραμμίζει ένα σύνολο θεωριών που μπορούν να παρέχουν μια ενδογενή στρατηγική παιγνιοποίησης. Η Organismic integration theory (OIT), η οποία είναι υπο-θεωρία του Self-determination theory, προτείνει τη χρήση κινήτρων με βάση τις ενδογενής και εξωγενής μεθόδους ελέγχου, ξεκινώντας από την έλλειψη πρόθεσης (χωρίς ενδιαφέρον ή κίνητρο), προχωρώντας στα εξωγενή κίνητρα σε διαφορετικό επίπεδο από τον εξωτερικό και

εσωτερικό έλεγχο και τελειώνοντας με ολοκληρωτικά ελεγχόμενο ή αυτόνομο ενδογενές κίνητρο (Ryan et al., 1997) [1]. Πιο συγκεκριμένα, αυτή η θεωρία προτείνει ότι τα ουσιώδεις στοιχεία του παιχνιδιού είναι ενδογενή κίνητρα άσχετα με το αν περιέχουν εξωτερική επιβράβευση. Ο Nicholson καταλήγει στο ότι ο σχεδιασμός με επίκεντρο το χρήστη ενώνει όλες αυτές τις θεωρίες μαζί.

Με βάση, λοιπόν, όλες αυτές τις έρευνες, μπορούν να συγκεντρωθούν γενικά τα στοιχεία των παιχνιδιών που βοηθάνε στην παιγνιοποίηση. Τα κυριότερα και αυτά, τα οποία εμφανίζονται στις περισσότερες λίστες στοιχείων είναι: τα σημεία (points), ο πίνακας αποτελεσμάτων (leaderboard), τα εμβλήματα (badges), τα επίπεδα (levels), οι επιβραβεύσεις (rewards), το θέμα/ το στόρι (story/theme), οι ξεκάθαροι στόχοι (clear goals), η ανατροφοδότηση (feedback), οι δοκιμασίες (challenges), η εξέλιξη (progress) και οι ρόλοι (roles). Τα τρία πρώτα στοιχεία είναι αυτά, στα οποία συμφωνούν όλοι οι ερευνητές [6].

Σε θεωρητικό επίπεδο ισχύουν όλες αυτές οι απαιτήσεις. Στην πράξη όμως, υπάρχουν κάποια στάδια που χρειάζεται να ακολουθηθούν για να κατασκευαστεί σωστά μια εφαρμογή με τη χρήση της παιγνιοποίησης. Σε αυτό συνέβαλαν οι Morschheuser B., Werder K., Hamari J. και Abe J. (2017) [7] με κείμενο που δημοσίευσαν και συγκέντρωσαν τα στάδια σχεδιασμού για την παιγνιοποίηση. Μέσα από έρευνα που έκαναν με βάση τη βιβλιογραφία αλλά και συνεντεύξεων σε ειδικούς και σχεδιαστές παιχνιδιών, κατέληξαν σε εφτά βασικές φάσεις που πρέπει να υλοποιηθούν κατά τη διαδικασία σχεδιασμού. Οι φάσεις είναι οι εξής:

- Προετοιμασία πρότζεκτ (project preparation)
- Ανάλυση (analysis)
- Ιδεασμός (ideation)
- Σχεδίαση (design)
- Εφαρμογή (implementation)
- Αξιολόγηση (evaluation)
- Παρακολούθηση/ Εποπτεία (Monitoring)

Στη φάση της προετοιμασίας, ελέγχονται όλες οι δραστηριότητες που πρέπει να εκτελεστούν πριν την έναρξη του πρότζεκτ. Στη δεύτερη φάση, γίνεται ανάλυση των δραστηριοτήτων που χρησιμοποιούνται για να προσδιοριστούν οι απαραίτητες γνώσεις των χρηστών. Έπειτα, στον ιδεασμό συγκεντρώνονται οι δραστηριότητες που σχετίζονται με τον σχεδιασμό για την παιγνιοποίηση και στην τέταρτη φάση γίνεται ο σχεδιασμός όπου σχεδιάζονται οι προσεγγίσεις με παιγνιοποίηση και δημιουργούνται τα πρωτότυπα. Στην

πέμπτη φάση, εφαρμόζονται οι προσεγγίσεις, έτσι ώστε στην επόμενη φάση να δοκιμαστούν και να αξιολογηθούν. Τέλος στην έβδομη φάση, γίνεται παρακολούθηση των προσεγγίσεων μετά την έκδοση τους.

Στη συνέχεια, παρουσιάζουν μία λίστα με τις απαιτήσεις των πρότζεκτ της παιγνιοποίησης. Συγκέντρωσαν τις απαραίτητες απαιτήσεις με βάση την ανάλυση της βιβλιογραφίας τους, θεωρώντας πως αυτές μπορούν να οδηγήσουν σε έναν πετυχημένο σχεδιασμό παιγνιοποίησης. Οι απαιτήσεις, λοιπόν, είναι οι εξής:

- Κατανόηση των αναγκών του χρήστη, των κινήτρων και της συμπεριφοράς του, όσο και των χαρακτηριστικών του ευρύτερου πλαισίου,
- Αναγνώριση των στόχων του πρότζεκτ και σαφείς προσδιορισμός τους,
- Δοκιμές των ιδεών του σχεδιασμού με παιγνιοποίηση όσο νωρίτερα γίνεται,
- Ακολουθία μιας επαναληπτικής διαδικασίας σχεδίασης,
- Βαθιά γνώση στο σχεδιασμό παιχνιδιού και την ανθρώπινη ψυχολογία,
- Αξιολόγηση για το κατά πόσο η παιγνιοποίηση είναι η σωστή επιλογή στην επίτευξη των στόχων,
- Οι ενδιαφερόμενοι και οι οργανισμοί πρέπει να κατανοήσουν και να υποστηρίξουν την παιγνιοποίηση,
- Εστίαση στις ανάγκες του χρήστη κατά την φάση του ιδεασμού,
- Προσδιορισμός και χρήση μετρήσεων για την εκτίμηση και την παρακολούθηση της επιτυχίας μιας παιγνιώδης προσέγγισης,
- Έλεγχος για εξαπάτηση (cheating) στο σύστημα,
- Διαχείριση και παρακολούθηση για τη συνεχή βελτιστοποίηση του σχεδιασμού της παιγνιοποίησης,
- Εξέταση νομικών και ηθικών περιορισμών στη φάση της σχεδίασης,
- Συμμετοχή χρηστών στη φάση του ιδεασμού και του σχεδιασμού.

Προτείνουν, επίσης, και κάποια εργαλεία που μπορούν να βοηθήσουν στη σχεδίαση, τα οποία σχετίζονται με τα βιντεοπαιχνίδια, τις κάρτες σχεδιασμού, την απεικόνιση, τα μοτίβα στο σχεδιασμό παιχνιδιών, τους κύβους ιστορίας, τους καμβάδες, τα δέντρα αποφάσεων και τα καλύτερα μοτίβα παιγνιοποίησης.

Με βάση όλες αυτές τις αρχές και ακολουθώντας τα στάδια, οι ερευνητές πιστεύουν πως μπορεί κάποιος να δημιουργήσει μια πετυχημένη εφαρμογή με την παιγνιοποίηση στο κέντρο της.

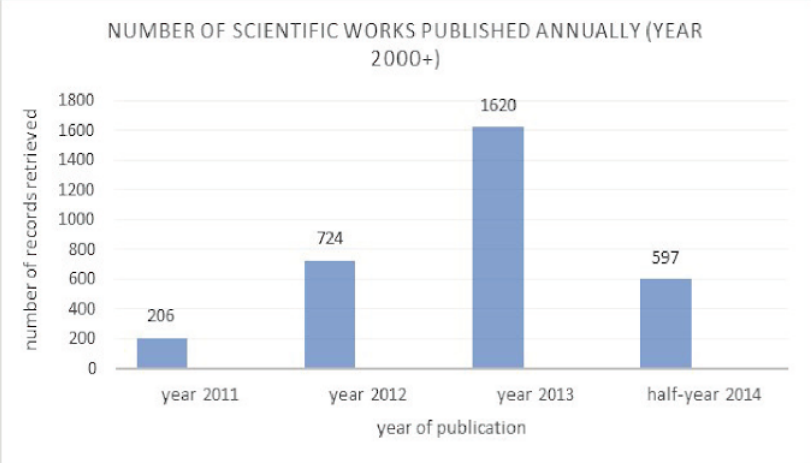
2.3 Η παιγνιοποίηση σε διάφορους τομείς

Στο τρίτο και τελευταίο μέρος αυτού του κεφαλαίου θα αναλυθούν οι τομείς στους οποίους έχει εφαρμοστεί η μέθοδος «παιγνιοποίηση», αναφέροντας μερικά παραδείγματα εφαρμογών για τον κάθε τομέα.

2.3.1 Εκπαίδευση (Education)

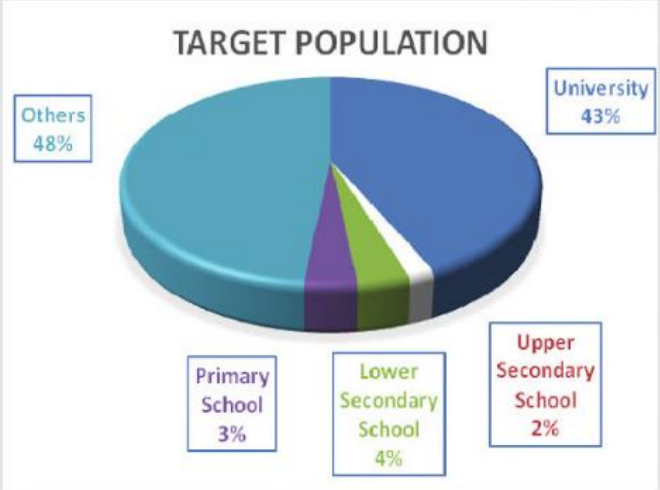
Η παιγνιοποίηση στον τομέα της εκπαίδευσης έχει αναπτυχθεί αρκετά. Οι παιγνιώδεις εκπαιδευτικές εφαρμογές αναφέρονται κυρίως στη χρήση στοιχείων παιχνιδιού για την ανάπτυξη συστημάτων που έχουν εκπαιδευτικό χαρακτήρα. Υπάρχει αρκετή βιβλιογραφία πάνω στην παιγνιοποίηση για την εκπαίδευση, με τα περισσότερα κείμενα να αναφέρονται και στην εκτέλεση κάποιας εφαρμογής. Για τον Kapp (2012) [1,8], η παιγνιοποίηση στην εκπαίδευση χρησιμοποιείται στην ψηφιακή εκπαίδευση βασισμένη σε παιχνίδια, δηλαδή στο digital game-based learning (DGBL). Ο ίδιος προσδιορίζει την παιγνιοποίηση ως τη χρήση μηχανισμών βασισμένων σε παιχνίδια, την αισθητική και τον τρόπο σκέψης, με στόχο να ενθαρρύνει τους ανθρώπους, ώστε να χρησιμοποιήσουν τις εφαρμογές, και να υποστηρίξει τη μάθηση.

Η χρήση της παιγνιοποίησης στην εκπαίδευση σαν ερευνητικό θέμα αυξάνεται αρκετά τα τελευταία χρόνια, με επικρατέστερη χρονιά έρευνας το 2013. Οι Caponetto, Earp και Ott σε κείμενο που δημοσίευσαν το 2014 [8] σημείωσαν τον αριθμό των κειμένων που δημοσιεύθηκαν τις χρονιές 2011-2014. Στον παρακάτω πίνακα δίνεται αναλυτικά ο αριθμός κειμένων με βάση τη χρονολογία δημοσίευσης.



Εικόνα 3 «Ο αριθμός των επιστημονικών άρθρων που έχουν δημοσιευτεί από το 2011 έως το 2014 σε σχέση με την παιγνιοποίηση στην εκπαίδευση.», Caponetto I., Earp J. & Ott M. (2014), Gamification and Education: A Literature Review, Germany: Research and Training Center for Culture and Computer Science (FKI), University of Applied Sciences HTW Berlin, Proceedings of the 8th European Conference on Games Based Learning ECGBL 2014

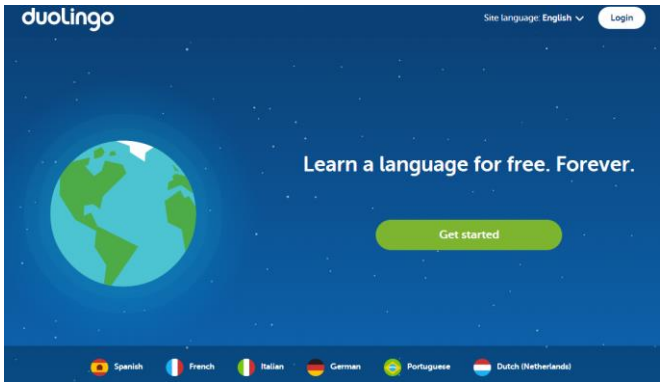
Στην ίδια έρευνα, βρέθηκε το ποσοστό των κειμένων που σχετίζεται με την παιγνιοποίηση στην εκπαίδευση ανάλογα με το μαθησιακό επίπεδο. Στον παρακάτω πίνακα δίνονται τα ποσοστά των ερευνών και παρατηρείται ότι τα περισσότερα άρθρα έχουν ως στόχο τη χρήση της παιγνιοποίησης σε πανεπιστημιακό επίπεδο, ενώ ένα ποσοστό του 48% των κειμένων αυτών στοχεύουν σε κάποιο άλλο επίπεδο μόρφωσης.



Εικόνα.4 «Ποσοστά ερευνητικών κειμένων που έχουν γραφτεί ανάλογα με την ομάδα που στοχεύουν.», Caponetto I., Earp J. & Ott M. (2014), Gamification and Education: A Literature Review, Germany: Research and Training Center for Culture and Computer Science (FKI), University of Applied Sciences HTW Berlin, Proceedings of the 8th European Conference on Games Based Learning ECGBL 2014

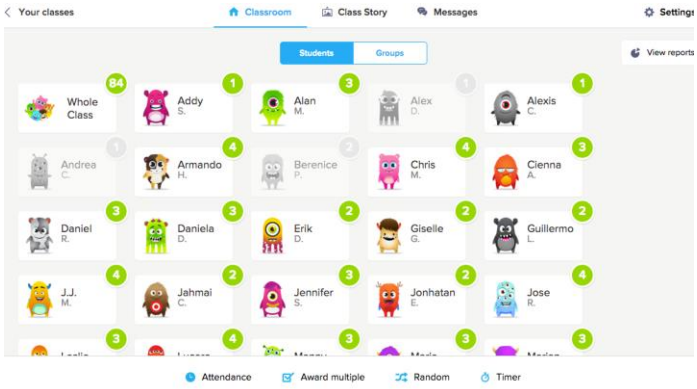
Ο Yu-kai Chou [9] προτείνει κάποιες εφαρμογές της παιγνιοποίησης στην εκπαίδευση. Μέσω του παιχνιδιού, αυξάνεται το ενδιαφέρον των μαθητών, η επικοινωνία με τον καθηγητή αλλά και μεταξύ των μαθητών, και με αυτό το τρόπο αντιμετωπίζουν με θετικό τρόπο την μάθηση. Ένα παράδειγμα παιγνιοποίησης που προτείνει είναι η ιστοσελίδα «Duolingo», μία εφαρμογή εκμάθησης ξένων γλωσσών, όπως φαίνεται και στην Εικόνα 5. Οι χρήστες μπορούν όχι μόνο να μάθουν ξένες γλώσσες αλλά και να βοηθήσουν στη μετάφραση κειμένων και άλλων ιστοσελίδων, συμβάλλοντας στη βελτίωση των γνώσεων τους. Μέσω της εφαρμογής, ο μαθητής κερδίζει βαθμούς ικανοτήτων και με την ολοκλήρωση ενός μαθήματος ανεβαίνει επίπεδο ή αντίστοιχα πέφτει επίπεδο σε

περίπτωση λάθους. Η εφαρμογή αυτή συνδυάζει αρκετά στοιχεία παιχνιδιού και είναι πολύ φιλική στο χρήστη, παρέχοντας διασκέδαση και ταυτόχρονα γνώσεις.



Εικόνα 5 «*Duolingo*», Διαθέσιμο σε: http://68.media.tumblr.com/267ea4ef7de0a91a4286e8760c5a2869/tumblr_nadqwhMAOw1rmr3dfo1_1280.png

Μία άλλη εφαρμογή που συστήνει ο Yu-kai Chou [9] είναι το ClassDojo. Το ClassDojo είναι ένα εργαλείο διαχείρισης της τάξης, το οποίο βοηθά τον καθηγητή να ελέγχει τη συμπεριφορά των μαθητών μέσα στην αίθουσα. Ο κάθε μαθητής έχει ένα δικό του avatar και ανάλογα με τη συμπεριφορά του μαθητή, βραβεύεται ή όχι από τον καθηγητή. Αυτή η επιβράβευση ωθεί τους μαθητές στο να έχουν μια καλύτερη συμπεριφορά μέσα στην αίθουσα, καθώς τους δίνεται ένα κίνητρο. Η εφαρμογή επίσης μπορεί να τυπώσει μια ανάλυση των βαθμολογιών του κάθε μαθητή, έτσι ώστε και οι γονείς να μπορούν να γνωρίζουν τις επιδώσεις του παιδιού τους. Στην Εικόνα 6 διακρίνεται μία από τις οθόνες της εφαρμογής.

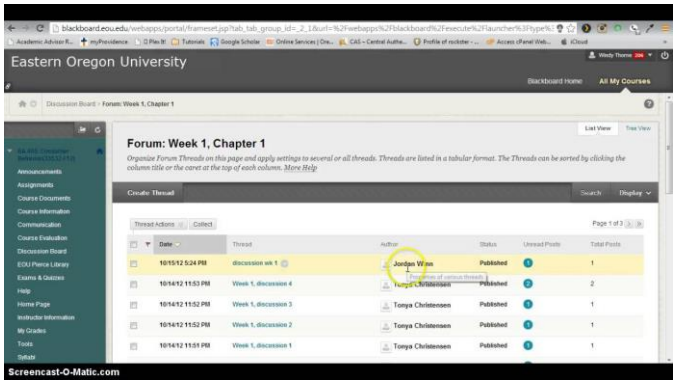


Εικόνα 6 «*ClassDojo*», Διαθέσιμο σε: http://ilearn.sbunified.org/wp-content/uploads/2015/11/class-dojo-screenshot.png

Ο Denny (2013) [1] έκανε μια έρευνα αναφορικά με το πώς τα εμβλήματα (badges) μπορούν να χρησιμοποίηθούν για να δόσουν κίνητρο στους χρήστες. Έφτιαξε ένα διαδικτυακό ερωτηματολόγιο πολλαπλών απαντήσεων και τα αποτελέσματα της έρευνάς

του έδειξαν ότι τα εμβλήματα έδωσαν κίνητρο στον αριθμό των απαντήσεων που υποβλήθηκαν και στη διάρκεια της δέσμευσης, χωρίς να υπάρχουν επιπτώσεις στην ποιότητα της ανταπόκρισης. Παρόλα αυτά, τα εμβλήματα δεν επηρέασαν τον αριθμό των ερωτήσεων που σχετίζονται με την ποιότητα του μαθησιακού περιβάλλοντος. Επιπλέον, οι μαθητές που υπέβαλαν απαντήσεις χωρίς τη χρήση εμβλημάτων, έδωσαν τέσσερις φορές περισσότερες απαντήσεις, δηλώνοντας ότι η δραστηριότητα έδινε αρκετά κίνητρα από μόνη της παρά τα χαρακτηριστικά της παιγνιοποίησης που χρησιμοποιήθηκαν. Ο πίνακας των αποτελεσμάτων της έρευνας του Denny έδειξε ότι οι μαθητές που συμπλήρωσαν το ερωτηματολόγιο είχαν διαφορετικά κίνητρα μεταξύ τους για διαφορετικούς λόγους.

Οι Dominguez et al. (2013) [1] ανέπτυξαν μια προέκταση με παιγνιοποίηση της πλατφόρμας e-learning Blackboard, η οποία φαίνεται και στην Εικόνα 7. Η πλατφόρμα Blackboard βοηθάει τόσο τους μαθητές, όσο και τους καθηγητές στο να βελτιώσουν τις μαθησιακές τους δεξιότητες μέσω διάφορων προγραμμάτων που περιέχει. Οι ομάδες και οι μαθητές που συνδέονται με αυτές επιλέχθηκαν τυχαία για τον έλεγχο και τις πειραματικές ομάδες. Η πειραματική ομάδα εκπαιδεύτηκε να χρησιμοποιεί την προέκταση και κάποια προεραιτικά χαρακτηριστικά της παιγνιοποίησης, τα οποία περιλαμβάνουν τριανταέξι δοκιμασίες – προκλήσεις, με στόχο να αποκτύσουν τρόπαια (trophies) και εφτά συμμετοχικές προκλήσεις, ώστε να κερδίσουνεμβλήματα (badges) ή μετάλια (metals). Επίσης, υπήρχε κι ένας πίνακας που σύγκρινε τις επιδώσεις των παικτών.Το 44% των ατόμων που συμμετείχαν στην πειραματική ομάδα χρησιμοποίεισαι την παιγνιοποίηση ως επιπλέον χαρακτηριστικό στην πλατφόρμα. Τα αποτελέσματα γενικά και στις συμμετοχικές προκλήσεις ήταν πολύ καλύτερα σε αυτή την ομάδα αλλά υπήρξε έλλειψη στην απόδοση στις γραπτές εργασίες και στη συμμετοχή. Παράλληλα, τα αποτελέσματα έδειξαν ότι κάποιοι μαθητές δεν ευχαριστήθηκαν το ανταγωνιστικό κομμάτι της διαδικασίας και ειδικά στο κομμάτι της συμπλήρωσης του πίνακα σύγκρισης του εαυτού τους με τους άλλους.



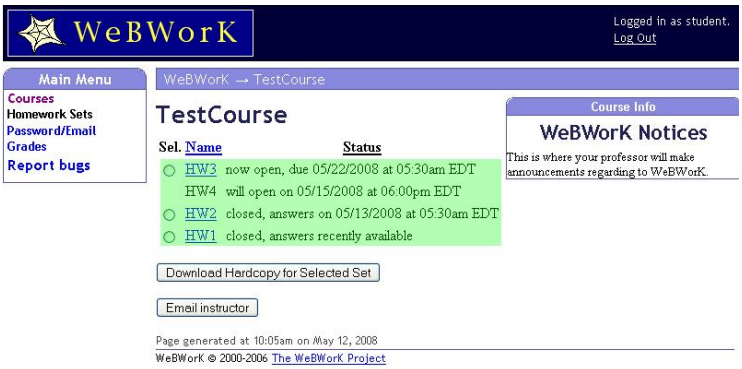
Εικόνα 7 «*Blackboard e-learning*», Διαθέσιμο σε: https://i.ytimg.com/vi/341wvuyv4hU/maxresdefault.jpg

Η παιγνιοποίηση έχει χρησιμοποιηθεί, επίσης, για να υποστηρίξει μια άτυπη, μη δομημένη δραστηριότητα σε ένα ηλεκτρομηχανικό μάθημα (Foster et al., 2012) [1]. Τα επιτεύγματα αναπτύχθηκαν με διαφορετικούς στόχους, περιλαμβάνοντας όμως την ασφάλεια, την προετοιμασία, την επιλογή συσκευών και τη χρήση σε συγκεκριμένα θέματα μηχανικής σχεδίασης. Οι μαθητές είχαν κάποια επιτεύγματα σε σχέση με τη δραστηριότητα. Στην διάρκειά της, το εκπαιδευτικό προσωπικό ενθάρρυνε τους μαθητές να ολοκληρώσουν τα επιτεύγματά τους. Μία σύγκριση της παιγνιώδους εκδοχή της δραστηριότητας σε δύο προηγούμενες, μη-παιγνιώδεις εκδοχές έδειξε ότι τα επιτεύγματα ασφάλειας είχαν επιτυχημένα μια βελτίωση της συμπεριφοράς των χρηστών και έδωσαν μια μαθησιακή δομή, η οποία περιλαμβάνει συνθήματα και οδηγίες για τους μαθητές, για να επιδιώξουν τους μαθησιακούς στόχους τους. Παρόλα αυτά πολλοί μαθητές χρειάστηκαν και εξωτερικά κίνητρα με τη μορφή προκλήσεων, που δόθηκαν από το εκπαιδευτικό προσωπικό, για να αρχίσουν να εμπλέκονται με την δραστηριότητα και να συνεχίσουν το στόχο τους.

Ο Gasland (2011) [1] δημιούργησε ένα σύστημα e-learning, το οποίο συνδυάζει ερωτήσεις και απαντήσεις. Το “StudyAid” χρησιμοποιήθηκε από μαθητές για να διευκολυνθούν στην εύρεση του βοηθητικού υλικού των μαθημάτων τους και για να τους βοηθήσει να διαβάσουν για τις τελικές εξετάσεις τους. Μία έρευνα έδειξε ότι το “StudyAid” θεωρούταν γενικά χρήσιμο και εύκολο στη χρήση. Παρόλα αυτά, τα στοιχεία της παιγνιοποίησης δεν είχαν μεγάλη επίδραση, λόγω της φύσης της εργασίας που είναι το διάβασμα, της δομής του συστήματος που θύμιζε περισσότερο δουλεία από ότι διασκέδαση και του γεγονός ότι σαν καινούργιο σύστημα είχε στέρηση περιεχομένου. Σε ερώτηση που έγινε πάντως στους μαθητές, το 80% απάντησε ότι δε θεωρούσε την πλατφόρμα αυτή ως παιχνίδι.

