# Ανοικτό Πανεπιστήμιο Κύπρου

## Σχολή Θετικών και Εφαρμοσμένων Επιστημών


## Μεταπτυχιακή Διατριβή
## στα Πληροφοριακά και Επικοινωνιακά Συστήματα

# Μελέτη Τεχνικών Απομνημόνευσης Περίπλοκων Κωδικών και Δοκιμή σε Εταιρικά Περιβάλλοντα, με Σκοπό την Αύξηση Ασφάλειας Χρηστών.


**Δημήτρης Παπαδημητρίου**

**Επιβλέπων Καθηγητής**
**Δρ. Σταύρος Σιαηλής**



**Μάιος 2015**

# Ανοικτό Πανεπιστήμιο Κύπρου

## Σχολή Θετικών και Εφαρμοσμένων Επιστημών


# Μελέτη Τεχνικών Απομνημόνευσης Περίπλοκων Κωδικών και Δοκιμή σε Εταιρικά Περιβάλλοντα, με Σκοπό την Αύξηση Ασφάλειας Χρηστών.


**Δημήτρης Παπαδημητρίου**

**Επιβλέπων Καθηγητής**
**Δρ. Σταύρος Σιαηλής**


Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

**Μάιος 2015**

# Περίληψη

Οι πολιτικές ασφαλείας που χρησιμοποιούνται από μεγάλες εταιρείες ώστε να διασφαλιστεί η πολυπλοκότητα των κωδικών, δημιουργούν πολλά προβλήματα στους χρήστες της με αποτέλεσμα να τοποθετούν το κωδικό τους πάνω στην οθόνη ή κάτω από το πληκτρολόγιο μηδενίζοντας έτσι και τους πιο αυστηρούς κανόνες.

Πρωταρχικός σκοπός της συγκεκριμένης διατριβής είναι η μελέτη του κατά πόσο είναι εφικτή η χρήση πολύπλοκων κωδικών αλλά ταυτόχρονα ευκολομνημόνευτων ώστε να αποτραπούν φαινόμενα όπως τα προαναφερθέντα. Η ευαισθητοποίηση και η αφύπνιση για τους κινδύνους που ελλοχεύουν στο διαδίκτυο είναι ένας ακόμη στόχος που πραγματεύεται η διατριβή αυτή. Στα πειράματα που διεξάχθηκαν κατά την εκπόνηση αυτής της διατριβής μελετήθηκε και η αλλαγή συμπεριφοράς των χρηστών όσο αφορά τη χρήση αδύναμων κωδικών σε εργασιακό και προσωπικό περιβάλλον.

Συνολικά μελετήθηκαν πέντε (5) διαφορετικές μέθοδοι για τη παραγωγή και απομνημόνευση ισχυρών κωδικών. Συγκεκριμένα, χρησιμοποιήθηκαν κωδικοί που περιείχαν σε τυχαία σειρά πεζά και κεφαλαία γράμματα, αριθμούς και ειδικούς χαρακτήρες, κωδικοί που μπορούν να προφέρονται, κωδικοί με τη χρήση του πρώτου γράμματος από μια μεγάλη πρόταση προσθέτοντας ένα αριθμό ή και ειδικό χαρακτήρα σε τυχαία θέση, κωδικοί από δημοφιλείς φράσεις και στίχους τραγουδιών και τέλος κωδικοί που προκύπτανε μετά από συνδυασμό λέξεων.

Τα αποτελέσματα αυτής της έρευνα έδειξαν ότι με την κατάλληλη εκπαίδευση και τον κατάλληλο τρόπο δημιουργίας κωδικών μπορούμε να μετατρέψουμε τον αδύναμο κρίκο της ασφάλειας δεδομένων μιας εταιρίας σε ένα σημαντικό παράγοντα ασφάλειας.

# Summary

Security policies used by large scale companies to ensure the complexity of their passwords, generates problems to their users. As a result many employees write their password on a sticker next to monitor or even below keyboard. This thesis deals with the above problem and research's the possibility of using complex password but also simple for someone to remember it in order to avoid the problems above.

Users' awakening for the risks lurking on the internet was also an object of this research. In the experiments that were conducted during this thesis users' behavior adjustment regarding the usage of weak passwords, was also monitored.

This research studies five (5) methods for creating and memorizing strong passwords. To be more precise, the password methods that were used contained lower and upper case letters, numbers and special characters in random positions, pronounceable passwords, passwords created by extracting the first letter of a phrase and combined them with a number and/or special characters, passwords created using popular phrases and song lyrics and passwords created by combining different words.

The results of this research showed that people with the right method and training can be transformed from Companies data security problem to a valuable partner in the fight of Companies data breaches.

# Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον επιβλέποντα καθηγητή μου Δρ. Σταύρο Σιαηλή για τη συνεχή καθοδήγηση, τις πολύτιμες πληροφορίες και ενδείξεις που μου έδωσε καθ' όλη τη διάρκεια για τη εκπλήρωση της διατριβής. Την υπομονή και επιμονή που είχε δείξει ώστε να βρεθεί ένα θέμα αντάξιο των δυνατοτήτων και γνώσεων μου που θα είχε θετικό αντίκτυπο στη δουλεία μου και στη μετέπειτα πορεία μου.

Ιδιαίτερες ευχαριστίες θέλω να απευθύνω στο κ. Θεόδωρο Θεοδώρου, υπεύθυνο του Τμήματος Πληροφορικής της εταιρείας Totalserve Management Ltd, για τη πολύτιμη βοήθεια κατά τη διάρκεια των τεστ. Επίσης να ευχαριστήσω όλους τους συναδέλφους μου που έλαβαν μέρος στα τεστ δίνοντάς μου τη ευκαιρία να διεξάγω τη έρευνά μου αποκομίζοντας πολύτιμες πληροφορίες.

Τέλος να ευχαριστήσω το κ. Christian Thoeing για τη χρήση και αξιοποίηση του προγράμματος PWGen για τη παραγωγή των κωδικών στα τεστ μας.

# Περιεχόμενα

# Εικόνες

# Πίνακες

# Γραφήματα

# Κεφάλαιο 1
# Εισαγωγή

Το τεράστιο πλήγμα που δέχτηκε η Sony Entertainment που είχε σαν αποτέλεσμα την απώλεια μεγάλου όγκου εταιρικών δεδομένων και μελλοντικών σχεδίων σε ανταγωνιστές καθώς και η ανακάλυψη από τα Kaspersky Labs ενός από τα μεγαλύτερα κτυπήματα στα τραπεζικά συστήματα με οικονομικές απώλειες να υπολογίζονται στο 1 δισεκατομμύριο ευρώ, μας δείχνει ότι οι εταιρείες επικεντρώνονται στην περιμετρική ασφάλεια των υποδομών τους ξεχνώντας τον ανθρώπινο παράγοντα. Οι άνθρωποι έχουνε αδυναμίες και ελαττώματα που μερικές φορές δρούνε συναισθηματικά και επιπόλαια. Αυτά τα έμφυτα χαρακτηριστικά της ανθρώπινης φύσης εκμεταλλεύονται οι κυβερνοεγκληματίες και χρησιμοποιώντας διάφορες τεχνικές προσπαθούν να αποσπάσουν προσωπικές ή εταιρικές πληροφορίες με απώτερο σκοπό τη διείσδυση στα συστήματα. Μελέτη που έγινε από τον Florencio et al. [06], έχει δείξει ότι είναι πολύ εύκολο για κάποιο να καταφέρει να βρει το κωδικό του χρήστη απλά χρησιμοποιώντας προσωπικές πληροφορίες και δεδομένα από τους χρήστες. Η ίδια έρευνα έδειξε επίσης ότι με τη αποστολή παραπλανητικών μηνυμάτων (spam emails) στο ηλεκτρονικό τους ταχυδρομείο καθώς και με χρήση προγραμμάτων που υποκλέπτουν κωδικούς όπως για παράδειγμα keyloggers, ο κωδικός του χρήστη γνωστοποιείται στο κυβερνοεγκληματία. Προχωρώντας ένα βήμα παραπέρα η έρευνα επικεντρώνεται και στα κενά ασφαλείας τα οποία είναι η χρήση αριθμητικού κωδικού (PIN) 6 χαρακτήρων και η αμέλεια που επιδεικνύουν οι χρήστες στη δημιουργία κωδικών

πληρώντας στο ελάχιστο τις απαιτήσεις που προνοούνται. Ο ειδικός σε θέματα ασφάλειας και διάσημος συγγραφέας βιβλίων στο χώρο της ασφάλειας και προστασίας δεδομένων Bruce Shneier, αναφέρεται πολύ συχνά στο πόσο σημαντικό είναι να έχουμε δύσκολους κωδικούς πρόσβασης [28] και με ένα χιουμοριστικό τρόπο δίνει ένα παράδειγμα για το ποιος είναι ο καλύτερος τρόπος για να προστατεύουμε τους κωδικούς μας, μέσα στο πορτοφόλι μας [29]. Το πρόβλημα που αναφέρεται πιο πάνω, η μειωμένη αντίληψη του κινδύνου που εγκυμονεί καθώς και προτάσεις επίλυσης του προβλήματος, κυρίως για τις εταιρείες, είναι ο κύριος στόχος που πραγματεύεται η διατριβή αυτή. Θα μελετηθεί και θα προταθεί ο καλύτερος, ευκολότερος και αποδοτικότερος τρόπος ώστε να αυξήσουμε τη πολυπλοκότητα των κωδικών των χρηστών μιας εταιρείας, αλλά ταυτόχρονα να βοηθήσουμε και τους χρήστες να αναπτύξουν καλύτερες δυνατότητες απομνημόνευσης των κωδικών τους.

## 1.1 Σκοπός και στόχος της διατριβής

Η ραγδαία αύξηση επιθέσεων κατά οργανισμών, εταιρειών και ηλεκτρονικών υποδομών, έχει φτάσει σε ανησυχητικά επίπεδα τα τελευταία χρόνια. Προσωπικές πληροφορίες, δεδομένα χρηστών και εταιρειών, μηνύματα ηλεκτρονικού ταχυδρομείου και κωδικοί χρηστών κατακλύζουν σε συχνή βάση διάφορα αμφιβόλου αξιοπιστίας και κακόβουλης χρήσης ιστοσελίδες που αποσκοπούν στο να πετύχουν οικονομικό όφελος. Η άγνοια ή και η αδιαφορία που επιδεικνύουν οι χρήστες όσον αφορά τη διαδικτυακή τους ασφάλεια, έχει σαν αποτέλεσμα τη παραβίαση της ιδιωτικής τους ζωής και την απώλεια χρημάτων. Σκοπός μας μέσα από τη παρούσα διπλωματική εργασία είναι η ευαισθητοποίηση, η αφύπνιση και η αντίληψη των κινδύνων που υπάρχουν και εγκυμονούν για τους χρήστες στο διαδίκτυο και να κατανοήσουν ποια μέτρα ασφαλείας πρέπει να χρησιμοποιούν ώστε να προστατευθούν και ταυτόχρονα να προστατεύσουν τους γύρω τους[01].

Επίσης θέλουμε ο χρήστης να αλλάξει τον τρόπο με τον οποίο είναι συνηθισμένος να σκέφτεται μέχρι τώρα τη δημιουργία ενός νέου κωδικού και στη συνέχεια να αλλάξει όλους τους κωδικούς του που κρίνονται ανασφαλής. Να ξεφύγει από το στερεότυπο της χρήσης ημερομηνιών γέννησης, ονομάτων συγγενών/φίλων και με ένα ευφάνταστο και απλοϊκό τρόπο να έχει δύσκολους κωδικούς που δεν μπορεί κανείς να τους μαντέψει, αλλά συνάμα να είναι εύκολοι να τους θυμάται.

## 1.2 Μεθοδολογία και Περιγραφή κεφαλαίων

Για τη επιτυχή ολοκλήρωση των τεστ, περιγράφεται πιο αναλυτικά η κάθε μέθοδος που χρησιμοποιήθηκε στο κεφάλαιο 4, χρησιμοποιήθηκαν συνολικά 5 διαφορετικές μέθοδοι παραγωγής κωδικών. Όλοι οι κωδικοί παράχθηκαν με τη βοήθεια του δωρεάν και εύχρηστου προγράμματος παραγωγής κωδικών PWGen [03]. Το κάθε τεστ είχε διάρκεια 3 εβδομάδων.

Στο κεφάλαιο 2 γίνεται μια εισαγωγή για τη αναγκαιότητα να προστατεύει το κάθε άτομο – χρήστης το κωδικό που χρησιμοποιεί, είτε είναι για το προσωπικό του ηλεκτρονικό ταχυδρομείο είτε για ιστοσελίδες κοινωνικής δικτύωσης είτε για συναλλαγές και αγορές μέσω διαδικτύου. Παρουσιάζονται 4 ενδεικτικά παραδείγματα από επιθέσεις που έγιναν τα τελευταία 2 χρόνια σε μεγάλες και γνωστές εταιρείες συνοδευόμενες από πίνακα με κάποιους από τους κωδικούς που είχαν διαρρεύσει στο διαδίκτυο δείχνοντας τη άγνοια και τη στάση που κρατούν απέναντι στα όποια προσωπικά τους δεδομένα. Συνεχίζοντας, θα παρουσιαστούν 6 προγράμματα που χρησιμοποιούνται από τους Διαχειριστές Συστημάτων (System Administrators) για να υποβάλλουν σε δοκιμή συνδυασμούς με όνομα χρήστη και κωδικό που χρησιμοποιούν σε μηχανήματα και συσκευές εντός του δικτύου τους για εξάλειψη των πιθανοτήτων να παραβιαστούν από κάποιο κακόβουλο χρήστη όπως επίσης και των κωδικών που έχουν οι χρήστες για αλλαγή του κωδικού σε περίπτωση που δεν πληροί τα κριτήρια και πολιτικές ασφαλείας που έχει καθορίσει η εκάστοτε εταιρεία / οργανισμός. Η χρήση τέτοιων προγραμμάτων από τους hackers γίνεται για σκοπούς αποκρυπτογράφησης κωδικών και υποκλοπή δεδομένων των χρηστών.

Στο κεφάλαιο 3 θα γίνει μια βιβλιογραφική αναφορά στο μνημονικό των ατόμων, πόσο δύσκολο είναι να απομνημονεύουν κωδικούς πέραν των 7 χαρακτήρων με βάση ένα επιστημονικό άρθρο του George A. Miller και στη συνέχεια θα σχολιαστούν και θα συγκριθούν παλαιότερα τεστ που έγιναν αλλά όχι σε εταιρικό περιβάλλον.

Στο κεφάλαιο 4 θα παρουσιαστούν και θα αναλυθούν σε μεγαλύτερο βάθος η πειραματική διαδικασία και οι μέθοδοι που ακολουθήθηκαν καθ' όλη τη πορεία των τεστ. Θα γίνει επεξήγηση της κάθε μεθόδου, γιατί επιλέγηκε η συγκεκριμένη μέθοδος, τι διαφοροποιήσεις έχουν γίνει και πώς έχουν παραχθεί όλοι οι κωδικοί. Ανάλυση των αποτελεσμάτων της κάθε μεθόδου και επεξήγηση του σκοπού που έγιναν τα 2 ερωτηματολόγια.

Στο κεφάλαιο 5, αφού συλλεχθούν, αναλυθούν και ταξινομηθούν τα δεδομένα από τα 2 ερωτηματολόγια, θα προταθεί μια νέα μέθοδος για παραγωγή κωδικών η οποία θα είναι η πιο προσιτή σε θέμα απομνημόνευσης και βαθμού δυσκολίας που πρέπει να έχει ένας κωδικός ούτως ώστε να υπάρχει ένα επίπεδο και αίσθηση ασφάλειας για το χρήστη.

# Κεφάλαιο 2
# Αναγκαιότητα προστασίας κωδικών

Στη καθημερινή ζωή οι άνθρωποι χρησιμοποιούν κωδικούς πρόσβασης για να ελέγξουν τα ηλεκτρονικά τους ταχυδρομεία, να συνδεθούν σε διάφορες σελίδες (Facebook, Twitter, LinkedIn, Pinterest κ.α.), καθώς και σε τράπεζες για διεκπεραίωση οικονομικής φύσεως συναλλαγές. Η χρήση ενός ονόματος χρήστη και κωδικού είναι απαραίτητη για τη επιτυχή εξακρίβωση του ατόμου που θα έχει πρόσβαση στις πληροφορίες του συγκεκριμένου συστήματος. Οι ανάγκες των ανθρώπων δεν περιορίζονται όμως σε χρήση δυο ή τριών κωδικών, υπάρχουν περιπτώσεις όπου άτομα πρέπει να διαχειρίζονται μέχρι και δέκα διαφορετικούς λογαριασμούς και αυτό απαιτεί να γίνεται χρήση διαφορετικών συνδυασμών κάθε φορά. Η συνήθης τακτική που ακολουθείται από τους πλείστους χρήστες, που διατηρούν αρκετούς λογαριασμούς, είναι η χρήση ίδιου ονόματος χρήστη και κωδικού σε περισσότερες από μια περιπτώσεις ή σε μερικές εξαιρέσεις να προβαίνουν σε μικροαλλαγές στο κωδικό πρόσβασης. Αυτό οδηγεί στο να θέτουν σε κίνδυνο τη διαδικτυακή τους ασφάλεια με συνέπεια μερικοί επιτήδειοι κυβερνοεγκληματίες να τους υποκλέψουν τα όποια δεδομένα τους και συγχρόνως να έχουν πρόσβαση και στους υπόλοιπους λογαριασμούς που διατηρούν.

## 2.1 Επιθέσεις σε εταιρικά περιβάλλοντα

Τα τελευταία χρόνια έχει παρατηρηθεί μια έξαρση στις διαδικτυακές επιθέσεις εναντίον εταιριών με διάφορους τρόπους, που σκοπό έχουν να υποκλέψουν δεδομένα σχετικά με τη εταιρική αλληλογραφία, εταιρικά δεδομένα πελατών ή άλλα ευαίσθητα δεδομένα που θα προκαλέσουν ζημιά στην ίδια τη εταιρία με άμεσο αντίκτυπο που μεταφράζεται σε οικονομικό κόστος και αναξιοπιστία. Πολλοί οργανισμοί και εταιρίες έχουν το λανθασμένο σκεπτικό ότι δεν θα αποτελέσουν ποτέ στόχο κάποιου κυβερνοεγκληματία για το λόγο ότι δεν έχουν σημαντικά αρχεία στη κατοχή τους που θα αποφέρουν κάποιο χρηματικό όφελος εάν πουληθούν σε τρίτα άτομα ή ακόμη ότι σαν εταιρία ή οργανισμός είναι μικρή για να γίνει στόχος. Ένας από τους πιο διαδεδομένους τρόπους είναι η αποστολή αλληλογραφίας εφαρμόζοντας τη τεχνική του ψαρέματος (phishing). Οι κυβερνοεγκληματίες προτρέπουν τα υποψήφια θύματα να εισάγουν το κωδικό τους αποκτώντας πρόσβαση στα υπολογιστικά συστήματα της εταιρείας. Αποκτώντας απομακρυσμένη πρόσβαση στον υπολογιστή του θύματος και με τη χρήση προγραμμάτων που χρησιμοποιούν τη μέθοδο bruteforce attack (αναφέρονται στο κεφάλαιο 2.2 πιο αναλυτικά) επιτυγχάνουν ταυτόχρονη πρόσβαση σε πολλαπλούς λογαριασμούς αυξάνοντας τις πιθανότητες απόκτησης διαβαθμισμένης πρόσβασης. Ο συνδυασμός λιστών που περιέχουν προκαθορισμένα ονόματα χρηστών και κωδικών υποβοηθάει το όλο εγχείρημα του κυβερνοεγκληματία στη περίπτωση που οι κωδικοί είναι πολύ εύκολοι, σε αντίθετη περίπτωση θα χρειαστεί να σπαταλήσει περισσότερο χρόνο.

Μια πιο εξειδικευμένη μέθοδος που χρησιμοποιείται ευρέως για υποκλοπή κωδικών είναι η SQL Injection. Εισάγοντας εντολές με στοχευόμενα ερωτήματα (queries) όπως προσθήκη χρήστη, διαγραφή ή και αλλαγή δικαιωμάτων διαχείρισης που έχει, ανάγνωση ευαίσθητων αρχείων και δεδομένων από μια βάση και εκτέλεση εντολών σε επίπεδο system administrator, με αυτό τον τρόπο ο επιτιθέμενος είναι σε θέση να πάρει στη κατοχή του πέραν των κωδικών, αρχεία που περιέχουν προσωπικές και άλλες πληροφορίες. Επειδή το αρχείο των κωδικών στις πλείστες των περιπτώσεων είναι σε κρυπτογραφημένη μορφή, θα γίνει και σε αυτή τη περίπτωση χρήση των εργαλείων που αναφέρονται πιο κάτω. Ο βαθμός δυσκολίας αποκρυπτογράφησης των κωδικών κρίνεται με βάση τη καινοτομία και πρωτοτυπία που τον χαρακτηρίζει, δυσκολεύοντας το κυβερνοεγκληματία και έτσι αποκτούν πλεονέκτημα χρόνου για εναλλαγή των κωδικών τους με νέους.

Άλλος παράγοντας που οδηγεί στο να γίνει στόχος επίθεσης μια εταιρία είναι τα αντίπαλα συμφέροντα. Υποκλέπτοντας τα δεδομένα της που αφορούν σε μελλοντικά πλάνα συνεργασίας

με στρατηγικούς εταίρους, σχέδια, απόρρητα ή ευαίσθητα αρχεία για εμπορικούς και οικονομικούς σκοπούς, δημιουργείται ένα μεγάλο πλεονέκτημα στο μερίδιο της αγοράς από μεριάς του ανταγωνιστή ενώ η εταιρία-θύμα χάνει τη αξιοπιστία της.

Ένας ύπουλος αλλά ευφάνταστος τρόπος απόκτησης των κωδικών από τους χρήστες είναι να παριστάνουν τους πελάτες. Εισερχόμενος σε ένα γραφείο με το πρόσχημα του πελάτη, πλησιάζοντας κάποιο υπάλληλο για να πάρει μερικές πληροφορίες για μια υποτιθέμενη συμφωνία, παρατηρεί το χώρο γύρο από το γραφείο για τυχόν χαρτάκια με το κωδικό αναγραμμένο. Εφόσον πετύχει το εγχείρημά του, θα είναι σε θέση να αποκτήσει πρόσβαση στα συστήματα.

Η εταιρία RockYou, εταιρία κατασκευής παιχνιδιών για σελίδες κοινωνικής δικτύωσης και προώθησης προϊόντων, δέχτηκε επίθεση το Δεκέμβριο του 2009 με αποτέλεσμα να δημοσιοποιηθούν οι κωδικοί και τα ηλεκτρονικά ταχυδρομεία 32 εκατομμυρίων χρηστών της είναι ένα από τα παραδείγματα επιθέσεων που περιγράφηκαν πιο πάνω. Το γεγονός αυτό οδήγησε τη συγκεκριμένη εταιρία στο να πληρώσει πρόστιμο ύψους 290,000 δολαρίων για ανεπαρκή μέτρα ασφαλείας καθώς όλοι οι κωδικοί ήταν αποθηκευμένοι σε απλή μορφή κειμένου (plain text format). Τόσο για τους χρήστες της όσο και για τη ίδια, τέθηκε υπό καθεστώς επιτήρησης από δυο ανεξάρτητες εταιρίες συμβούλους ασφαλείας. Η πολιτική της εταιρίας για αποδοχή κωδικού μεταξύ 5 και 15 χαρακτήρων δίχως τη χρήση ειδικών χαρακτήρων, αποτελούσε ένα μεγάλο κενό ασφαλείας γιατί είναι σχετικά εύκολο να βρεθεί ο κωδικός πρόσβασης του κάθε χρήστη. Με τη προτροπή αυτής της μεθόδου δημιουργίας κωδικού, αρκετοί ήταν οι χρήστες που αρκέστηκαν στο να δημιουργήσουν ένα απλό και κοινό κωδικό. Λόγο της εργασιακής φύσης, η RockYou προέτρεπε τους χρήστες που δημιουργούσαν εφαρμογές να καταχωρήσουν τα διαπιστευτήρια που είχαν για τις συνεργαζόμενες σελίδες όταν θα διαμοίραζαν δεδομένα ή κοινοποιούσαν κάποια εφαρμογή που μόλις έφτιαξαν. Φυσικό επακόλουθο αυτής της τακτικής ήταν οι κυβερνοεγκληματίες να αποκτήσουν πρόσβαση και στους υπόλοιπους λογαριασμούς των ανυποψίαστων χρηστών. Ενδεικτικά παραδείγματα της συχνότητας των πιο δημοφιλών κωδικών που χρησιμοποιούνταν, βρίσκονται στο πιο κάτω πίνακα [38].

| Α/Α | Χρήστες | Κωδικός χρηστών | Α/Α | Χρήστες | Κωδικός χρηστών |
|---|---|---|---|---|---|
| 1 | 290729 | 123456 | 11 | 16227 | nicole |
| 2 | 79076 | 12345 | 12 | 15308 | daniel |
| 3 | 76789 | 123456789 | 13 | 15163 | babygirl |
| 4 | 59462 | password | 14 | 14726 | monkey |
| 5 | 49952 | iloveyou | 15 | 14331 | lovely |
| 6 | 33291 | princess | 16 | 14103 | jessica |
| 7 | 21725 | 1234567 | 17 | 13984 | 654321 |
| 8 | 20901 | rockyou | 18 | 13981 | michael |
| 9 | 20553 | 12345678 | 19 | 13488 | ashley |
| 10 | 16648 | abc123 | 20 | 13456 | qwerty |

**Πίνακας 2.1:** Μερικοί από τους κωδικούς που είχαν οι χρήστες της RockYou[1].

Όπως φαίνεται και από το πίνακα 2.1 πολλοί από τους κωδικούς μπορούσε πολύ εύκολα κάποιος να τους μαντέψει ή να δοκιμάσει να πετύχει είσοδο στο σύστημα κάνοντας χρήση ενός word list.

Μια άλλη επίθεση τέτοιου είδους είχε γίνει τον Μάιο του 2013 στη εταιρία Drupal, μια ανοικτού κώδικα πλατφόρμα διαχείρισης περιεχομένου κατάλληλη για ιστοσελίδες και εφαρμογές για χρήση τόσο από ιδιώτες αλλά και από μεγάλες εταιρίες και οργανισμούς. Αποτέλεσμα ήταν να

[1] Αρχείο με τους κωδικούς: https://www.dropbox.com/s/3r843u09lc5blxg/rockyou.rar?dl=0

δημοσιοποιηθούν αρκετά σημαντικά στοιχεία των χρηστών, όπως για παράδειγμα το όνομα χρήστη, η ηλεκτρονική διεύθυνση, ο κωδικός πρόσβασης και η χώρα κατοικίας τους. Η λίστα περιείχε στο σύνολό της 16449 κωδικούς αλλά με τη μόνη διαφορά ότι σε αυτή τη περίπτωση όλοι οι κωδικοί είχαν προηγουμένως κρυπτογραφηθεί σαν ένα επιπλέον μέτρο ασφαλείας από μεριάς των υπεύθυνων ασφαλείας. Η κρυπτογράφηση που έτυχαν οι κωδικοί, δεν στάθηκε εμπόδιο στο να μετατραπούν στη κανονική τους μορφή. Αν και ακούγεται αρκετά ασφαλές, παρατηρήθηκε η χρήση κοινότυπων και απλών κωδικών που φαίνονται στο πιο κάτω πίνακα [27].

| | | | | |
|---|---|---|---|---|
| 123456 | 1234567 | password | letmein | Destiny21 |
| pizzapizza | p@$$word | 123456789j | letmein1! | LETMEin3 |
| kristyjimmy | InsertPassword | gonefishing1125 | iloveyousomuch | 1234menarmy |

**Πίνακας 2.2:** Μερικοί από τους κωδικούς που είχαν οι χρήστες του Drupal.

Μια άλλη περίπτωση επιτυχούς επίθεσης και κλοπής των ηλεκτρονικών διευθύνσεων και κωδικών πρόσβασης από συνολικά 7 εκατομμύρια χρήστες, έγινε στη εταιρεία Dropbox τον Οκτώβριος του 2014. Η συγκεκριμένη εταιρεία ειδικεύεται στη ασφαλή διαμοίραση και διαχείριση αρχείων κάθε είδους που αναρτούν οι χρήστες μέσω διαδικτύου. Παρά τα μέτρα και τις δικλείδες ασφαλείας που χρησιμοποιεί, οι κυβερνοεγκληματίες κατάφεραν να διεισδύσουν μέσα στα συστήματα και τους εξυπηρετητές της εταιρείας και να αποκρυπτογραφήσουν ένα σημαντικό αριθμό κωδικών. Όπως μπορούμε να παρατηρήσουμε στο πίνακα που ακολουθεί, οι χρήστες και σε αυτή τη περίπτωση χρησιμοποιούσαν εύκολους και επαναλαμβανόμενους κωδικούς θέτοντας έτσι σε άμεσο κίνδυνο τα αρχεία τους, που μπορεί να περιλαμβάνουν από προσωπικά αρχεία κειμένου, λογιστικά φύλλα, αρχεία παρουσιάσεων μέχρι και προσωπικού χαρακτήρα φωτογραφίες και βίντεο [40].

| | | | | |
|---|---|---|---|---|
| 001971 | 3564472 | 21282128 | otford666 | france |
| kamikaze | osborne42 | 13241324 | visavisa | Benji1999 |
| master12 | helicopter | melbourne | tatata | zerozero |
| 271188 | mother | water31 | brazil1 | banana |

**Πίνακας 2.3:** Μερικοί από τους κωδικούς που είχαν οι χρήστες του Dropbox[2].

Η τελευταία περίπτωση που θα δούμε συνέβη το Σεπτέμβριος του 2014 στο γίγαντα του διαδικτύου, όπως την αποκαλούν, τη Google. Μετά από μια επιτυχή επίθεση, είχαν κλαπεί οι ηλεκτρονικές διευθύνσεις και οι κωδικοί πρόσβασης από σχεδόν 5 εκατομμύρια χρήστες. Αυτό ήταν ένα σημαντικό πλήγμα στη εταιρεία για το λόγο ότι αρκετά άτομα αλλά και εταιρείες μικρού ή μεσαίου μεγέθους χρησιμοποιούν τις υπηρεσίες και τα εργαλεία της Google για προσωπική και για επαγγελματική χρήση. Οι υπηρεσίες της περιλαμβάνουν εκτός από τη χρήση ηλεκτρονικού ταχυδρομείου, το συγχρονισμό και διαφύλαξη ή και διαμοίραση αρχείων στο Google Drive όπως επίσης και τη χρήση των Google Docs για δημιουργία αρχείων κειμένου και παρουσίασης. Μόλις είχε γίνει γνωστό στο ευρύ κοινό η επίθεση αυτή, η Google προσέτρεξε να ανακοινώσει ότι μόλις το 2% των κωδικών ήταν σε χρήση αλλά προέτρεπε όλους τους χρήστες της να αλλάξουν το κωδικό τους για λόγους ασφαλείας. Συνοπτικά μπορούμε να δούμε μερικούς κωδικούς στο πιο κάτω πίνακα [08].

| | | | | |
|---|---|---|---|---|
| Qwerty | 123456 | 123qwe | 1q2w3e | 123456789 |
| 1q2w3e4r5t | q1w2e3r4t5 | 123456789a | 123456q | qwerty1 |
| 25011990 | ghhh47hj7649 | 666666 | 112233 | asdasd |
| Adidas | master | 123qweasdzxc | qaz123 | 12344321 |

**Πίνακας 2.4:** Μερικοί από τους κωδικούς που είχαν οι χρήστες της Google[3].

[2] Αρχείο με τους κωδικούς: https://www.dropbox.com/s/dconj6n0e93168l/DropBox%20User%26Pass.txt?dl=0

Παρόλο που η επίθεση στη Google επετεύχθη με τη τεχνική SQL Injection, ο πίνακας 2.4 περιέχει κωδικούς που μας αποδεικνύει ότι και πάλι με χρήση ενός word list κάποιος μπορεί να πετύχει σχετικά εύκολα πρόσβαση σε ένα λογαριασμό.