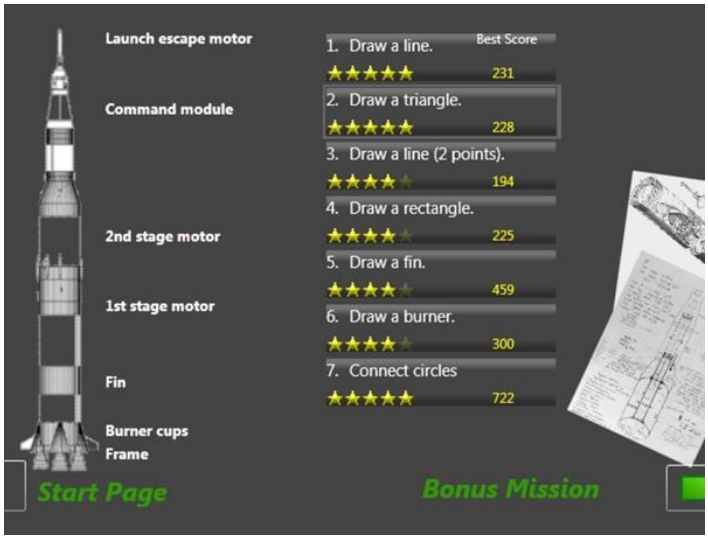
Το “WeBWorK” (Εικόνα 8) είναι μια πλατφόρμα για την ολοκλήρωση εργασιών που σχετίζονται με τα μαθήματα των μαθηματικών και της φυσικής. Ο Goehle (2013) [1] αύξησε την εφαρμογή “WeBWorK” προσθέτοντας αρκετά στοιχεία παιγνιοποίησης: έβαλε σημεία (points) εμπειρίας με βάση την εξέλιξη των εργασιών που είχε ο μαθητής για το σπίτι, επίπεδα, τα οποία περνάει ο μαθητής, όταν φτάσει συγκεκριμένα ορόσημα μέσω συσσωρευμένων πόντων εμπειρίας και μια μπάρα προόδου, επιτευγμάτων και επιβραβεύσεων με τη μορφή πρόσθετων βαθμών. Οι μετρήσεις των επιτευγμάτων έδειξαν ότι τουλάχιστον οι μισοί από τους μαθητές που ολοκλήρωσαν το 90% των ασκήσεων τους, έβαλαν παραπάνω προσπάθεια για να αποκτήσουν κι άλλα επιτεύγματα. Μια άλλη έρευνα που έγινε σε 29 μαθητές έδειξε ότι το 93% των μαθητών έλεγχαν την πρόοδο τους και το

89% προσπάθησε να αποκτήσει επιτεύγματα. Οι μαθητές τόνισαν ότι το σύστημα τους έκανε να αισθάνονται ότι αναγνωρίζεται η προσπάθεια τους [1]



Εικόνα 8 «*WeBWork*», Διαθέσιμο σε: http://webwork.maa.org/w/images/4/44/Mainpage.jpg

Οι Li et al. (2012) [1] ανέπτυξαν το "GamiCAD" (Εικόνα 9), ένα παιγνιώδες σύστημα εκμάθησης (tutorial), το οποίο βοηθάει νέους χρήστες να μάθουν να χρησιμοποιούν το AutoCAD μέσω αποστολών, βαθμολογιών, επιπέδων παιχνιδιών, πίεσης χρόνου, μίνι-παιχνιδιών και επιβραβεύσεων με τη μορφή των έξτρα επιπέδων. Τα αποτελέσματα δείχνουν ότι υπάρχει αύξηση της συμμετοχής, της διασκέδασης και της απόδοσης κυρίως στους αρχάριους χρήστες. Συγκεκριμένα, υπήρξε μια αύξηση από 20 έως 76% της ταχύτητας ολοκλήρωσης που ήταν σημαντική σε τέσσερις ασκήσεις.

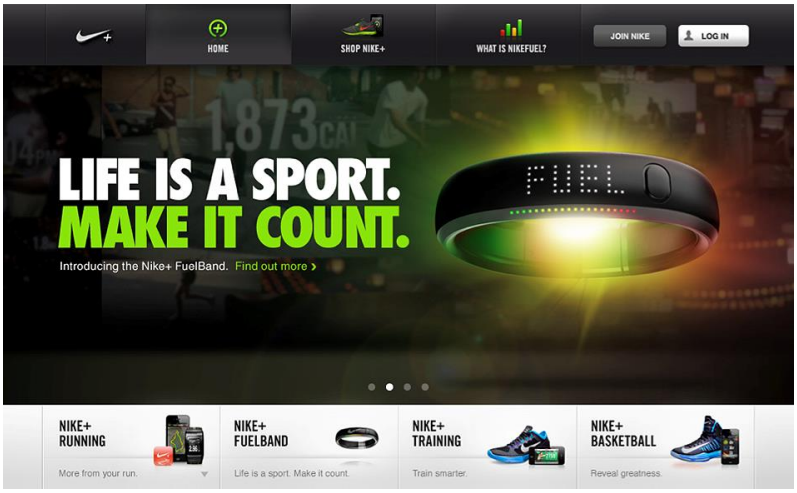


Εικόνα 9 «*GamiCAD*», Διαθέσιμο σε: https://www.autodeskresearch.com/publications/gamicad

2.3.2 Μάρκετινγκ

Στον τομέα του μάρκετινγκ η παιγνιοποίηση είναι αρκετά χρήσιμη, καθώς διευκολύνει τον τρόπο διαφήμισης των προϊόντων. Η ραγδαία εξέλιξη της τεχνολογίας έχει ωθήσει πολλές εταιρίες στην αναζήτηση νέων τρόπων διαφήμισης των προϊόντων τους. Για το συγκεκριμένο τομέα δεν υπάρχει αρκετή βιβλιογραφία, παρόλο που έχουν δημιουργηθεί πολλές εφαρμογές, οι οποίες αποδεικνύουν και τη χρησιμότητα της παιγνιοποίησης [4].Τα παραδείγματα στο μάρκετινγκ είναι άπειρα και τα περισσότερα είναι πασίγνωστα και δημοφιλή.

Το 2012 η εταιρεία Nike [10,11] θέλοντας να δημιουργήσει προϊόντα πέρα από τα συνηθισμένα της, παρουσίασε την εφαρμογή ‘’Nike+ Fuelband’’. Η εφαρμογή συνδέεται με ένα βραχιόλι, το οποίο περιέχει μια ειδική τεχνολογία που καταγράφει την κίνηση του χρήστη. Ο στόχος της εφαρμογής είναι να κινητοποιήσει το χρήστη, ώστε να αθληθεί[11]. Με το βραχιόλι αυτό ο χρήστης μπορεί να δει τις επιδόσεις του, καθώς κρατάει αρχείο τα δεδομένα του, δείχνοντας μάλιστα και στατιστικά στοιχεία για τον καθένα ξεχωριστά. Κάθε φορά που ο χρήστης πετυχαίνει το στόχο του, ένα κινούμενο σχέδιο εμφανίζεται στην οθόνη και πανηγυρίζει μαζί του. Οι σχεδιαστές της εφαρμογής πρόσθεσαν, επίσης, τη δυνατότητα επικοινωνίας με άλλους χρήστες. Με αυτόν τον τρόπο, ο χρήστης μπορεί να προκαλέσει ένα φίλο του σε μια δοκιμασία. Ταυτόχρονα μπορεί να δει τις επιδόσεις του και να βρει ποιος έχει συγκεντρώσει τους περισσότερους βαθμούς. Το Nike+Fuelband από την αρχή χρησιμοποιήθηκε από εκατομμύρια κόσμο, κάτι που έκανε την εταιρεία ακόμα πιο γνωστή και βοήθησε πολύ στη διαφήμισή της [10,11].



Εικόνα 10 «*Nike+ Fuelband*», Διαθέσιμο σε: http://payload106.cargocollective.com/1/8/265669/4437294/1_nike_fuelband_launch_1500.png

Μια, επίσης, μεγάλη και γνωστή εταιρεία που χρησιμοποίησε την παιγνιοποίηση για να πετύχει τους διαφημιστικούς της στόχους είναι η Starbucks. Η φιλοσοφία της εταιρείας ήταν πάντα επικεντρωμένη στην παροχή προσωπικών υπηρεσιών στους πελάτες της [10,11]. Δίνοντας βάση στην ατμόσφαιρα που έχει ο χώρος, το κάθε κατάστημα έχει διαφορετική διακόσμηση, θέλοντας να παροτρύνουν τους πελάτες να καθίσουν περισσότερο και να απολαύσουν τον καφέ τους. Η εφαρμογή "My Starbucks Reward" [10,11] (Εικόνα 11) δημιουργήθηκε για να βοηθήσει σε αυτό το στόχο και να αυξήσει τις πωλήσεις της εταιρείας. Ο χρήστης κάνει εγγραφή στο My Reward και κάθε φορά που αγοράζει ένα προϊόν της εταιρείας επιβραβεύεται με ένα αστέρι. Υπάρχουν τρία επίπεδα, τα οποία εξαρτώνται από τη συχνότητα επίσκεψης του χρήστη σε κατάστημα της εταιρίας Starbucks. Όσο πιο συχνά επισκέπτεται το χώρο, τόσο πιο εύκολα ανεβαίνει επίπεδο. Ταυτόχρονα, υπάρχουν και άλλα θετικά της χρήσης της εφαρμογής, όπως ένα ποτήρι καφέ δώρο, μια δωροεπιταγή ή ακόμα και ιδικές προσφορές σε προϊόντα για ξεχωριστούς πελάτες.

Εικόνα 11 «*My Starbucks Reward*», Διαθέσιμο σε: http://www.starbucksmelody.com/wp-content/uploads/2010/04/MyStarbucksRewards-Overview.jpg

Ένα ακόμα πετυχημένο παράδειγμα παιγνιοποίησης στο μάρκετινγκ είναι η περίπτωση της Samsung [11]. Η εταιρεία το 2013 θέλοντας να διαφημίσει το νέο της κινητό Samsung Galaxy S4, χρησιμοποίησε την τεχνική του pranksvertising, όπως φαίνεται και στην Εικόνα 12, μια μέθοδο που αναπτύσσεται πολύ σε μεγάλες εταιρείες. Μέσω αυτής της διαδικασίας, παρουσίασε το κινητό στο κοινό δίνοντάς του κίνητρο για να το αγοράσει. Τοποθέτησαν δηλαδή ένα σύστημα στο οποίο έπρεπε ο χρήστης να κοιτάξει για εξήντα δευτερόλεπτα την οθόνη του κινητού. Όποιος το κατάφερνε, έπαιρνε δώρο το κινητό. Η παγίδα όμως ήταν στο ότι σε αυτά τα εξήντα δευτερόλεπτα, γύρω από τον χρήστη στο οπτικό του πεδίο συνέβαιναν διάφορες δραστηριότητες με στόχο να του αποσπάσουν την προσοχή. Αν το βλέμμα του χρήστη έφευγε έστω και για κλάσματα του δευτερολέπτου από την οθόνη, τότε έχανε την ευκαιρία του και συνεπώς,το κινητό. Η Samsung κατάφερε με αυτό τον τρόπο να κερδίσει πολύ κόσμο, καθώς παρόλο που ελάχιστοι από όσους το

δοκίμασαν κατάφεραν να κρατήσουν το βλέμμα τους στην οθόνη, το θέαμα τους εντυπωσίασε όλους. [11].

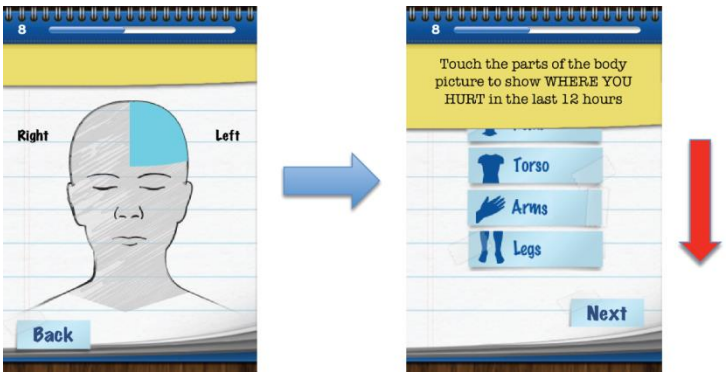
Εικόνα 12 «*Samsung Galaxy s4, pranksvertising*», Διαθέσιμο σε: https://www.feeldesain.com/feel/wp-content/uploads/2013/05/Samsung-S4-Challenges-adv-viral-video.jpg

2.3.3 Τομείς Υγείας (Health)

Η παιγνιοποίηση στο κομμάτι της υγείας είναι σχετικά ένα καινούργιο θέμα. Συγκεκριμένα, υπάρχουν ακόμα πολλά ζητήματα από πλευράς νομοθεσίας και κόστους. Γι' αυτό και οι περισσότερες εφαρμογές ανήκουν στην κατηγορία της ''ευεξίας'' (wellness). Πρόσφατα βέβαια υπήρξε ένα κύμα εφαρμογών που στοχεύουν στην αντιμετώπιση της αποκατάστασης, στις γνωστικές διαταραχές, ακόμη και στην ιατρική έρευνα και ανάλυση [12]. Η παιγνιοποίηση σίγουρα θα αναπτυχθεί περισσότερο στο μέλλον, καθώς θα γίνει αναπόσπαστο κομμάτι σε πολλούς τομείς, αλλά κυρίως και της υγείας. Έχει παρατηρηθεί μάλιστα ότι η χρήση εφαρμογών με στοιχεία παιγνιοποίησης δημιουργούν περισσότερα κίνητρα τόσο στους απλούς χρήστες, όσο και στους υπαλλήλους των νοσοκομείων. Σύμφωνα με έρευνα του Yu-kai Chu [13] και με βάση το Partnership for Prevention, πάνω από 100.000 άνθρωποι μπορούν να σώσουν τη ζωή τους στις ΗΠΑ κάθε χρόνο. Η πρόληψη βοηθάει στο να εντοπιστεί κάποιο θέμα υγείας.

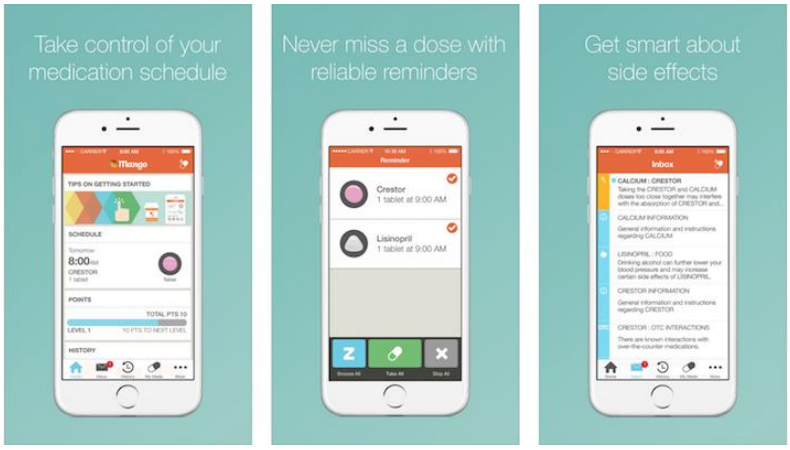
Υπάρχουν πολλές εφαρμογές που αφορούν στην προσωπική φροντίδα μέχρι και στην επαγγελματική ανάπτυξη. Οι Stinson et al. (2013) [14] στην προσπάθειά τους να προωθήσουν σε ασθενείς με καρκίνο την διαδικασία συγγραφής ενός ημερολογίου ''πόνου'', δημιούργησαν μία εφαρμογή που λέγεται ''Pain Squad'' (Εικόνα 13). Μέσω της εφαρμογής, ο χρήστης μπορεί να σημειώνει τα επίπεδα πόνου που νιώθει μέσα στην ημέρα του και ανάλογα με την περίπτωση του υπάρχουν και διαφορετικές μετρήσεις. Με την

καταμέτρηση του πόνου τους ανεβαίνουν επίπεδα και αποκτούν εμβλήματα (badges) και βραβεία (rewards), όπως για παράδειγμα αν συμπληρώσουν κάποιες συγκεκριμένες αναφορές θα επιβραβευτούν με το βίντεο ενός ηθοποιού από κάποια σειρά. Οι ερευνητές αρχικά σχεδίασαν ένα ερωτηματολόγιο που είχε ως επίκεντρο τον πόνο από καρκίνο, με βάση ένα ημερολόγιο αρθρίτιδας για νέους. Υπήρξαν δύο πρωτότυπα, ένα με χαμηλή πιστότητα και ένα με υψηλή, τα οποία αναπτύχθηκαν και δοκιμάστηκαν σε μια έρευνα χρηστικότητας. Οι ερευνητές στη συνέχεια μέτρησαν τα αποτελέσματα της έρευνας και έδωσαν το τελικό πρωτότυπο για αξιολόγηση σε ένα τεστ κλινικής σκοπιμότητας. Ο μέσος όρος συμμόρφωσης ήταν στο 88% . Οι χρήστες χρησιμοποίησαν την εφαρμογή μέρα-νύχτα, όλη την εβδομάδα και το σαββατοκύριακο και μετά από δύο εβδομάδες χρήσης της εφαρμογής, δεν υπήρχαν διαφορές ανάμεσα στα φύλλα ή στην αρχική θέση θεραπείας. Τα αποτελέσματα ήταν ικανοποιητικά, η εφαρμογή χρησιμοποιείται με ευκολία και η χρήση της δεν διέκοπτε την καθημερινή ζωή των χρηστών.



Εικόνα 13 «*Pain Squad*», Διαθέσιμο σε: http://lab.research.sickkids.ca/iouch/wp-content/uploads/sites/33/2016/07/60933-Tip03.png

Ο Yu-kai Chu [13] προτείνει κάποιες εφαρμογές πάνω στον τομέα της υγείας. Μια εφαρμογή για κινητά είναι η “Mango Health” στην οποία ο χρήστης μπορεί να καταγράφει τα φάρμακα που παίρνει, τις δοσολογίες και να βάλει υπενθύμιση για το πότε πρέπει να πάρει το φάρμακο του, όπως φαίνεται και στην Εικόνα 14. Ο χρήστης κερδίζει πόντους κάθε φορά που θυμάται να πάρει το φάρμακο του και όσο περισσότερο τηρεί το πρόγραμμά του κερδίζει και μεγαλύτερα δώρα, όπως για παράδειγμα μια δωροεπιταγή στο Target ή στην GAP. Επίσης, ένας άλλος τρόπος επιβράβευσης είναι η δωρεά κάποιου χρηματικού ποσού σε ένα ίδρυμα, όπως για παράδειγμα το ASPA.

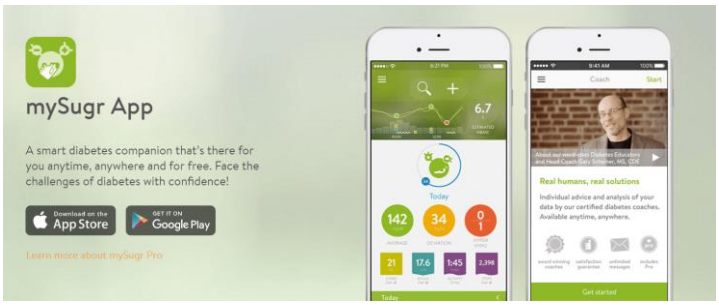


Εικόνα 14 «*Mango Health*», Διαθέσιμο σε: http://www.mobihealthnews.com/sites/default/files/Mango%20Health_0.png

Μια άλλη εφαρμογή που προτείνει ο Yu-kai Chu [13] είναι η "Respond Well" (Εικόνα 15), η οποία βοηθάει άτομα που κάνουν φυσιοθεραπείες να εκτελέσουν τις καθημερινές τους ασκήσεις. Χρησιμοποιεί τις τεχνολογίες εντοπισμού κίνησης, μέσω της χρήσης του Kinect της Microsoft και περιέχει μια ποικιλία από δραστηριότητες για να κρατάει τους χρήστες σε εγρήγορση και να ενημερώνει τους γιατρούς για τις επιδόσεις των ασθενών. Οι χρήστες έχουν τη δυνατότητα να επιλέξουν ανάμεσα σε διάφορα εικονικά περιβάλλοντα, τα οποία είτε περιέχουν έναν εικονικό εκπαιδευτή, είτε έχουν μουσική και τρισδιάστατα τοπία και γραφικά. Κερδίζουν πόντους, όταν εκτελούν σωστά τις ασκήσεις και μπορούν να βάλουν ακόμα και δοκιμασίες στον εαυτό τους. Επίσης, μπορούν να προσκαλέσουν και φίλους τους να συμμετέχουν. Η χρήση του Kinect βοηθάει όχι μόνο στον εντοπισμό της κίνησης του χρήστη, αλλά κάνει καταμέτρηση των επαναλήψεων και αποθηκεύει τα δεδομένα στο cloud για ανάλυση και για λόγους αναφοράς.

Εικόνα 15 «*Respond Well*», Διαθέσιμο σε: https://i.ytimg.com/vi/nMvR-UN7oKA/maxresdefault.jpg

Οι Rose et al. (2013) [14] μελέτησαν τη χρήση της εφαρμογής για κινητά “mySugr” (Εικόνα 16) στην συμμόρφωση της συμπεριφοράς ατόμων με διαβήτη. Σύμφωνα με τους συγγραφείς, παρά την σημαντικότητά του, το 73% των ασθενών δεν καταγράφουν την πρόοδο τους και το 57% δίνει λανθασμένα δεδομένα. Τα αποτελέσματα δείχνουν ότι η συχνή μέτρηση του ζαχάρου βελτιώθηκε κατά 10-20% και τα επίπεδα του ζαχάρου στο αίμα ήταν στο 0.4-1.1%. Επίσης, και η ποιότητα ζωής των χρηστών φαίνεται ότι βελτιώθηκε. Μέχρι το τέλος μιας τρίμηνης περιόδου, το 85% των χρηστών που συμμετείχαν στην έρευνα συνέχισε να χρησιμοποιεί την εφαρμογή.



Εικόνα 16 «*mySugr*», Διαθέσιμο σε: https://wrm5sysfkg-flywheel.netdna-ssl.com/wp-content/uploads/2017/06/Roche-Acquires-Mobile-Diabetes-Management-Platform-mySugr.png

Η εταιρία American Red Cross [14] σε συνεργασία με την Disney δημιούργησε μια εφαρμογή για παιδιά που ονομάζεται “Monster Guard”. Η εφαρμογή αυτή για κινητά προετοιμάζει τα παιδιά ηλικίας 7-11 ετών να αντιμετωπίσουν οποιοδήποτε θέμα υγείας χρειαστεί. Με την βοήθεια των τεράτων φίλων, όπως φαίνεται και στην Εικόνα 17, το παιδί μπορεί να μάθει να προστατεύει τον εαυτό του και να είναι έτοιμο για οτιδήποτε του συμβεί σε σχέση με την υγεία του, μέσω προκλήσεων που υπάρχουν στα επίπεδα. Οι χρήστες μπορούν επίσης να μοιραστούν τις γνώσεις και τις εμπειρίες τους με τους φίλους τους.

Εικόνα 17 «*Monster Guard*», Διαθέσιμο σε: https://is2-ssl.mzstatic.com/image/thumb/Purple1/v4/91/16/9c/91169c9f-4e2e-75ab-a8f1-aa77bfd901a6/pr_source.jpg/643x0w.jpg

2.3.4 Επιχειρήσεις (Business)

Ο χώρος των επιχειρήσεων δεν απέχει πολύ από τον χώρο του μάρκετινγκ. Στις μέρες μας υπάρχει μεγάλος ανταγωνισμός στις επιχειρήσεις μεταξύ τους, γι' αυτό και παρατηρείται η ανάγκη για την εύρεση νέων μεθόδων που να ανταπεξέρχονται στις καταστάσεις της εποχής και να επιφέρουν κέρδη στην ίδια την επιχείρηση.

Ένα παράδειγμα της χρήσης της παιγνιοποίησης σε μια επιχείρηση είναι η εφαρμογή "Samsung Nation" [15] (Εικόνα 18). Η Samsung θέλοντας να έρθει πιο κοντά στους καταναλωτές της, έφτιαξε μια εφαρμογή που περιέχει περιεχόμενο που δημιουργεί ο χρήστης, επιβραβεύοντας τους χρήστες για να συνδεθούν με την κοινότητα, συμμετέχοντας σε συζητήσεις και κουίζ ερωτήσεων, βλέποντας βίντεο και κάνοντας άλλες δραστηριότητες. Σε αντάλλαγμα για τη συμμετοχή τους οι χρήστες ανταμείβονται με εμβλήματα και προχωρούν μέσω επιπέδων. Η Samsung είχε ήδη εκατοντάδες χιλιάδες επισκέπτες, οπότε δεν χρειάστηκε να καταβάλει μεγάλη προσπάθεια για να οδηγήσει τους επισκέπτες στην περιοχή. Αντ 'αυτού, επικεντρώθηκε στην εξήγηση των πλεονεκτημάτων της εμπλοκής με την κοινότητα για να ενθαρρύνει τους χρήστες να αναθεωρήσουν τα προϊόντα και να δημιουργήσουν πολύτιμο εμπορικό περιεχόμενο για την εταιρεία.

Εικόνα 18 «*Samsung Nation*», Διαθέσιμο σε: https://www.veryconnect.com/uploads/images/5b707b4eb52d4a85f6d34259a571bf85.png

Η Bluewolf [15] χρησιμοποίησε την παιγνιοποίηση ως έναν τρόπο για να εμπλακούν οι εργαζόμενοι περισσότερο και να συμμετάσχουν ενεργά στην οικοδόμηση της μάρκας Bluewolf. Χρησιμοποιώντας την τεχνολογία του Bunchball, η Bluewolf δημιούργησε το δικό της #GoingSocial πρόγραμμα, χρησιμοποιώντας ποικίλες πρωτοβουλίες, συμπεριλαμβανομένων των ''προφίλ πακέτων'' των εργαζομένων, προσφέροντας σημεία και ανταμοιβές για εσωτερική και εξωτερική συνεργασία, δημοσιεύοντας στο blog της εταιρείας, κερδίζοντας σκορ Klout 50 ή παραπάνω, και άλλα επιτεύγματα. Το αποτέλεσμα

είναι μια ισχυρότερη κοινωνική παρουσία για μια κοινωνική μάρκα που εμπλέκει πιθανούς πελάτες και οδηγεί στην επένδυση των εργαζομένων.

Η Nissan, μέσω της εφαρμογής ‘’Nissan Carwings’’ [15] (Εικόνα 19), η οποία δημιουργήθηκε από την Nissan Innovation για το Nissan Leaf, το 100% ηλεκτρικό αυτοκίνητο της Nissan, παίζει ρόλο οδήγησης και τραβάει τους πελάτες σαν μαγνήτες. Με ένα περιφερειακό ταμπλό ταξινόμησης, οι ιδιοκτήτες μπορούν να συγκρίνουν τις επιδόσεις τους με άλλους τοπικούς οδηγούς, να κερδίσουν χάλκινα, ασημένια και χρυσά μετάλλια ή για τις πιο εντυπωσιακές βαθμολογίες, ένα φανταχτερό βραβείο πλατίνας. Μια δωρεάν υπηρεσία τριών ετών για τους νέους ιδιοκτήτες , το Carwings κάνει πολύ περισσότερα από ό, τι να κατατάσσει τα στατιστικά της οδήγησης σε έναν πίνακα. Μπορείτε να επικοινωνήσετε με το αυτοκίνητό σας μέσω του smartphone σας και να λάβετε υπενθυμίσεις, να αρχίσετε να φορτίζετε την μπαταρία, να ρυθμίζετε χρονοδιακόπτες, να ενεργοποιείτε τον κλιματισμό και άλλα, ακόμα και αν δεν βρίσκεστε κοντά στο αυτοκίνητό σας τη δεδομένη στιγμή.

Εικόνα 19 «*Nissan Carwings*», Διαθέσιμο σε: https://www.japanbullet.com/images/pozeauto/leafgsma.jpg

Το ‘’U.S Army’’ [15] είναι μια εφαρμογή του Αμερικανικού στρατού. Ο αμερικανικός στρατός δεν είναι ξένος στη χρήση παιχνιδιών για εκπαιδευτικούς σκοπούς, αλλά τώρα χρησιμοποιεί την παιγνιοποίηση για να προσελκύσει νέους ανθρώπους και γενικά να προωθήσει την επίγνωση των αμερικανικών ενόπλων δυνάμεων. Ο στρατός της Αμερικής έχει προσελκύσει εκατομμύρια πιθανών νέων στρατολόγων. Η προσπάθεια αυτή ξεκίνησε το 1999 και η πρώτη έκδοση κυκλοφόρησε το 2002. Μέχρι το 2008, τέσσερις μεταφερόμενες μονάδες "Virtual Army Experience" χτύπησαν εμπορικά κέντρα και δημόσιες εκδηλώσεις. Πάνω από μια δεκαετία, ο Στρατός των ΗΠΑ έχει μετατρέψει τις γνώσεις και την εμπειρία του στα παιχνίδια εκπαίδευσης σε ένα ισχυρό εργαλείο στρατολόγησης.

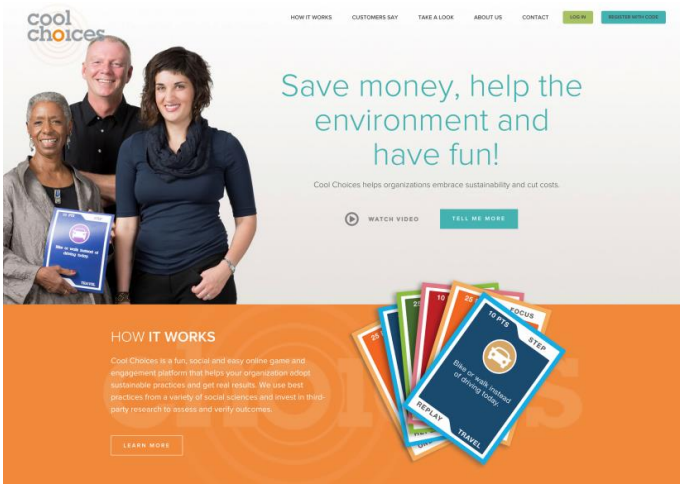
Το Πανεπιστήμιο Kaplan εφάρμοσε λύσεις Badgeville [15] για να ενισχύσει το πρόγραμμα σπουδών του με την ενθάρρυνση μεγαλύτερης συμμετοχής. Με την ενσωμάτωση προκλήσεων και κονδυλωμάτων, ο Kaplan είδε αποτελέσματα, όπως υψηλότεροι βαθμοί σπουδαστών, μειωμένα ποσοστά μαθητών που δεν ολοκλήρωσαν μαθήματα και προγράμματα και διενήργησε ανάλυση συμπεριφοράς για να διαφοροποιήσει αυτό που διακρίνει τους πιο επιτυχημένους φοιτητές από τους υπόλοιπους, προκειμένου να αντλήσουν διαδικασίες τυχερών παιχνιδιών που θα προωθούσαν τις ίδιες πρακτικές σε όλο τον φοιτητικό πληθυσμό, σύμφωνα με το Information Week [15].

2.3.5 Περιβάλλον (Environment)

Η ανάγκη για αλλαγή συμπεριφοράς απέναντι στο περιβάλλον, έχει αναγνωριστεί τόσο από τους επιστήμονες του κλίματος όσο και από αναλυτές συμπεριφοράς. Ένας τρόπος για να επιτευχθεί αυτό είναι μέσω της παιγνιοποίησης.

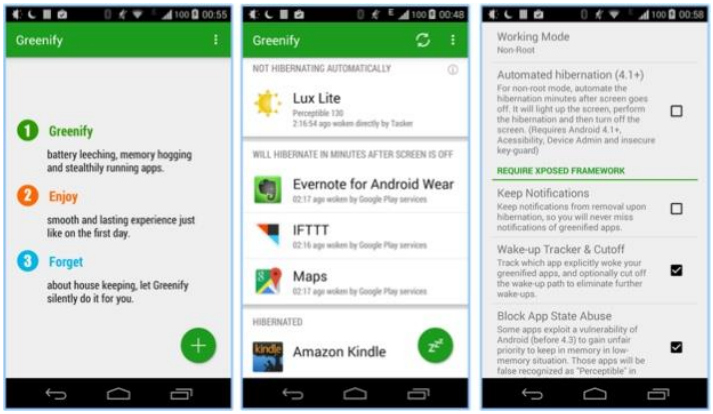
Ένα από τα πιο γνωστά παραδείγματα είναι η εφαρμογή ‘’PowerHouse’’ του πανεπιστημίου του Stanford [16], η οποία είναι ένα διαδικτυακό παιχνίδι σχεδιασμένο για να μειώσει τη χρήση της ενέργειας που χρησιμοποιείται στα σπίτι των χρηστών. Συνδέεται με τις υπηρεσίες παροχής υπηρεσιών των χρηστών και εντοπίζει τις πηγές ενέργειας στο σπίτι. Το πρόγραμμα περιλαμβάνει κάποια μίνι-παιχνίδια που μπορεί να παίξει ο χρήστης, τα οποία είναι βασισμένα σε σενάρια του πραγματικού κόσμου και ο χρήστης παίζει ψηφιακά για να καταφέρει να ανταπεξέλθει στις ανάγκες ενέργειας του πραγματικού του σπιτιού. Οι χρήστες επίσης μπορούν να δουν ένα διάγραμμα με την ενέργεια που καταναλώνουν καθημερινά, να δουν τα στατιστικά τους στο παιχνίδι, και να ανταγωνιστούν με άλλους χρήστες.

Η εταιρία Cool Choices [16] (Εικόνα 20) έφτιαξε μια εφαρμογή για κινητά για να δημιουργήσει μια διαρκής αλλαγή συμπεριφοράς σε σχέση με την διατήρηση της ηλεκτρονικής ενέργειας, του νερού και την απόδοση οδήγησης. Η εφαρμογή δοκιμάστηκε από τους υπαλλήλους της εταιρίας για έξι μήνες. Οι χρήστες κερδίζουν πόντους με την κοινοποίηση φωτογραφιών και ιστοριών σχετικά με τις ενέργειες τους και έναν αριθμό πόντων τον κερδίζουν με βάση τις οικονομίες που κάνουν με την δραστηριότητα και το βαθμό δυσκολίας της εργασίας. Με τη χρήση της εφαρμογής παρατηρήθηκε η μείωση της κατανάλωσης ενέργειας, νερού, πετρελαίου και φυσικού αερίου.



Εικόνα 20 «*Cool Choices*», Διαθέσιμο σε: https://coolchoices.com/wp-content/uploads/2015/07/CoolChoicesHomepageimage.png

Το ‘’Greenify’’ [16] (Εικόνα 21) είναι μια διαδικτυακή κοινωνική πλατφόρμα που αναπτύχθηκε στο Institute for Sustainable Communities at the Teacher’s College στο πανεπιστήμιο του Colombia και στοχεύει στην προώθηση βιώσιμων κοινοτήτων. Η πλατφόρμα σχεδιάστηκε έτσι ώστε να τονίζει τρία στοιχεία των βιώσιμων κοινοτήτων: ένα υγιεινό κλίμα και περιβάλλον, κοινωνική ευημερία και οικονομική ασφάλεια. Το ‘’Greenify’’ προκαλεί τους χρήστες να δημιουργήσουν και να επιτύχουν αποστολές σχετικά με την αλλαγή ενέργειας, φαγητού, κατανάλωσης, σπιτιού και των μέσων μετακίνησης. Οι χρήστες κερδίζουν βραβεία ανάλογα με τις επιτυχημένες ολοκληρωμένες προκλήσεις τους και μπορούν επίσης να συμμετέχουν και σε κοινωνικά δίκτυα χρησιμοποιώντας ακόμα και το Google+ αλλά και το Facebook. Οι ενέργειές τους και τα αποτελέσματα τους είναι ορατά στους υπόλοιπους χρήστες και μπορούν να πάρουν μέρος και σε ομαδικές αποστολές. Ταυτόχρονα, κερδίζουν και κάποιους έξτρα πόντους οι οποίοι μπορούν να καταναλωθούν σε τοπικές επιχειρήσεις ανάλογα με την περιοχή του χρήστη, ενώνοντας έτσι την εφαρμογή με την τοπική κοινωνία.



Εικόνα 21 «*Greenify*», Διαθέσιμο σε: https://zdnet3.cbsistatic.com/hub/i/2016/03/12/8d213ced-f096-431d-a6f4-358ad000949c/558e19e13796445c89f33fb90313c981/2016-03-1122-17-46.jpg

2.3.6 Crowdsourcing

Το Crowdsourcing είναι μια μορφή συλλογικής διαδικτυακής δραστηριότητας, στην οποία ένα άτομο ή μια οργάνωση ή μια ομάδα, δίνει σε μια άλλη ομάδα ή οργάνωση ή άτομο μια εθελοντική δραστηριότητα. Με αυτόν τον τρόπο ωφελούνται και οι δύο πλευρές, μέσω του αισθήματος της ικανοποίησης, οι μεν ότι κατάφεραν να ηγηθούν μια ομάδα και οι δε ότι κατάφεραν κάποιο στόχο.

Οι Liu et al. (2011) [1] ανέπτυξαν την κινητή εφαρμογή ‘’UbiAsk’’ για ανθρωποδυναμική μετάφραση εικόνων σε κείμενο. Η εφαρμογή χρησιμοποιεί πολλά χαρακτηριστικά της παιγνιοποίησης για να ενθαρρύνει τους χρήστες να μεταφράζουν εικόνες από ταξιδιώτες ξένων γλωσσών. Οι έρευνες έδειξαν ότι οι μισοί από τους αιτούμενους για μετάφραση, είχαν απάντηση μέσα σε λιγότερο από δέκα λεπτά, τα τρία τέταρτα από αυτούς είχαν απάντηση σε λιγότερο από μισή ώρα και κάθε αίτημα είχε περίπου 4.2 απαντήσεις κατά μέσο όρο.

Ο Yu-kai Chu [17] προτείνει την εφαρμογή ‘’Play to Cure’’, στην οποία οι παίκτες πρέπει να συλλέξουν γενετικά δεδομένα σχετικά με τον σχηματισμό καρκίνου. Μέσα στο παιχνίδι αυτή είναι μια ουσία που ονομάζεται "άλφα". Καθώς αυτό συλλέγεται, οι παίκτες έχουν την εξουσία να πυροβολούν αστεροειδείς και να φτάσουν στο επόμενο επίπεδο αναβαθμίζοντας το διαστημικό τους πλοίο για να γίνουν ακόμα πιο ισχυροί και ως εκ τούτου επιτυχημένοι στο να διαλύσουν τους αστεροειδείς . Στην Εικόνα 22 δίνεται ένα παράδειγμα ενός από τα αεροσκάφη της εφαρμογής. Η συγκέντρωση του "άλφα" κατά μήκος της γραμμικής πορείας είναι το τυποποιημένο κέλυφος του πραγματικού καθήκοντος εντοπισμού σφαλμάτων σε πραγματικά δεδομένα γονιδίων. Οι γενετικές πληροφορίες των αμέτρητων όγκων είναι ενσωματωμένες στο παιχνίδι και, όπως προχωράτε, είστε πραγματικά crowdsource που συμμετέχουν σε σημαντική έρευνα για τον καρκίνο! Εκτός από το παιχνίδι για μια μεγαλύτερη αιτία, το παιχνίδι προωθείται επίσης από την ανάπτυξη και την ολοκλήρωση, καθώς συλλέγονται περισσότερα "άλφα", οι παίκτες είναι εξουσιοδοτημένοι να χτυπήσουν περισσότερους αστεροειδείς και να ανέβουν στην κατάταξη.

Εικόνα 22 «*Play to Cure*», Διαθέσιμο σε: https://betanews.com/wp-content/uploads/2014/03/play-to-cure.jpg

Μία άλλη εφαρμογή είναι η ‘’The Great Brain Experiment’’ [17]. Το Μεγάλο Πείραμα Εγκεφάλου αναπτύχθηκε στο Κέντρο Trust για Νευροαπεικόνιση στο Λονδίνο. Οι παίκτες δυσκολεύονται να συνειδητοποιήσουν ότι συμβάλλουν στην επιστημονική έρευνα καθώς συμμετέχουν σε παιχνίδια διασκέδασης (Εικόνα 23). Αυτό που είναι κάπως μοναδικό για αυτό το παιχνίδι είναι ότι δεν αποσκοπεί να υποχρεώσει τους παίκτες προς υψηλότερα επίπεδα επιδόσεων. Εξάλλου, οι ερευνητές ενδιαφέρονται κυρίως για τον τρόπο με τον οποίο οι άνθρωποι αντιδρούν και συμπεριφέρονται υπό κανονικές συνθήκες. Αν και παίζουν για να συνεισφέρουν στην επιστημονική κατανόηση, η πραγματική εμπειρία βασίζεται σε άλλους παράγοντες. Ένα βασικό στοιχείο του παιχνιδιού είναι η σχετική βαθμολογία. Οι παίκτες λαμβάνουν βαθμολογίες ως εκατοστημόρια της μεγαλύτερης ομάδας. Για παράδειγμα, μπορεί να τους λεχθεί ότι έχουν καλύτερη ερεθιστικότητα σε σχέση με το 90% του πληθυσμού. Τα υψηλά ποσοστά επιτυχίας προκαλούν συναισθήματα ενδυνάμωσης καθώς οι παίκτες λαμβάνουν άμεση ανατροφοδότηση ότι διαθέτουν ικανότητες ή ικανότητες μεγαλύτερες από τον μέσο όρο [17].

Εικόνα 23 «*The Great Brain Experiment*», Διαθέσιμο σε: https://wellcometrust.files.wordpress.com/2013/11/coconut-shy-triplet.jpg?w=580&h=290

Κεφάλαιο 3ο: Ζητήματα ασφάλειας και ιδιωτικότητας (Security and Privacy Awareness)

Σε αυτό το κεφάλαιο παρουσιάζεται η βιβλιογραφία που υπάρχει σχετικά με τα ζητήματα επίγνωσης ασφάλειας (security awareness) και ιδιωτικότητας (privacy awareness), τονίζοντας την αναγκαιότητα εκπαίδευσης των χρηστών αναφορικά με αυτά τα ζητήματα. Επίσης, παρουσιάζονται οδηγίες σχεδιασμού πληροφοριακών συστημάτων.

3.1 Ζητήματα Ασφάλειας πληροφοριακών συστημάτων (Security Awareness)

Η επίγνωση ασφάλειας των πληροφοριακών συστημάτων είναι ένα ζήτημα αρκετά σημαντικό για την προστασία των πληροφοριών. Ο Jeager (2018) [18] προσπαθεί να αποσαφηνίσει την έννοια της επίγνωσης (awareness). Η επίγνωση σαν έννοια μπορεί να συσχετιστεί με την διανοητική κατάσταση του ατόμου, καθώς μια ερμηνεία της έννοιας μπορεί να είναι το να έχει κάποιος συνείδηση ή να γνωρίζει κάτι. Κάποιοι ορισμοί συμπεριλαμβάνουν τις διαδικαστικές πτυχές δηλαδή τις διαδικασίες που γίνονται για να επιτευχθεί η γνώση στο άτομο. Υπάρχουν, όμως, και ελάχιστοι ορισμοί, οι οποίοι δεν μπορούν να διακρίνουν την επίγνωση από ένα ορισμένο είδος συμπεριφοράς [18].

Από την οπτική της επίγνωσης ασφάλειας πληροφοριών (information security awareness) ως μια γνωστική κατάσταση του νου, οι Bulgurcu et al. διακρίνουν αρχικά την έννοια της επίγνωσης μέσω της συνολικής γνώσης. Στη συνέχεια, διακρίνουν τα ζητήματα ασφάλειας και τις πιθανές συνέπειές τους. Επίσης αναλύουν τις απαιτήσεις που προβλέπουν οι πολιτικές ασφάλειας των πληροφοριών των οργανισμών [18].

Οι Rhee et al. ορίζουν την επίγνωση ασφάλειας πληροφοριών ως «την εγρήγορση στην κατανόηση των διαφόρων απειλών της ασφάλειας πληροφοριών και στην αντίληψη του κάθε ατόμου σχετικά με αυτές τις απειλές» [18].

Από την πλευρά της συμπεριφοράς, οι Spears και Barki, ορίζουν την επίγνωση ασφάλειας πληροφοριών ως μια κατάσταση που αντανακλάται στην συμπεριφορά των ατόμων της ομάδας [18].

Οι Τσώχου, Κοκολάκης, Καρύδα και Κιουντούζης το 2008 [19] διεξήγαν μια έρευνα σχετικά με την επίγνωση ασφάλειας. Στην έρευνά τους κατέγραψαν τη βιβλιογραφία που υπάρχει σχετικά με το θέμα και πρότειναν έναν οδηγό στους ερευνητές για να τον

χρησιμοποιούν, όταν σχεδιάζουν την έρευνά τους και την πρακτική τους σχετικά με την επίγνωση ασφάλειας των πληροφοριών.

Κάποιες έρευνες που αφορούν στην ασφάλεια υποδεικνύουν την προσοχή που έχει δοθεί στην ύπαρξη επίγνωσης στην ασφάλεια της πληροφορίας (information security awareness, ISA). Οι Ernst & Young (2004) [19] αναγνωρίζουν την έλλειψη της επίγνωσης ασφάλειας από τους χρήστες ως ένα εμπόδιο στην αποτελεσματική ασφάλεια των πληροφοριών. Οι ίδιοι ασχολήθηκαν και αργότερα με το θέμα, αναγνωρίζοντας την επίγνωση ασφάλειας ως ένα από τα μέτρα που χρήζουν σημασίας για την κάλυψη του κενού που υπάρχει ανάμεσα στους αυξανόμενους κινδύνους ασφάλειας πληροφοριακών συστημάτων και στα μέτρα που είναι απαραίτητο να ληφθούν για την αντιμετώπισή τους. Επιπλέον, οι Ernst & Young (2006) [19] θεωρούν την επίγνωση ως μια διαδικασία, που θα πρέπει να θεωρείται μια από τις πιο σημαντικές προτεραιότητες παγκοσμίως για την ασφάλεια των πληροφοριών, η οποία θα έχει επιταχυνόμενη επίδραση στην ικανότητα των οργανισμών να διαχειρίζονται τους κινδύνους τους.

Επίσης, από το 2004 το θέμα της επίγνωσης ασφάλειας των πληροφοριών άρχισε να απασχολεί και το CSI (Crime Scene Investigation) και FBI (Federal Bureau of Investigation) [19], οι οποίοι ανέφεραν ότι οι οργανισμοί δεν επενδύουν αρκετά στη συγκεκριμένη περιοχή. Αναφέρουν ότι έχει αυξηθεί η αντίληψη των ατόμων σχετικά με το πόσο σημαντικό είναι να αποκτήσουν επίγνωση στην ασφάλεια, χωρίς ωστόσο να έχουν τις κατάλληλες σχετικές επενδύσεις. Το CSI (2007) αναφέρει ότι η επίγνωση ασφάλειας πληροφοριών αποτελεί ένα από τα πιο σημαντικά ζητήματα ασφάλειας των πληροφοριακών συστημάτων για τα επόμενα χρόνια. Εκτός από την αυξημένη προσοχή για την επιτακτική ανάγκη της επίγνωσης ασφάλειας των πληροφοριών στους οργανισμούς, η ανάλυση των ερευνών στην ασφάλεια των πληροφοριών, υποδηλώνει ότι οι οργανισμοί δεν έχουν εφαρμόσει σωστές και αποτελεσματικές λύσεις για την επίγνωση ασφάλειας με αποτέλεσμα την έλλειψη λύσεων σε σχετικά ζητήματα [19].

Οι περισσότεροι ορισμοί υπονοούν ότι η επίγνωση ασφάλειας πληροφοριών είναι το κατώτερο επίπεδο της πυραμίδας της μάθησης ασφάλειας, έχει δηλαδή ως στόχο να προσελκύσει τους χρήστες πληροφοριακών συστημάτων στο να καταλάβουν τη σημαντικότητα της ασφάλειας της πληροφορίας και των υποχρεώσεων τους ως προς την ασφάλεια. Η εξάσκηση έχει ως στόχο την ανάπτυξη της γνώσης και την ανάπτυξη σχετικών ικανοτήτων, ενώ η εκπαίδευση στοχεύει στη δημιουργία εξειδίκευσης πάνω σε ζητήματα ασφάλειας [19].

Οι συγγραφείς Τσώχου, Κοκολάκης, Καρύδα και Κιουντούζης στο κείμενό τους [19], παρουσίασαν έναν πίνακα με όλους τους ερευνητές που ασχολήθηκαν με τον ορισμό της επίγνωσης ασφάλειας πληροφοριών.

ISA as the primary issue		
Benjamin et al. (2007)	Hawkins et al. (2000)	Security Awareness Index Report (2002)
Casmir and Yngstrom (2005)	Kritzinger (2006)	Siponen (2000)
Chen et al. (2006)	Kruger and Kearney (2006)	Spurling (1995)
Cox et al. (2006)	Maeyer (2008)	Steyn etn al. (2007)
Danuvasin (2008)	Mathisen (2004)	Thomson (1999)
Dodge et al. (2007)	McCoy and Fowler (2004)	Thomson and von Solms (1998)
Drevin et al. (2007)	NIST (2003)	Valentine (2006)
ENISA (2006)	Okenyi and Owens (2007)	van Wyk and Steven (2006)
Everett (2006)	Peltier (2005)	Vroom and von Solms (2002)
Furnell et al. (2002)	Power M.(2007)	Yngström and Björck (1999)
Furnell et al. (2006)	Power R. and Forte (2006)	Wood (1995)
Goucher (2008)	Puhakainen (2006)	
Hansche (2001a)	Qing et al. (2007)	

Table 1: Sample analysis regarding topic of investigation (ISA as primary issue)

Πίνακας 1: «Δείγμα ανάλυσης με βάση το θέμα έρευνας», Tsohou A., Kokolakis S., Karyda M. & Kiountouzis E. (2008), Investing Information Security Awareness: Research and Practice Gaps, Greece: Information Security Journal A Global Perspective, December 2008

Ο Hansche (2001) [19] υιοθετεί ρητά τη διάκριση της επίγνωσης και της εξάσκησης και δηλώνει ότι «η επίγνωση ασφάλειας δε θεωρείται το ίδιο με την εξάσκηση». Ο ENISA (European Union Agency for Network and Information Security) είναι ένας οργανισμός που ασχολείται με την αντιμετώπιση προβλημάτων που αφορούν στην ασφάλεια των δικτύων και πληροφοριών. Το 2006, ο ENISA [19] διαφοροποιεί τις έννοιες «επίγνωση», «εξάσκηση» και «εκπαίδευση» και δίνει τη δυνατότητα στον οργανισμό που θα χρησιμοποιήσει μια από αυτές τις έννοιες, να αποφασίσει αν το πρόγραμμα θα πρέπει να επικεντρωθεί αποκλειστικά στην επίγνωση ή επίσης και στην εξάσκηση και εκπαίδευση. Η Maeyer (2007) [19] δίνει το δικό της ορισμό, λέγοντας ότι είναι μια οργανωμένη και σε εξέλιξη προσπάθεια καθοδήγησης της συμπεριφοράς και της κουλτούρας ενός οργανισμού σε θέματα ασφάλειας. Ο Kritzinger (2006) [19] αναγνωρίζει την υπάρχουσα ορολογία και καθορίζει τις τρείς έννοιες.