Τα παραδείγματα που προαναφέρθηκαν αντιστοιχούν σε ένα πάρα πολύ μικρό δείγμα τόσο των επιθέσεων που γίνονται σ' ολόκληρο τον κόσμο αλλά και των στοιχείων που υποκλέπτονται ανάλογα με τη κάθε περίσταση. Και στις 4 περιπτώσεις υπήρχαν κωδικοί με ικανοποιητικό βαθμό δυσκολίας και με περισσότερους χαρακτήρες, οι πίνακες όμως παρουσιάζουν τους πιο εύκολους και συχνούς κωδικούς. Παρατηρώντας τους πίνακες με τους κωδικούς, οι χρήστες θυσιάζουν για χάριν της δικής ευκολίας τους και μόνο, τη ασφάλεια, τη ακεραιότητα των δεδομένων και των πληροφοριών που ανταλλάζουν με φίλους, γνωστούς αλλά και πελάτες, ενδεχομένως, με το να χρησιμοποιούν ένα εύκολο και σε αρκετές περιπτώσεις μάλιστα κοινό κωδικό. Αυτή η συνήθης και πάγια τακτική του εύκολου κωδικού οφείλεται, κατά κύριο λόγο, στη έλλειψη γνώσεων για τη δημιουργίας ενός ασφαλούς και δυνατού κωδικού από πλευράς χρηστών και κατά δεύτερο λόγο στη άγνοια και το σκεπτικό ότι δεν έχουν στη κατοχή τους σημαντικά δεδομένα που χρήζουν προστασίας.

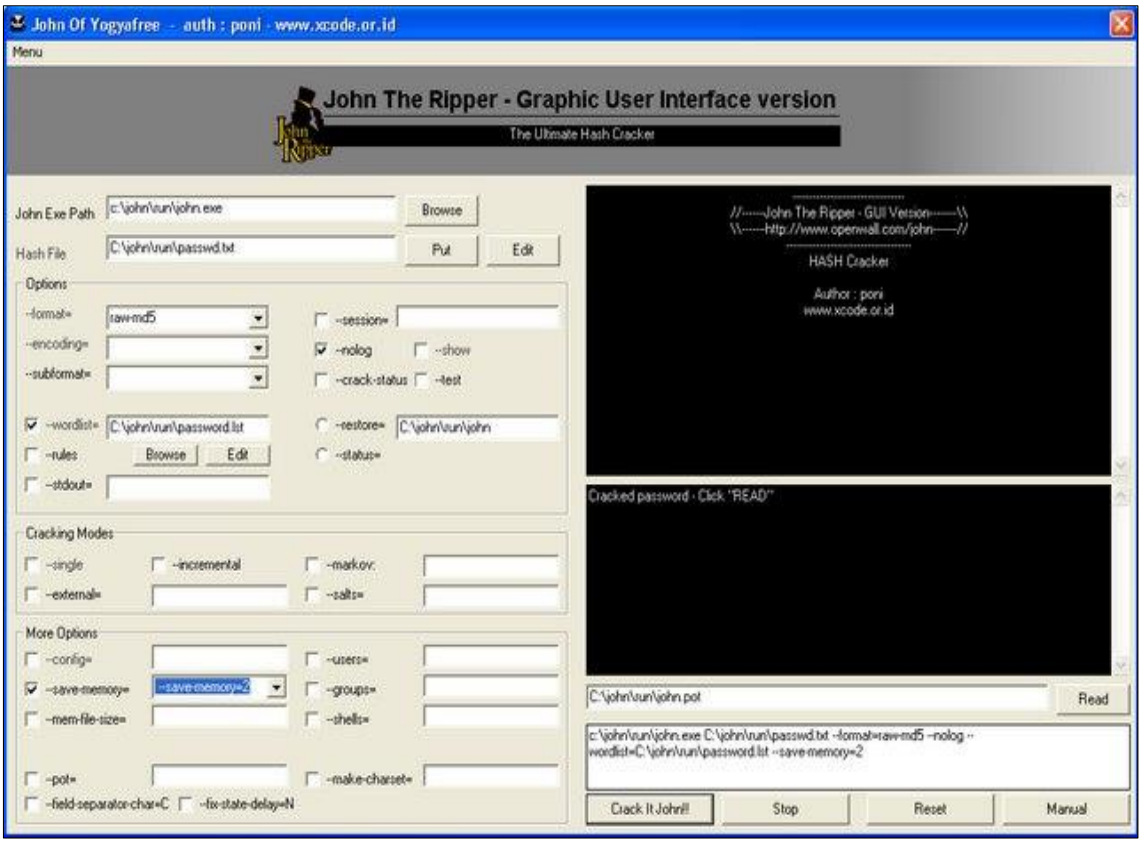
## 2.2 Εργαλεία ανεύρεσης και ανάκτησης κωδικών

Στη συνέχεια θα αναφερθούν μερικά κορυφαία προγράμματα ανάκτησης και ανεύρεσης κωδικών. Χρησιμοποιούνται από τους κυβερνοεγκληματίες για ανάκτηση και αποκρυπτογράφηση κωδικών που έχουν στη κατοχή τους μετά από μια επιτυχή επίθεση σε ένα εταιρικό δίκτυο ή κάποιο διακομιστή. Οι διαχειριστές συστημάτων τα χρησιμοποιούν για σκοπούς διενέργειας ελέγχων ανεύρεσης αδύναμων κωδικών που κατέχουν οι χρήστες όπως επίσης για τα συστήματα, υπηρεσίες και διαδικτυακές εφαρμογές που χειρίζονται και επιβλέπουν. Η χρήση τέτοιου είδους προγραμμάτων είναι ουσιαστικά δίκοπο μαχαίρι, από τη μια γίνεται αλόγιστη χρήση με απώτερο στόχο να καταφέρουν διείσδυση σε διάφορα συστήματα όπως εξυπηρετητές που διατηρεί η εταιρία και υποκλοπή δεδομένων ενώ από τη άλλη να γίνουν διάφοροι εσωτερικοί έλεγχοι ασφαλείας για όπως κωδικούς των χρηστών αλλά και των ίδιων των συστημάτων.

[3] Αρχείο με τους κωδικούς: https://www.dropbox.com/s/sg23gsc54fp76mp/gmail%20pass.txt?dl=0

### 2.2.1 John the Ripper

Ένα από τα πιο γνωστά εργαλεία στη κατηγορία αυτή [25], είναι δωρεάν και ανοικτού κώδικα. Αυτό του δίνει τη δυνατότητα να δέχεται επιπρόσθετα αρχεία κειμένου που περιέχουν εντολές για δημιουργία κωδικών όπως επίσης σύνολα κανόνων που χρησιμεύουν στη αποκρυπτογράφηση. Ο κυρίως σκοπός του είναι με τη διεξαγωγή πειραμάτων και δοκιμών, να ανευρεθούν αδύναμοι και επισφαλής κωδικοί ασφαλείας που χρησιμοποιούνται από διάφορα λειτουργικά συστήματα αλλά και στη δημιουργία περίπλοκων κωδικών χρησιμοποιώντας διάφορους συνδυασμούς, όπως αυτοί αναφέρονται στα 4 βήματα πιο πάνω, τόσο για προσωπική χρήση όσο και για τους χρήστες εντός μιας εταιρείας [34]. Με τη ίδια ευκολία μπορεί να χρησιμοποιηθεί κακόβουλα, από μεμονωμένα άτομα για να αποκρυπτογραφήσουν κωδικούς που έχουν προηγουμένως υποκλέψει ή τους έχουν δοθεί από κάποιο τρίτο άτομο.

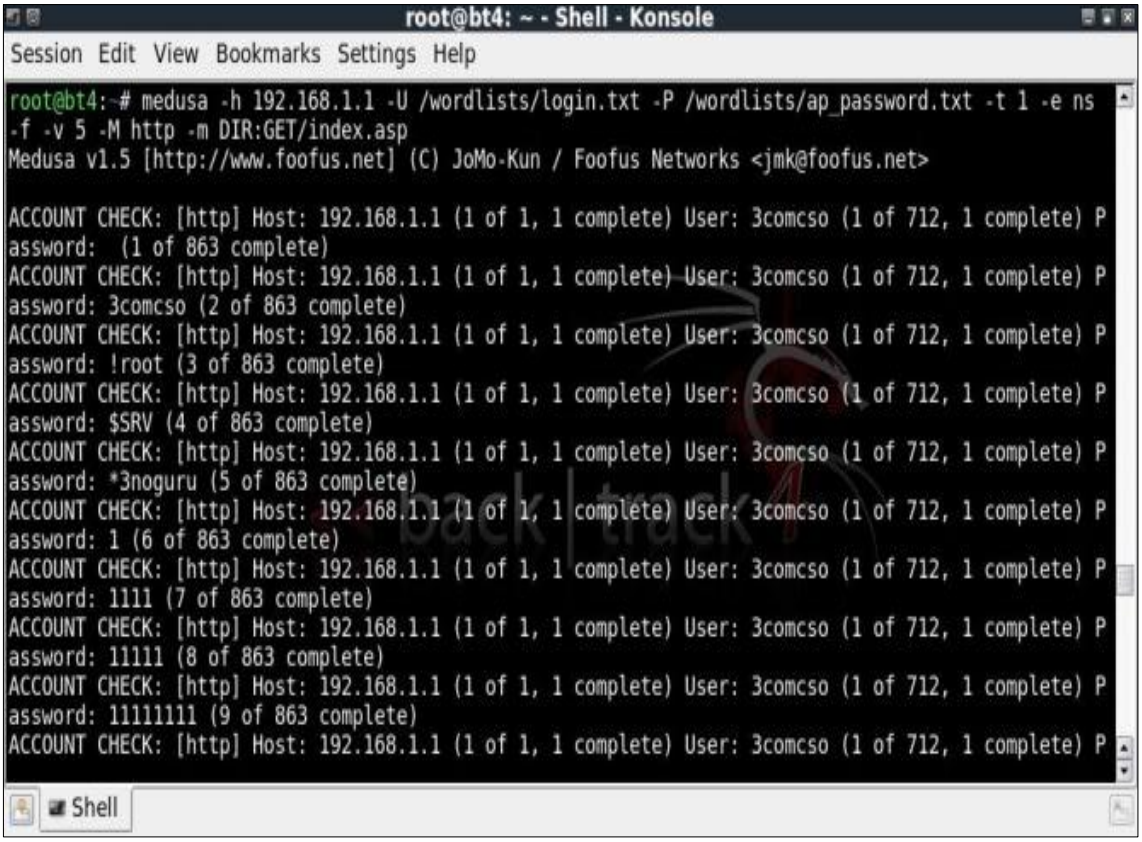



**Εικόνα 2.1:** Το γραφικό περιβάλλον του προγράμματος John the Ripper.

### 2.2.2 Medusa

Ένα ακόμη εργαλείο για τον έλεγχο των κωδικών πρόσβασης [07], ανοικτού κώδικα αλλά με τη διαφορά ότι η χρήση του γίνεται κατά κόρον για τον παράλληλο έλεγχο κωδικών σε αρκετά

διαδικτυακά πρωτόκολλα, συσκευές και υπηρεσίες [02] έχοντας τη δυνατότητα να δέχεται αρχεία κειμένου που περιέχουν συνδυασμούς όνομα χρήστη και κωδικό για να διενεργήσει ελέγχους. Μπορεί να χρησιμοποιηθεί από διαχειριστές συστημάτων για έλεγχο ρουτίνας των συστημάτων που έχουν συγκρίνοντας τον υπάρχων συνδυασμό ονόματος χρήστη και κωδικού με λίστες άλλων τέτοιων συνδυασμών έτσι ώστε να αυξήσουν ακόμη περισσότερα τα μέτρα ασφάλειας. Δεν έχει γραφικό περιβάλλον και δέχεται μόνο εντολές από τη γραμμή εντολών.

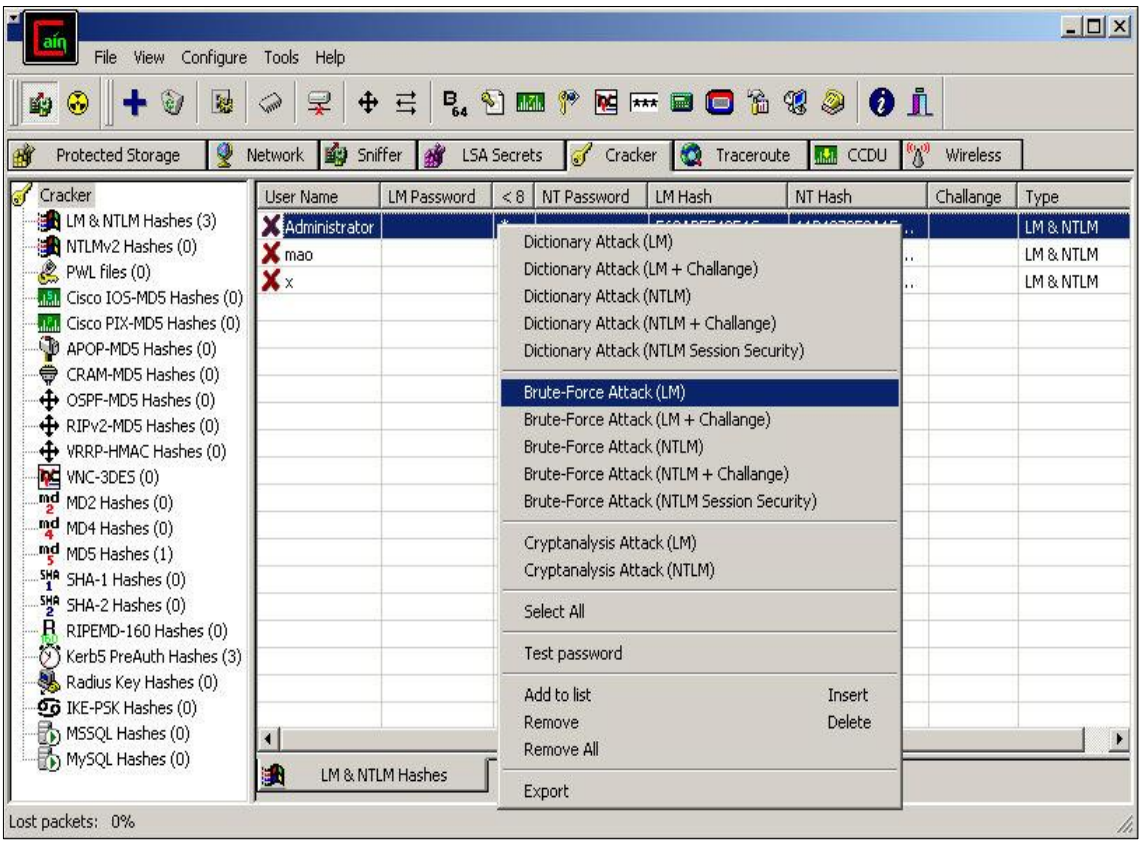



**Εικόνα 2.2:** Το περιβάλλον Linux του προγράμματος Medusa.

### 2.2.3 Cain and Abel

Δωρεάν εργαλείο κλειστού κώδικα, απευθύνεται για λειτουργικά συστήματα της Microsoft, που όχι μόνο χρησιμεύει στο να ανακτηθούν κωδικοί πρόσβασης και διαπιστευτήρια σε περίπτωση απώλειας αλλά οι δυνατότητές του επεκτείνονται στο έλεγχο διάφορων πρωτοκόλλων ασφαλείας, καταγραφή και παρακολούθηση της ροής δεδομένων σε ένα δίκτυο για εντοπισμό κωδικών, αποκρυπτογράφηση κωδικών με διάφορες μεθόδους όπως επίσης ανάκτηση κωδικών για ασύρματα δίκτυα. Το συγκεκριμένο πρόγραμμα δημιουργήθηκε με μοναδικό σκοπό και σκεπτικό να βοηθήσει τους διαχειριστές συστημάτων, σύμβουλους και υπεύθυνους ασφαλείας, εταιρείες που ασχολούνται με τη δημιουργία λογισμικών ασφαλείας και γενικά οποιονδήποτε

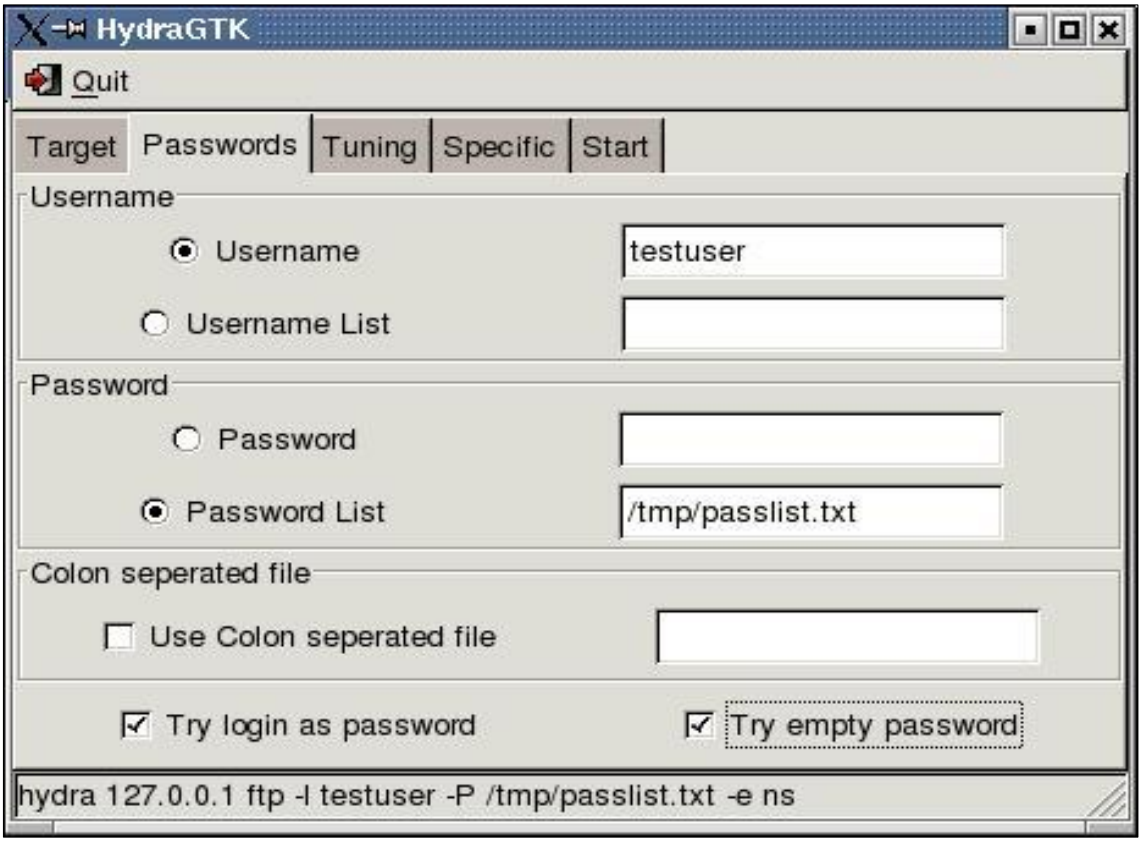
σκοπεύει να το χρησιμοποιήσει για ελέγχους ασφαλείας νοουμένου ότι θα κινηθεί μέσα στα πλαίσια ηθικής [26].




**Εικόνα 2.3:** Το γραφικό περιβάλλον του προγράμματος Cain and Abel.

### 2.2.4 THC Hydra

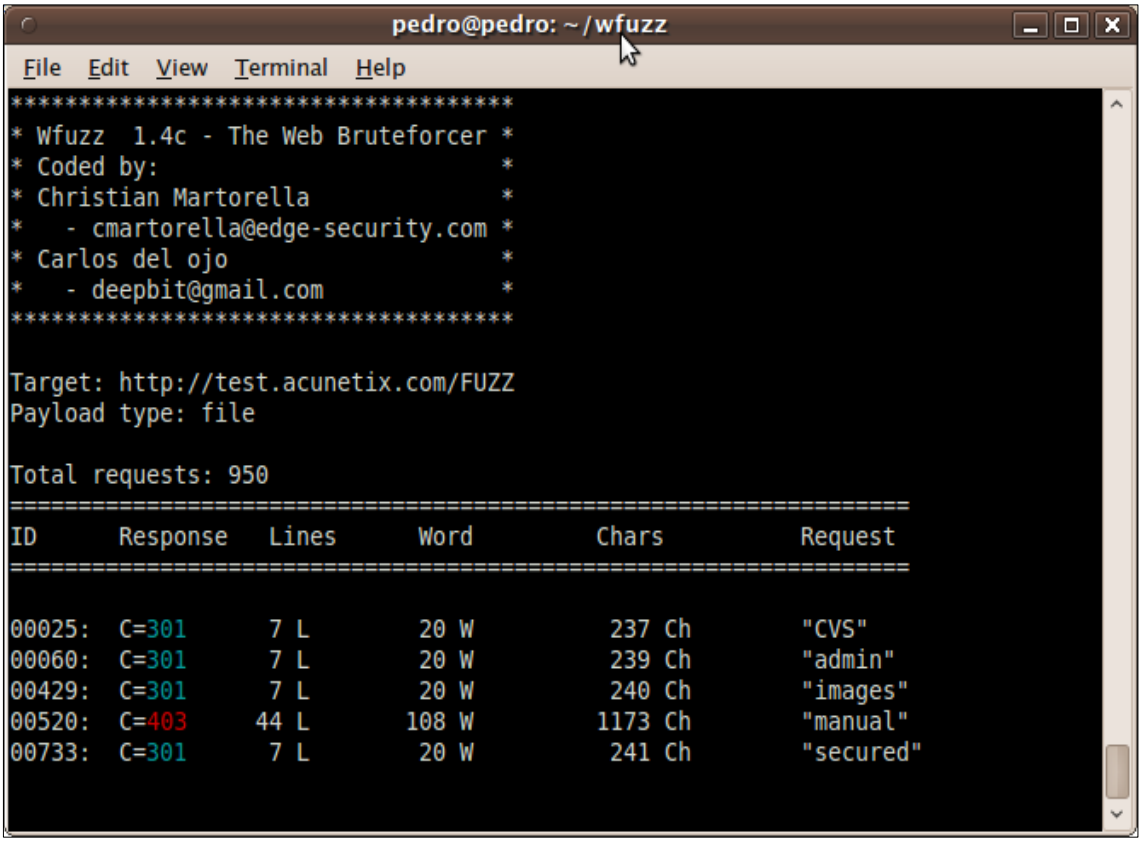
Εργαλείο παραπλήσιο των δυνατοτήτων του Medusa με τη διαφορά ότι διενεργεί ελέγχους ασφαλείας πολύ πιο ταχύτερα και με καλύτερη απόκριση. Είναι επίσης δωρεάν και διατίθεται για όλα τα λειτουργικά συστήματα [36], τόσο εκτελώντας εντολές από τη γραμμή εντολών όσο και μέσω γραφικού περιβάλλοντος. Χρησιμοποιεί συνδυασμούς από προκαθορισμένες λίστες με όνομα χρήστη και κωδικό έχοντας τη δυνατότητα προσθήκης περαιτέρω λιστών με συνδυασμούς που μπορεί να δημιουργήσει ο χρήστης [33].




**Εικόνα 2.4:** Το περιβάλλον Linux του προγράμματος THC Hydra.

### 2.2.5 Wfuzz

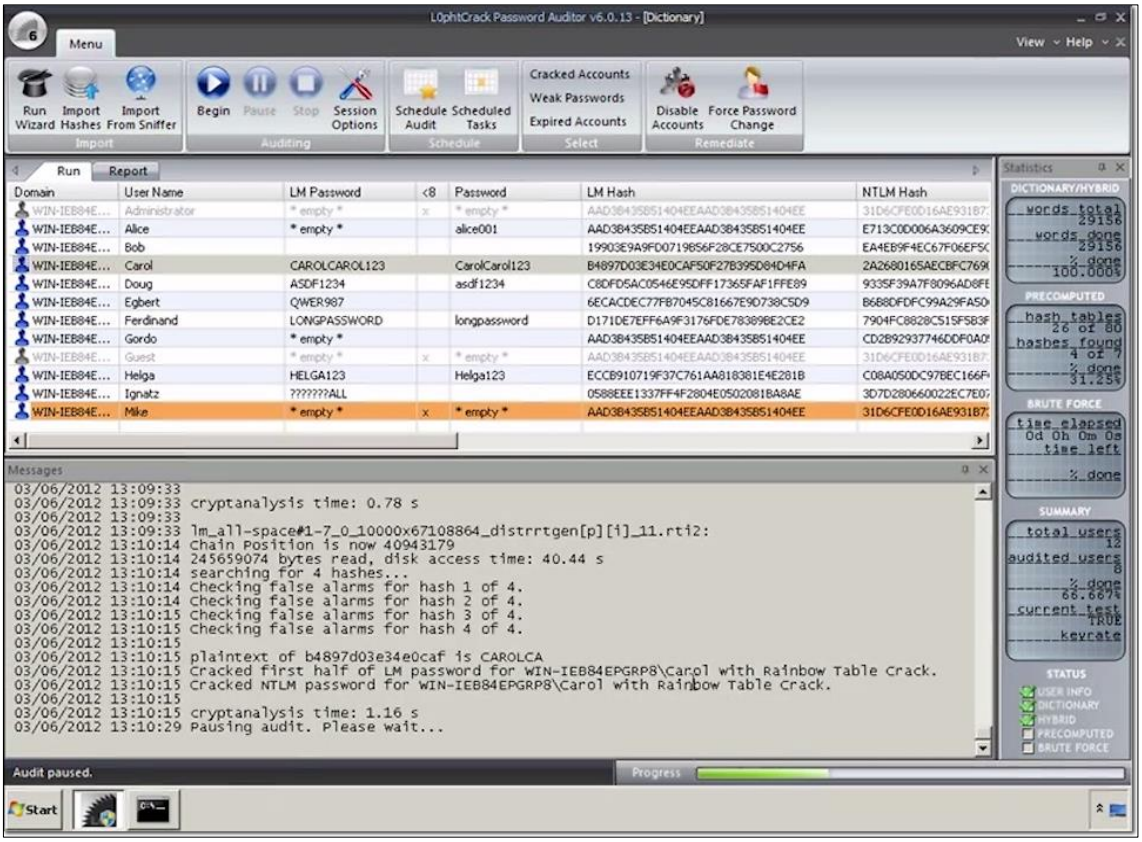
Το συγκεκριμένο εργαλείο [41] είναι κλειστού κώδικα, τρέχει σε υπολογιστικά συστήματα Windows και υποστηρίζει πλήθος λειτουργιών [05] που χρήση έχουν να κάνουν με τη ανεύρεση όνομα χρήστη και κωδικού σε διάφορες διαδικτυακές εφαρμογές όπως εφαρμογές ηλεκτρονικού ταχυδρομείου (webmail), ιστοσελίδες με φόρμα καταχώρησης στοιχείων για σύνδεση, φόρμα υποβολής αιτήματος και υποστήριξης και φόρμες συμπλήρωσης στοιχείων για αγορές μέσω διαδικτύου. Επιπρόσθετα μπορεί να χρησιμοποιηθεί και για άλλες παραμέτρους όπως για παράδειγμα στη μέθοδο GET και τη μέθοδο POST [37].