Παρόμοια και η Mathisen (2004) [19] διαφοροποιεί τις τρεις έννοιες, ενώ οι Chen et al. (2006) [19] συμφωνούν με τον ορισμό που δόθηκε από το NIST (National Institute of Standards and Technology) το 2003 [19] και αντιλαμβάνονται την διάκριση ανάμεσα στην εξάσκηση και την εκπαίδευση. Οι Schlienger και Teufel (2003) [19] ορίζουν και χρησιμοποιούν τις έννοιες της επίγνωσης ασφάλειας, της εξάσκησης και της εκπαίδευσης, με σαφήνεια και προτείνουν ένα πρόγραμμα ‘’σχολικής εξάσκησης’’ που περιλαμβάνει όλα αυτά τα στοιχεία και στοχεύει στην αλλαγή της κουλτούρας απέναντι σε ζητήματα ασφάλειας της πληροφορίας.

Ακριβώς την ίδια προοπτική υιοθετούν και οι Okenyi και Owens (2007) [19], οι οποίοι διαφοροποιούν τις τρείς έννοιες και υποστηρίζουν μια διαδικασία εκμάθησης, η οποία ξεκινά με την επίγνωση, συνεχίζει με την εξάσκηση και εξελίσσεται σε εκπαίδευση, δηλαδή στην εκμάθηση. Παρόλο που στην αρχή δηλώνουν ότι ο σκοπός του προγράμματος επίγνωσης ασφάλειας είναι να αυξηθεί η επίγνωση και να διευκολυνθεί η κατανόηση μέσω της εξάσκησης, στο τέλος της έρευνάς τους διαφοροποιούν ρητά όλες τις έννοιες.

Ο κάθε ένας από αυτούς τους συγγραφείς αναφέρει, επίσης, τα επιθυμητά αποτελέσματα, όπως για παράδειγμα η αλλαγή της αντίληψης των ατόμων απέναντι σε ζητήματα ασφάλειας πληροφοριών μαζί με τις μεθόδους που χρησιμοποιήθηκαν για την επίγνωση ασφάλειας. Ο οδηγός από τον ENISA (2006) [19] διαφοροποιεί την επίγνωση από την εξάσκηση και την εκπαίδευση, προσφέροντας «μια προσέγγιση διαχείρισης αλλαγών», η οποία έρχεται σε αντίθεση με το στόχο της αύξησης της προσοχής του κοινού σε ζητήματα ασφάλειας. Αυτή η αλλαγή αναγνωρίζεται ως μια πολιτιστική αλλαγή και αναφέρεται στην αλλαγή:

α) της αντίληψης του χρήστη (user's perception),

β) της οργανωτικής κουλτούρας (organizational culture),

γ) της συμπεριφοράς του χρήστη (user's behavior),

δ) της οικειότητας του κοινού με τις πολιτικές ασφάλειας (audience's familiarity with security policies and procedures) και

ε) του ενδιαφέροντος του κοινού προς την ασφάλεια (audience's interest towards security).

Προς την ίδια κατεύθυνση, οι Power R. και Forte (2006) [19] προσδιόρισαν το σκοπό των προγραμμάτων επίγνωσης ασφάλειας και εκπαίδευσης ως μια «αλλαγή εταιρικής κουλτούρας». Ωστόσο, για την επίτευξη αυτού του γενικού στόχου επίγνωσης ασφάλειας πληροφοριών χρειάζεται να γίνει αλλαγή στη δομή του οργανισμού. Επιπλέον, είναι απαραίτητη η εξειδικευμένη εκπαίδευση σε θέματα ασφάλειας, καθώς και η ενημέρωση των στελεχών για την ενίσχυση της επίγνωσης.

Από την άλλη πλευρά, ο Hansche (2001) [19], διακρίνει τους όρους της επίγνωσης και της εξάσκησης και προτείνει ένα πρόγραμμα επίγνωσης ασφάλειας, στοχεύοντας στην αλλαγή των ενεργειών του χρήστη κατά τη διάρκεια των εργασιών του, έτσι ώστε να αποκτήσει καλές συνήθειες ασφάλειας και να αλλάξει τη συμπεριφορά του. Παρόλα αυτά, δεν είναι ξεκάθαρο το πώς αυτές οι αλλαγές μπορούν να επιτευχθούν μέσω μιας διαδικασίας κατά τη διάρκεια της οποίας οι χρήστες λαμβάνουν απλώς πληροφορίες.

Οι Chen et al. (2006) [19] στοχεύουν στην αλλαγή συμπεριφοράς και ενισχύουν τις πρακτικές ασφάλειας. Για να το πετύχουν αυτό, βασίζονται σε διαδικτυακές μαθησιακές τεχνικές, οι οποίες αποτελούν ενεργητικές προσπάθειες ενημέρωσης. Το σύστημα επίγνωσης ασφάλειας πληροφοριών που δημιούργησαν παρέχει ένα αμφίδρομο κανάλι επικοινωνίας, δεδομένου ότι το υλικό επίγνωσης απευθύνεται στους χρήστες, υποστηρίζεται το εξατομικευμένο περιεχόμενο και επίσης, τα φόρουμ συζητήσεων αλλάζουν το ρόλο των χρηστών από παθητικούς παραλήπτες πληροφοριών σε ενεργά μέλη της διαδικασίας [19].

Παράλληλα οι Cox et al. (2001) [19] θεωρούν την αύξηση της επίγνωσης ως ένα θέμα της αλλαγής της συμπεριφοράς των χρηστών και της κατανόησης της ασφάλειας. Προτείνουν τη χρήση: α) συνέδριων συζητήσεων (discussion sessions), β) λιστών με ενέργειες που μπορούν να πραγματοποιηθούν ή όχι (do and don't chelists) και γ) διαδικτυακά μαθήματα-φροντιστήρια (online tutorial), τα οποία είναι ένας συνδυασμός των μονόδρομων και των αμφίδρομων καναλιών επικοινωνίας.

Οι Drevin et al. (2008) [19] διερευνούν εκτεταμένα τους στόχους της επίγνωσης ασφάλειας και θεωρούν ότι στοχεύει στη μείωση των ανθρώπινων λαθών, την κλοπή, την απάτη και την κακή χρήση των περιουσιακών στοιχείων του υπολογιστή. Η έρευνά τους έδειξε ότι οι θεμελιώδεις στόχοι της επίγνωσης ασφάλειας πληροφοριών πρέπει να συνδέονται με τους βασικούς στόχους της ασφάλειας, δηλαδή την εμπιστευτικότητα (confidentiality), την ακεραιότητα (integrity) και τη διαθεσιμότητα (availability). Ωστόσο, προέκυψαν κάποιοι πρόσθετοι κοινωνικοί και διαχειριστικοί στόχοι, όπως η αποδοχή της ευθύνης για τις ενέργειες και την αποτελεσματικότητα της χρήσης των πηγών. Η έρευνά τους επικεντρώνεται στον προσδιορισμό των θεμελιωδών στόχων της επίγνωσης ασφάλειας πληροφοριών και δεν έχει σκοπό να προτείνει κάποια μέθοδο επίτευξής τους [19].

3.1.1 Επεξήγηση όρων: Επίγνωση (awareness), Εξάσκηση (training) και Εκπαίδευση (education)

Το Εθνικό Ινστιτούτο Πρωτοτύπων και Τεχνολογίας (NIST) το 2003 [20], δημοσίευσε ένα κείμενο με τους κανονισμούς και τις τεχνικές για τη δημιουργία προγραμμάτων επίγνωσης ασφάλειας πληροφοριών και εξάσκησης. Σύμφωνα με το NIST, ένα πετυχημένο πρόγραμμα ασφάλειας πληροφοριών αποτελείται από: 1) την ανάπτυξη της πολιτικής ασφάλειας πληροφοριών, η οποία αντανακλάται στις ανάγκες της επιχείρησης και μετριάζεται από

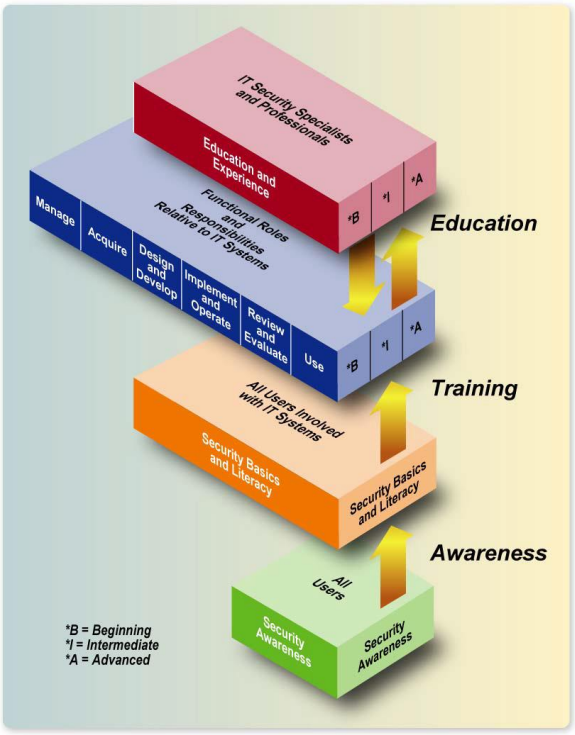
γνωστούς κινδύνους, 2) την πληροφόρηση των χρηστών για τις υποχρεώσεις τους στην ασφάλεια πληροφοριών, όπως καταγράφονται στην πολιτική ασφάλειας του οργανισμού και 3) την θέσπιση διαδικασιών για την παρακολούθηση και την αναθεώρηση του προγράμματος [20].

Η επίγνωση της ασφάλειας και η εξάσκηση θα πρέπει να είναι επικεντρωμένες στο σύνολο του πληθυσμού των χρηστών του οργανισμού. Η διαχείριση πρέπει να θέσει το παράδειγμα για τη κατάλληλη συμπεριφορά στην ασφάλεια των πληροφοριών σε έναν οργανισμό. Ένα πρόγραμμα επίγνωσης οφείλει να ξεκινήσει με μια προσπάθεια που μπορεί να αναπτυχθεί και να υλοποιηθεί με διάφορους τρόπους και απευθύνεται σε όλα τα επίπεδα της οργάνωσης συμπεριλαμβανομένων των ανώτερων και εκτελεστικών διευθυντών. Η αποτελεσματικότητα αυτής της προσπάθειας συνήθως θα καθορίσει την αποτελεσματικότητα του προγράμματος επίγνωσης και εξάσκησης. Αυτό είναι κάτι που είναι απαραίτητο για ένα πετυχημένο πρόγραμμα ασφάλειας πληροφοριών [20].

Ένα πρόγραμμα επίγνωσης και εξάσκησης σε μια επιχείρηση είναι βασικό, καθώς είναι το «μέσο» για τη διάδοση των πληροφοριών στους χρήστες, συμπεριλαμβανομένων και των διευθυντών, και απαιτείται για να μπορούν να ολοκληρώσουν με ασφάλεια τις αρμοδιότητές τους. Στη περίπτωση του προγράμματος ασφάλειας πληροφοριών, το «μέσο» χρησιμοποιείται για να μεταφέρει τις απαιτήσεις της ασφάλειας σε όλη την επιχείρηση [20].

Ένα αποτελεσματικό πρόγραμμα επίγνωσης ασφάλειας πληροφοριών και εξάσκησης εξηγεί τους κύριους κανόνες συμπεριφοράς των χρηστών ενός συστήματος πληροφοριών τεχνολογίας. Το πρόγραμμα κοινοποιεί τις πολιτικές ασφάλειας πληροφοριών και τονίζει ότι είναι σημαντικό να ακολουθηθούν. Αυτό πρέπει να προηγείται και να θέτει τη βάση για τυχόν κυρώσεις που επιβάλλονται λόγω μη εκπαίδευσης. Οι χρήστες πρώτα πρέπει να πληροφορούνται για τις προσδοκίες. Η λογοδοσία πρέπει να προέρχεται από ένα πλήρως ενημερωμένο, καλά εκπαιδευμένο και ευαισθητοποιημένο εργατικό δυναμικό [20].

Παράλληλα, δίνεται ένα σχεδιάγραμμα με το συνεχές της εξάσκησης ασφάλειας πληροφοριών, στο οποίο φαίνεται η επίγνωση που είναι η αρχή της εκμάθησης, μέσω της οποίας δημιουργείται η εξάσκηση, καταλήγοντας στην εκπαίδευση [20].



Εικόνα 24: «Το συνεχές της μάθησης ασφάλειας πληροφοριακών τεχνολογιών», Wilson M. & Hash J. (2003, October), Building an Information Technology Security Awareness and Training Program, Computer Security Division Information Technology Laboratory , National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8933

Οι προσπάθειες της επίγνωσης ασφάλειας είναι σχεδιασμένες για να αλλάξουν τη συμπεριφορά ή να ενισχύσουν τις καλές πρακτικές ασφάλειας. Ο NIST [20] ορίζει την επίγνωση (awareness) ως εξής: «Η επίγνωση δεν είναι εξάσκηση. Ο σκοπός της παρουσίασης της επίγνωσης είναι απλώς για να επικεντρώσει την προσοχή στην ασφάλεια. Η παρουσίαση της επίγνωσης έχει ως στόχο να επιτρέψει στα άτομα να αναγνωρίζουν τις ανησυχίες της ασφάλειας πληροφοριών και να αντιδρούν άμεσα. Στις δραστηριότητες επίγνωσης, οι μαθητές είναι οι δέκτες της πληροφορίας, ενώ ο μαθητής σε ένα εκπαιδευτικό περιβάλλον έχει πιο ενεργό ρόλο. Η επίγνωση βασίζεται στην επίτευξη ευρέων ακροατηρίων με ελκύστηκες τεχνικές. Η εξάσκηση είναι πιο επίσημη, έχοντας στόχο την απόκτηση γνώσης και δεξιοτήτων που θα διευκολύνουν την απόδοση της εργασίας[20].

Η εξάσκηση (training) ορίζεται από το NIST [20] με τα εξής: « Το επίπεδο της εξάσκησης στο συνεχές της μάθησης στοχεύει στην παραγωγή σχετικών και απαραίτητων ικανοτήτων ασφάλειας από τους υπαλλήλους, οι οποίοι έχουν γνώσης σε θέματα διαφορετικά από την ασφάλεια πληροφοριών». Η βασική διαφορά της εξάσκησης με την επίγνωση είναι ότι η εξάσκηση στοχεύει στην διδασκαλία ικανοτήτων που επιτρέπουν στο άτομο να διαχειριστεί συγκεκριμένες λειτουργίες, ενώ η επίγνωση στοχεύει στην προσοχή του ατόμου σε ένα

θέμα ή ένα σύνολο θεμάτων. Οι ικανότητες που χρειάζονται κατά την εξάσκηση δημιουργούνται στη βάση της επίγνωσης, και συγκεκριμένα, στις βασικές γνώσης για την ασφάλεια. Ένα εκπαιδευτικό πρόγραμμα δεν πρέπει απαραίτητα να οδηγεί σε πτυχίο από πανεπιστήμιο τριτοβάθμιας εξάσκησης. Παρόλα αυτά, ένα εκπαιδευτικό μάθημα μπορεί να περιέχει το ίδιο περιεχόμενο με ένα μάθημα από κολέγιο ή πανεπιστήμιο που συμπεριλαμβάνεται σε ένα συγκεκριμένο πρόγραμμα σπουδών [20].

Η εκπαίδευση (education) είναι: «Το επίπεδο που ενσωματώνει όλες τις δεξιότητες και τις ικανότητες ασφάλειας των διάφορων λειτουργικών ειδικοτήτων σε ένα κοινό σώμα της γνώσης, προσθέτει μια διεπιστημονική μελέτη των εννοιών, των ζητημάτων και των αρχών (τεχνολογικών και κοινωνικών) και προσπαθεί να παραγάγει ειδικούς και επαγγελματίες ικανούς για όραμα και προορατική ανταπόκριση» [20]. Για παράδειγμα, ένα εκπαιδευτικό πρόγραμμα σε κάποιο πανεπιστήμιο ή κολλέγιο αποτελεί ένα παράδειγμα εκπαίδευσης. Κάποια άτομα επιλέγουν ένα μάθημα για να αναπτύξουν τις δεξιότητές τους με ιδιαίτερη πειθαρχία. Αυτό είναι εξάσκηση σε αντίθεση με την εκπαίδευση. Πολλά πανεπιστήμια και κολλέγια προσφέρουν προγράμματα με πιστοποίηση, στα οποία ο φοιτητής μπορεί να παρακολουθήσει αρκετά μαθήματα, με μια σχετική πειθαρχία και να απονεμηθεί ένα πιστοποιητικό κατά την ολοκλήρωση των μαθημάτων. Συχνά, αυτά τα προγράμματα πιστοποίησης διεξάγονται ως μια κοινή προσπάθεια ανάμεσα στα σχολεία και στους πωλητές λογισμικού. [20]. Οι υπεύθυνοι των εκπαιδευτικών προγραμμάτων είναι αρμόδιοι να κρίνουν τι είναι κατάλληλο ως περιεχόμενο εκπαίδευσης ανάλογα με τις ανάγκες του κοινού.

Στο πλαίσιο της εκπαίδευσης των χρηστών είναι σημαντική η επαγγελματική ανάπτυξη (professional development), ώστε να διασφαλιστεί ότι οι χρήστες, από τον αρχάριο μέχρι τον επαγγελματία σε θέματα ασφάλειας, διαθέτουν το απαιτούμενο επίπεδο γνώσης και ικανότητας που χρειάζεται για το ρόλο τους. Η επαγγελματική ανάπτυξη επικυρώνει ικανότητες μέσω της πιστοποίησης. Τέτοιου είδους ανάπτυξη και επιτυχημένη πιστοποίηση μπορεί να χαρακτηριστεί ως "επαγγελματισμός". Οι προπαρασκευαστικές εργασίες για την εξέταση σε τέτοια πιστοποίηση περιλαμβάνει την μελέτη ενός καθορισμένου σώματος γνώσεων ή τεχνικού προγράμματος σπουδών που συμπληρώνεται με εμπειρία στην εργασία [20].

Η κίνηση προς την εξειδίκευση στον τομέα της ασφάλειας της τεχνολογίας πληροφοριών μπορεί να υπάρξει ανάμεσα στους υπεύθυνους ασφάλειας, τους ελεγκτές, τους κατασκευαστές και τους διαχειριστές του συστήματος και εξελίσσεται. Υπάρχουν δύο είδη πιστοποίησης: γενική και τεχνική. Η γενική πιστοποίηση επικεντρώνεται στη δημιουργία

μιας βάσης γνώσεων των πολλών πτυχών του επαγγέλματος ασφάλειας τεχνολογιών πληροφοριών. Η τεχνική πιστοποίηση επικεντρώνεται κυρίως στα τεχνικά ζητήματα ασφάλειας που σχετίζονται με συγκεκριμένες πλατφόρμες, λειτουργικά λογισμικά, προϊόντα πωλητών κλπ. [20].

Κάποιες εταιρίες και οργανισμοί επικεντρώνονται στους επαγγελματίες ασφάλειας τεχνολογιών πληροφοριών, οι οποίοι έχουν πιστοποίηση ως βασικό τους προσόν. Άλλοι οργανισμοί προσφέρουν αύξηση μισθών και μπόνους για να διασφαλίσουν χρήστες με πιστοποίηση και να ενθαρρύνουν κι άλλους να αποκτήσουν πιστοποίηση πάνω στον τομέα της ασφάλειας [20].

3.1.2 Οδηγίες σχεδιασμού προγραμμάτων εκπαίδευσης σε ζητήματα ασφάλειας

Στόχος των προγραμμάτων εξοικείωσης και εξάσκησης αναφορικά με ζητήματα ασφάλειας (Security Awareness and Training programs - SAT) είναι η επεξήγηση/αφομοίωση των κανόνων ασφάλειας και η απόκτηση δεξιοτήτων των χρηστών, ώστε να χειρίζονται ορθά τα συστήματα, αποφεύγοντας παραβιάσεις ασφάλειας που βλάπτουν τους ίδιους αλλά και τα συστήματα.

Το 2010 ο ENISA [21] δημοσίευσε έναν οδηγό για τη σωστή ανάπτυξη της επίγνωσης της ασφάλειας. Δίνεται έμφαση στο σωστό χρόνο που θεωρείται απαραίτητη η δημιουργία προγραμμάτων για την ασφάλεια των πληροφοριών. Διαχωρίζει τις περιπτώσεις, ανάλογα με τους παράγοντες που μπορεί να επηρεάσουν τη χρησιμότητα της δημιουργίας προγράμματος, σε εξωτερικούς και εσωτερικούς. Οι εξωτερικοί παράγοντες είναι η ψήφιση νέων νόμων σχετικά με την ασφάλεια των πληροφοριών, μια νέα κυβέρνηση, τα νέα εθνικά, περιφερειακά ή τοπικά προγράμματα ασφάλειας βασικών πληροφοριών για τους πολίτες κ.α. Οι εσωτερικοί παράγοντες που μπορεί να οδηγήσουν στην ανάγκη δημιουργίας προγράμματος ασφάλειας πληροφοριών είναι οι νέοι κανονισμοί που σχετίζονται με τον οργανισμό, μια νέα πολιτική απορρήτου, η αναβάθμιση ή η αλλαγή της πολιτικής ασφάλειας των πληροφοριών, των διαδικασιών και των οδηγιών. Επίσης, η εφαρμογή νέων τεχνολογιών, η πρόσληψη νέου προσωπικού, η αλλαγή διαχείρισης, η αυτονομία και η βασική εκπαίδευση του προσωπικού σε θέματα ασφάλειας πληροφοριών, οι καινούργιοι κίνδυνοι κ.α. εντάσσονται στους εσωτερικούς παράγοντες.

Η στρατηγική λοιπόν, που προτείνει ο ENISA [21] για τη διαχείριση προγραμμάτων επίγνωσης ασφάλειας πληροφοριών, περιέχει τρείς βασικές διαδικασίες, οι οποίες είναι: α) η οργάνωση, η αξιολόγηση και ο σχεδιασμός, β) η εκτέλεση και διαχείριση, και γ) η

αξιολόγηση και προσαρμογή. Στον πίνακα 2 δίνεται μια περιγραφή για αυτές τις τρεις διαδικασίες.

Στην πρώτη διαδικασία τα προγράμματα επίγνωσης θα πρέπει να σχεδιαστούν έχοντας κατά νου το στόχο του οργανισμού. Είναι σημαντικό να υποστηρίζουν τις ανάγκες της επιχείρησης του οργανισμού και να σχετίζονται με την κουλτούρα και την αρχιτεκτονική του. Τα πιο πετυχημένα προγράμματα είναι αυτά στα οποία οι χρήστες τους αισθάνονται ότι σχετίζονται με το θέμα και τα προβλήματα που παρουσιάζονται.

Η δεύτερη διαδικασία περιλαμβάνει οποιαδήποτε δραστηριότητα είναι απαραίτητη για την εφαρμογή του προγράμματος επίγνωσης ασφάλειας πληροφοριών. Η πρωτοβουλία μπορεί να εκτελεστεί και να διαχειριστεί μόνο όταν έχει διεξαχθεί αξιολόγηση των αναγκών, έχει αναπτυχθεί μια στρατηγική, έχει ολοκληρωθεί η σχεδίαση ενός προγράμματος επίγνωσης για την εφαρμογή της στρατηγικής και έχει αναπτυχθεί το υλικό του προγράμματος [21].

Στην τρίτη διαδικασία, η επίσημη αξιολόγηση και οι μηχανισμοί ανατροφοδότησης είναι κριτικά στοιχεία οποιουδήποτε προγράμματος. Η συνεχιζόμενη βελτίωση δεν μπορεί να εγγυηθεί χωρίς την γνώση του πώς λειτουργεί το υπάρχον πρόγραμμα. Επιπλέον, ο μηχανισμός ανατροφοδότησης πρέπει να σχεδιαστεί με τέτοιο τρόπο ώστε να είναι σε θέση να ανταπεξέρχεται στους αρχικούς στόχους του προγράμματος. Μόλις σταθεροποιηθούν οι βασικές απαιτήσεις, η στρατηγική ανατροφοδότησης μπορεί να σχεδιαστεί και να υλοποιηθεί [21].

Process	Description
Plan, assess and design	Awareness programmes must be designed with the organisation mission in mind. It is important that they support the business needs of the organisation and be relevant to the organisation's culture and eventually IT architecture. The most successful programmes are those that users feel are relevant to the subject matter and issues presented. In the design step of the programme, the awareness needs are identified, an effective awareness plan is developed, organisational buy-in is sought and secured, and priorities are established.
Execute and manage	This process includes any activity necessary to implement an information security awareness programme. The initiative can be executed and managed only when: ✓ A needs assessment has been conducted. ✓ A strategy has been developed. ✓ An awareness programme plan for implementing that strategy has been completed. ✓ Material has been developed.
Evaluate and adjust	Formal evaluation and feedback mechanisms are critical components of any security awareness programme. Continuous improvement cannot occur without a good sense of how the existing programme is working. In addition, the feedback mechanism must be designed to address objectives initially established for the programme. Once the baseline requirements have been solidified, a feedback strategy can be designed and implemented.

Πίνακας 2: « Διαδικασίες διαχείρισης προγραμμάτων επίγνωσης ασφάλειας», ENISA (2010), The new users' guide: How to raise information security awareness

Τα προγράμματα επίγνωσης και εκπαίδευσης θα πρέπει να είναι σχεδιασμένα έχοντας υπόψη το σκοπό του οργανισμού για τον οποίο σχεδιάζονται. Είναι σημαντικό το πρόγραμμα να υποστηρίζει τις επιχειρησιακές ανάγκες του οργανισμού και να σχετίζεται με την κουλτούρα και την αρχιτεκτονική της τεχνολογίας πληροφοριών. Τα πιο πετυχημένα προγράμματα είναι αυτά στα οποία οι χρήστες θεωρούν ότι σχετίζονται με το αντικείμενο και τα θέματα που παρουσιάζονται [20].

Η ανάπτυξη ενός προγράμματος επίγνωσης και εκπαίδευσης ασφάλειας πρέπει να απαντά στην εξής ερώτηση: «Ποιο είναι το σχέδιο για την ανάπτυξη και εφαρμογή ευκαιριών επίγνωσης και εκπαίδευσης που συμμορφώνεται με τις ισχύουσες οδηγίες;». Στο στάδιο του σχεδιασμού του προγράμματος, η επίγνωση και εκπαίδευση του οργανισμού χρειάζεται να αναγνωριστεί. Ένα αποτελεσματικό πρόγραμμα επίγνωσης και εκπαίδευσης των πρακτόρων αναπτύσσεται και επιδιώκεται ένα οργανωτικό buy-in και εξασφαλίζεται[20].

Για την δημιουργία των προγραμμάτων επίγνωσης ασφάλειας και εξάσκησης έχει οριστεί από το NIST ένας κύκλος εργασιών που περιέχει τα εξής τρία στάδια:

α) *Σχεδιασμός ενός προγράμματος επίγνωσης και εξάσκησης* (Designing an Awareness and Training Program)

Ένα πρόγραμμα επίγνωσης και εκπαίδευσης σχεδιάζεται, αναπτύσσεται και εφαρμόζεται με διάφορους τρόπους. Στη συνέχεια, θα αναπτυχθούν οι τρεις πιο συνηθισμένοι μέθοδοι ή τα πιο συνηθισμένα μοντέλα προγραμμάτων. Το κάθε μοντέλο που καθιερώνεται για να επιβλέπει τη δραστηριότητα του προγράμματος επίγνωσης και εκπαίδευσης εξαρτάται από το μέγεθος και τη γεωγραφική διασπορά του οργανισμού, τον ορισμό των ρόλων του οργανισμού και των υποχρεώσεών του και από τη κατανομή του προϋπολογισμού και των αρμοδιοτήτων [20].

Το πρώτο μοντέλο, όπως απεικονίζεται και στην εικόνα 3, είναι το «Κεντρικό Μοντέλο Διαχείρισης Προγράμματος» (Centralized Program Management Model). Σε αυτό το μοντέλο, η ευθύνη και ο προϋπολογισμός ολόκληρου του προγράμματος επίγνωσης και εκπαίδευσης του οργανισμού, δίνεται στους αρμόδιους υπάλληλους ή την αρμόδια υπηρεσία (central authority). Όλες οι οδηγίες, η ανάπτυξη στρατηγικής, η οργάνωση και ο προγραμματισμός συντονίζονται μέσω αυτών των υπαλλήλων της «επίγνωσης ασφάλειας και εκπαίδευσης».

Εικόνα 25: «Μοντέλο 1ο - το Κεντρικό Μοντέλο Διαχείρισης Προγράμματος (Centralized Program Management Model)», Wilson M. & Hash J. (2003, October), Building an Information Technology Security Awareness and Training Program, Computer Security Division Information Technology Laboratory , National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8933

Λόγω της ανάπτυξης της στρατηγικής επίγνωσης και εκπαίδευσης από τους αρμόδιους υπάλληλους ή την αρμόδια υπηρεσία, η αξιολόγηση των αναγκών διεξάγεται επίσης, από τους αρμόδιους. Οι αρμόδιοι, παράλληλα, αναπτύσσουν ένα σχέδιο εκπαίδευσης μαζί με το υλικό επίγνωσης και εκπαίδευσης. Η μέθοδος της υλοποίησης των υλικών σε όλο τον οργανισμό, καθορίζεται και επιτυγχάνεται από τους αρμόδιους [20]. Η επικοινωνία μεταξύ των αρμόδιων υπαλλήλων και των οργανωτικών μονάδων (organizational units) γίνεται και από τις δύο πλευρές. Οι αρμόδιοι επικοινωνούν τις οδηγίες πολιτικής του οργανισμού σχετικά με την επίγνωση και την εκπαίδευση, τη στρατηγική για τη διεξαγωγή του προγράμματος και το υλικό και τις μεθόδους εφαρμογής στις οργανωτικές μονάδες. Οι μονάδες αυτές παρέχουν τις πληροφορίες που απαιτούνται από τους αρμόδιους. Παρέχουν επίσης, ανατροφοδότηση για την αποτελεσματικότητα των υλικών επίγνωσης και εκπαίδευσης και την καταλληλότητα ή τις μεθόδους που χρησιμοποιήθηκαν για την υλοποίηση του υλικού. Αυτό επιτρέπει στους αρμόδιους να ελέγξουν, να προσθέσουν ή να διαγράψουν υλικά ή να τροποποιήσουν τη μέθοδο εφαρμογής [20]. Αυτό το Κεντρικό Μοντέλο Διαχείρισης Προγραμμάτων χρησιμοποιείται συνήθως από εταιρίες που έχουν τα εξής χαρακτηριστικά:

- Είναι σχετικά μικρές ή διαθέτουν υψηλό βαθμό δομής και κεντρικής διαχείρισης των περισσότερων λειτουργιών τεχνολογίας πληροφοριών,

- έχουν στο επίπεδο των κεντρικών γραφείων τις απαραίτητες πηγές, την εξειδίκευση και τη γνώση της αποστολής και των λειτουργιών στο επίπεδο των μονάδων, ή
- έχουν υψηλό βαθμό ομοιότητας στους στόχους αποστολής και στους επιχειρησιακούς στόχους σε όλες τις συνιστώσες τους.

Το δεύτερο μοντέλο προγράμματος είναι το «Πρόγραμμα Μερικής Αποκεντρωμένης Διαχείρισης» (Partially Decentralized Program Management Model) [20]. Σε αυτό το μοντέλο, η πολιτική και στρατηγική της επίγνωσης ασφάλειας και της εκπαίδευσης ορίζονται από τους αρμόδιους, αλλά η εφαρμογή μεταβιβάζεται στους υπαλλήλους της γραμμής διαχείρισης στον οργανισμό. Οι υπάλληλοι αυτοί είναι υπεύθυνοι για τον προϋπολογισμό, την ανάπτυξη του υλικού και την οργάνωση.

Εικόνα 26: «Μοντέλο 2ο - Πρόγραμμα Μερικής Αποκεντρωμένης Διαχείρισης (Partially Decentralized Program Management Model)», Wilson M. & Hash J. (2003, October), Building an Information Technology Security Awareness and Training Program, Computer Security Division Information Technology Laboratory , National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8933

Η αξιολόγηση των αναγκών διεξάγεται από τους αρμόδιους, επειδή καθορίζουν την στρατηγική του προγράμματος επίγνωσης ασφάλειας και εκπαίδευσης. Η πολιτική, η στρατηγική και ο προϋπολογισμός διαβιβάζονται από τους αρμόδιους στις οργανωτικές μονάδες. Με βάση την στρατηγική, οι οργανωτικές μονάδες αναπτύσσουν τα δικά τους σχέδια εκπαίδευσης, καθώς επίσης και τα δικά τους υλικά επίγνωσης και εκπαίδευσης και καθορίζουν τις μεθόδους ανάπτυξης του υλικού μέσα στις δικές τους μονάδες [20]. Όπως

και στο πρώτο μοντέλο, έτσι και σε αυτό, η επικοινωνία μεταξύ των αρμόδιων υπαλλήλων και των οργανωτικών μονάδων γίνεται και από τις δύο μεριές. Οι αρμόδιοι διαβιβάζουν τις οδηγίες πολιτικής του οργανισμού σχετικά με την επίγνωση και την εκπαίδευση, τη στρατηγική για τη διεξαγωγή του προγράμματος και το υλικό και τις μεθόδους εφαρμογής στις οργανωτικές μονάδες. Οι ίδιοι μπορούν επίσης, να συμβουλέψουν τις μονάδες ότι είναι υπεύθυνες για την ανάπτυξη σχεδίων κατάρτισης και για την εφαρμογή του προγράμματος. Παράλληλα, μπορεί να τους παρέχουν καθοδήγηση ή εκπαίδευση, έτσι ώστε να μπορέσουν να ανταπεξέλθουν στις υποχρεώσεις τους [20]. Οι αρμόδιοι μπορεί να απαιτήσουν περιοδική εισαγωγή από την κάθε μονάδα ξεχωριστά, αναφέροντας τις δαπάνες του προϋπολογισμού που πραγματοποιήθηκαν, την κατάσταση των σχεδίων εκπαίδευσης των μονάδων και τις εκθέσεις προόδου σχετικά με την εφαρμογή του υλικού επίγνωσης και εκπαίδευσης. Επίσης, έχουν τη δυνατότητα να απαιτήσουν από τις οργανωτικές μονάδες να αναφέρουν τον αριθμό των συμμετοχών στα σεμινάρια επίγνωσης, τον αριθμό των ατόμων που εκπαιδεύτηκαν στο συγκεκριμένο θέμα και τον αριθμό των ανθρώπων που δεν έχουν παρακολουθήσει τα σεμινάρια επίγνωσης και εκπαίδευσης [20]. Μπορεί να ζητηθεί από τις μονάδες να περιγράψουν τα μαθήματα που διδάχτηκαν, έτσι ώστε οι αρμόδιοι να μπορέσουν να παρέχουν αποτελεσματική καθοδήγηση και σε άλλες μονάδες.

Αυτό το εν μέρει αποκεντρωμένο μοντέλο διαχείρισης προγραμμάτων χρησιμοποιείται συχνά από οργανισμούς οι οποίοι:

- Είναι σχετικά μεγάλοι ή έχουν μια αρκετά αποκεντρωμένη δομή με σαφείς αρμοδιότητες που έχουν ανατεθεί τόσο στα κεντρικά γραφεία όσο και επίπεδα των μονάδων,
- έχουν λειτουργίες που είναι διασκορπισμένες σε μια ευρεία γεωγραφική περιοχή, ή
- έχουν οργανωτικές μονάδες με ποικίλες αποστολές, έτσι ώστε τα προγράμματα επίγνωσης και εκπαίδευσης να διαφέρουν σημαντικά ανάλογα με τις ειδικές ανάγκες την μονάδας

Το τρίτο και τελευταίο μοντέλο, είναι το «Πλήρως Αποκεντρωμένο Μοντέλο Διαχείρισης Προγράμματος» (Fully Decentralized Program Management Model) [20]. Σε αυτό το μοντέλο, οι αρμόδιοι επίγνωσης ασφάλειας και εκπαίδευσης διαδίδουν ευρεία πολιτική και προσδοκίες σχετικά με τις απαιτήσεις επίγνωσης ασφάλειας και εκπαίδευσης αλλά η ευθύνη εκτέλεσης ολόκληρου του προγράμματος δίνεται στις οργανωτικές μονάδες. Το

μοντέλο αυτό, χρησιμοποιεί μια σειρά από οδηγίες κατανεμημένης αρχής, καθοδηγούμενο από τους αρμόδιους.

Εικόνα 27: «Μοντέλο 3ο- Πλήρως Αποκεντρωμένο Μοντέλο Διαχείρισης Προγράμματος (Fully Decentralized Program Management Model)», Wilson M. & Hash J. (2003, October), Building an Information Technology Security Awareness and Training Program, Computer Security Division Information Technology Laboratory , National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8933

Η αξιολόγηση των αναγκών διεξάγεται από κάθε οργανωτική μονάδα, επειδή σε αυτό το μοντέλο, οι μονάδες καθορίζουν την στρατηγική του προγράμματος. Η πολιτική και ο προϋπολογισμός μεταφέρονται από τους αρμόδιους στις μονάδες. Με βάση αυτή τη στρατηγική, οι μονάδες αναπτύσσουν τα δικά τους σχέδια εκπαίδευσης, καθώς επίσης και τα δικά τους υλικά επίγνωσης και εκπαίδευσης και καθορίζουν τις μεθόδους ανάπτυξης των υλικών μέσα στις δικές τους μονάδες [20]. Όπως και στα δύο προηγούμενα μοντέλα έτσι και σε αυτό, η επικοινωνία μεταξύ των αρμόδιων και των οργανωτικών μονάδων πραγματοποιείται και από τις δύο πλευρές. Και σε αυτή τη περίπτωση οι αρμόδιοι μπορεί να απαιτήσουν την έκδοση αναφορών από τις μονάδες, όπως εξηγήθηκε και στο δεύτερο μοντέλο.

Αυτό το πλήρες αποκεντρωμένο μοντέλο διαχείρισης προγραμμάτων χρησιμοποιείται συχνά από οργανισμούς οι οποίοι:

- Είναι σχετικά μεγάλοι,
- έχουν μια πολύ αποκεντρωμένη δομή με γενικές ευθύνες που ανατίθενται στα κεντρικά γραφεία και συγκεκριμένες ευθύνες που έχουν ανατεθεί σε επίπεδο μονάδων,
- έχουν λειτουργίες που είναι διασκορπισμένες σε μια ευρεία γεωγραφική περιοχή, ή

- έχουν σχεδόν αυτόνομες οργανωτικές μονάδες με ξεχωριστές αποστολές, έτσι ώστε τα προγράμματα επίγνωσης και εκπαίδευσης να μη διαφέρουν σημαντικά.

Μόλις το μοντέλο που πρόκειται να χρησιμοποιηθεί αναγνωριστεί, η προσέγγιση για τη διενέργεια εκτίμησης των αναγκών πρέπει να καθοριστεί σύμφωνα με το οργανωτικό μοντέλο που επιλέχθηκε [20].

Στη συνέχεια το NIST, προτείνει την διεξαγωγή αξιολόγησης αναγκών (Conducting a needs assessment). Η αξιολόγηση των αναγκών είναι μια διαδικασία, η οποία μπορεί να χρησιμοποιηθεί για τον καθορισμό των αναγκών ενός οργανισμού για επίγνωση και εξάσκηση. Τα αποτελέσματα της αξιολόγησης αυτής μπορούν να αποτελέσουν αιτιολόγηση για να πείσουν τη διοίκηση να διαθέσει επαρκείς πόρους για τη διαδικασία της επίγνωσης και της εξάσκησης [20]. Στη διεξαγωγή αξιολόγησης των αναγκών, είναι σημαντικό να συμμετέχει το βασικό προσωπικό. Για οποιαδήποτε ειδική εξάσκηση αναγκών είναι βασικό να υπάρχουν οι παρακάτω ρόλοι: εκτελεστική διοίκηση (executive management), προσωπικό ασφάλειας (security personnel), ιδιοκτήτες συστημάτων (system owners), διαχειριστές συστήματος και προσωπικό υποστήριξης τεχνολογιών (system administrators and IT support personnel) και λειτουργικοί διευθυντές και χρήστες συστήματος (operational managers and system users).

Έπειτα, για το πρώτο στάδιο χρειάζεται η ανάπτυξη στρατηγικής και σχεδίου για επίγνωση και εξάσκηση (Developing an awareness and training strategy and plan). Η ολοκλήρωση της αξιολόγησης των αναγκών επιτρέπει σε έναν οργανισμό να αναπτύξει μια στρατηγική για την ανάπτυξη, εφαρμογή και διατήρηση του προγράμματος επίγνωσης και εξάσκησης. Το σχέδιο είναι το έγγραφο εργασίας που περιέχει τα στοιχεία που αποτελούν τη στρατηγική. Το σχέδιο πρέπει να περιέχει τα ακόλουθα στοιχεία: α) την υπάρχουσα εθνική πολιτική που απαιτεί την πραγματοποίηση της επίγνωσης και της εξάσκησης, β) τον σκοπό του προγράμματος, γ) τους ρόλους και τις ευθύνες του προσωπικού, δ) τους στόχους που πρέπει να επιτευχθούν για κάθε πτυχή του προγράμματος, ε) την στόχευση κοινού για κάθε πτυχή του προγράμματος κ.α. [20].

Το επόμενο βήμα είναι η καθιέρωση των προτεραιοτήτων (Establishing priorities). Μόλις οριστικοποιηθεί η στρατηγική και το σχέδιο της επίγνωσης ασφάλειας και εξάσκησης, πρέπει να καθοριστεί ένα χρονοδιάγραμμα υλοποίησης. Αν αυτό πρέπει να συμβεί σε φάσεις, είναι σημαντικό να αποφασιστούν οι παράγοντες που θα ληφθούν υπόψη για τον πρώτο προγραμματισμό, καθώς και η σειρά προτεραιότητας αυτών. Οι βασικοί παράγοντες που πρέπει να ληφθούν υπόψη είναι: α) διαθεσιμότητα υλικών/ πηγών (availability of material/resources), β) ρόλος και οργανωτική επίδραση (role and organizational impact), γ)

κατάσταση τρέχουσας συμμόρφωσης (state of current compliance) και δ) κρίσιμες εξαρτήσεις έργου (critical project dependencies) [20].

Στη συνέχεια, πρέπει να ρυθμιστεί η γραμμή (setting the bar). Η "ρύθμιση της γραμμής" σημαίνει ότι πρέπει να παρθεί μια απόφαση σχετικά με την πολυπλοκότητα του υλικού που θα αναπτυχθεί. Η πολυπλοκότητα πρέπει να είναι ανάλογη με τον ρόλο του ατόμου που θα υποβάλλει τη μαθησιακή προσπάθεια. Το υλικό θα αναπτυχθεί βάση δύο βασικών κριτηρίων: 1) τη θέση του συμμετέχοντος στο πλαίσιο του οργανισμού και 2) τη γνώση των απαραίτητων ικανοτήτων ασφάλειας για αυτή τη θέση. Η πολυπλοκότητα του υλικού καθορίζεται πριν ξεκινήσει η ανάπτυξη. Η ρύθμιση της γραμμής εφαρμόζεται και στους τρεις τύπους μάθησης: επίγνωση, εξάσκηση και εκπαίδευση [20].

Για να ολοκληρωθεί το πρώτο στάδιο δημιουργίας προγραμμάτων επίγνωσης και εκμάθησης των ζητημάτων ασφάλειας, το τελευταίο που χρειάζεται να υλοποιηθεί είναι η χρηματοδότηση του προγράμματος (funding the security awareness and training program). Μόλις η στρατηγική επίγνωσης και εξάσκησης δομηθεί και καθοριστούν οι προτεραιότητες, τότε οι απαιτήσεις χρηματοδότησης πρέπει να προστεθούν στο σχέδιο. Πρέπει να καθοριστεί η έκταση της χρηματοδότησης που θα διατεθεί με βάση τα μοντέλα εφαρμογής που αναφέρθηκαν προηγουμένως. Η CIO του πρακτορείου πρέπει να καθορίσει τις απαιτούμενες προσδοκίες της συμμόρφωσης σε αυτή τη περιοχή. Οι πηγές της χρηματοδότησης πρέπει να προέρχονται από το πρακτορείο με βάση το υπάρχον ή προσδοκώμενο προϋπολογισμό και τις άλλες προτεραιότητες. Το σχέδιο επίγνωσης ασφάλειας και εξάσκησης πρέπει να εξεταστεί ως σύνολο των ελάχιστων απαιτήσεων που πρέπει να πληρούνται και αυτές οι απαιτήσεις, καθώς πρέπει να υποστηρίζονται από τον προϋπολογισμό [20]. Οι απαιτήσεις χρηματοδότησης μπορεί να περιλαμβάνουν:

- το ποσοστό του συνολικού προϋπολογισμού της εξάσκησης
- τη κατανομή των χρηστών με βάση το ρόλο τους
- το ποσοστό του συνολικού προϋπολογισμού των τεχνολογιών πληροφοριών ή
- τις αναλυτικές κατανομές δολαρίων ανά συνιστώσα με βάση το συνολικό κόστος εφαρμογής.

β) *Ανάπτυξη υλικού προγραμμάτων επίγνωσης και εξάσκησης* (Developing Awareness and Training Material)

Μόλις σχεδιαστεί το πρόγραμμα επίγνωσης και εξάσκησης, μπορεί να αναπτυχθεί το υποστηρικτικό υλικό. Για να γίνει αυτό, θα πρέπει να ισχύουν οι εξής ερωτήσεις: «ποια συμπεριφορά επιθυμούμε να ενισχύσουμε» και «ποιες ικανότητες επιθυμούμε να

αποκτήσει το κοινό και να αξιοποιήσει» [20]. Και στις δύο περιπτώσεις, πρέπει να δίνεται προσοχή στις δεξιότητες, τις οποίες θα ενσωματώσει ο χρήστης στην δουλεία του. Οι συμμετέχοντες θα δώσουν έμφαση σε ό,τι ακούν και βλέπουν στα σεμινάρια, εάν θεωρήσουν ότι το υλικό αναπτύχθηκε για τις δικές τους ανάγκες. Οποιαδήποτε παρουσίαση έχει έναν απρόσωπο χαρακτήρα, δίνει στο συμμετέχοντα την αίσθηση ότι παρακολουθεί το σεμινάριο επειδή «είναι υποχρεωμένος». Ένα πρόγραμμα επίγνωσης και εξάσκησης μπορεί να είναι αποτελεσματικό όταν το υλικό είναι ενδιαφέρον και έγκυρο [20].

Προκύπτει, ωστόσο, το ερώτημα «κατά πόσο αναπτύσσω υλικό επίγνωσης ή εξάσκησης». Γενικά, εφόσον ο στόχος του υλικού επίγνωσης είναι απλώς να επικεντρώσει την προσοχή σε καλές πρακτικές ασφάλειας, το μήνυμα που στέλνει η προσπάθεια επίγνωσης πρέπει να είναι απλό και σύντομο. Αυτό το μήνυμα μπορεί να απευθύνεται σε ένα θέμα ή σε διάφορα θέματα, τα οποία πρέπει να γνωρίζει το κοινό [20]. Το κοινό της επίγνωσης πρέπει να περιλαμβάνει όλους τους χρήστες του οργανισμού. Το μήνυμα, το οποίο θα στείλει ένα πρόγραμμα επίγνωσης ή μια καμπάνια πρέπει να ευαισθητοποιήσει όλους τους συμμετέχοντες για τις ευθύνες τους σχετικά με την ασφάλεια των πληροφοριών. Από την άλλη μεριά, το μήνυμα σε ένα εκπαιδευτικό σεμινάριο απευθύνεται σε συγκεκριμένο κοινό. Ένα μήνυμα σε υλικό εξάσκησης πρέπει να περιλαμβάνει οτιδήποτε σχετίζεται με την ασφάλεια, το οποίο οι συμμετέχοντες πρέπει να γνωρίζουν για να είναι αποδοτικοί κατά την εργασία τους. Το υλικό εξάσκησης εμβαθύνει περισσότερο σε σχέση με το υλικό που χρησιμοποιείται σε σεμινάρια επίγνωσης [20].

Για να αναπτυχθεί το υλικό επίγνωσης πρέπει να διευκρινιστούν οι γνώσεις που χρειάζεται να αποκτήσει το προσωπικό ενός οργανισμού σχετικά με την ασφάλεια τεχνολογικών πληροφοριών. Το σχέδιο επίγνωσης και εξάσκησης πρέπει να περιέχει μια λίστα με θέματα. Οι συμβουλές ηλεκτρονικού ταχυδρομείου, οι ηλεκτρονικές ιστοσελίδες ειδήσεων στον τομέα της πληροφορικής και τα περιοδικά αποτελούν καλές πηγές ιδεών και υλικού. Η πολιτική του οργανισμού, οι αναθεωρήσεις των προγραμμάτων, οι εσωτερικοί έλεγχοι, οι αναθεωρήσεις του προγράμματος εσωτερικών ελέγχων, οι αυτοαξιολογήσεις και οι επιτόπιοι έλεγχοι μπορούν, επίσης, να εντοπίσουν πρόσθετα θέματα προς αντιμετώπιση [20]. Για την επιλογή των θεμάτων επίγνωσης ασφάλειας, υπάρχει μια λίστα με προτεινόμενα θέματα που μπορούν να χρησιμοποιήσουν οι οργανισμοί. Μερικά παραδείγματα αυτών των θεμάτων είναι τα εξής:

- Χρήση και διαχείριση του κωδικού πρόσβασης
- Προστασία από υιούς και κακόβουλο λογισμικό

- Χρήση του Διαδικτύου
- Δημιουργία αντιγράφων ασφαλείας και αποθήκευση δεδομένων
- Απόδοση ευθύνης ατυχήματος
- Αλλαγές στο περιβάλλον του συστήματος
- Ζητήματα ασφάλειας φορητών συσκευών
- Ζητήματα ελέγχου πρόσβασης κ.α.