**Εικόνα 2.5:** Το περιβάλλον Linux του προγράμματος Wfuzz.

### 2.2.6 L0phtCrack

Το μοναδικό εργαλείο στο οποίο αναφέρεται η διάθεσή του μόνο επί πληρωμή. Αν και η εγκατάσταση του γίνεται σε περιβάλλον Windows, μπορεί πολύ εύκολα να χρησιμοποιηθεί και για άλλα λειτουργικά συστήματα. Διαθέτει πλειάδα χαρακτηριστικών καθιστώντας το ένα από τα πιο κορυφαία προγράμματα. Χρησιμοποιείται για τον εντοπισμό και αποκατάσταση ευπαθών κενών ασφαλείας από τη χρήση αδύναμων κωδικών, για να ανακτηθούν χαμένοι ή ξεχασμένοι κωδικοί πρόσβασης από Η/Υ αλλά και για να τεθούν υπό δοκιμασία και τεστ οι κωδικοί με σκοπό να ελεγχθεί το πόσο εύκολα μπορεί να ανακαλυφθεί για εξάλειψη ρίσκων ασφαλείας [19].




**Εικόνα 2.6:** Το γραφικό περιβάλλον του προγράμματος L0phtCrack.

Στις επόμενες γραμμές θα αναφερθούν επιγραμματικά οι μέθοδοι που χρησιμοποιούν τα προγράμματα που αναφέρθηκαν. Η επίθεση με τη χρήση λεξιλογίου (Dictionary Attack) αναφέρεται στη μέθοδος κατά την οποία χρησιμοποιούνται λίστες με κοινές λέξεις που μπορούν πολύ εύκολα να βρεθούν σε ένα λεξιλόγιο ή ακόμη από προκαθορισμένες λίστες με τις ίδιες λέξεις να έχουν μικρές αλλαγές όπως γραμμένες ανορθόγραφα. Αυτή η μέθοδος έχει αρκετό ποσοστό επιτυχίας για τον απλό λόγο ότι οι άνθρωποι τείνουν να χρησιμοποιούν απλές λέξεις σαν κωδικό [12]. Η επίθεση τύπου Brute Force attack επιτρέπει τη χρήση προκαθορισμένων κωδικών και λέξεων για να ανακαλύψει το κωδικό του χρήστη. Μπορεί επίσης να κάνει συνδυασμούς όλων των γραμμάτων, αριθμών και ειδικών χαρακτήρων μέχρι να ανευρεθεί ο σωστός συνδυασμός, με μοναδικό αρνητικό χαρακτηριστικό ότι απαιτείται αρκετός χρόνος για τη τελική επίτευξη του στόχου [04]. Η επίθεση υβριδικού τύπου (Hybrid Attack), μια πολύ ενδιαφέρουσα μέθοδος που παρομοιάζεται με τον τρόπο σκέψης ενός επιτιθέμενου, είναι ο συνδυασμός των μεθόδων Dictionary και Brute Force attack για περισσότερα και καλύτερα αποτελέσματα. Με αυτή τη μέθοδο η πιθανότητα επιτυχίας, δεδομένης μιας λίστας με κοινές λέξεις και της προσθήκη αριθμών και συμβόλων είναι μεγαλύτερη [31]. Η χρήση των Rainbow Tables[4] σε μια επίθεση

[4] https://www.freerainbowtables.com/en/tables2/

είναι μια σχέση μεταξύ χρόνου (πόσος απαιτείται μέχρι να βρεθεί ο σωστός κωδικός) και χώρου (πόσους διαφορετικούς κωδικούς έχουμε παράγει και έχουμε στη διάθεσή μας για δοκιμή). Βασίζεται σε προκαθορισμένες λίστες με όλους τους πιθανούς συνδυασμούς και παραλλαγές κρυπτογραφημένων κωδικών βάση συγκεκριμένου αλγόριθμου κρυπτογράφησης. Η διαδικασία για να βρεθεί ο κάθε κωδικός από τον επιτιθέμενο γίνεται μετά από σύγκριση των κρυπτογραφημένων κωδικών από μια βάση δεδομένων που υπέκλεψε και της δικής του βάσης που προηγουμένως έχει δημιουργήσει [17]. Η χρήση μιας λίστας λέξεων (Word List[5]) σε μια επίθεση είναι μια συλλογή λέξεων πανομοιότυπη με τη μέθοδο Dictionary Attack. Η διαφορά βρίσκεται στη προσθήκη λέξεων που προέρχονται από κάποια αργκό, από κάποια άλλη γλώσσα / διάλεκτο [32] ή ακόμη με τη χρήση κεφαλαίων γραμμάτων και αριθμών. Η καταγραφή ροής πακέτων δικτύου (Network Packet Sniffing) είναι ένα πρόγραμμα ή μηχάνημα με μοναδικό σκοπό να καταγράφει όλη τη κίνηση που γίνεται μέσα σ' ένα δίκτυο. Μπορεί να χρησιμοποιηθεί από διαχειριστές δικτύου για διάγνωση και πρόληψη προβλημάτων για ομαλή λειτουργία του δικτύου αλλά και από επιτιθέμενους για να κατασκοπεύσουν τη κίνηση που έχει το συγκεκριμένο δίκτυο και να υποκλέψουν ευαίσθητα δεδομένα, συμπεριλαμβανομένου και κωδικών [35]. Τελευταίο στη λίστα μας είναι η κρυπτανάλυση (Cryptanalysis) όπου ο επιτιθέμενος προσπαθεί να βρει σημεία αδυναμίας και αστοχίας κατά τη συγγραφή του κώδικα στη κρυπτογραφική μέθοδο που χρησιμοποιήθηκε και να καταφέρει να ανακτήσει και αποκρυπτογραφήσει το κωδικό σε απλή μορφή. Πέραν της χρήσης της για κρυπτογράφηση των κωδικών των χρηστών, χρησιμοποιείται από κυβερνήσεις για στρατιωτικούς και διπλωματικούς σκοπούς όπως επίσης και από προγραμματιστές για ενδυνάμωση των μέτρων ασφαλείας και διασφάλιση των προγραμμάτων που δημιούργησαν [14].

## 2.3 Λόγοι ύπαρξης πολυπλοκότητας κωδικών

Η χρήση κωδικού είναι ο τρόπος με τον οποίο αναγνωρίζεται και αυθεντικοποιείται ένας χρήστης, ότι όντως είναι αυτός, σε ένα ηλεκτρονικό σύστημα ή μια online φόρμα συμπλήρωσης στοιχείων μιας ιστοσελίδας. Σαν θετικά στοιχεία μπορούμε να αναφέρουμε ότι πρόκειται για μια εύκολη διαδικασία ολοκλήρωσης που δεν απαιτεί χρόνο για να ολοκληρωθεί ή τη χρήση εξειδικευμένων και ακριβών υλικών και συσκευών [43] παρά μόνο ο χρήστης να τον θυμάται και να τον πληκτρολογήσει σωστά. Σαν αρνητικά όμως μπορούμε να θεωρήσουμε ότι μπορεί εύκολα κάποιος να τον μαντέψει, εφόσον κατέχει αρκετές γνώσεις που αφορούν στη προσωπική ζωή του ατόμου που έχει βάλει στόχο, μπορεί να παραβιαστεί χρησιμοποιώντας τα ειδικά

[5] https://crackstation.net/buy-crackstation-wordlist-password-cracking-dictionary.htm

προγράμματα που αναφέρθηκαν, η τυχών απώλεια της συσκευής αυθεντικοποίησης και στο ότι οι χρήστες συνηθίζουν να τοποθετούν σε φανερό σημείο και ιδίως κοντά στον υπολογιστή τους ένα κομμάτι χαρτί με αναγραμμένο το κωδικό τους, δίνοντας έτσι τη ευκαιρία στον οποιονδήποτε να μάθει το κωδικό τους.

Κατά τη διαδικασία δημιουργίας ενός νέου ηλεκτρονικού λογαριασμού από ένα υποψήφιο χρήστη τα ζητούμενα που χρειάζεται να έχει ένας κωδικός για να πληρούνται οι πολιτικές ασφαλείας που απαιτεί η κάθε εταιρεία ή οργανισμός, είναι κοινά στις πλείστες περιπτώσεις. Τα 4 βήματα που πρέπει να ακολουθούνται πιστά είναι:

- Χρήση κεφαλαίων λατινικών γραμμάτων ( A~Z )
- Χρήση πεζών λατινικών γραμμάτων ( a~z )
- Χρήση αριθμών και ( 0~9 )
- Χρήση ειδικών χαρακτήρων ( ! @ # $ κτλ. )

Ο μέσος χρήστης δεν είναι συνηθισμένος στο να συνδυάζει όλα τα βήματα με τον πιο αποτελεσματικό τρόπο, δημιουργώντας ένα φαινομενικά ισχυρό και μη προβλέψιμο κωδικό που στη πραγματικότητα ο χρήστης θέτει τον εαυτό του είναι σαν ένα ακόμη υποψήφιο για να του παραβιάσουν το λογαριασμό. Για παράδειγμα, υποθέτοντας ότι και τα 4 βήματα είναι προαπαιτούμενα στη φάση δημιουργίας κωδικού, ο χρήστης θα προτιμήσει να χρησιμοποιήσει για κεφαλαίο το πρώτο ή το μεσαίο ή το τελευταίο γράμμα, τα υπόλοιπα γράμματα θα είναι πεζά και στο τέλος του κωδικού θα χρησιμοποιήσει ένα ψηφίο αριθμού και για ειδικό χαρακτήρα θα βάλει είτε θαυμαστικό (!) είτε το λεγόμενο παπάκι (@) [20]. Υπάρχουν φυσικά περιπτώσεις όπου η ίδια η ιστοσελίδα δεν ακολουθεί μια ασφαλής πολιτική για θέματα κωδικών με αποτέλεσμα να θέτει σε κίνδυνο εξ αρχής το κάθε χρήστη θέτοντας περιορισμούς που φτάνουν στα όρια αμφισβήτησης των μέτρων ασφαλείας που την διέπουν [16] ή να καθορίσει το μέγιστο μήκος του κωδικού όπως στη περίπτωση του Outlook.com. Ιδανική λύση έρχεται από τη υπηρεσία Gmail δίνοντας στο χρήστη τη ευχέρεια να εισάγει μέχρι και 200 χαρακτήρες για κωδικό, ένα εκπληκτικά τεράστιο μήκος κωδικού [09].

## 2.4 Ασφάλεια κωδικών και ποιοι οι κίνδυνοι

Με δεδομένη τη ταχύτατη εξέλιξη του διαδικτύου και τους τρόπους που χρησιμοποιείται, σε μερικές περιπτώσεις δεν δίνεται η κατάλληλη βαρύτητα σε θέματα κωδικών ασφαλείας για το απλούστατο λόγο ότι δεν θεωρείται τόσο σημαντικός. Αρκετοί πιστεύουν ότι είναι χάσιμο χρόνου η δημιουργία ισχυρού κωδικού ή απλά δεν μπορούν να τον απομνημονεύσουν και με αυτό το σκεπτικό επιλέγουν κάτι που τους είναι εύκολο να το θυμούνται, όπως το όνομα του σκύλου, το όνομα του/της συζύγου, συνδυασμός ονομάτων των παιδιών τους, ημερομηνίες γενεθλίων ή ακόμη και αριθμούς τηλεφώνων. Με το ίδιο σκεπτικό θα δημιουργήσουν παρόμοιους κωδικούς για το ηλεκτρονικό ταχυδρομείο, για σελίδες κοινωνικής δικτύωσης, για το online banking, για τα παιχνίδια που παίζουν στο διαδίκτυο και γενικά όπου χρειάζεται να εισάγουν κωδικό. Ακόμη χειρότερο είναι η χρήση του ίδιου κωδικού σε περισσότερους από ένα λογαριασμούς. Εάν ένας επιτιθέμενος καταφέρει να μαντέψει επιτυχώς το κωδικό ή το πρότυπο που χρησιμοποίησε για ένα λογαριασμό, θα μπορεί να τον επαναχρησιμοποιήσει και να έχει πρόσβαση και σε άλλους λογαριασμούς, ακόμη και στη περίπτωση απόκτησης του κωδικού σε λογαριασμό που δεν περιέχει ευαίσθητα δεδομένα.

Σαν ένα επιπρόσθετο μέτρο ασφαλείας που μπορούν εύκολα οι χρήστες να χρησιμοποιήσουν για να έχουν ισχυρούς κωδικούς χωρίς να καταβάλουν ιδιαίτερη προσπάθεια απομνημόνευσης ή να είναι γραμμένοι σε ένα κομμάτι χαρτί, είναι η χρήση προγραμμάτων διαχείρισης κωδικών. Χρησιμεύουν για τη φύλαξη και διαχείριση όλων των κωδικών που έχει ένας χρήστης προστατευόμενοι σε μια τοποθεσία μόνο, τοπικά στον υπολογιστή, με ευκολία πρόσβασης, απαιτώντας τη απομνημόνευση ενός κυρίως κωδικού (master password). Είναι ένας από τους καλύτερους τρόπους για να έχει σε πλήρη έλεγχο όλους τους κωδικούς που χρησιμοποιεί για διάφορους λογαριασμούς χωρίς να είναι καταγεγραμμένοι σε ένα χαρτί με το ρίσκο να μπορέσει κάποιος να τους δει [15].

Η μελέτη των Li et al. που χρήζει ιδιαίτερης προσοχής και μεταχείρισης όσον αφορά το επίπεδο ασφάλειας που προσφέρουν τα προγράμματα διαχείρισης κωδικών. Οι συγγραφείς της συγκεκριμένης μελέτης έχουν καταδείξει κενά ασφαλείας σε μερικά τέτοια προγράμματα και προτρέπουν τους χρήστες να αναζητήσουν άλλο πρόγραμμα ή να καλυτερεύσουν τις μεθόδους και ικανότητες απομνημόνευσης [21].

## 2.5 Εργαλεία και τρόποι υποκλοπής κωδικών

Πιο κάτω θα μελετηθούν τα εργαλεία και οι τρόποι που χρησιμοποιούν οι επιτιθέμενοι για να υποκλέψουν και να έχουν στη κατοχή τους τόσο το όνομα χρήστη όσο και το κωδικό χωρίς να καταβάλουν ιδιαίτερη προσπάθεια. Θα αναφερθούμε στα hardware keyloggers και τα software keyloggers, όπου χαρακτηρίζει τη μέθοδο με τη οποία ότι πληκτρολογηθεί από το χρήστη, απλό κείμενο, σύνταξη ηλεκτρονικού ταχυδρομείου, εισαγωγή κωδικού, καταγράφεται και αναμεταδίδεται στο άτομο που έχει τοποθετήσει τη ανάλογη συσκευή ή πρόγραμμα στον υπολογιστή του θύματος.

Τα hardware keyloggers (υλικό / συσκευή καταγραφής πληκτρολόγησης) είναι συσκευές σε μορφή PS/2 για παλιά πληκτρολόγια ή USB για νέα πληκτρολόγια. Τελευταίος έχουν κάνει τη εμφάνισή τους και συσκευές με δυνατότητα ασύρματης σύνδεσης, για χρήση σε ασύρματα δίκτυα ή με Bluetooth, που διευκολύνει ακόμη καλύτερα την όλη διαδικασία [13]. Η συσκευή τοποθετείται ενδιάμεσα του ηλεκτρονικού υπολογιστή και του πληκτρολογίου και μπορεί να καταγράφει τα πάντα από τη στιγμή που τίθεται σε λειτουργία ο υπολογιστής. Διαθέτουν αρκετή εσωτερική μνήμη ώστε να καταγράψουν αρκετά δεδομένα για μεγάλο χρονικό διάστημα που μπορούν να χρησιμοποιηθούν σε μελλοντική κακόβουλη χρήση. Ο πιο εύκολος τρόπος ανίχνευσης είναι δια του οπτικού ελέγχου, εφόσον ο χρήστης ή κάποιος τεχνικός το αναγνωρίσει, υπάρχουν όμως περιπτώσεις όπου δεν είναι εφικτή η επαφή με τον υπολογιστή και έτσι μόνο το άτομο που έχει τοποθετήσει τη συσκευή το γνωρίζει. Το επόμενο στάδιο είναι η περισυλλογή της συσκευής και η καταγραφή των δεδομένων με όποια συνέπεια αυτό έχει [23].

Τα software keyloggers (λογισμικό καταγραφής πληκτρολόγησης) είναι πρόγραμμα παρακολούθησης του υπολογιστή του χρήστη και αυτό γίνεται εν αγνοία του. Η εγκατάσταση μπορεί να γίνει είτε αυτούσια από ένα κακόβουλο χρήστη, είτε όταν λάβει ένα μήνυμα ανεπιθύμητης αλληλογραφίας και ανοίξει το συνημμένο αρχείο ή το διαδικτυακό σύνδεσμο. Πέραν της καταγραφής των κωδικών που εισάγει ο χρήστης κάθε φορά, διαθέτουν δυνατότητες όπως καταγραφή των ιστοσελίδων που ανοίγει ο χρήστης, συνομιλίες που έχει με άλλα άτομα μέσω προγραμμάτων ανταλλαγής μηνυμάτων, καταγραφή προγραμμάτων που χρησιμοποιεί, να παίρνει στιγμιότυπα της οθόνης ανά τακτικά διαστήματα, καταγραφή των ηλεκτρονικών του μηνυμάτων και όλα αυτά να γίνονται χωρίς ο χρήστης να έχει κάποια ένδειξη ή υποψία. Έχουν εξελιχθεί σε μεγάλο βαθμό ώστε να μην ανιχνεύονται από προγράμματα καταπολέμησης ιών, δεν εμφανίζονται στη λίστα προσθαφαίρεσης προγραμμάτων και αυτό τα καθιστά πολύ δύσκολα στα να ανευρεθούν [11].

# Κεφάλαιο 3
# Υπόβαθρο – Σχετική βιβλιογραφία

Σε αυτό το κεφάλαιο θα αναφερθούμε στις δυνατότητες που έχει η ανθρώπινη μνήμη, αν και είναι πεπερασμένη, στο να συγκρατεί διάφορες πληροφορίες και τρόπους με τους οποίους τις ανακαλεί όταν και εφόσον χρειάζεται. Επίσης θα συζητηθούν παρόμοια τεστ που έγιναν με χρήση εθελοντών για τις συνήθειες και τις δυνατότητές τους στο να δημιουργήσουν ένα ισχυρό κωδικό με τη διαφορά όμως ότι κανένας εθελοντής την ώρα που διεξάγονταν τα τεστ δεν υπάγονταν σε κάποιο εταιρικό περιβάλλον αλλά ήταν μέσα στα πλαίσια διεξαγωγής έρευνας σε ελεγχόμενο περιβάλλον[6].

[6] Με τη έννοια ότι δεν χρησιμοποιούσαν τους πραγματικούς κωδικούς τους, υπάγονταν σε ορισμένους περιορισμούς και οι ερευνητές είχαν πλήρη πρόσβαση στον εκάστοτε κωδικό για μετέπειτα μελέτη και εξαγωγή συμπερασμάτων.

## 3.1 Ανθρώπινο μνημονικό

Οι άνθρωποι τείνουν να ξεχνάνε απλά καθημερινά πράγματα και γεγονότα που στη ουσία τους είναι αναγκαία. Ξεκινώντας για τη δουλειά μπορεί να ξεχάσουν ένα σημαντικό έγγραφο που θα τους είναι χρήσιμο σε μια προγραμματισμένη συνάντηση ή παρουσίαση, παίρνοντας το πορτοφόλι τους να ξεχάσουν ότι δεν πήγαν από τη τράπεζα να βγάλουν χρήματα όπως επίσης μια επέτειος γάμου, γενέθλια συγγενικού προσώπου είναι πιθανό να ξεχαστούν. Οι έντονοι και γρήγοροι ρυθμοί της ζωής σε συνδυασμό με το άγχος μας οδηγούν αρκετές φορές στο να μην μπορούμε να συγκρατήσουμε όλες τις αναγκαίες πληροφορίες που χρειαζόμαστε αφού καθημερινά είμαστε δέκτες ενός μεγάλου όγκου πληροφοριών, εκ των οι περισσότερες συχνά μας είναι αχρείαστες.

Η μελέτη που εκπονήθηκε από τον ειδήμονα της γνωστικής ψυχολογίας το 1956 George A. Miller [24] μελετά σε βάθος την ικανότητα που έχει ο άνθρωπος και κατά συνέπεια το ανθρώπινο μυαλό στο να συγκρατεί όσες περισσότερες πληροφορίες μπορεί. Παραθέτοντας και αναλύοντας μια σειρά από πειράματα που είχαν διεξαχθεί για το σκοπό αυτό, φάνηκε η αδυναμία των εθελοντών να συγκρατήσουν περισσότερα των 7 αντικειμένων σε κάθε πείραμα. Όσο τα αντικείμενα ήταν λιγότερα ή ίσα των 7, ήταν πολύ εύκολο να τα αποστηθίσουν και να τα αναφέρουν με τη σωστή σειρά. Πηγαίνοντας όμως τα πειράματα ένα βήμα παρακάτω και αυξάνοντας το πλήθος των αντικειμένων, παρατηρήθηκε σημαντική μείωση στη ικανότητα αποστήθισης καθιστώντας έτσι σχεδόν αδύνατη τη ολοκλήρωση των πειραμάτων με τα αναμενόμενα αποτελέσματα. Ο Miller αναφέρει μέσα στο άρθρο του «*ότι ο αριθμός των δεδομένων (bits) πληροφορίας είναι συνεχής για τη απόλυτη κρίση ενώ ο αριθμός των κομματιών (chunks) της πληροφορίας είναι συνεχής για τη άμεση μνήμη. Η διάρκεια της άμεσης μνήμης φαίνεται να είναι σχεδόν ανεξάρτητη του αριθμού των δεδομένων (bits) ανά κομμάτι*». Χωρίζοντας και οργανώνοντας την προς απομνημόνευση πληροφορία σε κομμάτια, είναι ένας ευκολότερος τρόπος να γίνει η αποστήθιση των αντικειμένων και γενικά των πληροφοριών που χρειαζόμαστε μπορώντας έτσι να δημιουργήσουμε ακόμη μεγαλύτερα κομμάτια με περισσότερη πληροφορία.

Περνώντας τώρα σε νεότερα πειράματα, θα μελετήσουμε προτάσεις και εισηγήσεις άλλων ερευνητών που αποσκοπούν στη περαιτέρω ασφάλεια χρηστών και Η/Υ μέσω της απομνημόνευσης κωδικών. Ενδιαφέρων παρουσιάζει η πρόταση της συγγραφέας Manasa [22] όπου γίνεται λόγος για τη χρήση εικόνων αντί για των καθιερωμένων κωδικών κειμένου. Οι χρήστες σε αυτή τη περίπτωση δεν χρειάζεται να απομνημονεύουν κάποιο κωδικό αλλά να

θυμούνται ποια είναι η εικόνα που επέλεξαν καθώς και ποια τα σημεία που επέλεξαν σαν περιοχή για κωδικό, δίνοντας έτσι τη δυνατότητα σε κάθε χρήστη να χρησιμοποιήσει εικόνα του δικού του ενδιαφέροντος που θα τον διευκολύνει. Όταν θα εμφανίζεται στη οθόνη η εκάστοτε εικόνα, η μόνη ενέργεια που χρειάζεται να γίνει από μεριάς χρήστη είναι να χρησιμοποιήσει το ποντίκι του Η/Υ και να επιλέξει τη συγκεκριμένη περιοχή στη εικόνα που αποτελεί ένα μέρος του κωδικού του. Στη συνέχεια και αφού επιλεγεί το σωστό σημείο, ο χρήστης προτρέπεται στο να επιλέξει το επόμενο σημείο. Η διαδικασία επαναλαμβάνεται μέχρι να ολοκληρωθεί επιτυχώς η επιλογή όλων των σωστών σημείων (στη συγκεκριμένη μελέτη γίνεται αναφορά για σύνολο πέντε σημείων). Η μέθοδος αυτή αποτρέπει την υποκλοπή κωδικών, μιας και δεν εισάγεται κάποιος κωδικός αλλά επιλέγονται μερικά σημεία στη εικόνα. Η ίδια τεχνική περιγράφεται και με μια μικρή παραλλαγή. Αντί να επιλέγονται πέντε διαφορετικά σημεία στη ίδια εικόνα, η νέα μέθοδος κάνει λόγο για χρήση πέντε διαφορετικών εικόνων με σειριακό τρόπο εμφάνισης. Σε αυτή τη περίπτωση ο κάθε χρήστης οφείλει να θυμάται έκτος των περιοχών επιλογής για κωδικό, τις εικόνες που αντιστοιχούν για τη ολοκλήρωση της διαδικασίας για εισαγωγή του στο σύστημα. Με τη νέα μέθοδο, αυξάνεται περισσότερο η πιθανότητα μη εύρεσης των σωστών περιοχών επιλογής της εικόνας αφού η χρήση περισσότερων της μιας εικόνας καθιστά την όλη διαδικασία ακόμη πιο περίπλοκη και δύσκολη για όποιο δεν γνωρίζει τα σωστά σημεία. Η τελευταία μέθοδος που περιγράφεται αναφέρεται στη χρήση εικονιδίων σε συνδυασμό με φόντο χρωμάτων. Ο κάθε χρήστης αρχικά πρέπει να επιλέξει το χρώμα που επιθυμεί (αναφέρονται 3 έως 5 χρώματα), τα εικονίδια που θα πρέπει να αναγνωρίζει (προτείνονται 2, περισσότερα θεωρούνται ακόμη πιο ασφαλή) και το επίπεδο ασφαλείας που θέλει (υπάρχουν 3 επίπεδα). Στη συνέχεια τα εικονίδια παρουσιάζονται με τυχαία σειρά κάθε φορά στη οθόνη του χρήστη και επιλέγοντας μόνο τη γραμμή που εμφανίζονται, όχι τα ίδια τα εικονίδια, αυτόματα τα εικονίδια της γραμμής αντικαθίστανται από το εικονίδιο της κλειδαριάς. Μετά τη σωστή επιλογή όλων των εικονιδίων ο χρήστης μπορεί να εργαστεί στον Η/Υ του.

Η πιο πάνω μελέτη της Manasa κρίνεται αρκετά ενδιαφέρουσα από τη άποψη ότι μια τέτοια μέθοδος απομακρύνει κάθε σκέψη μη εξουσιοδοτημένης πρόσβασης στον Η/Υ του χρήστη για υποκλοπή των δεδομένων του. Επίσης είναι αποτρεπτική και για άλλου είδους κακόβουλες επιθέσεις ή χρήσης προγραμμάτων εύρεσης κωδικών όπως έχουν αναφερθεί σε προηγούμενο κεφάλαιο. Στη δική μας περίπτωση όμως κρίνεται σαν μη αναγκαία και χρήσιμη για τους εξής λόγους:

1. Εάν αφήσουμε στη κρίση του κάθε χρήστη να προσκομίσει εικόνες δικής του επιλογής, ίσως παρατηρηθεί το φαινόμενο να δοθούν εικόνες που τις έχει ήδη μοιραστεί με άλλα

άτομα στη εταιρεία απλά και μόνο δείχνοντας τες από το κινητό του ή είναι ήδη αναρτημένες σε σελίδες κοινωνικής δικτύωσης όπου εκεί ο καθένας μπορεί να τις δει.

2. Εάν η επιλογή των εικόνων γίνει από το τμήμα Πληροφορικής της εταιρείας σίγουρα θα επιλεγούν εικόνες που απεικονίζουν αρκετή πληροφορία, δεν έχουν κάποιο συγκεκριμένο θέμα και αυτό ίσως οδηγήσει σε δυσφορία από μεριάς των χρηστών γιατί θα τους είναι δύσκολο να επιλέξουν.

3. Δεν γίνεται καμία αναφορά για τις απαιτήσεις που θα χρειαστούν σε υλικό και λογισμικό ώστε να μπορεί να εφαρμοστεί πλήρως και να λειτουργεί απρόσκοπτα το σύστημα που θα υποστηρίζει αυτό το μηχανισμό αυθεντικοποίησης των χρηστών.

4. Τέλος, η μέθοδος επιλογής χρωματικών εικονιδίων σε συνδυασμό με το επίπεδο ασφαλείας ίσως να μπερδεύει τους χρήστες οδηγώντας τους να επιλέγουν πάντοτε το πιο εύκολο επίπεδο. Στο παράδειγμα που δίνεται μέσα στη μελέτη αναφέρονται 3 επίπεδα ασφαλείας με χρήση 3 χρωμάτων και 81 εικονίδια.