Υπάρχει αρκετή ποικιλία πηγών πουμπορεί να αξιοποιηθεί σε ένα πρόγραμμα επίγνωσης. Το υλικό μπορεί να περιέχει ένα συγκεκριμένο ζήτημα ή σε κάποιες περιπτώσεις, μπορεί να περιγράφει πώς να ξεκινήσει η ανάπτυξη ολόκληρου του προγράμματος επίγνωσης, του σεμιναρίου ή της καμπάνιας [20]. Οι πηγές αυτές μπορεί να περιλαμβάνουν τα εξής:

- Συμβουλές ηλεκτρονικού ταχυδρομείου, οι οποίες εκδίδονται από ομάδες ειδήσεων που φιλοξενούνται από τη βιομηχανία, ακαδημαϊκά ιδρύματα ή το γραφείο ασφάλειας του οργανισμού
- Επαγγελματικές οργανώσεις και πωλητές
- Διαδικτυακές ιστοσελίδες με καθημερινή ενημέρωση σχετικά με την ασφάλεια τεχνολογιών πληροφοριών
- Περιοδικά και
- Συνέδρια, σεμινάρια και μαθήματα

Το υλικό επίγνωσης μπορεί να αναπτυχθεί με τη χρήση ενός θέματος κάθε φορά ή με τη δημιουργία συνδυαστικών θεμάτων σε μια παρουσίαση. Για παράδειγμα, μια αφίσα ή ένα σλόγκαν για ένα εργαλείο επίγνωσης μπορεί να περιέχει ένα θέμα, ενώ ένα εισαγωγικό μάθημα ή μια διαδικτυακή παρουσίαση μπορεί να περιέχει διάφορα θέματα. Ανεξάρτητα από την προσέγγιση, ο αριθμός των πληροφοριών δεν πρέπει να κατακλύζει το κοινό [20]. Κάποια από τα κύρια θέματα που πρέπει να καλυφθούν σε μια τυπική παρουσίαση επίγνωσης είναι η σύντομη αναφορά των απαιτήσεων (πολιτικές), των προβλημάτων για τα οποία σχεδιάστηκαν οι απαιτήσεις, έτσι ώστε να αντιμετωπιστούν, και των δράσεων που πρέπει να πραγματοποιηθούν. Μια περίπλοκη παρουσίαση επίγνωσης που ενσωματώνει βασικά στοιχεία και υλικό γνώσεων γραφής σχετικά με την ασφάλεια, χρειάζεται να εμβαθύνει σε ένα θέμα. Επειδή τα βασικά στοιχεία και η γνώση γραφής είναι η γέφυρα ανάμεσα στην επίγνωση και την εξάσκηση, είναι κατάλληλο αυτό το επιπλέον επίπεδο λεπτομερειών και πολυπλοκότητας [20].

Για να αναπτυχθεί το υλικό εξάσκησης πρέπει να διευκρινιστούν οι ικανότητες που χρειάζεται να εκπαιδευτεί το κοινό. Το σχέδιο επίγνωσης και εξάσκησης πρέπει να

προσδιορίσει ένα κοινό, το οποίο θα μπορεί να εκπαιδευτεί, ώστε να είναι σε θέση να αντιμετωπίζει ζητήματα ασφάλειας. Το NIST [20] προτείνει ένα μοντέλο για τη δημιουργία μαθημάτων εξάσκησης, το «NIST Special Pub. 800-16». Το μοντέλο αυτό παρέχει ένα χρήσιμο εργαλείο, το οποίο αναπτύσσει μαθήματα εξάσκησης ασφάλειας και αντιπροσωπεύει τις ανάγκες της εξάσκησης ασφάλειας στο υπάρχον περιβάλλον υπολογιστή. Προσδιορίζει 26 ρόλους, οι οποίοι έχουν κάποιο βαθμό ευθύνης για την ασφάλεια των πληροφοριών. Το μοντέλο αυτό παρέχει μια ευκαμψία στη μεθοδολογία του για επέκταση των ρόλων και άλλων παραμέτρων για να φιλοξενήσει μελλοντικές τεχνολογίες και οργανωτικούς ρόλους. Η μεθοδολογία επίσης, επιτρέπει στα μαθήματα εξάσκησης να αναπτυχθούν στην αρχή, στο ενδιάμεσο και σε εξελιγμένο επίπεδο της εκπαίδευσης [20]. Ταυτόχρονα, το μοντέλο αυτό περιλαμβάνει μια σειρά από πηγές που μπορεί να αναπτύξει ένας σχεδιαστής μαθήματος κατά τη δημιουργία του μαθήματος εξάσκησης. Αυτές οι πηγές είναι: το μοντέλο συνεχούς μάθησης για την ασφάλεια της πληροφορικής (the IT security learning continuum model), οι 26 ρόλοι, τα 46 κύτταρα κατάρτισης, 12 τμήματα γνώσης θεμάτων και εννοιών, τρεις κατηγορίες περιεχομένου εξάσκησης και έξι βασικές ειδικότητες. Υπάρχουν έξι κατηγορίες βασικών ειδικοτήτων, οι οποίες είναι οι εξής: α) Διαχείριση (Manage), β) Απόκτηση (Acquire), γ) Σχεδιασμός και ανάπτυξη (Design and Develop), δ) Λειτουργία (Operate), ε) Επανεξέταση και αξιολόγηση (Review and Evaluate) και στ) Χρήση (Use).

Κατά την αναζήτηση των πηγών για τα μαθήματα και το υλικό εξάσκησης, το πρώτο βήμα είναι να διευκρινιστεί αν το υλικό θα αναπτυχθεί εσωτερικά ή θα ανατεθεί σε εξωτερικούς συνεργάτες. Εάν η εταιρία αποφασίσει να αναθέσει σε κάποιον την ανάπτυξη της εξάσκησης, υπάρχουν διάφοροι προμηθευτές που προσφέρουν μαθήματα «off-the-shelf», τα οποία είναι κατάλληλα για συγκεκριμένο κοινό ή μπορούν να αναπτυχθούν για συγκεκριμένο κοινό [20]. Πριν από την επιλογή ενός συγκεκριμένου προμηθευτή, οι οργανισμοί θα πρέπει να έχουν πλήρη γνώση των εκπαιδευτικών αναγκών τους και να είναι σε θέση να προσδιορίσουν αν το υλικό του υποψήφιου προμηθευτή ανταποκρίνεται στις ανάγκες τους.

γ) *Εφαρμογή προγράμματος επίγνωσης και εξάσκησης* (Implementing the Awareness and Training Program)

Η εφαρμογή ενός προγράμματος επίγνωσης και εξάσκησης θα πρέπει να γίνει μόνο όταν: α) έχει πραγματοποιηθεί η αξιολόγηση αναγκών, β) έχει αναπτυχθεί η στρατηγική, γ) έχει ολοκληρωθεί το σχέδιο εφαρμογής της στρατηγικής του προγράμματος και δ) έχει

αναπτυχθεί το υλικό επίγνωσης και εξάσκησης [20]. Η εφαρμογή του προγράμματος πρέπει να εξηγηθεί πλήρως στον οργανισμό.. Είναι βασικό όσοι σχετίζονται με την εφαρμογή του προγράμματος να κατανοούν τους ρόλους και τις ευθύνες τους. Επιπλέον, πρέπει να ανακοινώνονται τα προγράμματα και οι απαιτήσεις ολοκλήρωσης. Η επικοινωνία του σχεδίου μπορεί να χαρτογραφηθεί στα τρία μοντέλα εφαρμογής που αναφέρθηκαν στο πρώτο στάδιο.

Υπάρχουν αρκετές τεχνικές για να διαδοθεί το μήνυμα της επίγνωσης ασφάλειας σε έναν οργανισμό και βασίζονται στις πηγές και τη πολυπλοκότητα του μηνύματος. Οι τεχνικές που ένας οργανισμός μπορεί να εξετάσει περιλαμβάνουν:

- Μηνύματα σχετικά με τα εργαλεία επίγνωσης
- Αφίσες και λίστες
- Screensavers και προειδοποιητικά πανό
- Ενημερωτικά δελτία
- Μηνύματα ηλεκτρονικού ταχυδρομείου σε όλο τον οργανισμό
- Ενημερωτικά βίντεο
- Διαδικτυακά σεμινάρια
- Τηλεπικοινωνιακά σεμινάρια
- Προγράμματα επιβράβευσης κ.α.

Οι τεχνικές που υπάρχουν για τη διάδοση του υλικού εξάσκησης πρέπει να χρησιμοποιούν διάφορες τεχνολογίες με τα ακόλουθα χαρακτηριστικά: ευκολία στη χρήση, ευελιξία, ευθύνη και μια ευρεία βάση στήριξης της βιομηχανίας [20]. Κάποιες από τις πιο συχνές τεχνικές που μπορούν να χρησιμοποιήσουν οι οργανισμοί περιλαμβάνουν:

- Διαδραστική εκπαίδευση με βίντεο (Interactive video training- IVT)
- Διαδικτυακή εκπαίδευση (Web-based training)
- Όχι διαδικτυακή, αλλά βασισμένη σε υπολογιστή εκπαίδευση (Non-web, computer-based training)
- Επιτόπια εκπαίδευση υπό την καθοδήγηση εκπαιδευτών (Onsite, instructor-led training)

Ο συνδυασμός διαφορετικών τεχνικών διάδοσης της εξάσκησης μπορεί να λειτουργήσει αποτελεσματικά στη παρουσίαση του υλικού και στην διατήρηση της προσοχής του κοινού.

Το NIST ωστόσο, προτείνει και ένα τέταρτο στάδιο για τη δημιουργία προγραμμάτων επίγνωσης ασφάλειας και εξάσκησης, το οποίο ονομάζεται *«Μετά-υλοποίηση»* (Post-Implementation)

Ένα πρόγραμμα επίγνωσης ασφάλειας και εξάσκησης ενός οργανισμού μπορεί πολύ εύκολα να απαρχαιωθεί αν δεν δοθεί επαρκής προσοχή στις τεχνολογικές εξελίξεις, στις αλλαγές του οργανισμού και στις προτεραιότητες του οργανισμού [20]. Οι διαχειριστές των προγραμμάτων πρέπει να είναι ενημερωμένοι για αυτό το πιθανό πρόβλημα και να συμπεριλαμβάνουν μηχανισμούς στη στρατηγική τους για να βεβαιωθούν ότι το πρόγραμμα θα συνεχίσει να είναι σχετικό και ότι συμμορφώνεται με τους γενικούς κανόνες. Η συνεχής βελτίωση του προγράμματος είναι σημαντική για την επίτευξη του στόχου του.

Μόλις εφαρμοστεί το πρόγραμμα, είναι σημαντικό να παρακολουθούνται τα αποτελέσματα χρήσης του προγράμματος.. Ένα αυτοματοποιημένο σύστημα εντοπισμού μπορεί να σχεδιαστεί για να εντοπίζει βασικές πληροφορίες σχετικά με τη δραστηριότητα του προγράμματος. Στη συνέχεια, αυτό εξυπηρετεί την καταγραφή των αποτελεσμάτων χρήσης του προγράμματος με απώτερο στόχο τη βελτίωσή του.[20]. Οι απαιτήσεις για τη βάση δεδομένων θα πρέπει να ενσωματώνουν τις ανάγκες όλων των επιδιωκόμενων χρηστών. Οι χρήστες μιας τέτοιας βάσης δεδομένων μπορεί να είναι οι διοικητικοί υπάλληλοι της εταιρίας, οι διαχειριστές των προγραμμάτων ασφάλειας πληροφοριών, το τμήμα ανθρώπινου δυναμικού, το τμήμα εξάσκησης οργανισμού, οι λειτουργικοί διευθυντές, οι ελεγκτές και οι διευθυντές οικονομικών υπηρεσιών.

Οι επίσημοι μηχανισμοί αξιολόγησης και ανατροφοδότησης είναι κριτικά στοιχεία οποιουδήποτε προγράμματος επίγνωσης ασφάλειας, εξάσκησης και εκπαίδευσης. Η συνεχιζόμενη βελτίωση δεν είναι εφικτή χωρίς την γνώση λειτουργίας του υπάρχοντος προγράμματος. Επιπλέον, ο μηχανισμός ανατροφοδότησης πρέπει να σχεδιαστεί για την επίτευξη των στόχων που καθορίστηκαν αρχικά για το πρόγραμμα. Μόλις στερεωθούν οι βασικές απαιτήσεις, μπορεί να σχεδιαστεί και να εφαρμοστεί μια στρατηγική ανάδρασης. Μια στρατηγική ανατροφοδότησης πρέπει να ενσωματώνει στοιχεία που θα αφορούν την ποιότητα, το πεδίο εφαρμογής, τη μέθοδο ανάπτυξης, το επίπεδο δυσκολίας, την ευκολία χρήσης, τη διάρκεια της συνεδρίασης, τη συνάφεια, το νόμισμα και τις προτάσεις τροποποίησης [20]. Πολλές μέθοδοι μπορούν να εφαρμοστούν για να ζητήσουν ανατροφοδότηση. Οι πιο συνηθισμένες περιλαμβάνουν τα εξής:

- Έντυπα Αξιολόγησης / Ερωτηματολόγια (Evaluation Forms/ Questionnaires)
- Ομάδες εστίασης (Focus Groups)
- Επιλεγμένες συνεντεύξεις (Selective Interviews)
- Αυτόνομη παρατήρηση / Ανάλυση (Independent Observation / Analysis)
- Επίσημες αναφορές κατάστασης (Formal Status Report)

- Συγκριτική αξιολόγηση του προγράμματος ασφάλειας (Security Program Benchmarketing)

Είναι απαραίτητο να διασφαλιστεί ότι το πρόγραμμα, όπως έχει δομηθεί, συνεχίζει να ενημερώνεται, καθώς δημιουργείται νέα τεχνολογία και συναφή ζητήματα ασφάλειας. Οι ανάγκες εξάσκησης θα αλλάζουν, καθώς νέες ικανότητες και δεξιότητες γίνονται απαραίτητες για την ανταπόκριση στις νέες αρχιτεκτονικές και τεχνολογικές αλλαγές. Μια αλλαγή στην αποστολή ή στους στόχους του οργανισμού μπορεί να επηρεάσει ιδέες σχετικά με τον καλύτερο τρόπο σχεδιασμού χώρων εξάσκησης και περιεχομένου [20]. ,. Οι νέοι νόμοι και οι δικαστικές αποφάσεις ενδέχεται να επηρεάσουν την πολιτική του οργανισμού, η οποία με τη σειρά της μπορεί να επηρεάσει την ανάπτυξη ή την εφαρμογή υλικού επίγνωσης και εξάσκησης. Επίσης, καθώς οι οδηγίες ασφάλειας αλλάζουν ή ενημερώνονται, το υλικό επίγνωσης και εξάσκησης πρέπει να αντικατοπτρίζει αυτές τις αλλαγές.

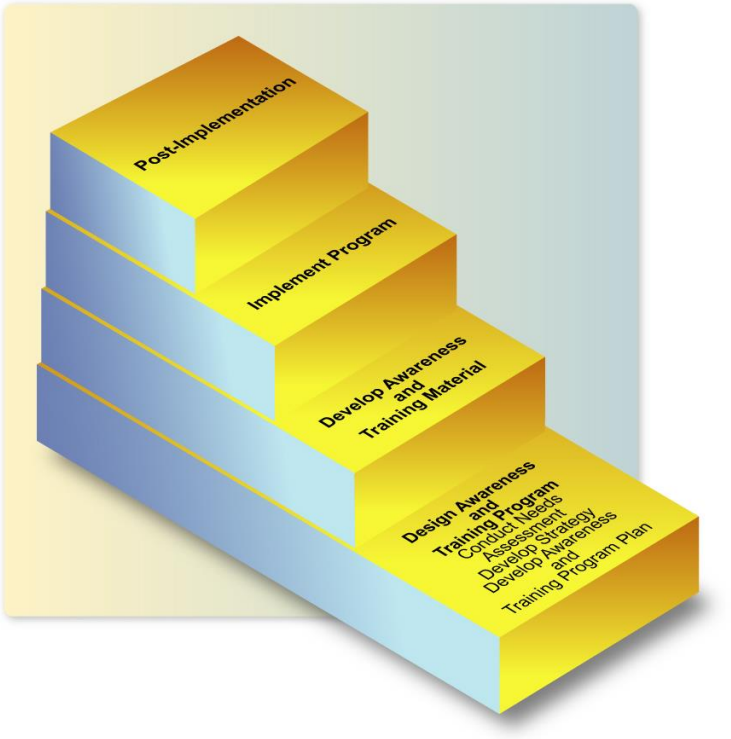
Στη συνέχεια, δίνεται έμφαση στη δημιουργία ενός επιπέδου επίγνωσης ασφάλειας, η οποία επιτυγχάνει μια διαδεδομένη παρουσία ασφαλείας στον οργανισμό. Οι διαδικασίες που παρέχουν επίγνωση, εξάσκηση και εκπαίδευση στο εργατικό δυναμικό θα πρέπει να ενσωματωθούν πλήρως στη συνολική επιχειρησιακή στρατηγική [20]. Ένα ώριμο πρόγραμμα επίγνωσης ασφάλειας και εξάσκησης καθορίζει ένα σύνολο μετρήσεων για αυτόν τον τομέα και θα πρέπει να υπάρχουν αυτοματοποιημένα συστήματα που θα υποστηρίζουν τη συλλογή ποσοτικών δεδομένων και την παροχή πληροφοριών διαχείρισης σε υπεύθυνους σε τακτικό, προκαθορισμένο κύκλο. Επίσης, οι οργανισμοί έχουν ενσωματώσει στο πρόγραμμα επίγνωσης και εξάσκησης τους επίσημους μηχανισμούς για συνεχή έρευνα στους τομείς της τεχνολογικής προόδου, των ορθών πρακτικών και των ευκαιριών συγκριτικής αξιολόγησης.

Τέλος, για να ολοκληρωθεί και το τέταρτο στάδιο πρέπει να εξεταστούν οι δείκτες επιτυχίας του προγράμματος. Οι διοικητικοί υπάλληλοι, οι επαγγελματίες και οι διαχειριστές του προγράμματος ασφάλειας πρέπει να είναι πρωτοπόροι υπέρ των συνεχών βελτιώσεων και να υποστηρίζουν το πρόγραμμα επίγνωσης ασφάλειας, εξάσκησης και εκπαίδευσης του οργανισμού. Είναι κρίσιμο ο καθένας να είναι ικανός και πρόθυμος να εκτελέσει τους καθορισμένους ρόλους ασφάλειάς του στον οργανισμό. Η εξασφάλιση της πληροφόρησης και της υποδομής ενός οργανισμού είναι μια ομαδική προσπάθεια. Παρακάτω παρατίθενται ορισμένοι βασικοί δείκτες για τη μέτρηση της υποστήριξης και της αποδοχής του προγράμματος:

- Επαρκής χρηματοδότηση για την εφαρμογή της συμφωνηθείσας στρατηγικής

- Κατάλληλη οργανωτική τοποθέτηση για να μπορέσουν όσοι έχουν βασικές ευθύνες να εφαρμόσουν αποτελεσματικά τη στρατηγική
- Υποστήριξη για ευρεία διανομή και δημοσίευση στοιχείων επίγνωσης ασφάλειας
- Εκτελεστικά / ανώτερα μηνύματα στο προσωπικό σχετικά με την ασφάλεια
- Χρήση μετρήσεων
- Οι διαχειριστές δεν χρησιμοποιούν την κατάστασή τους στον οργανισμό για να αποφύγουν τους ελέγχους ασφάλειας που ακολουθούνται συνεχώς από την τάξη και το αρχείο
- Επίπεδο συμμετοχής σε υποχρεωτικά φόρουμ / ενημερώσεις ασφαλείας
- Αναγνώριση των εισφορών ασφαλείας
- Τα κίνητρα αποδεικνύονται από εκείνους που παίζουν βασικούς ρόλους στη διαχείριση / συντονισμό του προγράμματος ασφαλείας

Το NIST [20], λοιπόν, προτείνει αυτά τα τέσσερα στάδια για τη δημιουργία προγραμμάτων επίγνωσης ασφάλειας και εξάσκησης. Στην εικόνα ;;;(αριθμός εικόνας) παρουσιάζονται συγκεντρωτικά τα στάδια αυτά, ξεκινώντας από το πρώτο στάδιο που βρίσκεται στην βάση της σκάλας, μέχρι το τέταρτο που βρίσκεται στην κορυφή.



Εικόνα:28 «Τα στάδια δημιουργίας προγραμμάτων επίγνωσης ασφάλειας και εξάσκησης», Wilson M. & Hash J. (2003, October), Building an Information Technology Security Awareness and Training Program, Computer Security Division Information Technology Laboratory , National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8933

3.2 Ζητήματα Ιδιωτικότητας (Privacy Awareness)

Εκτός από την εκπαίδευση των χρηστών σε θέματα ασφάλειας είναι σημαντικό να εκπαιδεύονται οι χρήστες και ως προς την προστασία της ιδιωτικότητας τους. Για να μπορέσει ένας χρήστης να προστατεύσει την ιδιωτικότητα του, θα πρέπει να είναι ενήμερος για τα εξής [22]:

- Αν λαμβάνουν άλλοι χρήστες τις πληροφορίες του,
- Πώς χρησιμοποιούνται αυτές οι πληροφορίες και
- Πώς η έκθεση αυτών των πληροφοριών μπορεί να βλάψει το άτομο που αφορούν οι πληροφορίες.

Ύστερα από τη βιβλιογραφική έρευνα που πραγματοποιήθηκε, διαπιστώθηκε ότι δεν έχουν δημιουργηθεί εκπαιδευτικά προγράμματα στον τομέα της ιδιωτικότητας.

Η ιδιωτικότητα ξεκίνησε να απασχολεί τους ανθρώπους από τον 19^{ο} αιώνα, όταν οι Warren και Brandeis [22] όρισαν την ιδιωτικότητα ως «*το δικαίωμα του να είναι κάποιος μόνος του*». Στις μέρες μας αυτός ο ορισμός παραφράστηκε ως «*το δικαίωμα του να επιλέγει κάποιος ποιες προσωπικές του πληροφορίες θα γίνονται γνωστές και σε ποια άτομα*». Κυρίως από το 1960 και μετά, λόγω κάποιων σοβαρών προβλημάτων που προκλήθηκαν, η ιδιωτικότητα έγινε ακόμα πιο σημαντικό θέμα, δημιουργώντας την ανάγκη θέσπισης νόμων για την προστασία της [22]. Με την πάροδο του χρόνου, ο κύριος στόχος της ιδιωτικότητας διαμορφώθηκε σύμφωνα με τις τεχνολογικές εξελίξεις. Έτσι, υπήρξε μια μετάβαση από την προστασία των ιδιωτικών μέσων (media privacy), στην χωρική ιδιωτικότητα (territorial privacy), έπειτα στην ιδιωτικότητα της επικοινωνίας (communication privacy), στην ατομική ιδιωτικότητα (bodily privacy), για να καταλήξει στην ιδιωτικότητα των πληροφοριών (information privacy) [22].

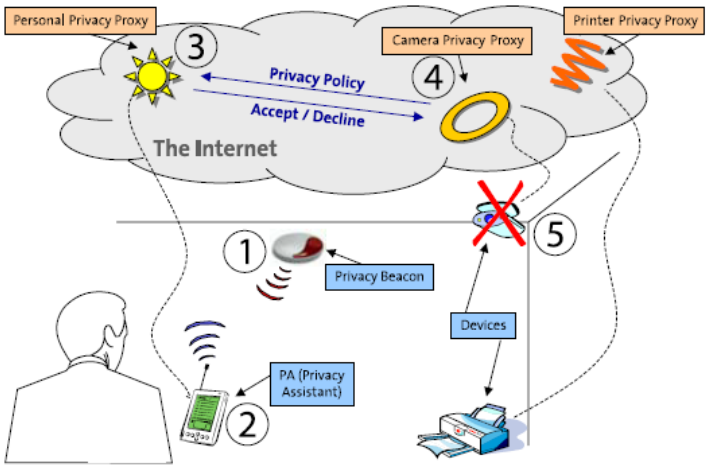
Ο Potzsch (2009) [5] ορίζει την επίγνωση ιδιωτικότητας ως τη γνώση του ατόμου για το ποιος, πότε, τι και το πώς οι προσωπικές του πληροφορίες σχετικά με τη δραστηριότητα του επεξεργάζονται και χρησιμοποιούνται. Η οπτική του στην επίγνωση ασφάλειας βοηθά στην παροχή ενός συνόλου δομών για τη δημιουργία ενός πλαισίου για το οποίο μπορεί να αξιολογηθεί η προσαρμοστική ιδιωτικότητα (adaptive privacy) [23].

Οι Featherman et al. (2010) [24], σε έρευνα τους εξηγούν τα ρίσκα της ιδιωτικότητας, κυρίως σε θέματα ηλεκτρονικών υπηρεσιών. Αναφέρουν ότι οι εκτιμήσεις των καταναλωτών και οι αποφάσεις τους για την πραγματοποίηση ηλεκτρονικών αγορών υλικών αγαθών, παραδοσιακών υπηρεσιών ή ηλεκτρονικών υπηρεσιών είναι καλύτερες, όταν λαμβάνουν υπόψη οι καταναλωτές τους κινδύνους. Η ιδιωτικότητα της πληροφορίας

έχει οριστεί ως «*ο ισχυρισμός των ατόμων να προσδιορίσουν τον εαυτό τους πότε, πώς και σε ποιο βαθμό οι πληροφορίες τους μεταδίδονται σε άλλους*» [24] και αποτελεί ένα σημαντικό ζήτημα για τους χρήστες. Οι έρευνες δείχνουν ότι η ανησυχία των χρηστών για την ιδιωτικότητά τους αυξάνεται, καθώς οι χρήστες ασχολούνται περισσότερο με το Διαδίκτυο[24]. Οι Featherman et al. (2010) [24] αναφέρουν ότι παρόλο που υπάρχουν αρκετοί ερευνητές, οι οποίοι έχουν ασχοληθεί με τις ανησυχίες και τα ρίσκα της ιδιωτικότητας, όπως οι Milne and Culnan (2004), Miyazaki and Krishnamurthy (2002), Phelps et al. (2000) και Wolfinbarger and Gilly (2003) [24] κανείς από αυτούς δεν έχει επικεντρωθεί συγκεκριμένα στα ρίσκα ασφάλειας ως προς τις ηλεκτρονικές υπηρεσίες. Υποστηρίζουν ότι μέσω της έρευνας των συστημάτων πληροφοριών, αναλύθηκαν οι κίνδυνοι της ιδιωτικότητας αλλά δεν μπορούν να βασιστούν εννοιολογικά στη θεωρία κινδύνου (risk theory). Οι Malhotra et al. (2004) [24] για παράδειγμα, επαναλαμβάνουν ότι οι χρήστες παίρνουν μεγάλο ρίσκο κατά την υποβολή των προσωπικών τους πληροφοριών, ενώ οι Suh and Han (2003) [24] τονίζουν ότι υπάρχει κίνδυνος υποκλοπής των πληροφοριών, της υπηρεσίας, καθώς και διαφθορά των δεδομένων.

Ο κίνδυνος της ιδιωτικότητας (privacy risk), είναι μια υποκειμενική εκτίμηση αξιολόγησης από το χρήστη. Ο χρήστης μπορεί να αξιολογήσει τον κίνδυνο ανάλογα με τις πιθανές απειλές στην ιδιωτικότητα των πληροφοριών της προσωπικής ταυτοποίησης. Σε αυτό συμπεριλαμβάνεται η αξιολόγηση της πιθανής κατάχρησης των πληροφοριών αυτών και αυτό μπορεί να οδηγήσει σε κλοπή της ταυτότητας [24]

Ο Langheinrich (2002) [25], παρουσίασε, όπως φαίνεται στην Εικόνα 29, ένα παράδειγμα ενός συστήματος επίγνωσης ιδιωτικότητας. Κατά την είσοδο σε περιβάλλον πανταχού παρόν υπολογιστή με πολλές διαθέσιμες υπηρεσίες, ένας φάρος ιδιωτικότητας (privacy beacon) ανακοινώνει τις συλλογές δεδομένων κάθε υπηρεσίας και των πολιτικών της, χρησιμοποιώντας ένα κανάλι ασύρματων επικοινωνιών, όπως Bluetooth ή IrDA. Για να γίνει αποθήκευση ενέργειας, ο κινητός βοηθός ιδιωτικότητας (privacy assistant) που έχει ο κάθε χρήστης, μεταφέρει τις πληροφορίες στο προσωπικό πολιτικό απόρρητο (privacy proxy) του χρήστη, το οποίο βρίσκεται κάπου στο Διαδίκτυο και αυτό με τη σειρά του επικοινωνεί με τους αντίστοιχους διακομιστές πληρεξούσιων με τις διαφημιζόμενες διευθύνσεις τους και εξετάζει τις πολιτικές απορρήτου (privacy policies). Μετά την σύγκριση αυτών των πολιτικών απορρήτου και με βάση τις προτιμήσεις ιδιωτικότητας των χρηστών, ο χρήστης αποφασίζει να αρνηθεί τη χρήση των υπηρεσιών εντοπισμού, το οποίο έχει ως αποτέλεσμα την απενεργοποίηση της υπηρεσίας εντοπισμού της θέσης μέσω της κάμερας της συσκευής [25].



Εικόνα 29: «Overview of the Privacy Management System», Langheinrich M. (2002), A Privacy Awareness System for Ubiquitous Computing Environments, Switzerland: Institute of Information Systems, International conference on Ubiquitous Computing

Κατά το σχεδιασμό της αρχιτεκτονικής τέτοιων συστημάτων επίγνωσης ιδιωτικότητας, εφαρμόζονται έξι αρχές που πρέπει να ισχύσουν εξαρχής για τη διατήρηση της ιδιωτικότητας στους πανταχού παρόν υπολογιστές (ubiquitous computing). Οι αρχές αυτές είναι: ειδοποίηση (notice), επιλογή και συγκατάθεση (choice and consent), εγγύτητα και τοπικότητα (proximity and locality), ανωνυμία και ψευδωνυμία (anonymity and pseudonymity), ασφάλεια (security) και πρόσβαση (access) και προσφυγή (recourse). Η ανωνυμία και η ψευδωνυμία είναι χρήσιμες απαιτήσεις όταν είναι ένα υποστηρικτικό μέρος της υποδομής αλλά δε θα πρέπει να θεωρούνται ως ξεχωριστές λύσεις. Συνεπώς, το σύστημα χρησιμοποιεί ανώνυμες και ασφαλείς συνδέσεις, όπως και λογικό έλεγχο πρόσβασης, όταν είναι δυνατόν να γίνει αποτροπή ανεπιθύμητων δεδομένων [25]. Σε αυτό το πρόγραμμα όμως, η προσοχή επικεντρώνεται στις τέσσερις άλλες αρχές για τη χρήση τους σε περιβάλλοντα πανταχού παρόν υπολογιστών:

- Ειδοποίηση (Notice): Σε ένα περιβάλλον πανταχού παρόν υπολογιστή είναι συχνά δύσκολο για τα υποκείμενα δεδομένων να αναγνωρίσουν ότι γίνεται συλλογή των δεδομένων. Σε τέτοιες περιπτώσεις δεν χρειάζονται μηχανισμοί για τη δήλωση πρακτικών συλλογής αλλά και αποτελεσματικών τρόπων επικοινωνίας τους με τον χρήστη.
- Επιλογή και συγκατάθεση (Choice and consent): Για να δοθεί στο χρήστη η επιλογή, πρέπει να του παρέχονται μηχανισμοί επιλογής, έτσι ώστε να μπορεί να υποδεικνύει ποιες υπηρεσίες προτιμά.

- Εγγύτητα και τοπικότητα (Proximity and locality): Το σύστημα πρέπει να υποστηρίζει μηχανισμούς για την κωδικοποίηση και τη χρήση της τοπικότητας των πληροφοριών (locality information), για τη συλλογή δεδομένων, τα οποία μπορούν να επιβάλλουν περιορισμούς πρόσβασης με βάση την τοποθεσία του ατόμου που θέλει να χρησιμοποιήσει τα δεδομένα.
- Πρόσβαση και προσφυγή (Access and recourse): Το σύστημα πρέπει να παρέχει έναν τρόπο στο χρήστη να έχει πρόσβαση στις προσωπικές του πληροφορίες με έναν απλό τρόπο μέσω τυποποιημένων διεπαφών. Ο χρήστης θα πρέπει να πληροφορείται σχετικά με τη χρήση των δεδομένων του, μόλις αποθηκευτούν, όπως γίνεται και με τις λίστες κλήσεων που αποτελούν συχνά μέρος των μηνιαίων τηλεφωνικών λογαριασμών [25].

Παρά το γεγονός ότι η προστασία της ιδιωτικότητας είναι ένα σημαντικό ζήτημα, δεν έχει πραγματοποιηθεί αρκετή έρευνα σε αυτό το θέμα. Γι' αυτό παρατηρείται η ανάγκη περαιτέρω αναζήτησης και έρευνας για να δοθούν περισσότερες επιλογές και λύσεις αναφορικά με το συγκεκριμένο ζήτημα.

Κεφάλαιο 4ο: Εξοικείωση σε ζητήματα ασφάλειας και ιδιωτικότητας μέσω της παιγνιοποίησης

Στο κεφάλαιο αυτό, αναλύεται η χρήση της παιγνιοποίησης για την επίγνωση της ασφάλειας και της ιδιωτικότητας. Αναφορικά με ζητήματα ιδιωτικότητας δεν υπάρχει σχετική βιβλιογραφία. Επομένως, δίνεται έμφαση στον τομέα της ασφάλειας, έτσι ώστε να αναλυθεί η υπάρχουσα βιβλιογραφία και να προωθηθεί η ανάγκη για περισσότερη μελέτη πάνω στο θέμα της ιδιωτικότητας . Παρουσιάζεται η χρησιμότητα της παιγνιοποίησης στα ζητήματα ασφάλειας και πώς αυτή μπορεί να αξιοποιηθεί για να βελτιωθούν οι γνώσεις των ατόμων σε σχέση με θέματα ασφάλειας.

Κατά την διάρκεια της έρευνας, παρατηρήθηκε το γεγονός ότι παρόλο που υπάρχουν προγράμματα που σχετίζονται με την επίγνωση ασφάλειας και ιδιωτικότητας, πολλά από αυτά δεν πετυχαίνουν το στόχο τους. Αυτό οφείλεται στο ότι τα προγράμματα αυτά δεν είναι ελκυστικά προς το χρήστη, καθώς οι δημιουργοί τους επικεντρώνονται στο στόχο της επίγνωσης και εκπαίδευσης σε θέματα ασφάλειας και ιδιωτικότητας και δεν δίνουν σημασία στο κατά πόσο φαίνονται ελκυστικά αυτά τα προγράμματα προς τη χρήση τους. Ένας τρόπος επίλυσης αυτού του προβλήματος είναι η εφαρμογή της παιγνιοποίησης στα εν λόγω προγράμματα. Μέσω της παιγνιοποίησης, τα προγράμματα επίγνωσης ασφάλειας και ιδιωτικότητας μπορούν να αποκτήσουν περισσότερο ενδιαφέρον, έτσι ώστε ο χρήστης να τα αντιμετωπίζει ως κάτι το διασκεδαστικό και όχι ως κάτι που είναι υποχρεωμένος να κάνει. Με τη χρήση των παιγνιωδών στοιχείων, το πρόγραμμα αποκτά μια διασκεδαστική διάσταση και ο χρήστης μπορεί εύκολα να κατανοήσει το περιεχόμενο του.

Η ιδέα της χρήσης παιγνιοποίησης σε προγράμματα επίγνωσης ασφάλειας και εκπαίδευσης δεν είναι κάτι το εξωπραγματικό. Στη συνέχεια παρουσιάζεται μια βιβλιογραφική ανασκόπηση αναφορικά με την παιγνιοποίηση και τη ασφάλεια συστημάτων. Οι Thornton και Francia (2014) [26,27] παρουσίασαν μια έρευνα σε ένα «παιχνίδι πύργου άμυνας» (tower defense game), το οποίο στοχεύει στη διδασκαλία των μαθητών σχετικά με την ισχύ του κωδικού πρόσβασης. Παρόλα αυτά, δεν είναι ξεκάθαρο το ποιες πτυχές της παιγνιοποίησης χρησιμοποιήθηκαν στο παιχνίδι.

Οι Baxter et al. (2015) [26] παρουσίασαν μια έρευνα, όπου χρησιμοποιεί στοιχεία, όπως η ιστορία ενός παιχνιδιού, οι στόχοι των υπαλλήλων, η ανατροφοδότηση και η πρόοδος. Οι συγγραφείς αναγνωρίζουν ότι οι λύσεις τους έχουν έλλειψη σε άλλες τεχνικές παιγνιοποίησης όπως ο ανταγωνισμός με βάση τα σημεία και τις κατατάξεις, τα επιτεύγματα, τα επίπεδα ή τα εικονικά νομίσματα. Η ιστορία του παιχνιδιού σχετίζεται με

μια έρευνα που αφορά στην παραβίαση της ασφάλειας της παγκόσμιας τράπεζας, συνεπώς την παραβίαση των δεδομένων των πολιτών. Με την έρευνα αυτή αξιολογήθηκε η αποτελεσματικότητα της λύσης με δύο διαφορετικά πειράματα. Πρώτα, αξιολογήθηκε ο τρόπος με τον οποίο η λύση βαθμολογήθηκε χωρίς εκπαίδευση για να αναγνωριστεί αν η παιγνιώδης εκπαίδευση είναι καλύτερη από την παραδοσιακή εκπαίδευση. Τα αποτελέσματα έδειξαν ότι η παιγνιώδης εκπαίδευση είναι καλύτερη από την έλλειψη εκπαίδευσης, αλλά λιγότερο αποτελεσματική από την παραδοσιακή εκπαίδευση. Σε δεύτερο πείραμα, χρησιμοποιήθηκε ένας μεγαλύτερος αριθμός δείγματος για να παρατηρηθεί η διαφορά ανάμεσα στην παιγνιώδη εκπαίδευση και στην έλλειψη εκπαίδευσης. Τα αποτελέσματα έδειξαν ότι η παιγνιώδης εκπαίδευση δεν βελτίωσε την απόκτηση γνώσης [26]. Και στα δύο πειράματα, οι χρήστες που χρησιμοποίησαν την παιγνιοποίηση βαθμολόγησαν την εκπαίδευση ως πιο ευχάριστη, πιο διασκεδαστική και λιγότερο βαρετή σε σχέση με αυτούς που χρησιμοποίησαν την παραδοσιακή εκπαίδευση. Οι συγγραφείς αναγνωρίζουν δυο βασικούς περιορισμούς στην έρευνα τους. Αρχικά, όπως ήδη αναφέρθηκε, η χρήση της παιγνιοποίησης είχε έλλειψη κάποιων στοιχείων, τα οποία θα μπορούσαν να έχουν καθοριστικό ρόλο στο συνολικό αποτέλεσμα. Δεύτερον, η περίοδος εκπαίδευσης ήταν μικρή σε έκταση και για αυτό δεν μπορούν να αξιολογηθούν μακροπρόθεσμα τα αποτελέσματα.

Αρκετές άλλες έρευνες έχουν προσπαθήσει να αξιολογήσουν την αποτελεσματικότητα της παιγνιοποίησης. Οι Hamari et al. (2014) [26] συνέθεσαν μια ανασκόπηση από 24 εμπειρικές μελέτες για να ερευνήσουν πώς λειτουργεί η παιγνιοποίηση. Το αποτέλεσμα ήταν ότι η παιγνιοποίηση έχει συνεισφέρει θετικά στη βελτίωση της εκπαίδευσης σε πολλαπλές περιπτώσεις. Ωστόσο, τονίστηκε ότι τα αποτελέσματα εξαρτώνται από τους χρήστες και το περιεχόμενο, στο οποίο εφαρμόζονται οι τεχνικές. Σημειώθηκε, επίσης, ότι υπάρχουν ελάχιστες υψηλής ποιότητας έρευνες αναφορικά με τα πραγματικά αποτελέσματα της παιγνιοποίησης.

Οι Gjertsen, Gjaere et al. (2017) [26,28] στην έρευνά τους μελέτησαν τη χρήστη της παιγνιοποίησης σε προγράμματα επίγνωσης ασφάλειας και εκπαίδευσης. Με βάση τις ενδείξεις ότι τα υπάρχοντα προγράμματα επίγνωσης ασφάλειας δεν είναι επιτυχημένα στο να παρέχουν στους υπαλλήλους τις απαραίτητες γνώσεις, συντάχθηκε ένα εναλλακτικό σενάριο και αναπτύχθηκε ένα πρωτότυπο. Για να διερευνηθεί η καταλληλότητα του πρωτοτύπου αυτού, συλλέχθηκαν ποιοτικά δεδομένα μέσω συνεντεύξεων με ειδικούς στην ασφάλεια και μέσω εργαστηρίων με ομάδες χρηστών. Κατά τη διάρκεια της έρευνας, ανακαλύφθηκε ότι πολλά από τα προβλήματα των προγραμμάτων επίγνωσης ασφάλειας

και εκπαίδευσης είναι προβλήματα, τα οποία προορίζονται να λυθούν μέσω της παιγνιοποίησης [26]. Η διαδικασία σχεδιασμού της παιγνιοποίησης έχει ως στόχο το χρήστη. Βρέθηκαν τέσσερις λόγοι για αυτό, μέσω των στόχων που συμφωνήθηκαν ως κοινοί μεταξύ εργοδοτών και εργαζομένων. Είναι σημαντικό τα προγράμματα να κατασκευάζονται για να εκπληρώσουν αυτούς τους στόχους. Ένα βασικό ερώτημα είναι το τι οδηγεί την εμπλοκή των εργαζομένων με θέματα ασφάλειας. Οι συγγραφείς βρήκαν ότι η γνώση και η εξέλιξη είναι οι δύο πιο σημαντικοί κινητήριοι παράγοντες. Επιπρόσθετα, όσο περισσότερο αυτό-καθορισμένη είναι η εκπαίδευση, τόσο πιο κινητήρια θα είναι. Όταν ο σκοπός η εκπαίδευση όλων των χρηστών, είναι σημαντικό να χρησιμοποιηθεί ο ανταγωνισμός σε συσχέτιση με την εξωτερική επιβράβευση. Η παιγνιοποίηση έχει περαιτέρω δυνατότητες να παραδώσει εξατομικευμένο περιεχόμενο στους χρήστες με βάση τις ικανότητες τους και το ρόλο τους στην εταιρία. Το πρωτότυπο που δημιούργησαν βασίστηκε στο ότι τα υπάρχοντα μαθήματα ήταν πολύ μεγάλα σε διάρκεια [26]. Μια σημαντική πτυχή που πρέπει να λαμβάνεται υπόψη είναι η χρήση μικρών, συνοπτικών εργασιών, κατά τη διάρκεια ενός διαδικτυακού μαθήματος. Έχει παρατηρηθεί ότι αυτό το χαρακτηριστικό μπορεί να έχει δύο σημαντικά αποτελέσματα. Πρώτον, μπορεί να παρέχει στους χρήστες μια αίσθηση αυτονομίας σχετικά με την εκπαίδευση και δεύτερον, βελτιώνει τα μαθησιακά αποτελέσματα λόγω του αποτελέσματος της απόστασης.

Τελικά, ο συνολικός σκοπός ενός προγράμματος επίγνωσης ασφάλειας και εκπαίδευσης είναι να δημιουργήσει μια καλή συμπεριφορά ασφάλειας ανάμεσα στους υπαλλήλους [26]. Υπάρχουν συγκεκριμένα πράγματα, τα οποία κάνουν οι υπάλληλοι, επειδή ακολουθούν κάποιες κοινωνικές νόρμες και τις προσδοκίες του οργανισμού σε σχέση με τη συμπεριφορά τους. Ωστόσο, η διείσδυση στην εταιρική κουλτούρα και η δημιουργία νέων κοινωνικών νορμών δεν είναι ένα ασήμαντο έργο.

Οι Thornton David και Francia (2014) [27], παρουσίασαν τα αποτελέσματα ενός πρότζεκτ που αφορούσε στην εκπαίδευση σε ζητήματα ασφάλειας μέσω της παιγνιοποίησης. Μελέτησαν την επίδραση της ανάπτυξης παιχνιδιών στους καθηγητές και στους μαθητές με βάση το πρόγραμμα σπουδών. Τα αποτελέσματα έδειξαν την ενθάρρυνση για την αξιοποίηση της παιγνιοποίησης στο πρόγραμμα σπουδών. Συμπληρωματικά, περιέγραψαν κάποια γενικού σκοπού εργαλεία παιγνιοποίησης για τη χρήση σε αίθουσες διδασκαλίας. Η συμπεριφορά των μαθητών ήταν θετική απέναντι σε αυτά τα εργαλεία και βελτιώθηκε η παρουσία των μαθητών.

Ο Wood (2014) [29] υποστηρίζει ότι το να πείσει κάποιος τους υπαλλήλους μιας εταιρείας να πάρουν σοβαρά την ασφάλεια όταν δεν είναι η δουλεία τους είναι μια

πρόκληση που μπορεί να αντιμετωπιστεί με τη βοήθεια της παιγνιοποίησης. Τα στοιχεία που μοιάζουν με το παιχνίδι μπορούν να χρησιμοποιηθούν για τη βελτίωση της συνειδητοποίησης της ασφάλειας και την τροποποίηση της συμπεριφοράς των χρηστών. Σε αυτή την περίπτωση, λοιπόν, παιγνιοποίηση σημαίνει επιβράβευση των υπαλλήλων με πόντους, όταν κάνουν κάτι σωστά, με διάφορες μορφές αναγνώρισης, συμπεριλαμβανομένων των βραβείων και ενός συγκεντρωτικού πίνακα με τις βαθμολογίες των συμμετεχόντων. Οι συμμετέχοντες στο πρόγραμμά είχαν 50% λιγότερες πιθανότητες να κάνουν κλικ σε ένα σύνδεσμο ηλεκτρονικού "ψαρέματος" (phishing) και το 82% πιθανότερο να αναφέρουν ένα μήνυμα ηλεκτρονικού "ψαρέματος" (phishing email) [29]. Οι συμπεριφορές που σχετίζονται με την ασφάλεια και επιβραβεύονται από τέτοια προγράμματα, περιλαμβάνουν την αναφορά e-mail ψαρέματος, την αποτροπή ή αναφορά πίσω πορτών ή άλλων αποπειρών εισβολής, την αναφορά σε περίπτωση που βρεθεί κάποιο USB μνήμη, κρατώντας το λογισμικό της επιφάνειας εργασίας του υπολογιστή κατάλληλα ενημερωμένο, τη διατήρηση ενός δυνατού κωδικού πρόσβασης, την παρουσία σε σεμινάρια ασφάλειας, το να μην αφήνει κάποιος το λάπτοπ του στο αυτοκίνητο και την αναφορά ευπαθειών. Παρόλα αυτά η παιγνιοποίηση δεν είναι ένας όρος που έχει εισέλθει ευρέως στον κόσμο των επιχειρήσεων [29]. Η εφαρμογή παιγνιωδών προγραμμάτων στον εργασιακό χώρο θεωρείται λανθασμένα μια ψυχαγωγική δραστηριότητα. Το γεγονός αυτό αποτρέπει τη χρήση τέτοιων προγραμμάτων, ενώ την ίδια στιγμή μη παιγνιώδη προγράμματα εκπαίδευσης σε ζητήματα ασφάλειας κρίνονται απαραίτητα για την αύξηση των γνώσεων των εργαζομένων αναφορικά με τέτοια ζητήματα. Πριν από την εκπαίδευση στην ασφάλεια, το 30% έως το 60% των χρηστών θα πέσουν θύματα ενός ψεύτικου ηλεκτρονικού ταχυδρομείου ηλεκτρονικού "ψαρέματος". Μετά την προπόνηση και έξι μηνών έως ένα έτος ενός παιγνιώδους προγράμματος, το ποσοστό μπορεί να μειωθεί στο 5% [29]. .

4.1 Παραδείγματα παιγνιωδών εφαρμογών σε ζητήματα ασφάλειας

Ένα παράδειγμα εφαρμογής για ζητήματα επίγνωσης ασφάλειας με παιγνιοποίηση είναι το Game of Threats [30]. Η εταιρία PwC δημιούργησε αυτό το ψηφιακό παιχνίδι, το οποίο σχεδιάστηκε για να προσομοιάσει την ταχύτητα και την πολυπλοκότητα μιας πραγματικής διαδικτυακής παραβίασης. Η λύση περιλαμβάνει στοιχεία παιγνιοποίησης και τη θεωρία του παιχνιδιού για να παρέχει μια διαδραστική εμπειρία στο χρήστη, όπου η ομάδα του προσπαθεί να υπερασπιστεί τον εαυτό της από μια ομάδα απειλών, η οποία επίσης παίζεται από άλλους χρήστες. Το περιβάλλον του παιχνιδιού δημιουργεί μια ρεαλιστική

εμπειρία, στην οποία και οι δύο πλευρές πρέπει να παίρνουν γρήγορες και σημαντικές αποφάσεις με τις ελάχιστες πληροφορίες που μπορεί να διαθέτουν. Στον πυρήνα του, το Game of Threats [30], είναι ένα παιχνίδι δημιουργίας κριτικών αποφάσεων, που σχεδιάστηκε για να επιβραβεύει τους παίχτες με τις καλύτερες αποφάσεις, ενώ τιμωρεί τις ομάδες που παίρνουν ανεπαρκείς αποφάσεις. Οι παίχτες μπορούν να αποκομίσουν από το παιχνίδι μια καλύτερη κατανόηση των βημάτων που χρειάζεται να γίνουν για την βελτίωση της ασφάλειας της εταιρίας τους.