Μια άλλη μελέτη από τους Weiss και De Luca [39] αναφέρεται στη χρήση και απομνημόνευση σχημάτων για αντικατάσταση του κωδικού. Η βασική ιδέα βασίζεται στο γεγονός ότι ο χρήστης δεν θα χρειάζεται πλέον να πληκτρολογεί κωδικό για να έχει πρόσβαση σε ένα σύστημα αλλά σχηματίζοντας ένα σχήμα από συνεχόμενες γραμμές της δικής του επιλογής, τότε και μόνο θα μπορεί να αναγνωριστεί από το σύστημα. Με τη ίδια σκέψη μπορεί να εφαρμοστεί κάπως διαφορετικά και για τον αριθμό PIN σε ένα μηχάνημα ATM. Οι ερευνητές είχαν διεξάγει 2 διαφορετικά τεστ για να αναδείξουν στο μεν πρώτο τη αποτελεσματικότητα όσον αφορά τη απομνημόνευση και στο δεύτερο τη χρηστικότητα που έχει. Το πρώτο τεστ είχε να κάνει με τη σύγκριση 3 διαφορετικών μεταβλητών, χρήση μόνο αριθμού PIN, χρήση μόνο σχήματος και χρήση σχήματος με επανάληψη για 3 διαφορετικές ομάδες. Το σχήμα και στις 2 περιπτώσεις αποτελείτο από 7 συνεχόμενες ευθείες γραμμές χωρίς να είναι κυκλικό. Στη πρώτη ομάδα είχε δοθεί στους εθελοντές ένας πενταψήφιος αριθμός PIN να αποστηθίσουν, στη δεύτερη ομάδα τους είχε δοθεί ένα σχήμα για να το αποστηθίσουν ενώ η τρίτη ομάδα έπρεπε να σχηματίσει το σχήμα που τους δόθηκε 24 φορές. Στη περίπτωση του σχήματος, οι εθελοντές έπρεπε να ακολουθήσουν τη ίδια πορεία σχηματισμού. Τα αποτελέσματα κατέδειξαν ότι στη πρώτη δοκιμή που είχε γίνει λίγο μετά τη φάση εκμάθησης, οι ομάδες 1 και 3 κατάφεραν πλήρη αποστήθιση ενώ στη ομάδα 2 παρατηρήθηκε ότι 4 άτομα ξέχασαν το σχήμα. Η επόμενη δοκιμή είχε πραγματοποιηθεί μετά από περίοδο 5 ημερών, τα αποτελέσματα ήταν θετικά για την ομάδα 1

αφού μόνο ένα άτομο δεν κατάφερε να αποστηθίσει τον αριθμό του. Οι ομάδες 2 και 3 δεν τα πήγαν και τόσο καλά, 6 και 4 άτομα αντίστοιχα είχαν ξεχάσει ποιο ήταν το σχήμα τους. Η τελευταία δοκιμή πραγματοποιήθηκε 10 μέρες μετά καταδεικνύοντας τη ομάδα 3 καλύτερη έχοντας μόνο ένα άτομο να ξεχνάει το σχήμα του. Οι ομάδες 1 και 2 είχαν αντίστοιχα 3 και 7 άτομα που ξέχασαν τον αριθμό και το σχήμα τους.

Το δεύτερο τεστ είχε σαν σκοπό να αναδείξει ποια μέθοδος, χρήση αριθμού PIN ή χρήση σχήματος, θα ήταν πιο εύχρηστη και λιγότερο χρονοβόρα ώστε οι εθελοντές αρχικά να εισάγουν τον αριθμό ή να σχηματίσουν το σχήμα τους και κατόπιν τούτου να προβούν σε αλλαγή. Για το συγκεκριμένο τεστ είχαν λάβει μέρος 12 εθελοντές, όλοι έπρεπε να ακολουθήσουν τη ίδια διαδικασία και για τις 2 μεθόδους από 4 επαναλήψεις στη κάθε μέθοδο. Τα αποτελέσματα είχαν καταδείξει ότι για εισαγωγή αριθμού PIN ο μέσος χρόνος ήταν τα 4,2 δευτερόλεπτα ενώ για εισαγωγή του σχήματος τα 6,5, ανάλογα ήταν και τα αποτελέσματα στη διαδικασία αλλαγής με το PIN να χρειάζεται 14,6 δευτερόλεπτα και το σχήμα 19,5. Όπως φάνηκε στο δεύτερο τεστ, η χρήση PIN είχε τη καλύτερη απόκριση χρόνου λόγο του γεγονότος ότι οι χρήστες γενικά γνωρίζουν και χρησιμοποιούν τακτικά αυτή τη μέθοδο σε σχέση πάντα με το να σχηματίζουν ένα σχήμα. Πέραν αυτού όμως, η χρήση σχήματος σαν εισαγωγή κωδικού φάνηκε σαν μια ενδιαφέρουσα μέθοδος που θα ήταν αποδεκτή από τους περισσότερους εθελοντές και δεν υπήρξαν παράπονα ή δυσανασχέτηση κατά τη διάρκεια των τεστ.

Τα συμπεράσματα που εκλαμβάνουμε από τη μελέτη αυτή είναι ότι πρόκειται για μια νέα μέθοδο όπου μπορούμε να αντικαταστήσουμε την εισαγωγή κωδικού με το σχηματισμό ενός σχήματος της επιλογής του χρήστη και θα του είναι πιο εύκολο στο να το θυμάται παρά να έχει ένα δύσκολο κωδικό. Η μέθοδος αυτή δεν βρίσκει εφαρμογή στη δική μας περίπτωση για τους λόγους:

1. Δεν υπάρχει επαρκής περιγραφή για τις ανάγκες σε υλικό και λογισμικό που θα υποστηρίζει τη βάση δεδομένων για επαλήθευση των σχημάτων που θα πρέπει να εισάγουν οι χρήστες.

2. Στο τεστ 2 είχε χρησιμοποιηθεί μια συσκευή tablet για να σχηματίσουν το σχήμα. Σε εταιρικό περιβάλλον, η εισαγωγή του σχήματος δεν είναι ξεκάθαρο εάν θα γίνεται με τη χρήση του ποντικιού ή εάν θα υπάρχει παρόμοια συσκευή. Στη περίπτωση ύπαρξης ανάλογης συσκευής, αυτό θα δυσχεραίνει οικονομικά την εκάστοτε εταιρεία.

3. Η χρήση πενταψήφιου κωδικού PIN κρίνεται ιδιαίτερα επιρρεπής σε επιθέσεις με υψηλό ποσοστό ανεύρεσης και δεν συστήνεται ο κωδικός να αποτελείται μόνο από 5 αριθμητικά ψηφία.

4. Εάν αφήσουμε στη κρίση του χρήστη τη δημιουργία του σχήματος, δεν μπορούμε να πούμε με απόλυτη βεβαιότητα ότι δεν θα είναι ένα απλό σχήμα.

Ακόμη ένας ενδιαφέρον τρόπος για τη παραγωγή κωδικού, περιγράφεται στη μελέτη του Schweitzer et al. [30] όπου οι χρήστες καλούνται να δημιουργήσουν το κωδικό τους με βάση ένα μοτίβο στο πληκτρολόγιο. Η μέθοδος αυτή αποσκοπεί στο να θυμάται ο κάθε χρήστης ποιο μοτίβο έχει ακολουθήσει και όχι ποιος είναι ο κωδικός του. Για τη διεξαγωγή του πειράματος χρησιμοποιήθηκαν σαν δείγμα πρωτοετείς φοιτητές όπου τους είχε ζητηθεί να δημιουργήσουν τα δικά τους μοτίβα. Οι ερευνητές είχαν δημιουργήσει γι' αυτό το σκοπό ένα διαδικτυακό οδηγό για να τους βοηθήσουν και να κατανοήσουν τι ακριβώς έπρεπε να κάνουν, επίσης τους δινόταν ανατροφοδότηση για το κατά πόσο ο υποψήφιος κωδικός που δημιουργούσαν εμπίπτει στους ζητούμενους όρους της έρευνας καθώς και πόσο ισχυρός ήταν. Όλοι οι κωδικοί καταγράφονταν και συλλέγονταν σε μια βάση δεδομένων για περαιτέρω ανάλυση σε επόμενο στάδιο, συνολικά είχαν λάβει μέρος 161 φοιτητές. Το τεστ αφορούσε 3 διαφορετικές κατηγορίες κωδικών που οι φοιτητές έπρεπε να δημιουργήσουν.

Η πρώτη κατηγορία δεν ζητούσε κανένα μοτίβο, η δεύτερη ζητούσε να ακολουθηθεί απλά ένα οποιονδήποτε μοτίβο ενώ η τρίτη είχε σαν περιορισμό το μοτίβο να πληροί περιορισμούς σε μήκος και χρήση αλφαριθμητικών σε συνδυασμό με ειδικούς χαρακτήρες. Μετά τη συλλογή όλων των κωδικών η ανάλυση έδειξε ότι υπήρχαν κοινά μοτίβα μεταξύ των 3 κατηγοριών ιδίως σε λέξεις που υπάρχουν στη αγγλική γλώσσα, συνεπώς μπορούμε να υπολογίσουμε ότι είναι λέξεις που χρησιμοποιούνται σε συχνή βάση, επανάληψη 2 ή 3 ιδίων χαρακτήρων σε σειρά ή ακολουθία χαρακτήρων. Επόμενο βήμα ήταν να τεθούν σε δοκιμή οι κωδικοί για να διαπιστωθεί ο βαθμός δυσκολίας ανεύρεσης του κάθε κωδικού χρησιμοποιώντας το πρόγραμμα John the Ripper [25], επιλέγοντας σαν βάση το μοτίβο «grouped 2/3/4's» (χρήση 2, 3 ή 4 χαρακτήρων σε σειρά ή διαγώνια) με ελάχιστο μήκος τους 8 χαρακτήρες και μέγιστο τους 12. Τα αποτελέσματα έδειξαν ότι το 20% των κωδικών που είχαν δημιουργήσει οι φοιτητές, μπορούσαν να ανευρεθούν με χρήση του προαναφερθέντος μοτίβου. Η ίδια δοκιμή πραγματοποιήθηκε σε 11 κωδικούς, αποκτήθηκαν μετά από συναίνεση από το ινστιτούτο των ερευνητών, με αποτέλεσμα σε χρόνο μόλις 1 δευτερολέπτου να ανευρεθούν οι 2 κωδικοί. Αυτό αναδεικνύει τη έλλειψη σε

θέματα ασφάλειας για τη χρήση μοτίβων όταν ο χρήστης θα δημιουργήσει ένα κωδικό ασφαλείας.

Η πιο πάνω μελέτη μπορεί μεν να χρησιμοποιεί ένα πιο απλό και ευκολομνημόνευτο τρόπο παραγωγής κωδικών από τους χρήστες, στη δική μας περίπτωσης κρίνεται ως ιδιαίτερα ανασφαλής για τους εξής λόγους:

1. Εάν αφήσουμε στη κρίση του χρήστη να δημιουργήσει το μοτίβο του, κανείς δεν εγγυάται ότι θα αξιοποιήσει τους όποιους περιορισμούς στο έπακρο και με τον πιο αποτελεσματικό τρόπο.

2. Θέτοντας σαν περιορισμό ότι το ελάχιστο μήκος του κωδικού πρέπει να είναι οι 10 χαρακτήρες, πολύ πιθανό να παρατηρηθούν φαινόμενα επανάληψης χαρακτήρων μόνο και μόνο για να εμπίπτει σ' αυτό το περιορισμό.

3. Τα προγράμματα ανάκτησης και ανεύρεσης κωδικών που αναφέρθηκαν στο προηγούμενο κεφάλαιο, με τις κατάλληλες γνώσεις προγραμματισμού είναι ικανά να χρησιμοποιούν κανόνες και λειτουργίες για να δημιουργούν λίστες με κωδικούς βασιζόμενοι σε παρόμοια μοτίβα ανακτώντας έτσι ακόμη πιο εύκολα τους δύσκολους κωδικούς.

Όπως μπορούμε να αντιληφθούμε από τις προαναφερθείσες μελέτες και όχι μόνο αυτές, υπάρχουν αρκετοί τρόποι για ένα χρήστη να δημιουργήσει το κωδικό της αρεσκείας του με όποιο τρόπο και σκεπτικό τον βολεύει καλύτερα. Έτσι θα πετύχει να χρησιμοποιεί δυσκολότερους και μεγαλύτερους κωδικούς με όσο το δυνατόν λιγότερη προσπάθεια και να μην τους ξεχνάει συχνά. Το αρνητικό στοιχείο στις 2 πρώτες μελέτες είναι πως για να λειτουργούν πλήρως, το πιθανότερο σενάριο είναι η χρήση κατάλληλων ηλεκτρονικών υποδομών που θα υποστηρίζουν το υλικό και λογισμικό που θα τρέχει για επιβεβαίωση της αυθεντικότητας του κάθε χρήστη ενώ η τελευταία μελέτη χρησιμοποιεί τη τεχνική του μοτίβου που είναι αρκετά προβλέψιμη με τη χρήση κατάλληλων προγραμμάτων. Στη περίπτωση της μελέτης μας δεν επιβαρύνουμε ούτε τον Η/Υ του χρήστη ούτε την υπάρχουσα υποδομή της εταιρείας με άλλα προγράμματα και ηλεκτρονικό εξοπλισμό.

## 3.2 Έρευνες σε ελεγχόμενα περιβάλλοντα

Στη συνέχεια θα αναφερθούμε σε έρευνες που έγιναν για να εξακριβωθεί η ικανότητα που έχει ο χρήστης δίνοντάς του συγκεκριμένες οδηγίες να δημιουργήσει το κωδικό της αρεσκείας του πληρώντας συγκεκριμένα κριτήρια. Στο τέλος θα γίνει συγκριτική αναφορά μεταξύ των ερευνών και της μελέτης που εκπονείται.

Στη έρευνα που πραγματοποιήθηκε από τον Yan et al., [42] πήρε σαν δείγμα 300 πρωτοετείς φοιτητές, τους χώρισε σε 3 ομάδες αναθέτοντας στη κάθε ομάδα διαφορετικές κατευθυντήριες γραμμές για το τι πρέπει να κάνουν ώστε να δημιουργήσουν ισχυρούς κωδικούς. Συγκεκριμένα η πρώτη ομάδα που αποτελείτο από 95 φοιτητές, οι οδηγίες έλεγαν για παραγωγή κωδικού τουλάχιστον 7 χαρακτήρων με τουλάχιστον ένας χαρακτήρας να μην είναι γράμμα. Στη δεύτερη ομάδα που αποτελείτο από 96 φοιτητές, είχε δοθεί μια κόλλα χαρτί με όλα τα γράμματα του λατινικού αλφαβήτου και τους αριθμούς 1 έως 9 τυπωμένα κατ' επανάληψη ζητώντας τους να επιλέξουν με κλειστά μάτια 8 τυχαίους χαρακτήρες. Τέλος στη τρίτη ομάδα που αποτελείτο από 97 φοιτητές, ζητήθηκε να σκεφτούν μια πρόταση 8 λέξεων και να επιλέξουν κάποιο γράμμα από κάθε λέξη για να σχηματίσουν το κωδικό τους συμπεριλαμβάνοντας πεζά, κεφαλαία, αριθμό ή και κάποιο ειδικό χαρακτήρα. Στη περίπτωση που κάποιος ξεχνούσε το κωδικό του, είχε τη επιλογή να ζητήσει από το διαχειριστή να γίνει επανακαθορισμός αλλά τους έδιναν και τη δυνατότητα να τον έχουν κάπου σημειωμένο μέχρι τη πλήρη απομνημόνευσή του. Μετά από περίοδο ενός μηνός διεξήγαγαν σειρά δοκιμών με 4 διαφορετικές μεθόδους επίθεσης, χρήση λεξιλογίου, αντικατάστασης γραμμάτων με αριθμούς, χρήση προσωπικών πληροφοριών των χρηστών και επίθεση τύπου brute force. Παράλληλα χρησιμοποίησαν τους ίδιους τύπους επίθεσης σε δεύτερο δείγμα 100 πρωτοετών φοιτητών που δεν είχαν λάβει μέρος στη έρευνα για σκοπούς σύγκρισης μεταξύ ατόμων με καθοδήγηση και ατόμων χωρίς καθοδήγηση για δημιουργία κωδικών. Τα αποτελέσματα έδειξαν ότι οι κωδικοί των ομάδων είχαν μέσο μήκος 7.6, 8 και 7.9 χαρακτήρες ενώ οι κωδικοί του δεύτερου δείγματος είχαν μέσο μήκος 7.3 χαρακτήρες. Η πιο επιτυχής μέθοδος ήταν η αντικατάσταση γραμμάτων με αριθμούς με αμέσως επόμενη το brute force. Παρατηρήθηκε το φαινόμενο μερικοί φοιτητές να αγνοήσουν τις οδηγίες που είχαν δοθεί με αποτέλεσμα να δημιουργήσουν κωδικό με λιγότερους χαρακτήρες ή να μην πληρούν τους περιορισμούς καθιστώντας έτσι τους κωδικούς τους ευάλωτους ενώ λίγοι ήταν αυτοί που ζήτησαν επανακαθορισμό. Μετά τη πάροδο 4 μηνών από το ξεκίνημα της έρευνας, είχαν ζητήσει απ' όλους τους συμμετέχοντες να απαντήσουν σε 2 απλές ερωτήσεις για να διαφανεί ο βαθμός

δυσκολίας και η διάρκεια που είχαν αναγραμμένο το κωδικό τους αναδεικνύοντας τη ομάδα 2 σαν το πιο δύσκολο κωδικό και με τη μεγαλύτερη χρονική διάρκεια.

Η έρευνα που διεξήγαγε η Kuo et al. [18] σύγκρινε τη χρήση κωδικού που βασίζεται στη απομνημόνευση μιας φράσης που επιλέγει ο χρήστης και στη χρήση κωδικού που παράγεται τυχαία από το χρήστη με περιορισμό το μέγεθος και το εύρος χαρακτήρων που μπορεί να χρησιμοποιήσει. Στη έρευνα πήραν μέρος συνολικά 290 εθελοντές χωρισμένοι σε 2 ομάδες με το 75% να δηλώνει ότι είχε κάποιου είδους εκπαίδευση για ένα καλό κωδικό. Η κάθε ομάδα είχε λάβει συγκεκριμένες οδηγίες για τα βήματα που έπρεπε να ακολουθήσουν για τη δημιουργία κωδικού. Στη πρώτη ομάδα οι οδηγίες ήταν η δημιουργία κωδικού τουλάχιστον 8 χαρακτήρων που να περιέχει συνδυασμό πεζών και κεφαλαίων γραμμάτων, αριθμούς και ειδικούς χαρακτήρες. Στη δεύτερη ομάδα οι οδηγίες ήταν πιο συγκεκριμένες, Ο κωδικός να βασίζεται σε μια πρόταση της αρεσκείας τους αποτελούμενη από τουλάχιστον 7 ή 8 λέξεις που τους είναι εύκολο να τη θυμούνται επιλέγοντας ένα γράμμα από κάθε λέξη για το σχηματισμό του κωδικού χρησιμοποιώντας και σε αυτή τη περίπτωση πεζά και κεφαλαία γράμματα, αριθμούς και ειδικούς χαρακτήρες.

Βασισμένοι σε αυτό τον τρόπο, οι ερευνητές είχαν δημιουργήσει ένα αρχείο από 400 χιλιάδες λέξεις-κωδικούς προερχόμενες τραγούδια, τηλεοπτικά σλόγκαν, δημοφιλείς φράσεις μετά από αναζήτηση στο διαδίκτυο. Η διάρκεια της έρευνας ήταν 15 μέρες, όλοι οι εθελοντές συνδέονταν σε ένα εξυπηρετητή του πανεπιστημίου Carnegie Mellon όπου τους διαχώριζε σε 2 διαφορετικά ερωτηματολόγιο ζητώντας τους να δημιουργήσουν ένα κωδικό ανάλογα με τους περιορισμούς. Μετά το πέρας της έρευνας όλοι οι κωδικοί θα δοκιμάζονταν για τη αντοχή τους ενάντια σε πρόγραμμα ανάκτησης κωδικών, το John the Ripper, χρησιμοποιώντας 3 διαφορετικές μεθοδολογίες, τη χρήση λεξιλογίου, χρήση λεξιλογίου με αντικατάσταση και brute force. Στις 2 πρώτες περιπτώσεις χρησιμοποιήθηκαν τόσο το αρχείο των ερευνητών όσο και το αρχείο που χρησιμοποιεί το ίδιο το πρόγραμμα με 1,2 εκατομμύρια λέξεις-κωδικούς.

Τα αποτελέσματα έδειξαν ότι με τη χρήση των αρχείων αυτών κατάφεραν να βρουν το 11% των κωδικών της πρώτης ομάδας σε σχέση με το 4% της δεύτερης, ένα αναμενόμενο αποτέλεσμα όπως αναφέρουν για το λόγο ότι το πλήθος των λέξεων-κωδικών που χρησιμοποίησαν στη πρώτη ομάδα ήταν 3 φορές περισσότερες. Επιπρόσθετα ποσοστό της τάξης του 8% και 4% αντίστοιχα είχε βρεθεί με τη μέθοδο brute force ενώ σε επίπεδο ισχύς και μήκος κωδικού δεν παρατηρήθηκαν σημαντικές διαφοροποιήσεις μεταξύ των ομάδων. Οι ερευνητές συμπέραναν πως η μέθοδος δημιουργίας κωδικού με χρήση φράσης είναι πιο ασφαλής αλλά χρήζει

περαιτέρω μελέτης για να καταστεί ακόμη πιο λειτουργική σε σχέση με το να πληροί μονάχα περιορισμούς για το μήκος και τη ποικιλότητα χαρακτήρων.

Σημαντικά στοιχεία αναφορικά με τις συνήθειες που έχουν οι χρήστες για δημιουργία και διαφύλαξη των κωδικών τους, έχουν οι Helkala και Hoddo [10] στη μελέτη που πραγματοποίησαν διαθέτοντας ένα ερωτηματολόγιο σε τυχαίο δείγμα 1003 υπαλλήλων σε όλη τη Νορβηγία. Σημαντικός παράγοντας αποδείχτηκε πως δεν ήταν η ηλικία μιας και δεν υπήρξε μεγάλη απόκλιση στις τιμές των στατιστικών δεδομένων αλλά η γνώση και η εκπαίδευση που κατείχε ο κάθε υπάλληλος στο να δημιουργεί κωδικούς. Ο μέσος όρος κωδικών που χειριζόταν ο κάθε υπάλληλος, προσωπικούς και εταιρικούς, ήταν 25. Τα αποτελέσματα έδειξαν ότι μόλις το 59% των ερωτηθέντων είχαν λάβει καθοδήγηση ενώ το 35% δήλωσε ότι δεν είχε λάβει καθόλου με κυριότερες πηγές καθοδήγησης τις εφημερίδες και ιστοσελίδες τεχνολογικού περιεχομένου. Αξιοσημείωτο της όλης έρευνας είναι το γεγονός ότι το 42% από τα διευθυντικά στελέχη δεν είχαν λάβει καμία καθοδήγηση θέτοντας σε πιθανό κίνδυνο εταιρικά και άλλα δεδομένα. Ερωτηθείς για το πώς αντιλαμβάνονται τη έννοια ενός ασφαλούς κωδικού, μερίδα των ερωτηθέντων απάντησαν ότι κάνει χρήση προσωπικών πληροφοριών ενώ άλλοι χρησιμοποιούν μεμονωμένες λέξεις ή σε συνδυασμό με αριθμούς ενώ η χρήση online προγράμματος που παράγει κωδικούς είναι άγνωστη έννοια σε ποσοστό 46% με ένα μικρότερο ποσοστό να μην το εμπιστεύονται. Οι πιο διαδεδομένοι τρόποι που χρησιμοποιούν για διαφύλαξη του κωδικού είναι να τον έχουν αναγραμμένο σε φανερό σημείο κοντά στον Η/Υ, φυλαγμένο στον Η/Υ ή κινητό και με χρήση προγραμμάτων διαφύλαξης κωδικών. Κανένας από τους ερωτηθέντες δεν δήλωσε ότι δεν κρατά σε καμία μορφή, γραπτή ή ηλεκτρονική, το κωδικό του. Το θετικό της όλης έρευνας είναι το γεγονός ότι οι πλείστοι σε ποσοστό 63% δεν γνωστοποιούσαν το κωδικό τους ενώ παρατηρήθηκε το φαινόμενο της επαναχρησιμοποίησης κωδικών. Η γενική αποδοχή και παραδοχή του συνόλου των ερωτηθέντων είναι ότι ένας καλός κωδικός πρέπει να αποτελείται από συνδυασμό γραμμάτων, αριθμών και ειδικών χαρακτήρων για να μπορεί να αποκαλείται ισχυρός κωδικός.

Οι μεθοδολογίες που χρησιμοποιήθηκαν στις 2 πρώτες έρευνες έδειξαν ότι παρά τους περιορισμούς και τις σαφείς οδηγίες που δόθηκαν, οι χρήστες αντιμετώπισαν δυσκολίες τόσο στο να δημιουργήσουν ισχυρούς κωδικούς όσο και στο να ακολουθήσουν πιστά τις οδηγίες με συνέπεια οι κωδικοί σε κάποιες των περιπτώσεων να πληρούν τους ελάχιστους περιορισμούς. Αυτό είχε σαν αποτέλεσμα να παρατηρηθούν κωδικοί με 7 χαρακτήρες αντί 8 που ζητούσαν, αρκετοί κωδικοί να έχουν κοινά χαρακτηριστικά με άλλους ή και ακόμη να είναι πανομοιότυποι. Έχοντας τη ευχέρεια της αναγραφής του κωδικού σε ένα κομμάτι χαρτί για να τον βλέπουν κάθε

φορά που δεν μπορούσαν να τον θυμηθούν, αυτό δεν μας δίνει μια ξεκάθαρη εικόνα του πραγματικού ποσοστού εθελοντών που όντως εισήγαγαν το κωδικό δίχως να τον ξεχνούν. Η χρήση του προγράμματος John the Ripper έδειξε ότι είναι σχετικά πολύ εύκολο να ανευρεθούν τέτοιου είδους απλοί κωδικοί. Στη έρευνα των Helkala και Hoddo παρατηρήθηκε το φαινόμενο οι χρήστες να αντλούν οδηγίες από άρθρα σε εφημερίδες και ιστοσελίδες τεχνολογικού περιεχομένου και όχι από άτομα συναφή με τη τεχνολογία, λόγου χάριν το προσωπικό του τμήματος Πληροφορικής της εταιρείας, για τη δημιουργία κωδικού. Μέσα από τη έρευνά τους πηγάζει το γεγονός ότι αρκετοί από τους υπάλληλους χρησιμοποιούν προσωπικά στοιχεία στους κωδικούς και πως τους μοιράζονται με άτομα του οικογενειακού περιβάλλοντος. Η δική μας μελέτη διαφέρει κατά κύριο λόγο στο ότι δεν ζητήθηκε από κανέναν να δημιουργήσει κωδικό έχοντας υπόψη τις προαναφερθείσες περιπτώσεις, δεν χρησιμοποιήθηκε κανένα προσωπικό στοιχείο και όλοι οι κωδικοί πληρούσαν στο μέγιστο τις δυνατότητές τους.

Σε περιπτώσεις παραβίασης του κωδικού, πρώτο μέλημα του κάθε χρήστη είναι να αλλάξει όσο πιο σύντομα γίνεται τον υφιστάμενο κωδικό του ώστε να μπορέσει να προστατεύσει και να αποτρέψει τη διαρροή των προσωπικών ηλεκτρονικών του δεδομένων ή ακόμη στη καλύτερη των περιπτώσεων, εάν δεν έχει προλάβει να το πράξει ο κυβερνοεγκληματίας, να μην υπάρξει καθόλου διαρροή. Θα χρειαστεί να περάσει και πάλι από τη διαδικασία δημιουργίας ενός νέου κωδικού αλλά ποια βήματα θα πρέπει να ακολουθήσει ο χρήστης; Θα δημιουργήσει από αρχής ένα ολότελα νέο κωδικό μπαίνοντας στη διαδικασία να τον απομνημονεύσει ή θα ακολουθήσει το παρόμοιο μοτίβο που είχε χρησιμοποιήσει στο προηγούμενο κωδικό θέτοντας σε κίνδυνο και πάλι τα προσωπικά του δεδομένα. Τα πιο πάνω παραδείγματα μας απέδειξαν τη αδυναμία των χρηστών να ακολουθήσουν πιστά τις οδηγίες και να εμμένουν στη δημιουργία κωδικών ακολουθώντας πάντοτε τα ίδια.