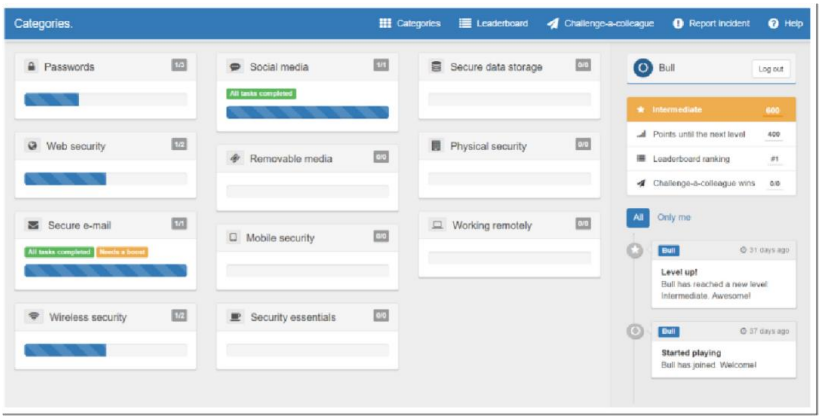
Εικόνα 30: «Game of Threats», Διαθέσιμο σε:: …https://www.afr.com/content/dam/images/g/n/c/4/6/9/image.imgtype.afrArticleInline.620x0.png/1457304468733.jpg

Ουσιαστικά, το Game of Threats [30] δημιουργήθηκε για να δώσει μια μοναδική εμπειρία, επιτρέποντας στο χρήστη να αισθανθεί πίεση μέσω των γρήγορων αποφάσεων που πρέπει να πάρει και να δει πιθανές συνέπειες των πράξεων του σε πραγματικό χρόνο. Το παιχνίδι αναγκάζει τους παίχτες να αποφασίσουν σχετικά με το πώς θα επιτεθούν και πώς θα προστατευθούν, ανάλογα με την ομάδα στην οποία συμμετέχουν. Επίσης, τους παρέχονται περιορισμένες πληροφορίες και πρέπει να εξισορροπήσουν τις ικανότητές τους και να ανταποκριθούν στις ενέργειες και τα σχέδια των άλλων ομάδων. Οι συντονιστές της PwC [30] έχουν έναν άμεσο διάλογο με τους χρήστες, παρακολουθούν τις επιλογές τους κατά τη διάρκεια του παιχνιδιού και παρέχουν επιτόπου σχόλια σχετικά με τη στρατηγική και τη λήψη αποφάσεών τους. Η προσέγγιση αυτή αυξάνει τον αντίκτυπο των χρηστών σε σχέση με την επίγνωση ασφάλειας μέσω της ανατροφοδότησης σε πραγματικό χρόνο ανάλογα με τις ενέργειές τους. Επίσης, γίνεται συζήτηση σχετικά με τις εναλλακτικές απαντήσεις και τα πιθανά αποτελέσματα των χρηστών.

Επιπλέον, η εταιρία Cyber Security Challenge UK [31], δημιούργησε μια σειρά από εθνικούς διαγωνισμούς, εκπαιδευτικά προγράμματα και πρωτοβουλίες δικτύωσης

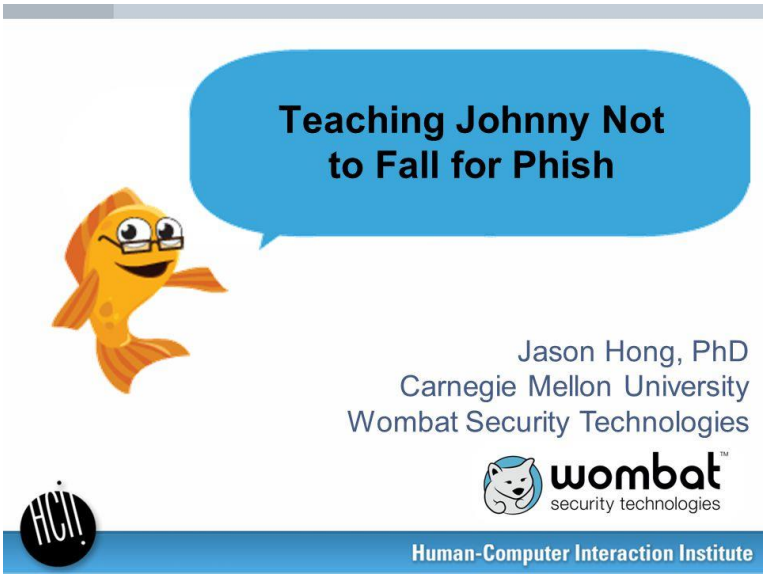
σχεδιασμένα να αναγνωρίζονται, να εμπνέουν και να ευαισθητοποιούν περισσότερους ανθρώπους να γίνουν επαγγελματίες σε ζητήματα ασφάλειας στο διαδίκτυο. Ιδρύθηκε για να ενισχύσει την εθνική δεξαμενή δεξιοτήτων στον κυβερνοχώρο και προσφέρει ένα μοναδικό πρόγραμμα δραστηριοτήτων για την εισαγωγή επαρκούς αριθμού κατάλληλα εξειδικευμένων ατόμων σε ευκαιρίες μάθησης και σταδιοδρομίας στο επάγγελμα. Οι διαγωνισμοί δοκιμάζουν διαφορετικές ικανότητες ανάλογα με το ηλικιακό γκρουπ του ατόμου. Το κύριο πρόγραμμα διαγωνισμών περιλαμβάνει διαδικτυακούς προκριματικούς και ημιτελικούς που κορυφώνονται στον ετήσιο τελικό του Masterclass.

Ένα παράδειγμα δημιουργίας ενός παιγνιώδους προγράμματος για εξοικείωση και εξάσκηση σε θέματα ασφαλείας σχεδιάστηκε στο πλαίσιο μιας μεταπτυχιακής διατριβής [34]. Το συγκεκριμένο πρόγραμμα περιέχει κατηγορίες θεμάτων σχετικών με την ασφάλεια, όπως κωδικοί πρόσβασης, ασφάλεια στο Διαδίκτυο κλπ. Επιλέγοντας μία κατηγορία, ο χρήστης απαντά σε σχετικές ερωτήσεις. Ανάλογα με τις σωστές ή λάθος απαντήσεις συγκεντρώνει τους αντίστοιχους πόντους. Συγκεντρώνοντας περισσότερους πόντους, μπορεί να ανέβει επίπεδο που περιέχει πιο εξειδικευμένες ερωτήσεις. Ο χρήστης μπορεί να δει τον αριθμό των χρηστών που βρίσκονται στο ίδιο επίπεδο, το βαθμό δυσκολίας και την περιγραφή της κατηγορίας. Μία επιπλέον ιδέα είναι να μπορεί ένας χρήστης να προκαλέσει έναν άλλον, ώστε να «μονομαχήσουν» και να αναδειχθεί ο νικητής. Με τη δημιουργία αντίστοιχων προγραμμάτων οι χρήστες εκπαιδεύονται μέσω ενός πιο ψυχαγωγικού τρόπου. Μία παιγνιώδη εφαρμογή εκπαίδευσης έχει περισσότερες πιθανότητες χρήσης από ένα άλλου είδους εκπαιδευτικό πρόγραμμα [34]. Η Στην εικόνα (αριθμο) απεικονίζεται η αρχική σελίδα του προγράμματος.



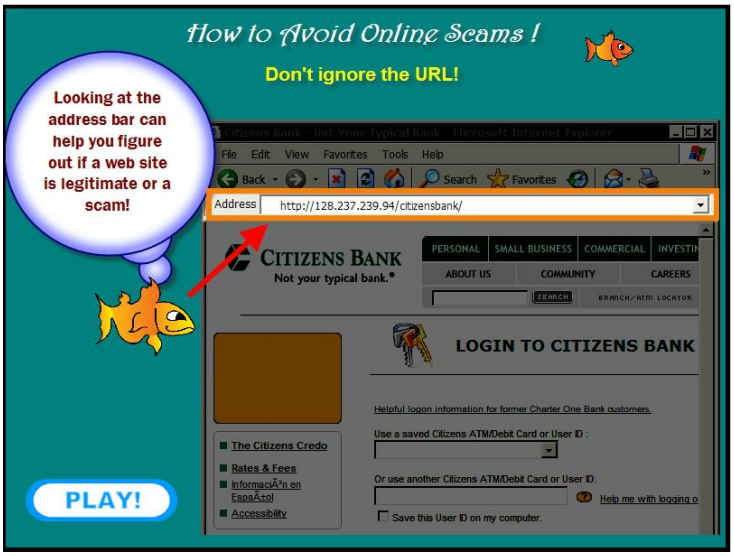
Εικόνα 31. «A Gamified Security Awareness and Training Program» Gjertsen B E. G., (2016), "Use of Gamification in Security Awareness and Training Programs", Norwegian University of Science and Technology.

Ένα άλλο παράδειγμα από την εταιρία Wombat Security [32] αφορά στη δημιουργία μαθημάτων εκπαίδευσης επίγνωσης ασφάλειας, όπως απεικονίζεται και στην εικόνα 32 και 33. Τα Security Awareness Training Modules στοχεύουν στην εκπαίδευση των υπαλλήλων, ώστε να αντιμετωπίζουν σωστά τις απειλές σε θέματα ασφάλειας. Η προσέγγιση της εταιρίας στην ανάπτυξη και το σχεδιασμό της επίγνωσης χρησιμοποιεί τις αρχές μάθησης και μεθόδους που αποδείχθηκαν πιο αποτελεσματικές από τις παρουσιάσεις και τα βίντεο επίγνωσης. Οι τεχνικές παιγνιοποίησης και τα διαδραστικά στοιχεία εισάγουν τους χρήστες, μέσω των αποφάσεων που παίρνουν, στη βελτίωση της γνώσης, τους καθώς επίσης και στη διατήρηση της αλλαγής συμπεριφοράς τους σε ζητήματα ασφάλειας.



Εικόνα 32: «Security Awareness Training Modules», Wombat Security, http://images.slideplayer.com/16/4970161/slides/slide_1.jpg

Επιπροσθέτων, το Anti-Phishing Phil [33] αναπτύχθηκε από την CMU Usable Privacy and Security Laboratory στο πανεπιστήμιο Carnegie Mellon. Έχει ως στόχο να εκπαιδεύσει το χρήστη στη προστασία από κακόβουλες ιστοσελίδες. Το περιβάλλον του παιχνιδιού βρίσκεται στο βυθό της θάλασσας όπου ο χρήστης ως το μικρό ψάρι, ο Phil, πρέπει να βρει ποια από τα δολώματα – ιστοσελίδες είναι ασφαλή και ποια όχι. Το παιχνίδι είναι απλό στη χρήση και απευθύνεται σε διάφορες ηλικίες.



*Εικόνα 33: «Anti-Phishing Phil»,*Διαθέσιμο σε: https://www.ucl.ac.uk/cert/antiphishing/

4.2 Παραδείγματα παιγνιωδών εφαρμογών σε ζητήματα ιδιωτικότητας

Όπως αναφέρθηκε στον τομέα των ζητημάτων επίγνωσης της ιδιωτικότητας δεν υπάρχει διαθέσιμη βιβλιογραφία. Ωστόσο, το 2011 το Κέντρο για τη Δημοκρατία και τη Τεχνολογία (Center for Democracy & Technology) [34] κοινοποίησε ένα άρθρο σχετικά με μια εφαρμογή. Η εφαρμογή αυτή δημιουργήθηκε από τον προγραμματιστή παιχνιδιών Zynga και στοχεύει στην πολιτική απορρήτου. Το PrivacyVille (Εικόνα 34) αρχικά αποτελούσε τη μορφή ενός κειμένου, το οποίο στη συνέχεια έγινε παιχνίδι όπου το μόνο που χρειάζεται να κάνει ο χρήστης είναι κλικ με το ποντίκι του υπολογιστή του. Οι παίχτες έρχονται αντιμέτωποι με θέματα όπως οι κωδικοί ασφάλειας, οι διαφημίσεις, η κοινοποίηση, η αποθήκευση και η ασφάλεια. Η εφαρμογή συνδέεται επίσης, και με άλλες ιστοσελίδες οι οποίες είναι χρήσιμες για τους χρήστες. Με την ολοκλήρωση του παιχνιδιού, υπάρχει ένα κουίζ ερωτήσεων, οι οποίες σχετίζονται με τα θέματα που έμαθε ο χρήστης από την εφαρμογή. Η υψηλή βαθμολογία ανταμείβεται. Το PrivacyVille χρησιμοποιεί μια εύκολα κατανοητή γλώσσα, κάτι το οποίο είναι πολύ βασικό καθώς έρευνες έχουν δείξει ότι η πλειοψηφία των πολιτικών απορρήτου απαιτούν 14 χρόνια εκπαίδευσης για να γίνουν κατανοητές. Η εφαρμογή είναι εύκολη στην ανάγνωση και δεν χρειάζεται περισσότερο από 15 λεπτά για να ολοκληρωθούν τα βήματά της.

Εικόνα 34: «PrivacyVille», Διαθέσιμο σε: https://www.digitaltrends.com/wp-content/uploads/2011/07/zynga-privacyville-game.jpg

Στο σημείο αυτό παρατηρείται η ανάγκη για περισσότερη έρευνα σε θέματα ιδιωτικότητας, καθώς και η ανάγκη δημιουργίας εφαρμογών αναφορικά με στην επίγνωση της ιδιωτικότητας.

Κεφάλαιο 5ο: Συμπεράσματα

Η χρήση του Διαδικτύου έχει γίνει ένα αναπόσπαστο κομμάτι της καθημερινότητας του ανθρώπου. Το γεγονός αυτό δημιουργεί την ανάγκη να γνωρίζει ο χρήστης τους κινδύνους που διατρέχει ως προς την ασφάλεια και την ιδιωτικότητά του. Για να επιτευχθεί αυτό, χρειάζεται να δημιουργηθούν κάποια προγράμματα εκπαίδευσης σε ζητήματα ασφάλειας και ιδιωτικότητας. Μέσω των προγραμμάτων αυτών, ο χρήστης θα μπορέσει να γνωρίσει τις ανάγκες που υπάρχουν σε αυτά τα θέματα, καθώς και να εκπαιδευτεί κατάλληλα, έτσι ώστε να μπορεί να προστατέψει την ασφάλεια και την ιδιωτικότητά του κατά τη χρήση των πληροφοριακών συστημάτων. Για να γίνουν όμως αυτά τα προγράμματα πιο διασκεδαστικά και ελκυστικά προς το χρήστη, είναι απαραίτητη η χρήση της παιγνιοποίησης. Μέσω αυτής της μεθόδου δημιουργούνται προγράμματα που παρέχουν πιο ελκυστικά και εκπαιδευτικά περιβάλλοντα. Επιπλέον, οι χρήστες εκπαιδεύονται μέσω ενός πιο ψυχαγωγικού τρόπου, χωρίς να επιβαρύνουν την καθημερινότητά τους με επιπλέον δραστηριότητες που δεν έχουν κάποιο ενδιαφέρον για τους ίδιους.

Στην εργασία αυτή, λοιπόν, πραγματοποιήθηκε μια βιβλιογραφική ανασκόπηση σχετικά με τη χρήση της παιγνιοποίησης σε ζητήματα επίγνωσης ασφάλειας και ιδιωτικότητας. Αρχικά, αναλύθηκαν οι υπάρχοντες ορισμοί ως προς την έννοια της παιγνιοποίησης, καθώς και τα στάδια σχεδιασμού παιγνιωδών εφαρμογών. Η παιγνιοποίηση είναι μια σχετικά καινούρια έννοια, που τα τελευταία χρόνια ήρθε στο προσκήνιο. Για αυτό το λόγο, δεν υπάρχει ένας ακριβής ορισμός, αν και οι περισσότεροι συμφωνούν σε κάποια συγκεκριμένα χαρακτηριστικά που μπορούν να περιγράψουν την έννοια. Κατά το σχεδιασμό εφαρμογών, χρησιμοποιούνται πολλά από τα στοιχεία των παιχνιδιών. Η παιγνιοποίηση επίσης, χρησιμεύει και σε διάφορους τομείς της καθημερινής ζωής. Ανάλογα με τον τομέα, έχουν αναπτυχθεί αρκετές εφαρμογές, οι οποίες φαίνονται αρκετά χρήσιμες για τους χρήστες. Από τη βιβλιογραφική ανασκόπηση, παρατηρήθηκε ότι παρόλο που στον τομέα της εκπαίδευσης, του μάρκετινγκ και των επιχειρήσεων υπάρχουν αρκετές παιγνιώδεις εφαρμογές, στο κομμάτι του περιβάλλοντος, της υγείας και του crowdsourcing παρατηρείται έλλειψη εφαρμογών. Αυτό είναι ένα ζήτημα που χρειάζεται περαιτέρω αναζήτηση και έρευνα.

Στη συνέχεια της βιβλιογραφικής ανασκόπησης, αναλύονται οι έρευνες που έχουν γίνει σχετικά με ζητήματα ασφάλειας και ιδιωτικότητας. Οι περισσότεροι συγγραφείς τονίζουν την ανάγκη για επίγνωση πάνω σε αυτά τα ζητήματα, καθώς και την εκπαίδευση των χρηστών, έτσι ώστε να είναι ενημερωμένοι. Στον τομέα της ασφάλειας έχουν δημιουργηθεί

παιγνιώδη προγράμματα εκπαίδευσης, τα οποία μπορούν να συμβάλουν στην ασφαλή χρήση των διάφορων τεχνολογιών. Αντίθετα όμως, στον τομέα της ιδιωτικότητας, παρατηρείται έλλειψη βιβλιογραφίας και είναι απαραίτητη η περαιτέρω διερεύνηση του θέματος.

Στο τελευταίο κεφάλαιο της εργασίας, δίνονται παραδείγματα εφαρμογών παιγνιοποίησης για επίγνωση ασφάλειας και ιδιωτικότητας. Όπως ήδη αναφέρθηκε, υπάρχει αρκετό υλικό για την ασφάλεια, ενώ παρατηρείται έλλειψη εφαρμογών για την ιδιωτικότητα. Οι παιγνιώδεις εφαρμογές είναι πιο εύκολα κατανοητές από τους χρήστες και τους δίνουν την δυνατότητα να μαθαίνουν διασκεδάζοντας. Συνολικά, υπάρχει ανάγκη για περισσότερη διερεύνηση του θέματος, καθώς πρόκειται για ένα σχετικά καινούριο ζήτημα, το οποίο όμως καθημερινά χρησιμοποιείται σε διάφορους τομείς και είναι κάτι που χρειάζεται να γνωρίζουν οι περισσότερες εταιρίες και οργανισμοί.

Βιβλιογραφία

1. Seaborn K. & Fels D. (2014), *Gamification in theory and action: A survey*, Int. J. Human-Computer Studies 74 (2015) 14-31
2. Mora A., Riera D., Gonzalez C. & Arnedo-Moreno J. (2015*), A literature review of gamification design frameworks*, Spain
3. Deterding S., Dixon D., Khaled R. & Nacke L. (2011), *From game design elements to gamefulness: defining 'Gamification'*, Finland: In Proceeding of the 15th International Academic MindTrek Conference, Tampere, ACM
4. Huotari K. & Hamari J.(2012*), Defining gamification: a service marketing perspective, Finland*, In Proceeding of the 16th International Academic MindTrek Conference, Tampere, ACM, pp.17-22
5. Nicholson, S. (2012, June). *A User-Centered Theoretical Framework for Meaningful Gamification.* Paper Presented at *Games+Learning+Society 8.0*, Madison, WI
6. Hamari J., Koivisto J., Sarsa H. (2014*), Does Gamification Work?- A Literature Review of Empirical Studies on Gamification*, Hawaii: 47th Hawaii International Conference on System Science
7. Morschheuser B., Werder K. Hamari J. & Abe J. (2017), *How to gamify? A method for designing gamification*, Hawaii: Published in Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS 2017) (pp. 1298-1307). University of Hawai´i at Manoa. ISBN: 978-0-9981331-0-2., Διαθέσιμο σε http://dx.doi.org/10.24251/HICSS.2017.155
8. Caponetto I., Earp J. & Ott M. (2014), *Gamification and Education: A Literature Review*, Germany: Research and Training Center for Culture and Computer Science (FKI), University of Applied Sciences HTW Berlin, Proceedings of the 8th European Conference on Games Based Learning ECGBL 2014
9. Yu-kai Chou, *Top 10 education gamification examples*, Διαθέσιμο σε http://yukaichou.com/gamification-examples/top-10-education-gamification-examples/
10. Garcia D. (2018), *Gamification in marketing: 16 gamification gurus share their favorite examples & insights for 2018*, Διαθέσιμο σε https://surveyanyplace.com/gamification-in-marketing-16-experts/
11. Yu-kai Chou, *Top 10 marketing gamification cases you won't forget*, Διαθέσιμο σε http://yukaichou.com/gamification-examples/top-10-marketing-gamification-cases-remember/
12. Warner A. (2016),*The aim of the game: how the gamification of medtech is putting the fun into healthier behavior*, Διαθέσιμο σε https://medtechengine.com/article/gamification-in-healthcare/
13. Yu-kai Chou, *Top 10 gamified healthcare games that will extend your life*, Διαθέσιμο σε http://yukaichou.com/gamification-examples/top-ten-gamification-healthcare-games/#.Ws44_y5ubIU

14. Dr. Bertalan Meskó MD, PhD, *The Top 15 Examples of gamification in healthcare*, Διαθέσιμο σε http://medicalfuturist.com/top-examples-of-gamification-in-healthcare/
15. Stanley R. (2014), *Top 25 best examples of gamification in business*, Διαθέσιμο σε https://www.clicksoftware.com/blog/top-25-best-examples-of-gamification-in-business/
16. Morford Z., Witts B., Killingworth K., Alavosius M. (2014), *Gamification: The Intersection between Behavior Analysis and Game Design Technologies*, USA: Behavior Analysis International 2014
17. Yu-kai Chou (2017), *Five Examples of Gamified Crowdsourcing to learn from*, Διαθέσιμο σε http://yukaichou.com/chou-musings/five-examples-of-gamified-crowdsourcing-to-learn-from/#.WtEA5C5ubIU
18. Jaeger L., (2018), *Information Security Awareness: Literature Review and Integrative Framework*, Hawaii: Proceedings of the 51st Hawaii International Conference on System Sciences, p. 4703-4712
19. Tsohou A., Kokolakis S., Karyda M. & Kiountouzis E. (2008), *Investing Information Security Awareness: Research and Practice Gaps*, Greece: Information Security Journal A Global Perspective, December 2008
20. Wilson M. & Hash J. (2003, October*), Building an Information Technology Security Awareness and Training Program*, Computer Security Division Information Technology Laboratory , National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8933
21. ENISA (2010), *The new users' guide: How to raise information security awareness*
22. Langheinrich M. (2001), Privacy *by Design- Principles of Privacy-Aware Ubiquitous Systems*, Switzerland: International conference on Ubiquitous Computing, Distributed Systems Group, Institute of Information Systems, IFW
23. Omoronyia I., Cavallaro L., Salehie M., Pasquale L. & Nuseibeh B. (2013*), Engineering Adaptive Privacy: On the Role of Privacy Awareness Requirements*, USA: Proceedin of the 2013 International Conference on Software Engineering, p.632-641
24. Featherman M., Miyazaki A. & Sprott D. (2010),*Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility*,USA: Journal of Services Marketing, Vol. 24 Issue: 3, pp.219-229, https://doi.org/10.1108/08876041011040622
25. Langheinrich M. (2002), *A Privacy Awareness System for Ubiquitous Computing Environments*, Switzerland: Institute of Information Systems, International conference on Ubiquitous Computing
26. Gjersen Eyvind Garder B., Gjaere Erlend Andreas, Barthnes Maria & Flores Waldo Rocha (2017), *Gamification of Information Security Awareness and Training*, Proceedings of the 3rd International Conference on Information Systems Security and Privacy, Porto, Portugal, 19 - 21 February, 2017, p. 59-70
27. Thornton David & Francia Guillermo III (2014), *Gamification of Information Systems and Security Training: Issues and Case Studies*, United States: Information Security Education Journal, Volume 1, number 1, June 2014, p. 16-29
28. Gjertsen Eyvind Garder B. (2016), *Use of Gamification in Security Awareness and Training Programs*, Norwegian University of Science and Technology, Master of Science in Communication Technology

29. Wood Lamont (2014), *Boost your security training with gamification*, Διαθέσιμο σε https://www.computerworld.com/article/2489977/security0/boost-your-security-training-with-gamification-really.html
30. Pwc, *Game of Threats- A cyber threat simulation*, United States, Διαθέσιμο σε: https://www.pwc.com/us/en/industries/financial-services/cybersecurity-privacy/game-of-threats.html
31. Cyber Security Challenge UK, Διαθέσιμο σε: https://www.cybersecuritychallenge.org.uk/about
32. Wombat Security, *Security Awareness Training Modules*, Διαθέσιμο σε: https://www.wombatsecurity.com/security-education/security-awareness-training-modules
33. CMU Usable Privacy and Security Laboratory, Anti-Phishing Phil, Carnegie Mellon University, Διαθέσιμο σε: https://www.ucl.ac.uk/cert/antiphishing/
34. Center for Democracy & Technology (2011), *The Gamification of Privacy*, Διαθέσιμο σε https://cdt.org/blog/the-gamification-of-privacy/