# Κεφάλαιο 4
# Πειραματική Διαδικασία – Μεθοδολογία

Μετά τη ενδελεχή μελέτη της βιβλιογραφίας που συζητήθηκε προηγουμένως, καταλήξαμε στη επιλογή των 5 πιο συχνών τρόπων παραγωγής κωδικών. Τα 5 διαφορετικά τεστ με διάρκεια 3 εβδομάδων το καθένα, ξεκίνησαν τη Δευτέρα 24 Νοεμβρίου 2014 και έληξαν τη Παρασκευή 06 Μαρτίου 2015. Η σειρά με την οποία έγιναν τα τεστ καθώς και η ονομασία τους έχει ως εξής: Κωδικός σε τυχαία σειρά (random password), Κωδικός που προφέρεται (pronounceable password), Κωδικός με αρχικά από μια μεγάλη πρόταση (big sentence password), Κωδικός με χρήση δημοφιλών φράσεων και ποιημάτων (most popular password) και Κωδικός από συνδυασμό λέξεων (word combination password), όλοι οι κωδικοί είχαν μήκος 8 χαρακτήρες και για κάθε μέθοδο είχαμε 60 διαφορετικούς κωδικούς (30 που δίνονταν και 30 σαν εφεδρικοί). Για τη δημιουργία όλων των κωδικών χρησιμοποιήθηκε το δωρεάν εργαλείο PWGen που μας παρείχε αρκετές επιλογές για να πετύχουμε το μέγιστο για κάθε μέθοδο. Υπολογίστηκε ο βαθμός εντροπίας[7] που είχε ο κάθε κωδικός για να διαφανεί η ισχύς του παρατηρώντας μια διαφορά της τάξης των 6.8 μονάδων μεταξύ των μεθόδων 1, 3, 4 και 2, 5. Το δείγμα μας αποτελείται από 30

[7] http://rumkin.com/tools/password/passchk.php, http://en.wikipedia.org/wiki/Password_strength

άτομα, γυναίκες σε αναλογία 80% (24) και άνδρες σε αναλογία 20% (6). Οι ηλικίες κυμαίνονται από 25 μέχρι 50 ετών με μέση τιμή τα 33,9 έτη. Ο τρόπος με τον οποίο επιλέγηκαν τα άτομα που θα συμμετείχαν στα τεστ ήταν με τυχαία επιλογή αποστέλλοντάς τους ένα ενημερωτικό email [Παράρτημα Β1] 10 μέρες πριν τη έναρξη γνωστοποιώντας, αναλύοντας και επεξηγώντας τους τι ακριβώς θα γινόταν κατά τη διάρκεια των τεστ. Παράλληλα είχε σταλεί επιστολή στον υπεύθυνο του τμήματος Πληροφορικής της εταιρείας για έγκριση ώστε να εξαιρεθούν τα συγκεκριμένα άτομα από τις εσωτερικές πολιτικές ασφαλείας και για γνωστοποίηση του τι ακριβώς θα γίνει μέχρι το πέρας των τεστ [Παράρτημα Β2]. Ακολουθεί επεξηγηματικός πίνακας για κατανόηση της έννοιας εντροπία κωδικού και πόσος χρόνος απαιτείται μέχρι τη επιτυχή ανεύρεσή του όπως δίνεται από τη ιστοσελίδα ss64.com.[8] .

| Entropy | Max Time to crack (@ 350 billion guesses/sec) |
|---|---|
| 47 bits | 0.223 hours |
| 59 bits | 457.50 hours |
| 65 bits | 3.342 years |
| 71 bits | 213.92 years |
| 77 bits | 13,690 years |
| 80 bits | 109,527.95 years |
| 89 bits | 56078315.93 years |
| 119 bits | 6.0213633 e+16 years |

**Πίνακας 4.1:** Εντροπία κωδικού και χρόνος ανεύρεσης.

Η διαδικασία που ακολουθήθηκε για το καθορισμό του κωδικού σε κάθε χρήστη για όλες τις μεθόδους απαιτούσε πρόσβαση στο Active Directory[9] της εταιρείας, ο χρήστης δεν είχε το δικαίωμα να αλλάξει κωδικό και επιπλέον εφαρμόστηκε ξεχωριστή πολιτική για να μην λήγει ο

[8] http://ss64.com/docs/security.html
[9] https://msdn.microsoft.com/en-us/library/aa746492(v=vs.85).aspx

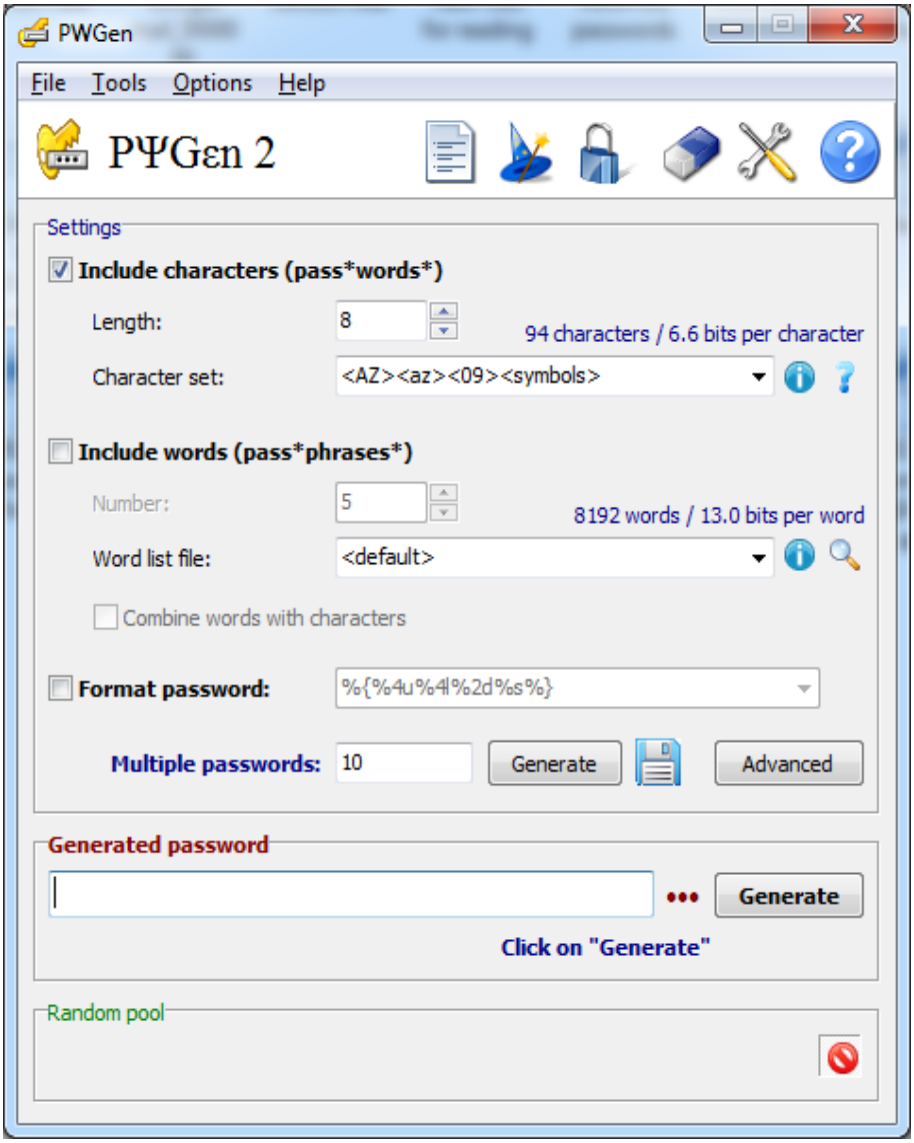
κωδικός σε σχέση πάντα με τους υπόλοιπους που δεν πήραν μέρος στα τεστ. Ο κωδικός αφορούσε το login password που έπρεπε να εισάγει ο χρήστης (2 φορές τη μέρα, πρωί και απόγευμα) ώστε να έχει πρόσβαση στον Η/Υ, ίσχυε επίσης για το πρόγραμμα ηλεκτρονικού ταχυδρομείου και για πρόσβαση σε αρχεία που βρίσκονταν σε κοινόχρηστο δίσκο. Οι κωδικοί ήταν σε εφαρμογή το Σάββατο βράδυ πριν τη έναρξη του κάθε τεστ. Η διαδικασία ενημέρωσης των χρηστών για ποιος ήταν ο κωδικός τους κάθε φορά όσο για τη καταγραφή υπενθύμισης και επανακαθορισμού ήταν ακριβώς η ίδια που εφαρμόστηκε και στις 5 μεθόδους. Τα κοινά βήματα που γίνονταν στο πρόγραμμα ήταν ο καθορισμός μήκους και η ποσότητα κωδικών ενώ αυτό που άλλαζε ήταν ο τρόπος που θα παρήγαγε τους κωδικούς. Για παράδειγμα, στο κωδικό από συνδυασμό λέξεων χρειάστηκε να ενσωματωθεί αρχείο που περιείχε λέξεις (wordlist) και να επιλέξουμε πώς ακριβώς θέλαμε να εμφανίζεται.

Τη τελευταία μέρα του πέμπτου τεστ δόθηκε ένα ερωτηματολόγιο που αναφερόταν στις εντυπώσεις που άφησε το κάθε τεστ και όλοι οι χρήστες που συμμετείχαν είχαν λάβει ένα μικρό δωράκι σαν ένδειξη ευγνωμοσύνης για τη συμμετοχή τους στα τεστ.

## 4.1 Κωδικός σε τυχαία σειρά

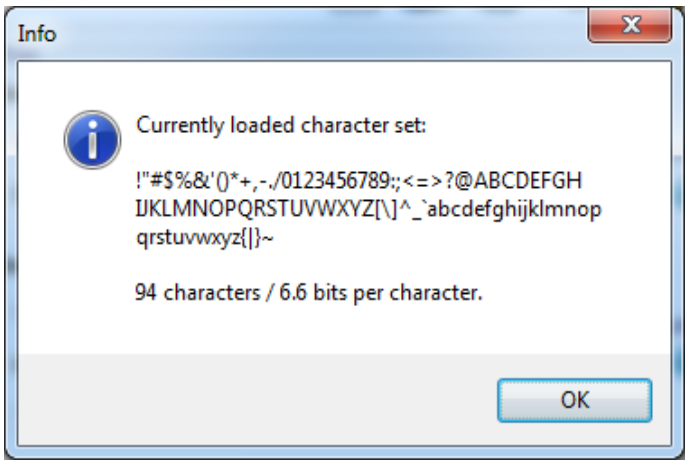
Η συγκεκριμένη μέθοδος θεωρείται ιδιαίτερα δύσκολη για το λόγο ότι, όπως λέει και η ονομασία της, όλοι οι χαρακτήρες που χρησιμοποιούνται μπαίνουν σε εντελώς τυχαία σειρά δίνοντάς μας σαν αποτέλεσμα ένα παράξενο κωδικό. Δεν βρίσκει ιδιαίτερη απήχηση στους απλούς και όχι μόνο χρήστες γιατί πολύ δύσκολα θα καταφέρει κανείς να τον θυμηθεί εκτός και εάν υπάρχει αναγραμμένος κάπου. Για το μέγιστο δυνατό αποτέλεσμα χρησιμοποιήσαμε και τους 94 χαρακτήρες του πληκτρολογίου κατά τη φάση παραγωγής κωδικών χωρίς να αλλάξουμε τις αρχικές ρυθμίσεις του προγράμματος. Ο βαθμός εντροπίας αυτής της μεθόδου είναι $94^8=6.09*10^{15}\approx2^{52.4}$. Στη συνέχεια θα παρουσιάσουμε βήμα προς βήμα τη διαδικασία που ακολουθήσαμε για τη παραγωγή κωδικών.

Τρέχουμε το πρόγραμμα και εμφανίζονται όλες οι διαθέσιμες επιλογές




**Εικόνα 4.1:** Το γραφικό περιβάλλον (GUI) της εφαρμογής.

Από το κομμάτι Settings, στο Length επιλέγουμε το επιθυμητό μήκος (=8) και στη επιλογή Character set διαλέγουμε τη κατηγορία με τους χαρακτήρες από τους οποίους θα αποτελείται ο κωδικός μας (η επιλογή <AZ> <az> <09> <symbol> θα χρησιμοποιήσει και τους 94 χαρακτήρες). Πατώντας το εικονίδιο των πληροφοριών που βρίσκεται δεξιά, μας εμφανίζει ένα παράθυρο που περιέχει όλους τους χαρακτήρες που θα χρησιμοποιηθούν για τη μέθοδο αυτή.

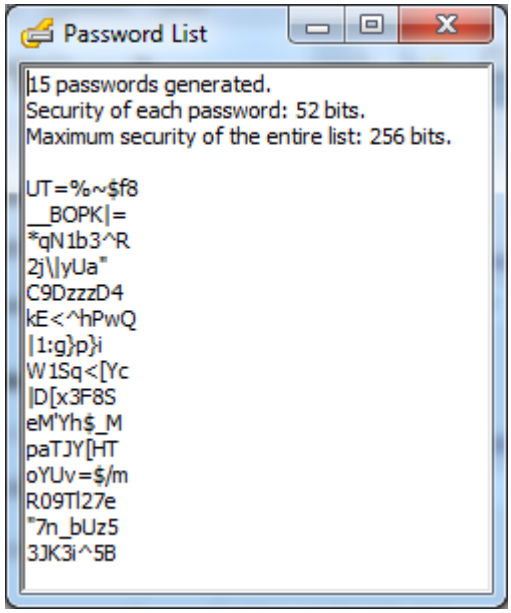



**Εικόνα 4.2:** Οι χαρακτήρες που θα χρησιμοποιηθούν.

Στη συνέχεια στη επιλογή Multiple passwords γράφουμε το πλήθος των κωδικών που επιθυμούμε να παράγει το πρόγραμμα και κατόπιν πατάμε το κουμπί Generate για να εμφανιστούν, έχουμε και τη επιλογή να τους αποθηκεύσουμε αμέσως πατώντας στο κουμπί της δισκέτας. Η επιλογή Advanced δίνει τη δυνατότητα να αλλάξουμε τις αρχικές ρυθμίσεις όπως να αποφεύγεται η χρήση 2 ή περισσοτέρων ίδιων χαρακτήρων σε σειρά, αποκλεισμός διφορούμενων χαρακτήρων (για παράδειγμα B με 8, 0 με O, S με 5 και Z με 2), ο πρώτος χαρακτήρας να μην είναι κεφαλαίο γράμμα ή αποφυγή διπλών κωδικών. Μερικές από τις επιλογές που υπάρχουν εάν επιλεχθούν μειώνουν το επίπεδο ασφαλείας των κωδικών που θα μας δώσει το πρόγραμμα και έτσι κρίθηκε σκόπιμο να μείνουν ως έχουν. Στο πεδίο Generated password υπάρχει προεπισκόπηση για το πώς θα είναι το τελικό αποτέλεσμα των κωδικών καθώς και ενδεικτική μπάρα για τη ισχύ του. Για σκοπούς επίδειξης θα δημιουργήσουμε 15 κωδικούς μόνο.


**Εικόνα 4.3:** Πλήθος κωδικών, δείγμα κωδικού και η ισχύς του.

Το αποτέλεσμα με τους κωδικούς που θα πάρουμε φαίνεται στη επόμενη εικόνα.




**Εικόνα 4.4:** Δείγμα κωδικών.

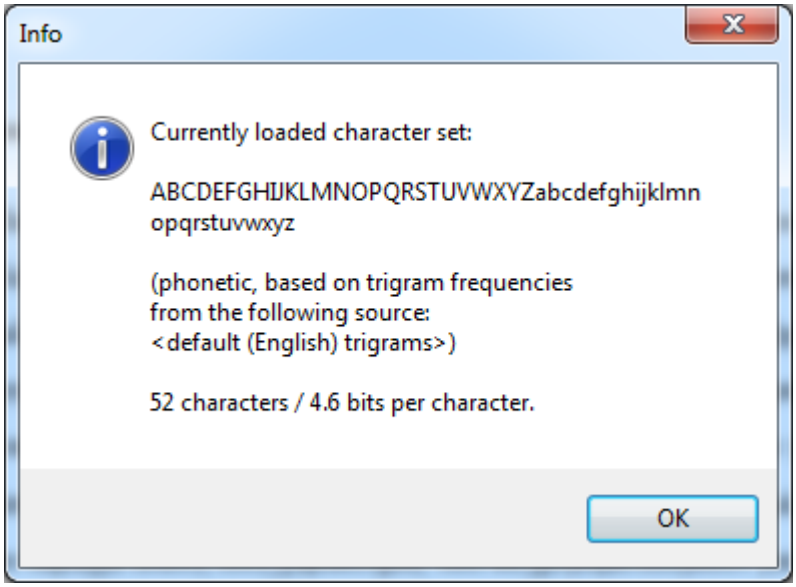
Σε ένα τυπωμένο πίνακα υπήρχαν τα ονοματεπώνυμα όλων των ατόμων που λάμβαναν μέρος και δίπλα τους αναγραφόταν ο κωδικός που τους αναλογούσε στη σειρά όπως ακριβώς τα εμφάνιζε το πρόγραμμα. Οι χρήστες μάθαιναν το κωδικό τους Δευτέρα πρωί όταν ξεκινούσε το τεστ. Στη περίπτωση που κάποιος είχε δυσκολία ή απορία σχετικά με τους χαρακτήρες τότε δίνονταν οι κατάλληλες επεξηγήσεις, η διαδικασία που επακολουθούσε ήταν η καταγραφή για το πόσες φορές ο κάθε χρήστης μέχρι το τέλος του τεστ χρειαζόταν υπενθύμιση ή επανακαθορισμό του κωδικού του, ανάλογα με το τι προτιμούσε και η διαδικασία συνεχιζόταν κανονικά. Ακολουθεί πίνακας με μερικούς από τους κωδικούς που είχαν δοθεί.

| | | | | |
|---|---|---|---|---|
| 3H:do<Ls | Y`9(q4,o | vL7Pz'&y | AHA)HF4n | L[K*iAt4 |
| L)p#^&3U | M4Ke_9Y^ | KCr>h3KX | C^cLz9eH | 4W=pE.AW |
| (mN=b4d3 | 3ycdW[,) | Tb3-C^C3 | aV#3b'@' | A!4,wH=4 |

**Πίνακας 4.2:** Κωδικοί που είχαν δοθεί στο συγκεκριμένο τεστ.

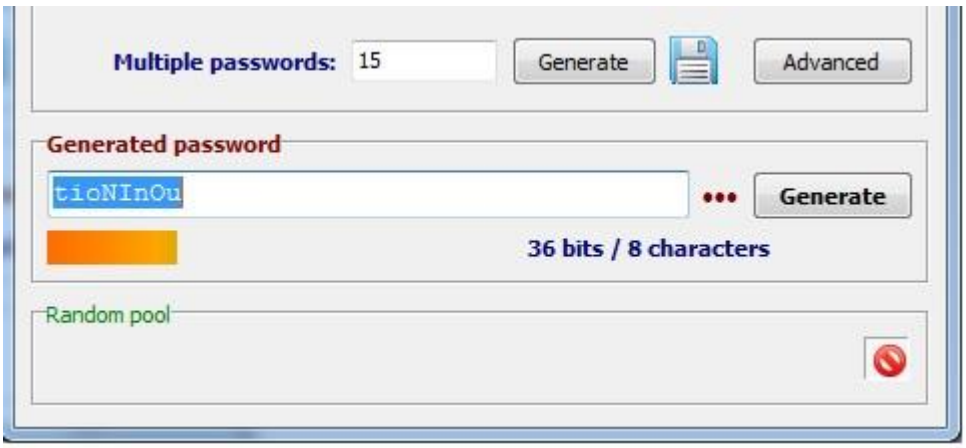
## 4.2 Κωδικός που διαβάζεται και προφέρεται εύκολα στα αγγλικά

Μια εκ των δυο εύκολων μεθόδων που χρησιμοποιήθηκε και άρεσε στους χρήστες για τον απλούστατο λόγο ότι δεν περιέχει κανένα ειδικό χαρακτήρα ούτε αριθμούς, αποτελείται μόνο από πεζά και κεφαλαία γράμματα και αυτή η ιδιότητα τους διευκόλυνε στην αποστήθιση με τη παραγωγή κωδικών να είναι πιο εύκολη. Ο βαθμός εντροπίας αυτής της μεθόδου είναι $52^8=5.34*10^{13}\approx2^{45.6}$. Τρέχουμε το πρόγραμμα και στη επιλογή Character set διαλέγουμε τη κατηγορία με τους χαρακτήρες από τους οποίους θα αποτελείται ο κωδικός μας (<phonetic> θα χρησιμοποιήσει όλα τα γράμματα, συνολικά 52 πεζά και κεφαλαία). Πατώντας το εικονίδιο των πληροφοριών που βρίσκεται δεξιά, μας εμφανίζει ένα παράθυρο που περιέχει όλους τους χαρακτήρες που θα χρησιμοποιηθούν για τη μέθοδο αυτή.



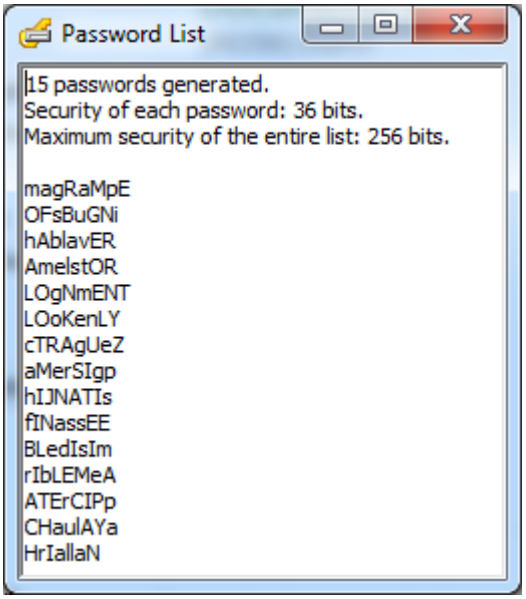

**Εικόνα 4.5:** Οι χαρακτήρες που θα χρησιμοποιηθούν.

Αφήσαμε τις ίδιες ρυθμίσεις, στο κομμάτι Multiple passwords γράψαμε τον αριθμό 15 και στη συνέχεια πατήσαμε το κουμπί Generate για να μας δώσει τους κωδικούς που θα χρησιμοποιήσουμε. Στο πεδίο Generated password είδαμε πως θα φαίνονται οι κωδικοί. Σε αυτή τη περίπτωση η ενδεικτική μπάρα ισχύος είναι σε πιο χαμηλό επίπεδο σε σχέση με τη προηγούμενη μέθοδο για το λόγο ότι χρησιμοποιούμε μόνο γράμματα.




**Εικόνα 4.6:** Πλήθος κωδικών, δείγμα κωδικού και η ισχύς του.

Το αποτέλεσμα με τους κωδικούς που θα πάρουμε φαίνεται στη επόμενη εικόνα.




**Εικόνα 4.7:** Δείγμα κωδικών.

Ακολουθεί πίνακας με μερικούς από τους κωδικούς που είχαν δοθεί.

| | | | | |
|---|---|---|---|---|
| EmIFOcAR | fAlOKAXA | DUFuXipU | XlRAtoYi | LonaTEWE |
| YeYUkENi | FanIzebo | WuCuwUpa | NukataXO | YAvIcIvo |
| eKozovuM | NoJeTeYO | ebevArer | CONenOsE | iFUTaLAL |

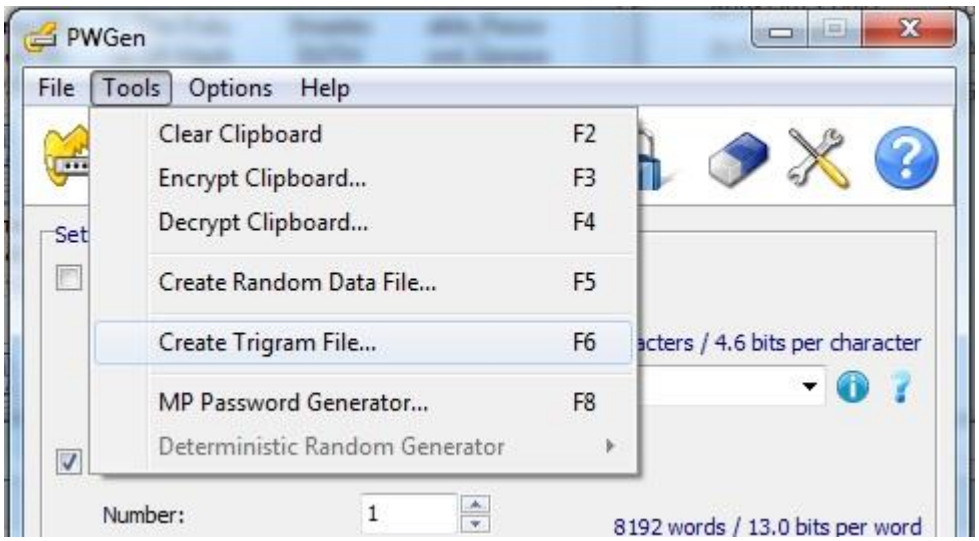
**Πίνακας 4.3:** Κωδικοί που είχαν δοθεί στο συγκεκριμένο τεστ.

## 4.3 Κωδικός με αρχικά από μια μεγάλη πρόταση

Για τη συγκεκριμένη μέθοδο χρησιμοποιήθηκαν προτάσεις στη αγγλική γλώσσα που μπορούν να βρεθούν ελεύθερα στο διαδίκτυο. Μετά από αναζήτηση καταλήξαμε στο να βασιστούμε σε 2 ιστοσελίδες που παράγουν διάφορες τυχαίες προτάσεις[10], προτιμήθηκαν όσες ήταν μεταξύ 6 και 8 λέξεων για να πληρούν το καθορισμένο μήκος των 8 χαρακτήρων αφού εκτός από γράμματα θα περιείχαν ένα αριθμό ή και ένα ειδικό χαρακτήρα. Ο βαθμός εντροπίας αυτής της μεθόδου είναι $94^8=6.09*10^{15}\approx2^{52.4}$. Δαπανήθηκε αρκετός χρόνος ώστε να παραχθούν αρκετές προτάσεις για να δημιουργηθούν σε επόμενο στάδιο οι κωδικοί, τα βήματα που πρέπει να ακολουθηθούν περιγράφονται αναλυτικά πιο κάτω.

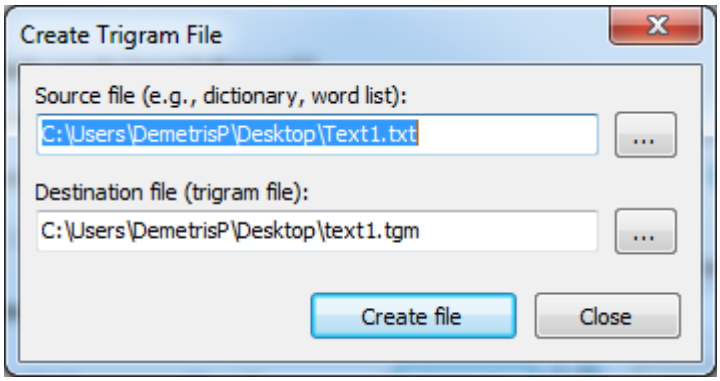
Συγκεντρώνονται όλες οι προτάσεις σε ένα αρχείο κειμένου, μια ανά γραμμή και μετά από το menu του προγράμματος στη καρτέλα Tools επιλέγουμε το Create Trigram File. Με αυτό τον τρόπο το πρόγραμμα θα διαβάσει τα περιεχόμενα του αρχείου και θα δημιουργήσει ένα νέο αρχείο για να προχωρήσει η διαδικασία.

[10] http://www.wordgenerator.net/random-sentence-generator.php και http://watchout4snakes.com/wo4snakes/Random/RandomSentence



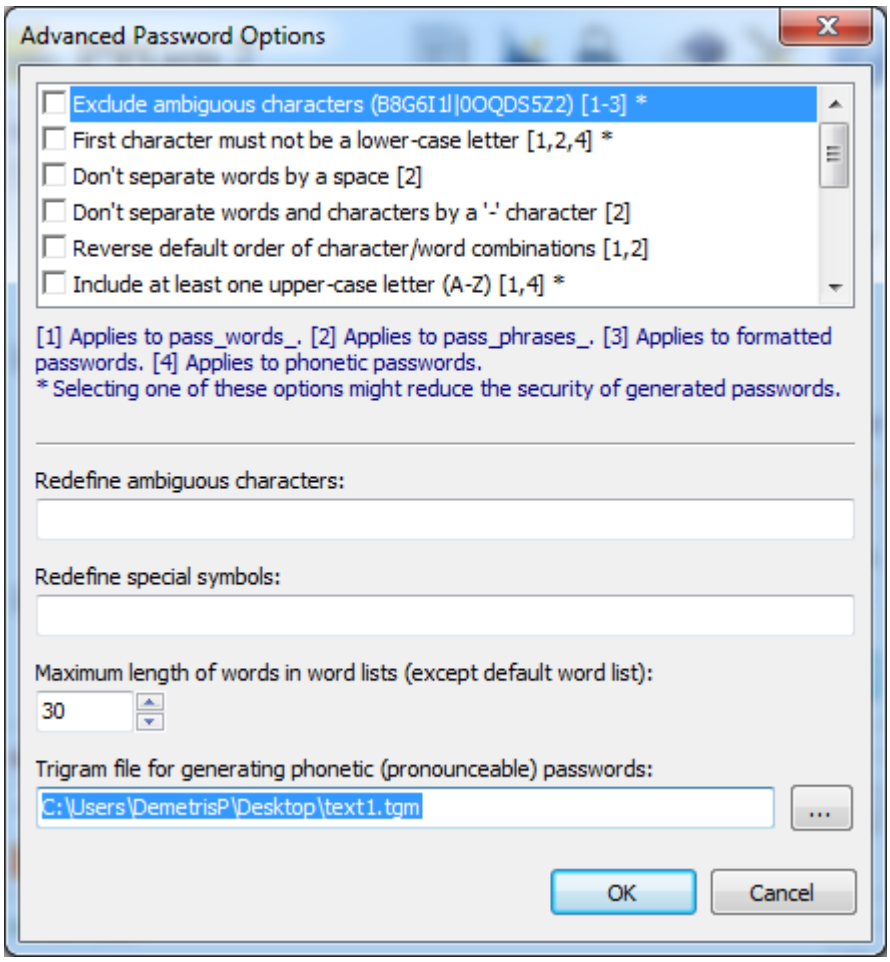

**Εικόνα 4.8:** Δημιουργία Trigram File.

Στο επόμενο παράθυρο επιλέγουμε το αρχείο που φτιάξαμε και μετά τη τοποθεσία που θέλουμε να το φυλάξουμε για να το εισάγουμε στο πρόγραμμα.



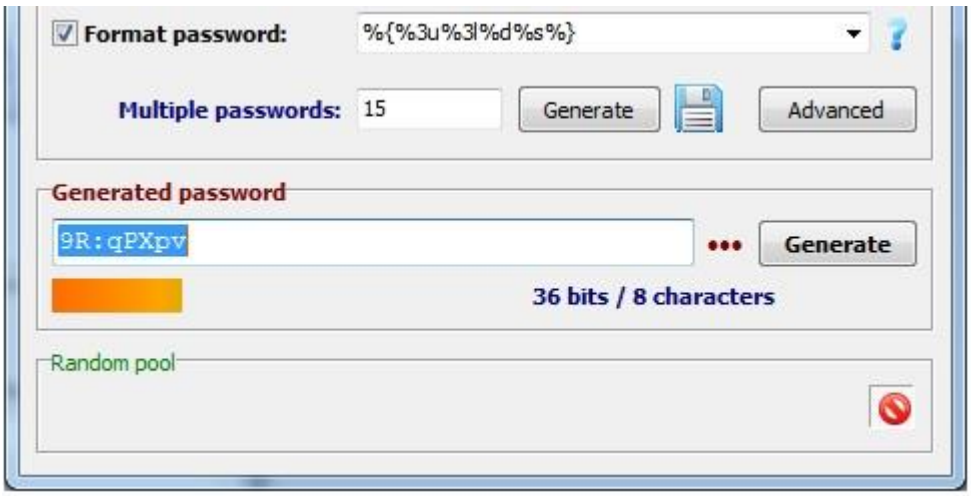

**Εικόνα 4.9:** Εισαγωγή του αρχείου μας και το φυλάμε με κατάληξη αρχείου.tgm.

Από το κυρίως παράθυρο του προγράμματος επιλέγουμε Advanced και έπειτα φορτώνουμε το αρχείου text1.tgm για να προχωρήσουμε στο επόμενο βήμα, καθορισμός των χαρακτηριστικών του κωδικού.



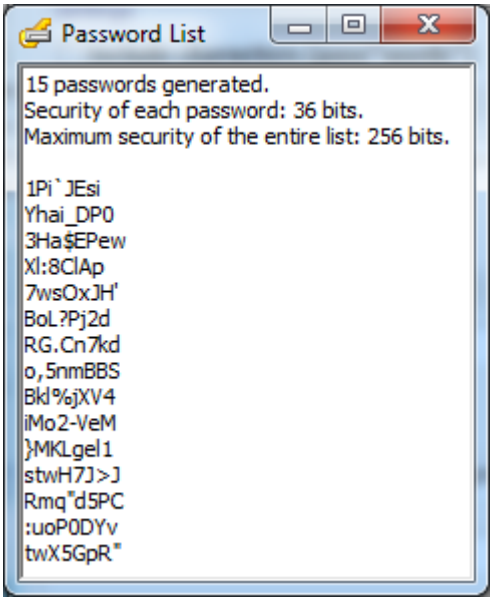

**Εικόνα 4.10:** Επιλογή του αρχείου μας.

Τέλος επιλέγουμε από το κομμάτι Format Password τον τρόπο με τον οποίο θέλουμε να δημιουργηθεί ο κωδικός. Στη δική μας περίπτωση χρησιμοποιήσαμε από 3 πεζά και κεφαλαία γράμματα, ένα αριθμό και ένα ειδικό χαρακτήρα όπως δείχνει η εικόνα πιο κάτω.




**Εικόνα 4.11:** Το μοτίβο που θα μας παράγει τους κωδικούς.

Στο πεδίο Generated password βλέπουμε παράδειγμα για το πώς θα φαίνεται ο κωδικός και πατάμε το κουμπί Generate για να πάρουμε τους κωδικούς μας.




**Εικόνα 4.12:** Δείγμα κωδικών.

Στο παράδειγμά μας χρησιμοποιήσαμε το μοτίβο 3 κεφαλαία, 3 πεζά, ένα αριθμό και ένα ειδικό χαρακτήρα. Για τη παραγωγή κωδικών του τεστ έγιναν άλλες 2 παραλλαγές, η μια με μοτίβο 3 κεφαλαία, 2 πεζά, 2 αριθμούς και ενός ειδικού χαρακτήρα και η άλλη με 2 χαρακτήρες από κάθε κατηγορία.

Ακολουθεί πίνακας με μερικούς από τους κωδικούς που είχαν δοθεί.

| | | | | | |
|---|---|---|---|---|---|
| assertion of displaces teleology of hidden | a$0D^tOh | asterisk lines a running midnight with family | *1sRm8wf | Can the dumped carrier strike across freeze | C+dc$A%F |
| invention of unnamed opens a space for cooptation | Iu0^Sf_c | economy mentions altoger without even earth | 3M=aWe8e | rhetoric of unspoken allegorizes politics of materiality | r0U^a9oM |
| charmed guideline lodges the statistical cheat | (gL,+Sc? | discourse of private chronicles invention of agency | 4OpC*I0A | divisibility of image specifies ideology of abyss | D0i$I&oa |
| The transformed whistle revolts in the drill | T+WR>Itd | The inhibited idiom commands the square continent | +I1(T{sC | The applicable biology obliges the unconvincing pin | tA8O+#Up |
| fiction history as such allegorizes logic of unknown | fH@sAL0u | idea of nationstate matizes hermeneutic of difference | I0%NmHoD | The alarming crush abides in the infant pad | +A(@iTIp |

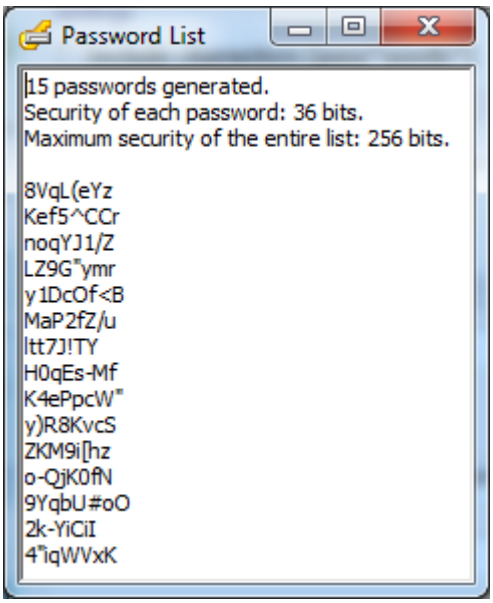
**Πίνακας 4.4:** Κωδικοί που είχαν δοθεί στο συγκεκριμένο τεστ.

## 4.4 Κωδικός με χρήση δημοφιλών προτάσεων και ποιημάτων

Μέθοδος παρόμοια της προηγούμενης με τη διαφορά ότι θα χρησιμοποιηθούν δημοφιλείς προτάσεις που ειπώθηκαν σε ταινίες, από αρχαίους φιλόσοφους, ανθρώπους των γραμμάτων και των τεχνών όπως επίσης αποσπάσματα από ποιήματα. Στη συγκεκριμένη μέθοδο είχαμε συμπεριλάβει κωδικούς από ελληνικά και ξένα τραγούδια με σκοπό τη καταγραφή της συμπεριφοράς των χρηστών όταν ο κωδικός προερχόταν από οικείο περιβάλλον, αφού όπως φάνηκε από τις απαντήσεις γνώριζαν σχεδόν όλους τους στίχους. Μετά από αναζήτηση στο διαδίκτυο για ιστοσελίδες[11] που περιέχουν αποσπάσματα και στίχους με προτίμηση και πάλι σε προτάσεις από 6 μέχρι 8 λέξεις, συγκεντρώθηκαν όλα σε ένα αρχείο κειμένου για περαιτέρω επεξεργασία. Ο βαθμός εντροπίας αυτής της μεθόδου είναι $94^8=6.09*10^{15}\approx2^{52.4}$. Ακολουθήσαμε τα ίδια βήματα με της προηγούμενης μεθόδου για δημιουργία ενός νέου αρχείου Trigram ( βλέπε εικόνες 4.8~4.10, νέο αρχείο text2.tgm) που θα το φορτώσουμε στο πρόγραμμα και στη συνέχεια το ίδιο μοτίβο κωδικού (βλέπε εικόνα 4.11) θα μας δώσει τους κωδικούς για το συγκεκριμένο τεστ. Η παραγωγή των κωδικών ακολούθησε την ίδια διαδικασία όπως και στη προηγούμενη μέθοδο.

Δείγμα των κωδικών βλέπουμε στη πιο κάτω εικόνα.

[11] http://www.stixoi.info/, http://www.azlyrics.com/ http://www.poetrysoup.com/famous_poets/most_popular_famous_poets.aspx , http://www.goodreads.com/quotes και http://www.filmsite.org/greatfilmquotes.html




**Εικόνα 4.13:** Δείγμα κωδικών.

Ακολουθεί πίνακας με μερικούς από τους κωδικούς που είχαν δοθεί.

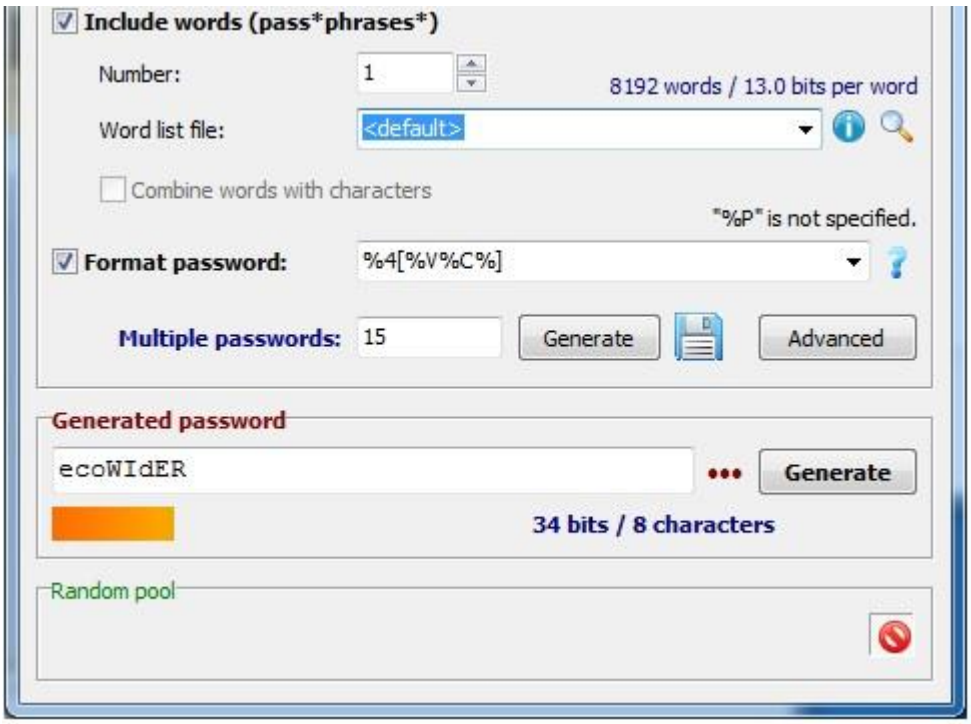
| | | | | | |
|---|---|---|---|---|---|
| Se eixa eroteftei poli mazi sou eixa trelathei | s3EpMse+ | Kai sou grafo tragoudia sou stelno louloudia | &sG+$Sl | Exo petaxei mazi sou se kathe fili | 3Pm$:sKF |
| countenance more in sorrow than in anger | C>mi$TiA | bird in hand worth two in the bush | B1Hw2i+b | It's something to do with your brain | i$2D"wYb |
| Be yourself everyone else is already taken | By3#eIa+ | May the force be with you | M+f:bWu" | Without music life would be a mistake | WM;lw8am |
| And we could be together baby As long | @Wc8+BaL | loneliness is killing me I must confess | *1iKm^Ic | The tropical scent of you Takes me up | +T$0ytMU |
| A feast for my womanly inner beast | @f5FMwi8 | But such a tide as moving seems asleep | 8$at@MsA | Perfectly happy now he looked at his estate | 9HNh1@hS |

**Πίνακας 4.5:** Κωδικοί που είχαν δοθεί στο συγκεκριμένο τεστ.

## 4.5 Κωδικός με συνδυασμό λέξεων

Η δεύτερη εύκολη μέθοδος που χρησιμοποιήθηκε αλλά και η τελευταία που σήμαινε τη λήξη των τεστ ήταν ο συνδυασμός διαφόρων λέξεων, άσχετες μεταξύ τους, για να δημιουργηθεί μια νέα λέξη. Είναι παρόμοια μέθοδος με το κωδικό που προφέρεται στα αγγλικά και η διαφορά είναι στο γεγονός ότι δεν θα χρησιμοποιηθούν υπαρκτές λέξεις για να έχουμε τους κωδικούς μας αλλά με τη χρήση μοτίβου καθορίζουμε πιο θέλουμε να είναι το επιθυμητό αποτέλεσμα. Αν και έχουμε τη δυνατότητα να φορτώσουμε ένα δικό μας αρχείο λέξεων με λατινικούς χαρακτήρες, δεν

αναζητήθηκαν λέξεις στο διαδίκτυο ούτε χρειάστηκε να δημιουργήσουμε νέα αρχεία για το απλούστατο λόγο ότι το πρόγραμμα παρέχει δικές του λέξεις, στο σύνολο 8192, που θα μας βοηθήσουν στο τελευταίο μας εγχείρημα. Ο βαθμός εντροπίας αυτής της μεθόδου είναι $52^8=5.34*10^{13}\approx2^{45.6}$. Η διαδικασία είναι πολύ απλή σε σχέση με τις προηγούμενες μεθόδους, αρκεί να επιλέξουμε από το κεντρικό παράθυρο της εφαρμογής το κομμάτι Include words (pass*phrases*) και στη επιλογή Word list file να αφήσουμε τη προεπιλογή (default) που έχει. Επόμενο βήμα είναι να επιλέξουμε το κομμάτι Format password βάζοντας το μοτίβο που θα ακολουθηθεί για τη παραγωγή κωδικών. Υπάρχουν έτοιμα μοτίβα αλλά δημιουργήσαμε το δικό μας που ακολουθούσε τη λογική να παράγει σε τυχαία θέση 4 τυχαία φωνήεντα και 4 τυχαία σύμφωνα. Η εικόνα πιο κάτω παρουσιάζει το μοτίβο μας όπως επίσης και δείγμα των κωδικών που θα παραχθούν.




**Εικόνα 4.14:** Το μοτίβο που χρησιμοποιήσαμε.

Ακολουθεί πίνακας με μερικούς από τους κωδικούς που είχαν δοθεί.

| | | | | |
|---|---|---|---|---|
| MolADORi | CifapezI | TutUpoQA | XUXUqIlU | AMANESAf |
| KeNAmAbO | vEKofUFE | PIzotuGu | NeneXuqU | NUrodiCO |
| UFUYalUd | ROzANeDA | roDIZuXA | UDABITAS | BUpALaSI |

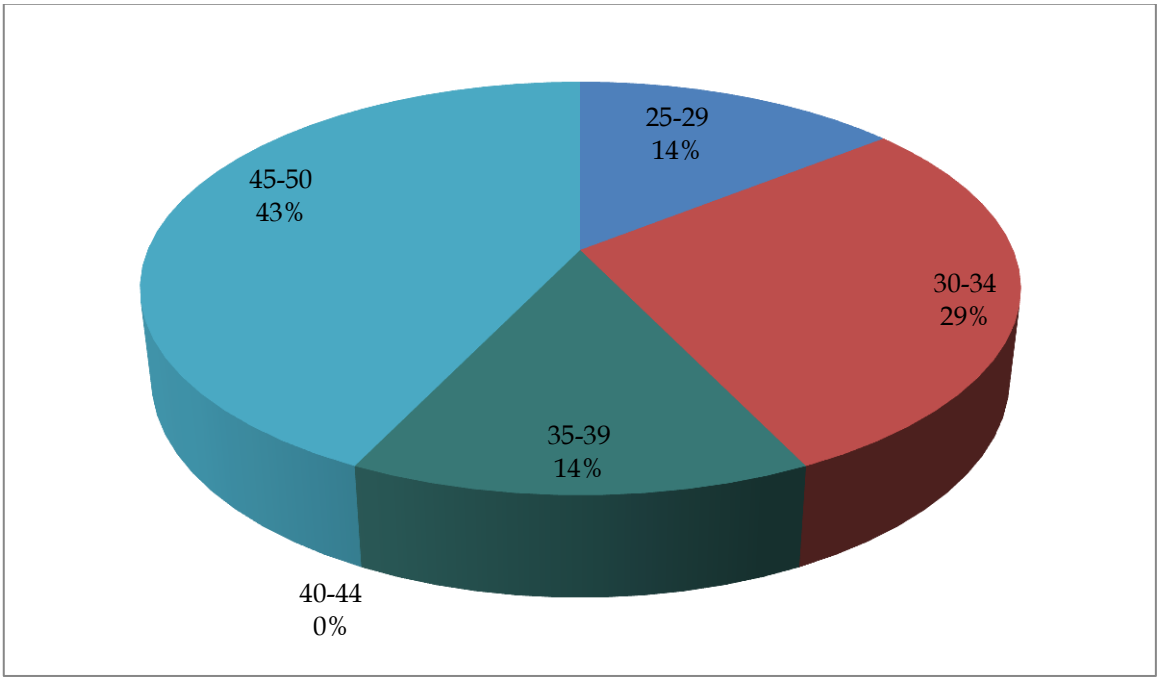
**Πίνακας 4.6:** Κωδικοί που είχαν δοθεί στο συγκεκριμένο τεστ.

## 4.6 Καταγραφή Αποτελεσμάτων

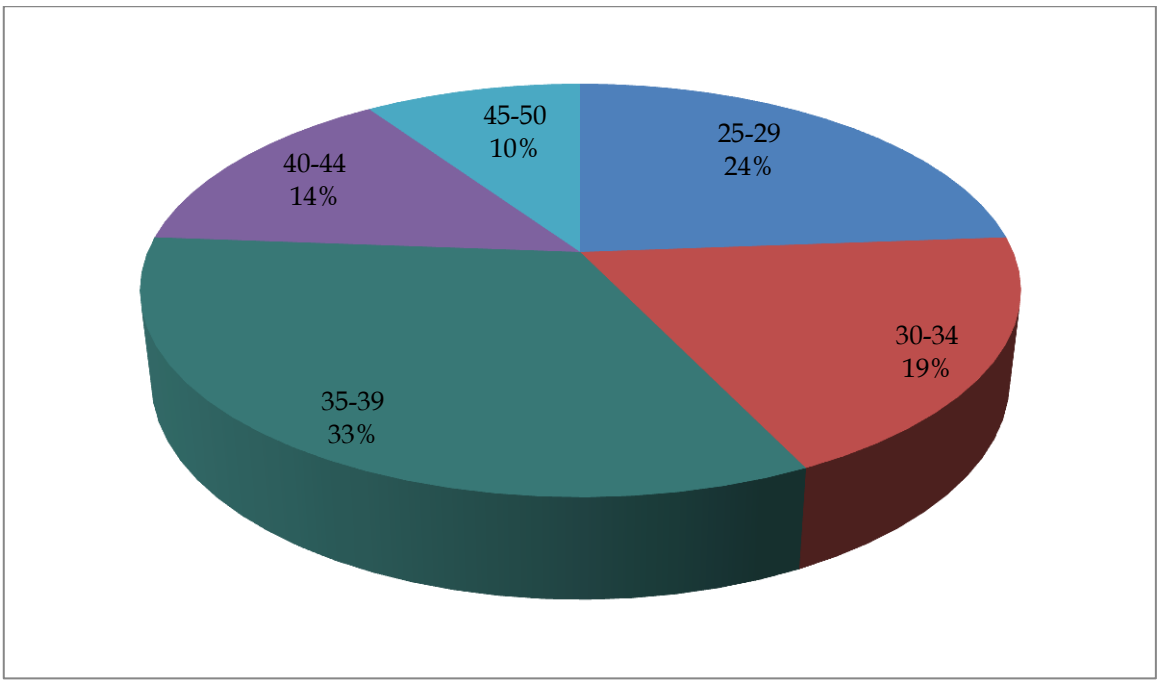
Σε αυτό το κομμάτι θα αναλυθούν και επεξηγηθούν οι αντιδράσεις που είχαν όλοι οι χρήστες κατά τη διάρκεια των τεστ, όπως επίσης ποιες ηλικιακές ομάδες είχαν τους περισσότερους επανακαθορισμούς κωδικών ή ζήτησαν αλλαγή του (συνολικά είχαμε 5 ομάδες, 1η από 25-29, 2η από 30-34, 3η από 35-39, 4η από40-44 και η 5η από 45-50 ετών). Δεν θα εξετάσουμε το παράγοντα φύλο χρήστη για το λόγο ότι η αναλογία που είχαμε μεταξύ ανδρών και γυναικών ήταν 1 προς 4. Τα αποτελέσματα μπορεί να κριθούν σαν αναξιόπιστα λόγο του πολύ μικρού αριθμού δείγματος που είχαμε αφού πήραν μέρος μόνο 30 άτομα.

Γνωστοποιώντας σε κάθε χρήστη το κωδικό που θα χρησιμοποιούσε στο πρώτο τεστ για τις επόμενες 3 εβδομάδες και αφού δόθηκαν όλες οι αναγκαίες διευκρινίσεις, σε ένα πίνακα με αναγραμμένα τα ονόματα των χρηστών καταγράφηκαν οι αντιδράσεις τους. Οι αρχικές τους αντιδράσεις είχαν να κάνουν καθαρά με το βαθμό δυσκολίας του κωδικού, μιας και σχεδόν κανείς δεν χρησιμοποιούσε ή είχε χρησιμοποιήσει κατά το παρελθόν τέτοιου είδους κωδικό. Αρκετοί ήταν αυτοί που δεν γνώριζαν ποιο ήταν το σύμβολο που έπρεπε να βάλουν, για παράδειγμα όταν κάποιος έπρεπε να χρησιμοποιήσει το σύμβολο της περισπωμένης ( ~ ) ή της κυρτής αγκύλης ( { ) δεν γνώριζε πού βρισκόταν στο πληκτρολόγιο δημιουργώντας του έτσι ένα κλίμα δυσφορίας και αγανάκτησης. Σε κάποιους από τους χρήστες παρατηρήθηκε ότι ξεχνούσαν να εισάγουν και τους 8 χαρακτήρες ιδίως αν υπήρχε το σύμβολο τονισμού ( ‘ ) ή το κόμμα ( , ), τέτοια προβλήματα αντιμετωπίστηκαν και λύθηκαν από τις πρώτες μέρες με επεξήγηση όλων των ειδικών χαρακτήρων που υπάρχουν στο πληκτρολόγιο, είτε περιλαμβανόταν είτε όχι στο κωδικό του κάθε χρήστη. Οι περισσότεροι χρήστες βλέποντας τη δυσκολία του κωδικού σε τυχαία σειρά επέλεγαν την υπενθύμιση παρά τον επανακαθορισμό για λόγους προσωπικής διευκόλυνσης, δηλαδή προτιμούσαν να εμπεδώσουν τον αρχικό κωδικό παρά να τους δοθεί άλλος. Υπήρξαν μερικές περιπτώσεις όπου χρήστες ζήτησαν επανακαθορισμό κωδικού γιατί,

όπως δήλωσαν, οπτικά ήταν δύσκολος στη εισαγωγή. Για παράδειγμα, ενώ είχε δοθεί ο κωδικός 'V:U4Vae ζητήθηκε και έγινε αλλαγή κωδικού τη πρώτη μάλιστα μέρα σε AHA)HF4n, άλλη περίπτωση ήταν με αρχικό κωδικό {YTsU\K7 ο χρήστης ζήτησε αλλαγή τη τρίτη μέρα γιατί όπως δήλωσε οι χαρακτήρες του κωδικού προκαλούσαν μπέρδεμα και ο νέος κωδικός που πήρε ήταν TB3-C^C3, άλλο παράδειγμα είναι με αρχικό κωδικό το Y`9)q4,o να ζητήσει αλλαγή και ο νέος κωδικός να είναι sprw_J7_ . Ένα θετικό στοιχείο που παρατηρήθηκε ήταν η πλήρης απομνημόνευση του κωδικού από 3 άτομα, ένα εκ των οποίων του είχε αλλαχθεί ο κωδικός. Τα επόμενα 2 γραφήματα δείχνουν, ανά ηλικιακή ομάδα, πόσοι ζήτησαν επανακαθορισμό και πόσοι υπενθύμιση του κωδικού τους μέχρι το τέλος του τεστ.

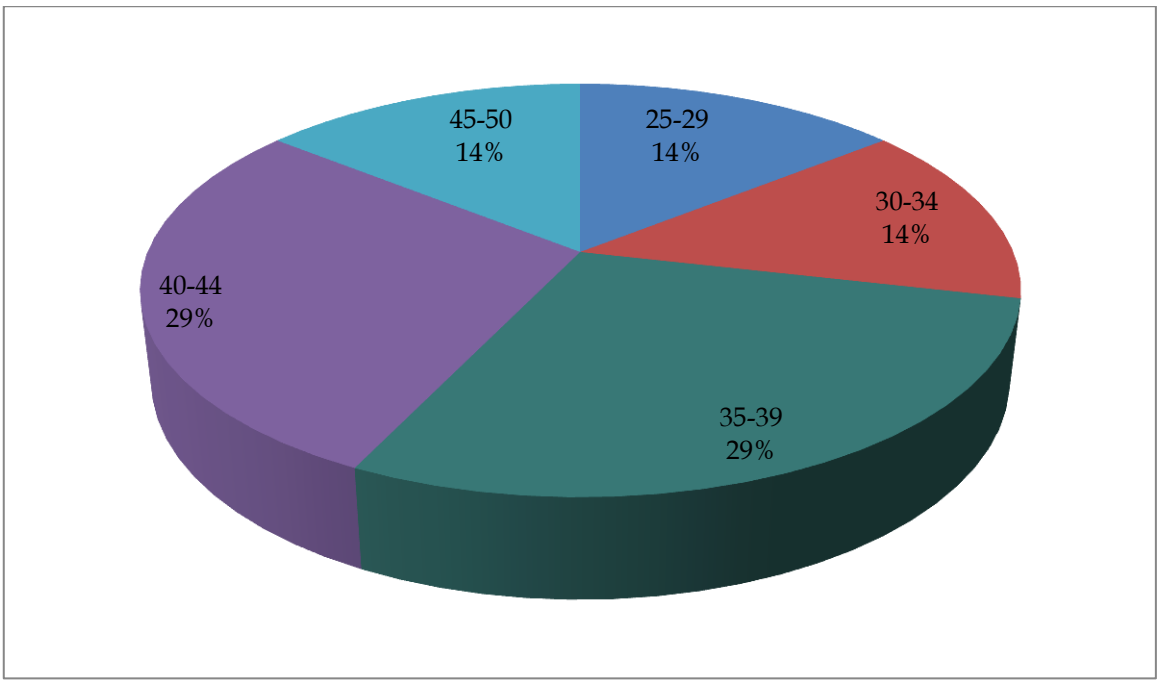



**Γράφημα 4.1:** Αίτημα αλλαγής κωδικού ανά ηλικία.



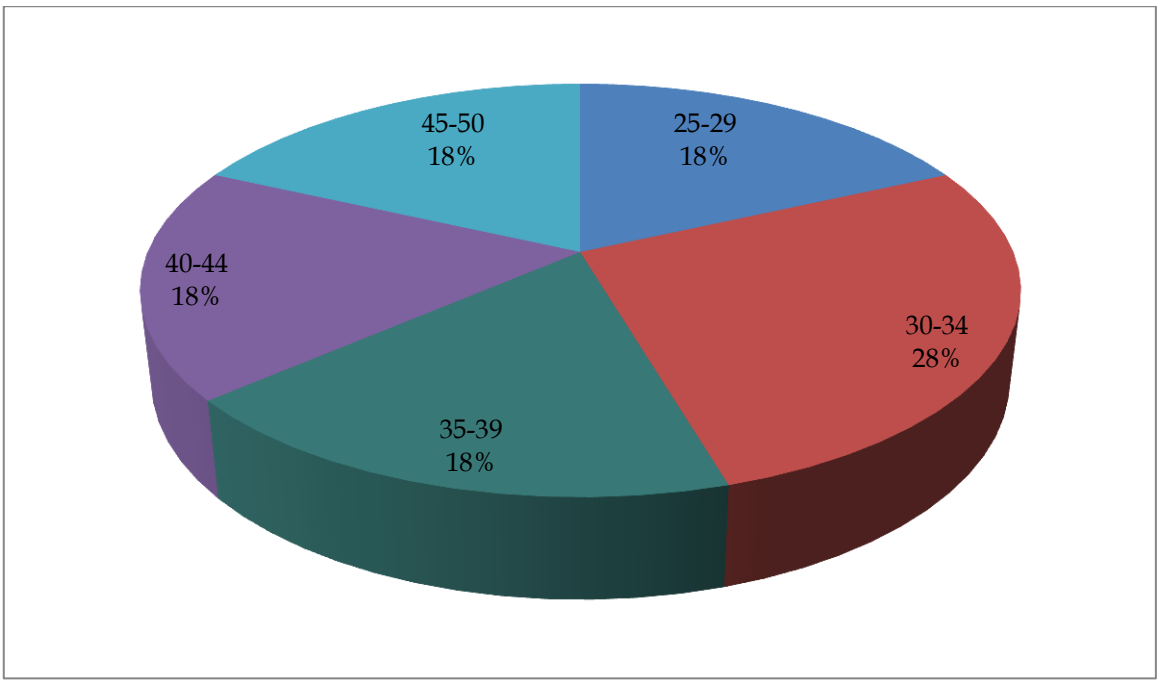

**Γράφημα 4.2:** Αίτημα υπενθύμισης κωδικού ανά ηλικία.

Στο δεύτερο τεστ παρατηρήθηκε ότι κανένας χρήστης δεν χρειάστηκε να προχωρήσει σε επανακαθορισμό κωδικού αφού η απουσία και μόνο αριθμών και ειδικών χαρακτήρων αποδείχθηκε μια πιο εύκολη διαδικασία. Σε ελάχιστες περιπτώσεις που δεν ξεπερνούν τις 10, μερικοί χρήστες ζήτησαν υπενθύμιση τους κωδικού γιατί είχαν μπερδέψει κεφαλαίο γράμμα με πεζό και το αντίστροφα. Δεν παρουσιάστηκαν αντιδράσεις ούτε προβληματισμοί όπως στο πρώτο τεστ και αυτό οδήγησε στο να μελετηθεί σε περισσότερο βάθος η συγκεκριμένη μέθοδος ώστε να βρεθούν τρόποι καλύτερης αξιοποίησης και ευρείας αποδοχής που να μην δυσκολεύουν τους χρήστες κατά τη διάρκεια εισαγωγής. Αρκετοί από τους χρήστες ήρθαν σε επαφή και ζήτησαν εάν γίνεται να χρησιμοποιήσουν το ίδιο ή άλλο κωδικό για προσωπική χρήση, αυτό έγινε αποδεχτό με ιδιαίτερη χαρά. Το επόμενο γράφημα δείχνει την υπενθύμιση που έγινε σε 7 άτομα.

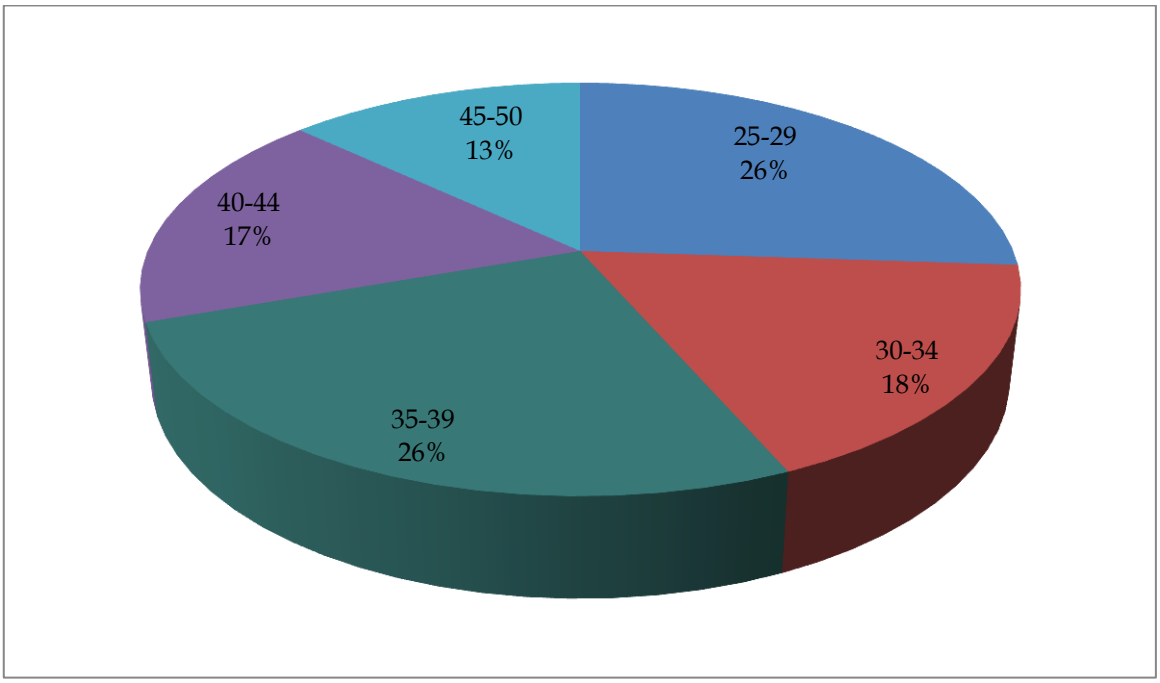



**Γράφημα 4.3:** Αίτημα υπενθύμισης κωδικού ανά ηλικία.

Περνώντας στο τρίτο κατά σειρά τεστ, υπήρχε η πεποίθηση ότι δεν θα επαναλαμβάνονταν τα προβλήματα που παρουσιάστηκαν στο πρώτο τεστ αφού είχαν ήδη επεξηγηθεί και όλες οι απορίες καλύφθηκαν. Ξεκινώντας με το τεστ αρκετά άτομα έδειξαν σημάδια δυσαρέσκειας επειδή ο κωδικός που έλαβαν περιείχε, όπως δημιουργήθηκε με βάση το μοτίβο στη εικόνα 4.11, αριθμούς και ειδικούς χαρακτήρες. Στο μεταξύ είχαν μεσολαβήσει οι γιορτές των Χριστουγέννων με τη διενέργεια του δεύτερου τεστ αποδεικνύοντας ότι όντως οι άνθρωποι τείνουν να ξεχνούν επιβεβαιώνοντας τη θέση που υποστηρίξαμε στο κεφάλαιο 3 για το ανθρώπινο μνημονικό. Αφού έγινε μια γρήγορη επανάληψη και επεξήγηση των ειδικών χαρακτήρων και για το πού βρίσκονται στο πληκτρολόγιο, κατά τη πρώτη μέρα του τρίτου τεστ δεν παρατηρήθηκαν άλλα παρόμοια φαινόμενα ή αντιδράσεις. Τις επόμενες μέρες μερικά άτομα ζήτησαν υπενθύμιση ή αλλαγή του κωδικού τους για τους ίδιους λόγους που έγιναν και στο πρώτο τεστ, το ευτύχημα ήταν πως δεν παρατηρήθηκαν στη ίδια συχνότητα. Τα πιο κάτω γραφήματα δείχνουν, ανά ηλικιακή ομάδα, πόσοι είχαν ζητήσει επανακαθορισμό και πόσοι υπενθύμιση του κωδικού τους.



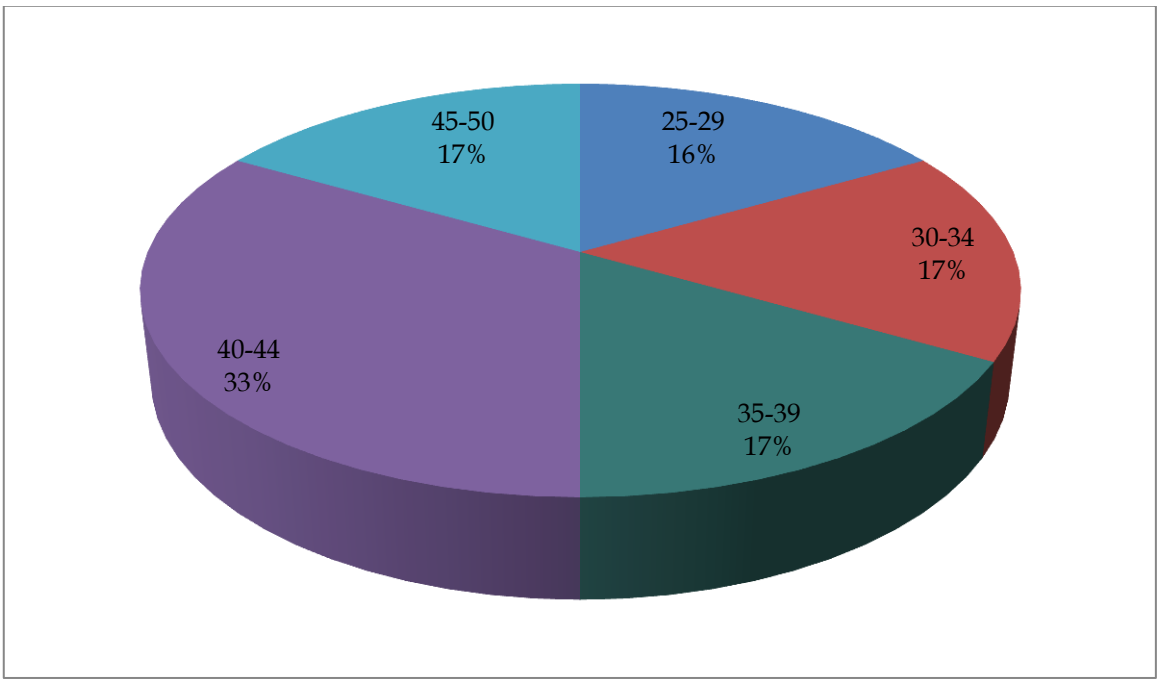

**Γράφημα 4.4:** Αίτημα αλλαγής κωδικού ανά ηλικία.



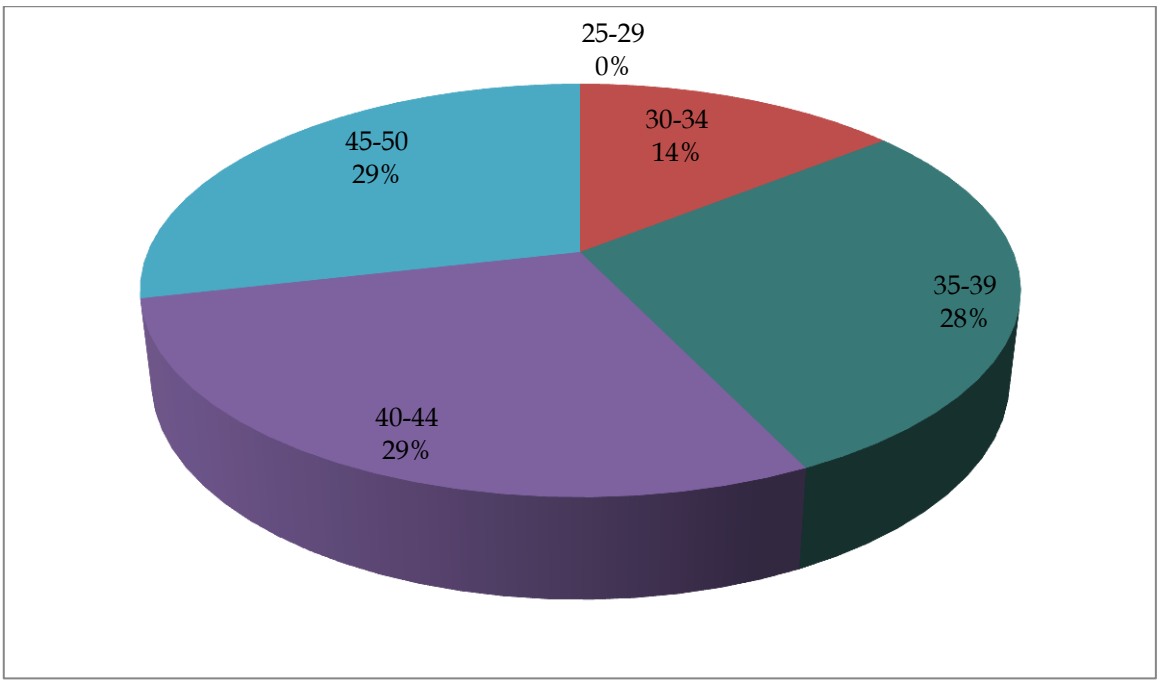

**Γράφημα 4.5:** Αίτημα υπενθύμισης κωδικού ανά ηλικία.

Περνώντας στο τέταρτο και προτελευταίο τεστ, οι χρήστες είχαν συνηθίσει στο να κάνουν χρήση ειδικών χαρακτήρων και αναμέναμε να μην παρουσιαστούν παρόμοια προβλήματα όπως είχαμε στο πρώτο και τρίτο τεστ, πράγμα που όντως έτσι είχε γίνει. Χρειάστηκε να γίνουν μερικές υπενθυμίσεις κωδικών και ακόμη λιγότεροι επανακαθορισμοί, γεγονός που μας χαροποίησε

ιδιαίτερα. Μερικοί χρήστες είχαν για κωδικό στίχους από τα τραγούδια που συμπεριλάβαμε στο πρώτο ερωτηματολόγιο που δόθηκε [Παράρτημα Α1] και αυτό τους βοήθησε στη καλύτερη απομνημόνευση του κωδικού, οι υπόλοιποι είχαν κωδικό από τις άλλες κατηγορίες και γι' αυτό υπήρξαν υπενθυμίσεις και επανακαθορισμοί. Τα γενικά σχόλια, όχι μόνο για το συγκεκριμένο τεστ αλλά για το πρώτο και το τρίτο, αναφέρονταν στο ότι ναι μεν συνήθισαν στη χρήση αριθμών και ειδικών χαρακτήρων για κωδικό αλλά τους φάνηκε κουραστικό σαν διαδικασία και θα προτιμούσαν κάτι πιο εύκολο όπως το κωδικό του δεύτερου τεστ, υπενθυμίζοντάς τους ποια διαδικασία θα ακολουθηθεί για το τελευταίο τεστ. Τα επόμενα 2 γραφήματα δείχνουν τον επανακαθορισμό και υπενθύμιση κωδικού ανά ηλικιακή ομάδα.

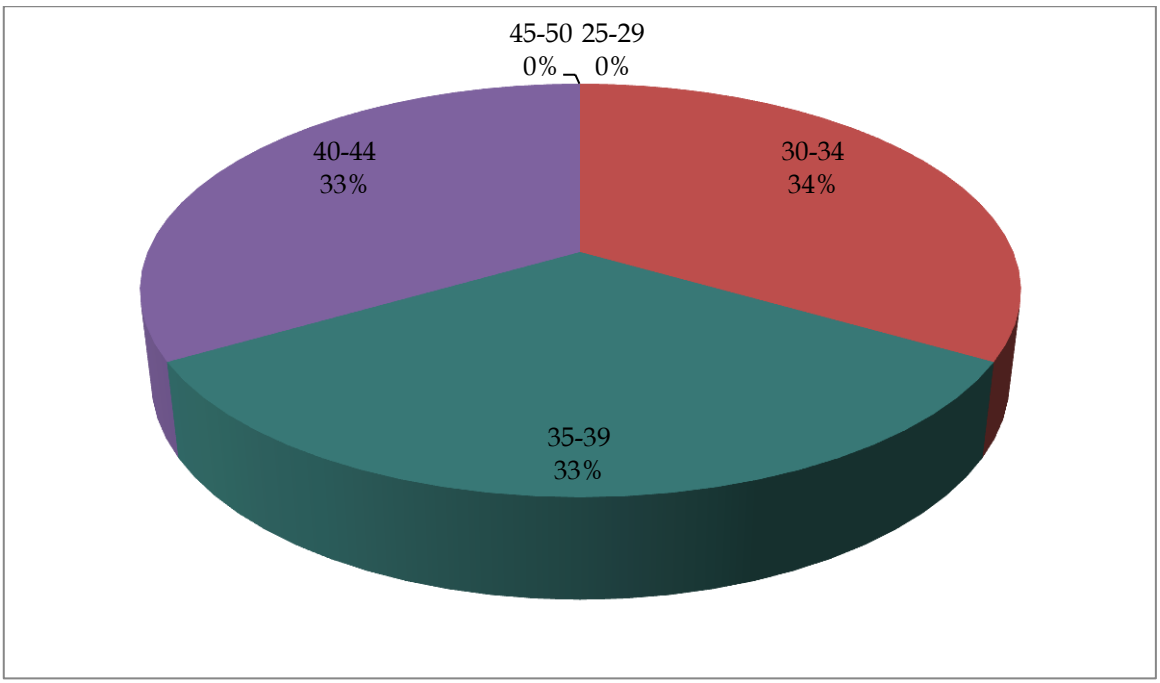



**Γράφημα 4.6:** Αίτημα αλλαγής κωδικού ανά ηλικία.




**Γράφημα 4.7:** Αίτημα υπενθύμισης κωδικού ανά ηλικία.

Στο πέμπτο και τελευταίο τεστ είχαν παρατηρηθεί τα καλύτερα αποτελέσματα. Κανένας χρήστης δεν ζήτησε να του γίνει επανακαθορισμός και μόνο 3 άτομα ζήτησαν υπενθύμιση για το λόγο ότι μπέρδεψαν πεζά με κεφαλαία γράμματα, γεγονός που θεωρήθηκε αμελητέο για το συγκεκριμένο τεστ. Μολονότι φάνηκε να είναι η καλύτερη λύση για περισσότερη μελέτη, οι χρήστες προτίμησαν να έχουν κωδικό που προφέρεται. Το επόμενο γράφημα δείχνει την υπενθύμιση κωδικού ανά ηλικιακή ομάδα.




**Γράφημα 4.7:** Αίτημα υπενθύμισης κωδικού ανά ηλικία.

## 4.7 Δημιουργία Ερωτηματολογίων

Για να μετρήσουμε το βαθμό αποδοχής που είχαν οι κωδικοί σε κάθε τεστ αλλά και για να έχουμε μια ιδέα σχετικά με τους τρόπους που δημιουργούν και προφυλάσσουν οι χρήστες τους κωδικούς τους, δόθηκαν 2 ερωτηματολόγια σε ξεχωριστές χρονικές περιόδους. Το προσωπικό ερωτηματολόγιο δόθηκε στα μέσα του τρίτου τεστ με το σκεπτικό ότι όλοι οι χρήστες είχαν αποκτήσει μια μικρή εμπειρία και εξοικείωση με δύσκολους κωδικούς επιλέγοντας τη απάντηση που τους άρμοζε καλύτερα. Οι ερωτήσεις είχαν να κάνουν με τη ποικιλία κωδικών εάν και εφόσον χρησιμοποιούν, εάν εφάρμοζαν τον ίδιο κωδικό σε περισσότερες των μια περιπτώσεων καθώς επίσης τρόπους που οι ίδιοι τους προστατεύουν ή απομνημονεύουν. Σαν επιπλέον ερώτημα που οι απαντήσεις θα χρησιμοποιούνταν στο τέταρτο τεστ, η τελευταία ερώτηση ζητούσε όπως συμπληρώσουν τη λέξη που έλειπε από κομμάτια στίχων. Οι στίχοι χωρίζονταν σε 2 κατηγορίες με συνολικούς στίχους από 41 τραγούδια, 29 ελληνικά και 12 αγγλικά. Υπήρξε υψηλό ποσοστό εύρεσης των στίχων και στις 2 κατηγορίες, 9% για τα ελληνικά και 95% για τα αγγλικά αντίστοιχα. Το τελικό ερωτηματολόγιο [Παράρτημα Α2] ζητούσε από τους χρήστες να αξιολογήσουν την εμπειρία που είχαν στο κάθε τεστ, το βαθμό δυσκολίας που αντιμετώπισαν και αν θα προτιμούσαν παρόμοιο κωδικό για προσωπική τους χρήση σε ποια μέθοδο να υπάγεται.

# Κεφάλαιο 5
# Αποτελέσματα και Συμπεράσματα

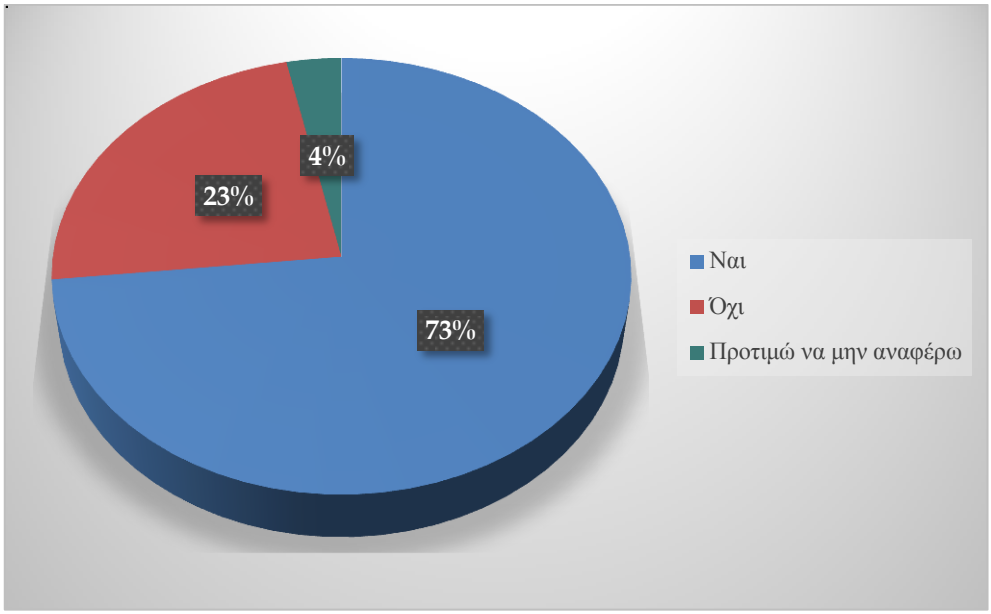
Τα αποτελέσματα που πήραμε από τα 2 ερωτηματολόγια και την καταγραφή των αλλαγών που έγιναν κατά τη διάρκεια των τεστ, μας έδωσαν μια σαφή εικόνα για τις δυνατότητες και τις συνήθειες που έχουν οι χρήστες αναφορικά με τους κωδικούς που διαχειρίζονται σε καθημερινή βάση, για προσωπική και επαγγελματική χρήση, καθώς επίσης τους τρόπους διαφύλαξης και δημιουργίας του. Το πιο θετικό αποτέλεσμα που παρατηρήθηκε μέχρι το τέλος των τεστ ήταν η δυνατότητα οι χρήστες να είναι σε θέση να θυμούνται πιο δύσκολους κωδικούς σε σχέση πάντοτε με αυτούς που χρησιμοποιούσαν. Στο επόμενο τμήμα του κεφαλαίου θα παρουσιαστούν συγκεντρωτικά οι απαντήσεις που έδωσαν μαζί με τις επεξηγήσεις τους.

## 5.1 Ανάλυση και επεξήγηση αποτελεσμάτων

Τα γραφήματα που ακολουθούν στις πιο κάτω ενότητες, αναφέρονται στις απαντήσεις που πήραμε για το προσωπικό και το τελικό ερωτηματολόγιο.

### 5.1.1 Αποτελέσματα προσωπικού ερωτηματολογίου

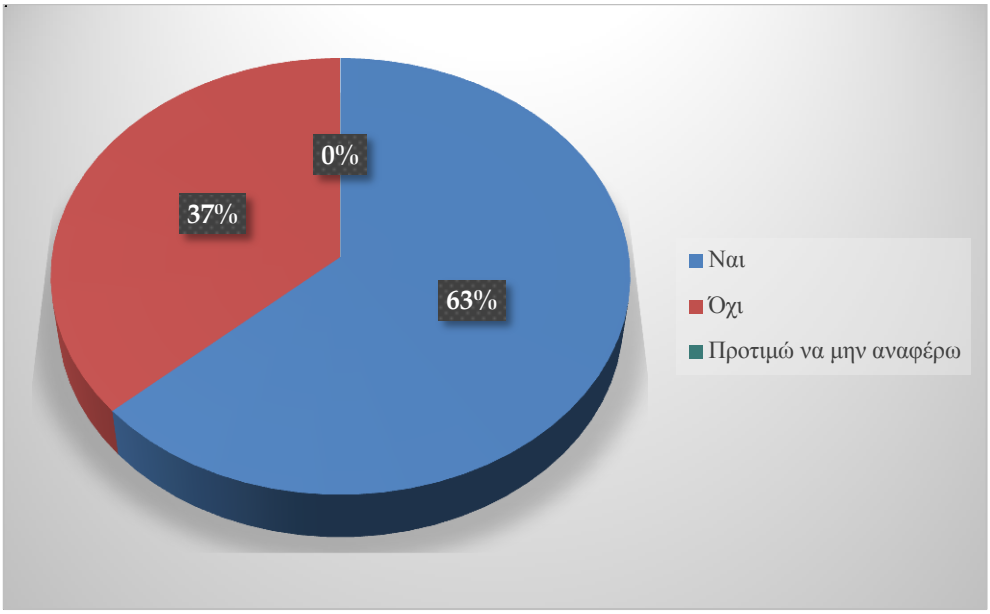
**Ερώτημα 1:** Έχετε κωδικό ή κωδικούς που τους χρησιμοποιείτε σε περισσότερες από μια περιπτώσεις;




**Γράφημα 5.1:** Αποτελέσματα ερωτήματος 1.

Όπως φαίνεται από το γράφημα, ένα πολύ μεγάλο ποσοστό των χρηστών τείνει να επαναχρησιμοποιεί τους κωδικούς, γεγονός που θέτει σε κίνδυνο υποκλοπής των ηλεκτρονικών τους δεδομένων.

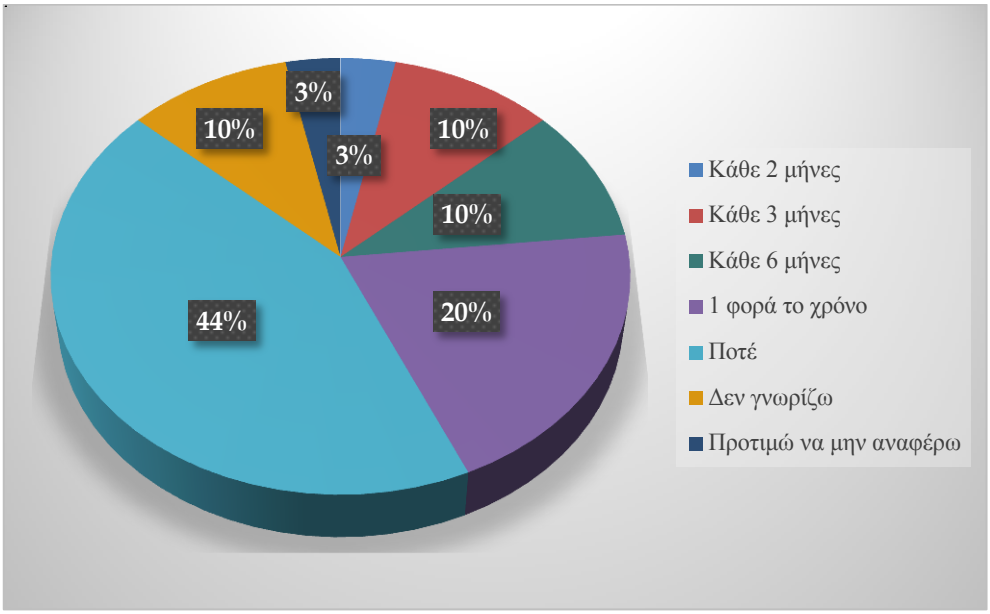
**Ερώτημα 2:** Έχετε κάποιο κωδικό που χρησιμοποιείτε σε περισσότερες από μια περιπτώσεις κάνοντας μικροαλλαγές κάθε φορά;




**Γράφημα 5.2:** Αποτελέσματα ερωτήματος 2.

Παρατηρήθηκε μεγάλο ποσοστό θετικών απαντήσεων, γεγονός που προκαλεί ανησυχία. Μικροαλλαγές εννοούμε είτε τη χρήση αριθμών (κωδικός1, κωδικός2 κτλ) είτε να αντιστοιχεί στη ιστοσελίδα (fbκωδικός για Facebook, gmκωδικός για το Gmail κτλ).

**Ερώτημα 3:** Κάθε πόσο αλλάζετε κάποιο προσωπικό σας κωδικό;

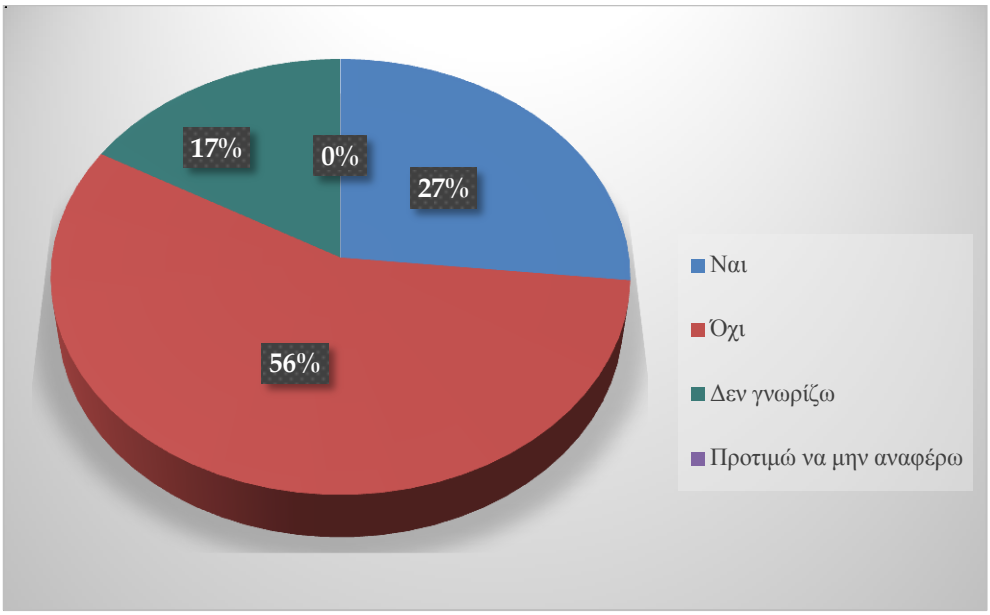



**Γράφημα 5.3:** Αποτελέσματα ερωτήματος 3.

Η συνήθεια να μην γίνεται αλλαγή κωδικού εφαρμόζεται από σχεδόν το μισό μας δείγμα. Στη δεύτερη θέση βλέπουμε το 20% να προβαίνει σε αλλαγή μια φορά το χρόνο ενώ μόλις το 3% τον αλλάζει κάθε 2 μήνες.

Οι ερωτήσεις 4 μέχρι 8 αφορούν στο κωδικό για το προσωπικό ηλεκτρονικό ταχυδρομείο του χρήστη.

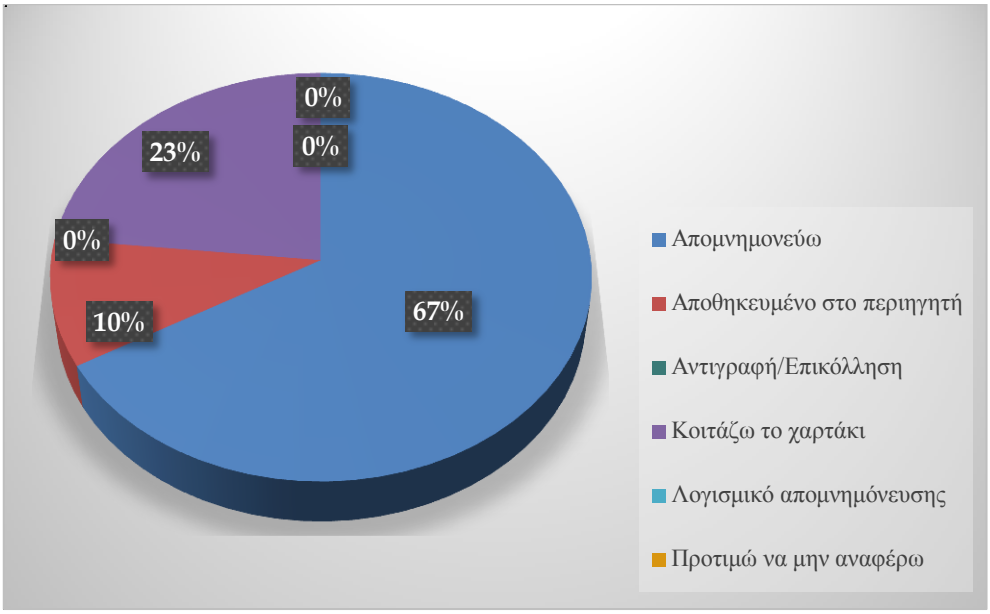
**Ερώτημα 4:** Στη περίπτωση του κωδικού για προσωπικό email, ο παροχέας σας ζητάει να αλλάζετε το κωδικό σας σε τακτά διαστήματα;




**Γράφημα 5.4:** Αποτελέσματα ερωτήματος 4.

Στη περίπτωση του προσωπικού ηλεκτρονικού ταχυδρομείου, εάν δεν τους ζητηθεί από το παροχέα, λίγο παραπάνω από τους μισούς δεν θα προβούν σε αλλαγή κωδικού διατηρώντας τον ήδη υπάρχων. Μόνο 1 στους 4 το πράττει.

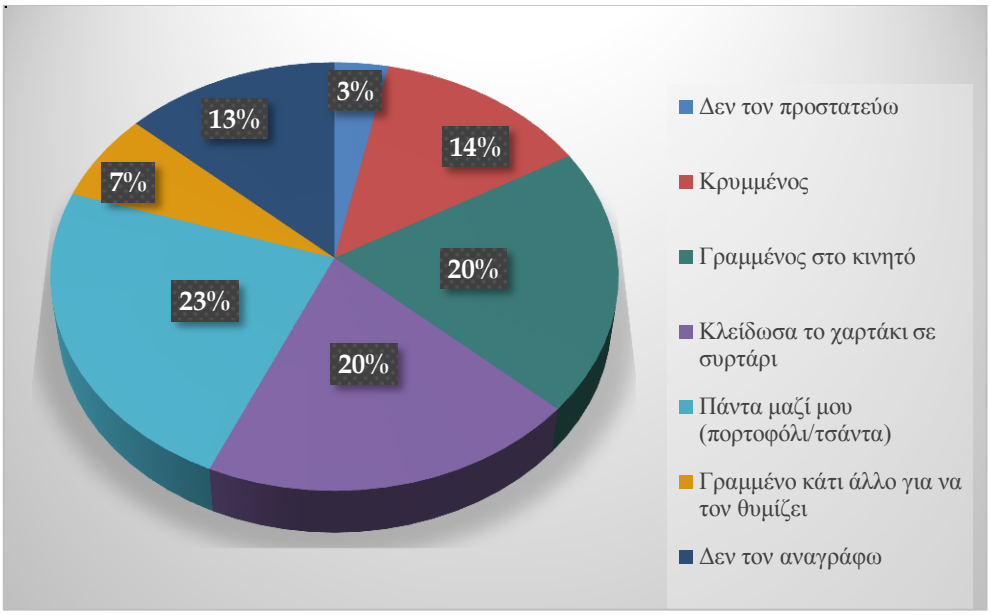
**Ερώτημα 5:** Όταν πρέπει να χρησιμοποιήσετε ένα κωδικό, τι κάνετε για να τον θυμάστε;




**Γράφημα 5.5:** Αποτελέσματα ερωτήματος 5.

Η απομνημόνευση κωδικού ανέρχεται σε ποσοστό του 67%, πολύ ικανοποιητικό αλλά κανείς δεν μπορεί να μας εγγυηθεί ότι ο κωδικός που χρησιμοποιούν έχει μεγάλο βαθμό δυσκολίας για να τον μαντέψει κάποιος. Η αποθήκευση στον περιηγητή εγκυμονεί κινδύνους, σε περίπτωση που μολυνθούν από ιό το πιο πιθανό είναι να γίνει υποκλοπή του.

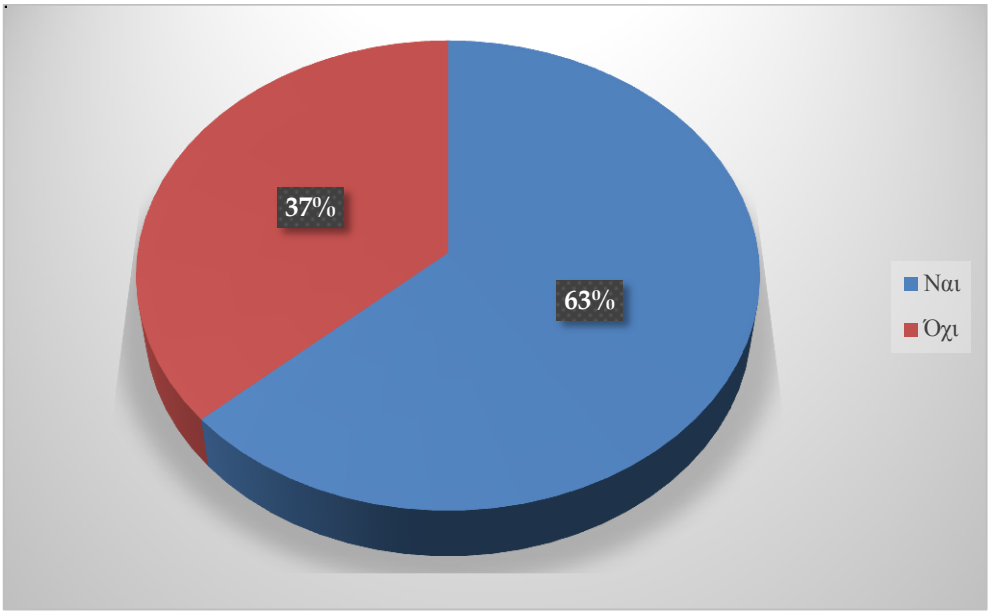
**Ερώτημα 6:** Εάν είχατε γραμμένο κάπου το κωδικό σας, πώς τον προστατεύσατε;




**Γράφημα 5.6:** Αποτελέσματα ερωτήματος 6.

Έχοντας φυλαγμένο στο πορτοφόλι/τσάντα το κωδικό, ο χρήστης έχει ένα αίσθημα ασφάλειας ότι δεν θα ξεχάσει ποτέ το κωδικό και υπάρχει περίπτωση να είναι ισχυρός. Το αντίθετο ισχύει όμως στη περίπτωση που τον κλέψουν. Σε δεύτερη θέση είναι το κινητό και να το έχει κλειδωμένο σε κάποιο συρτάρι.

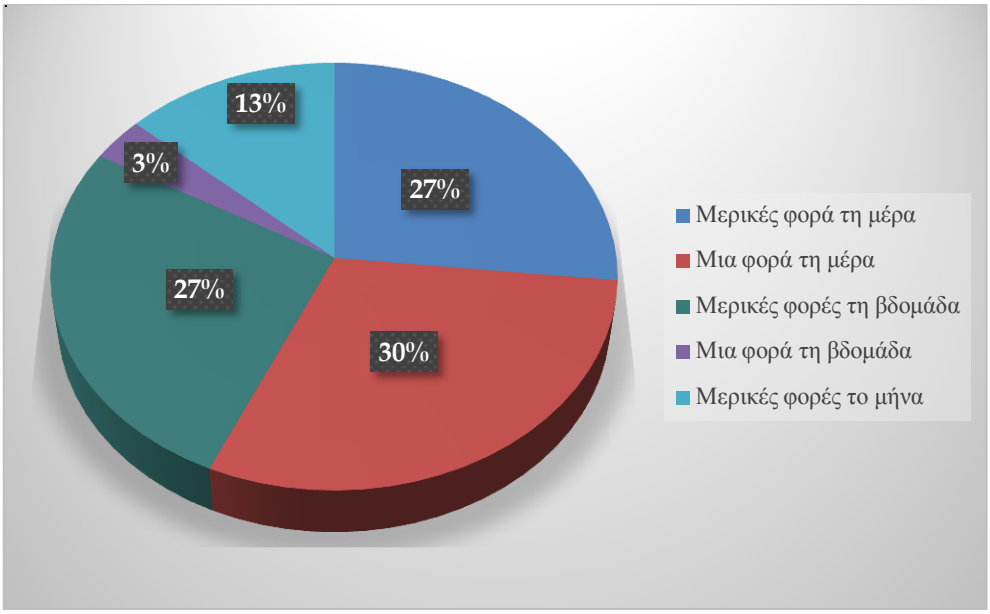
**Ερώτημα 7:** Συνδυάσατε το κωδικό σας με κάποια φράση ώστε να τον θυμάστε;




**Γράφημα 5.7:** Αποτελέσματα ερωτήματος 7.

Παρόλο που η χρήση φράσεων για τη παραγωγή κωδικού είχε θετική απάντηση από τους πλείστους χρήστες, δεν την αξιοποίησαν στο έπακρο αφού στο ανάλογο τεστ υπήρξαν υπενθυμίσεις και επανακαθορισμοί.

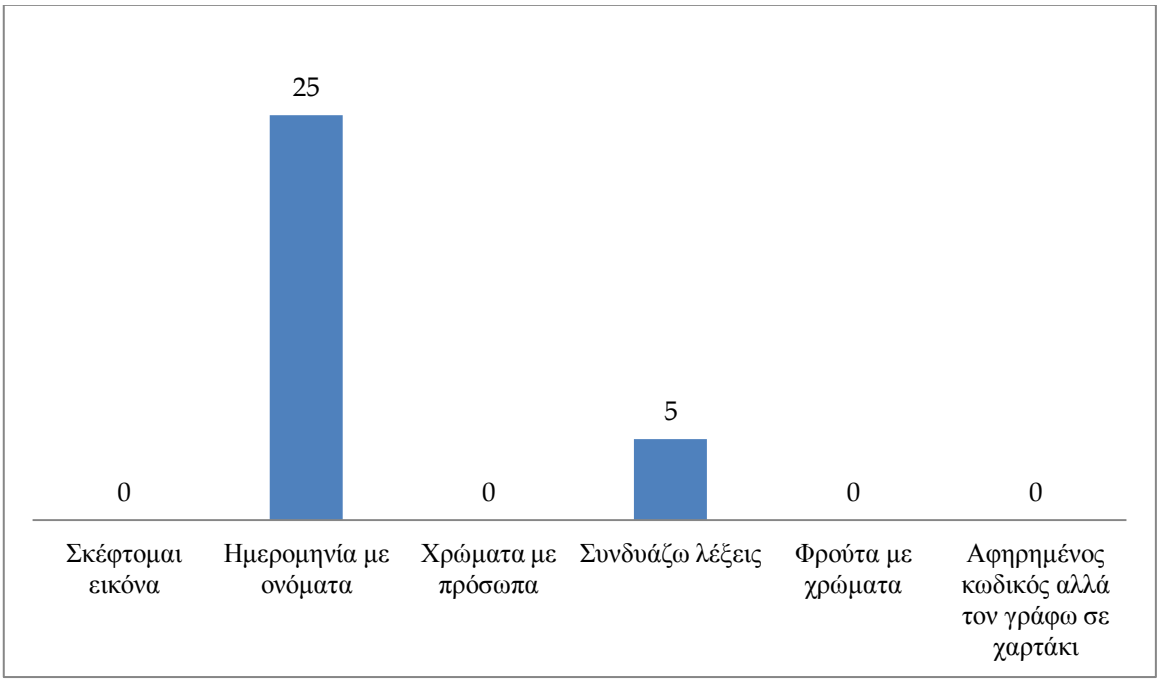
**Ερώτημα 8:** Πόσο συχνά πληκτρολογείτε το κωδικό σας;




**Γράφημα 5.8:** Αποτελέσματα ερωτήματος 8.

Η συχνή επανάληψη του κωδικού μπορεί να έχει θετικό αντίκτυπο στο χρήστη κάνοντας τον να θυμάται πιο εύκολα το κωδικό του. Στο γράφημα παρατηρούμε ότι το 1/3 των χρηστών πληκτρολογεί μια φορά τη μέρα, μικρό ποσοστό ακολουθούμενο με πολύ μικρή διαφορά από τις κατηγορίες Μερικές φορές τη μέρα και Μερικές φορές τη βδομάδα.

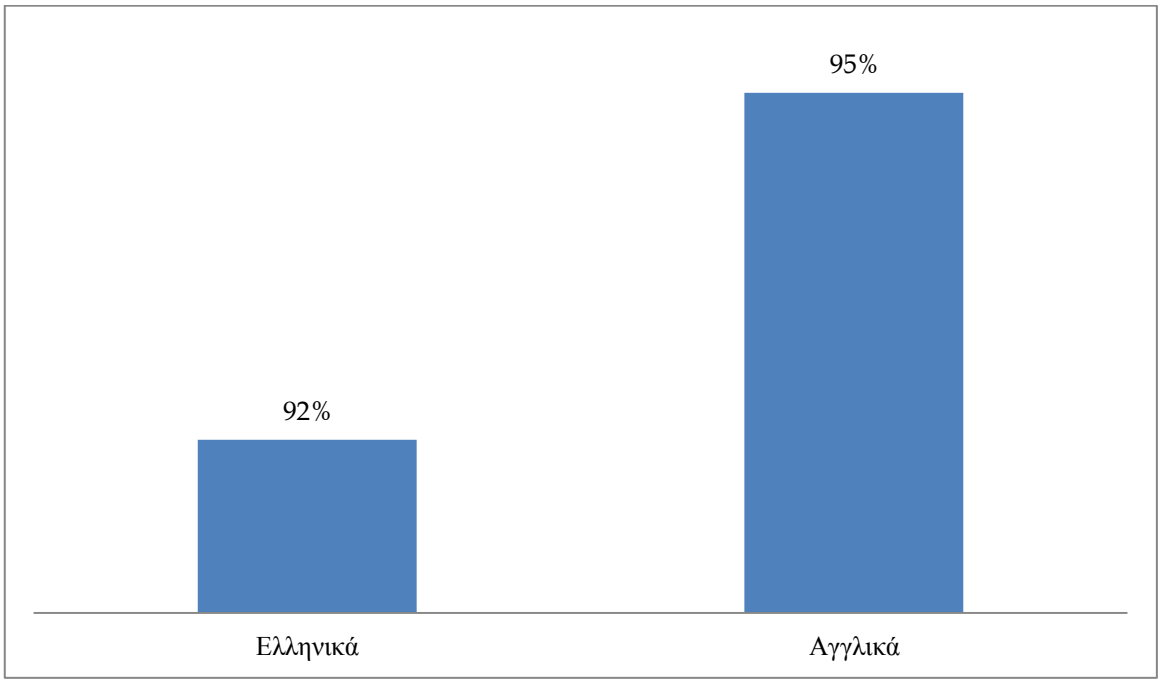
**Ερώτημα 9:** Όταν θέλετε αν δημιουργήσετε ένα καινούργιο κωδικό, με ποιο σκεπτικό το κάνετε;




**Γράφημα 5.9:** Αποτελέσματα ερωτήματος 9.

Σημαντικό μειονέκτημα που παρατηρείται σ' αυτό το γράφημα είναι το μεγάλο ποσοστό χρήσης ημερομηνιών με ονόματα για τη δημιουργία κωδικών, καθιστώντας έτσι τους λογαριασμούς των χρηστών ευάλωτους.

**Ερώτημα 10:** Συμπληρώστε τους αντίστοιχους ελληνικούς και αγγλικούς στίχους των τραγουδιών.

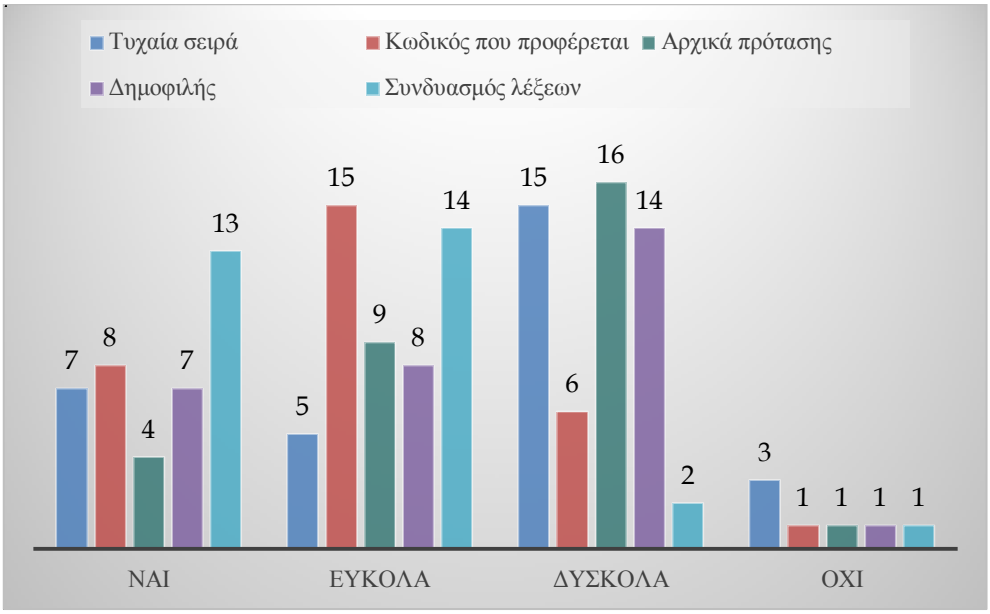



**Γράφημα 5.10:** Αποτελέσματα ερωτήματος 10.

Η ερώτηση 10, που αφορά στη συμπλήρωση των στοίχων με τη σωστή λέξη, έδωσε πολύ θετικά αποτελέσματα επιλέγοντας μερικούς για το τεστ κωδικός από δημοφιλή πρόταση.

### 5.1.2 Αποτελέσματα τελικού ερωτηματολογίου

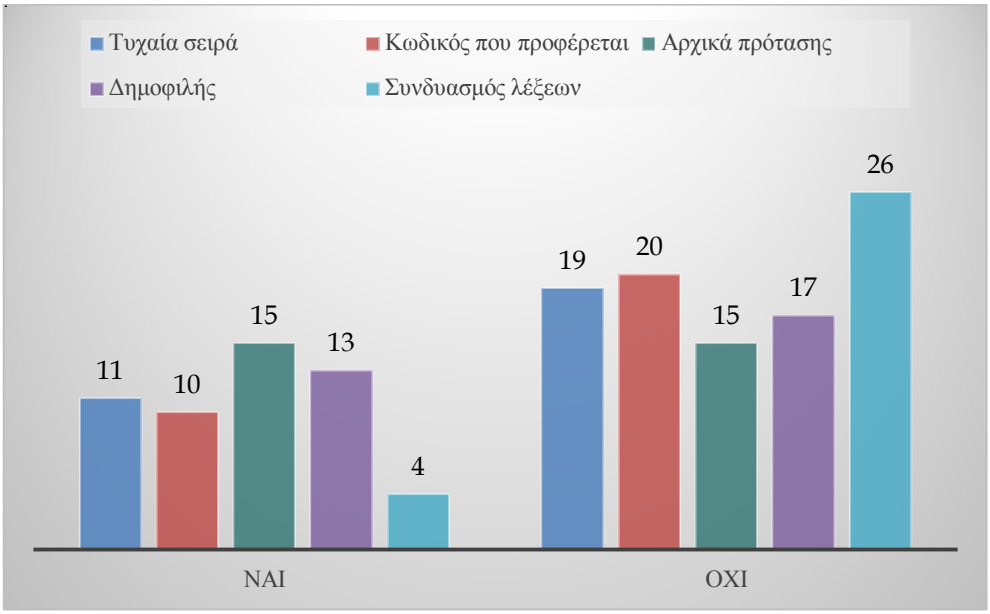
**Ερώτημα 1:** Μπορέσατε να απομνημονεύσετε πλήρως τον εκάστοτε κωδικό σας;




**Γράφημα 5.10:** Αποτελέσματα ερωτήματος 1.

Όπως φαίνεται και από το γράφημα, η μέθοδος του κωδικού που προφέρεται και του συνδυασμού λέξεων ήταν οι πιο εύκολες μέθοδοι σε αντίθεση με το κωδικό από αρχικά πρότασης και χρήση δημοφιλών φράσεων.

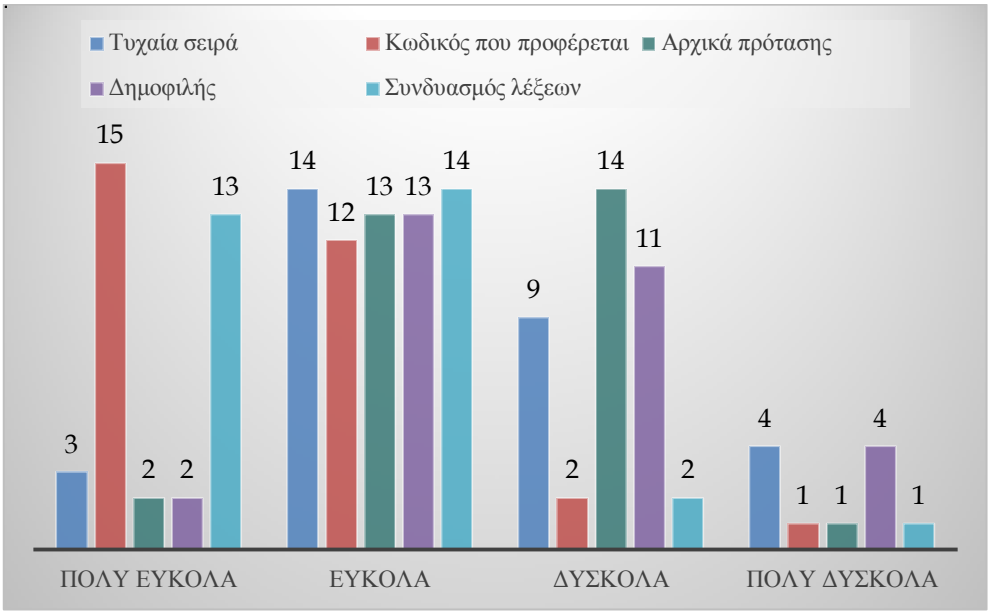
**Ερώτημα 2:** Είχατε σημειωμένο κάπου τον εκάστοτε κωδικό σας;




**Γράφημα 5.11:** Αποτελέσματα ερωτήματος 2.

Παρά τις όλες υπενθυμίσεις και επανακαθορισμούς κωδικών που είχαν γίνει κατά διαστήματα, μερικοί χρήστες παραδέχτηκαν ότι είχαν αναγραμμένο κρυφά το κωδικό τους. Αυτό ίσως δικαιολογηθεί από το φόρτο εργασίας που είχαν και τα χρονικά περιθώρια για ολοκλήρωση δουλείας που τους ανατέθηκε.

**Ερώτημα 3:** Πώς σας φάνηκε ο εκάστοτε κωδικός;

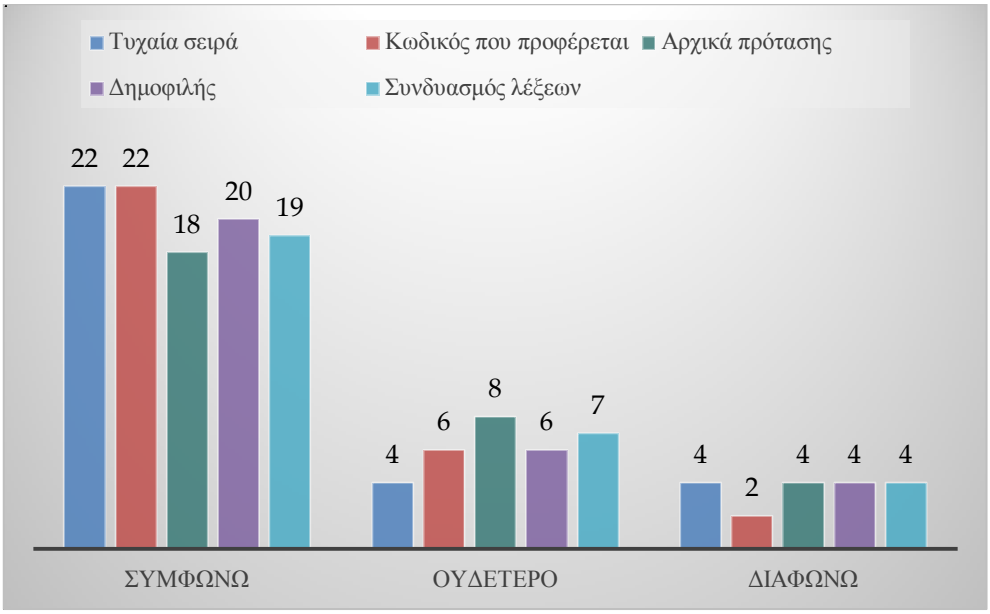



**Γράφημα 5.12:** Αποτελέσματα ερωτήματος 3.

Η πιο εύκολη μέθοδος φάνηκε να ήταν ο κωδικός που προφέρεται με δεύτερη πιο εύκολη το συνδυασμό λέξεων. Μέχρι ενός σημείου είχαν ευκολία και οι υπόλοιπες μέθοδοι, αν και αρκετοί ήταν αυτοί δήλωσαν ότι θα προτιμούσαν αν υπήρχε κατηγορία μεταξύ εύκολα και δύσκολα, το σχεδόν εύκολα.

Τα γραφήματα 4 μέχρι 7 αναφέρονται για κωδικό σε προσωπικό ηλεκτρονικό ταχυδρομείο.

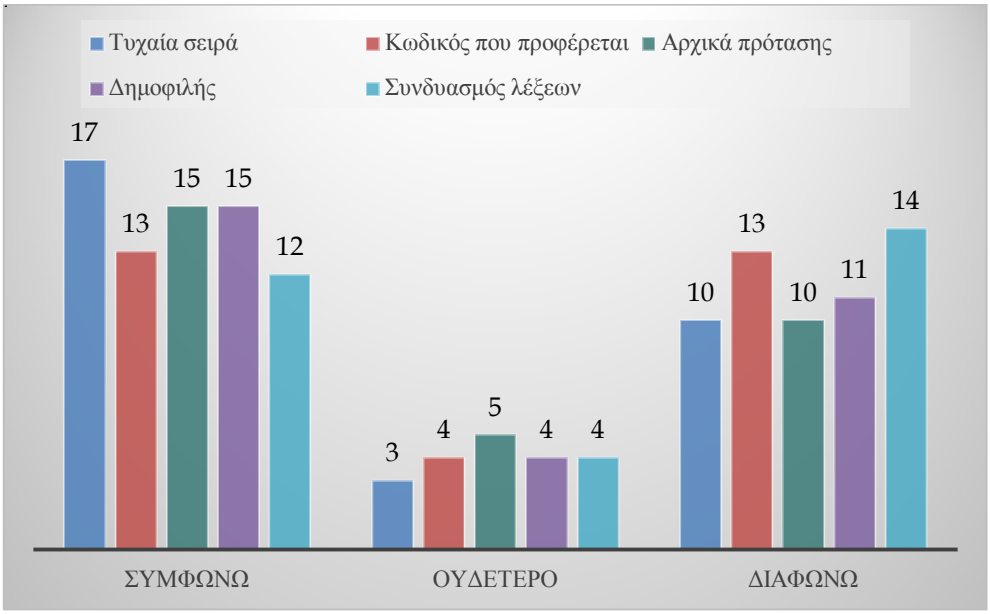
**Ερώτημα 4:** Εάν σας είχε ανατεθεί για το προσωπικό email ένας παρόμοιος κωδικός, θα ήταν πολύ πιο ασφαλής;




**Γράφημα 5.13:** Αποτελέσματα ερωτήματος 4.

Σχεδόν όλοι συμφώνησαν ότι όλες οι μέθοδοι κρίνονται πολύ πιο ασφαλής, ίσως με βάση τον υπάρχων κωδικό που έχουν στο ηλεκτρονικό τους ταχυδρομείο.

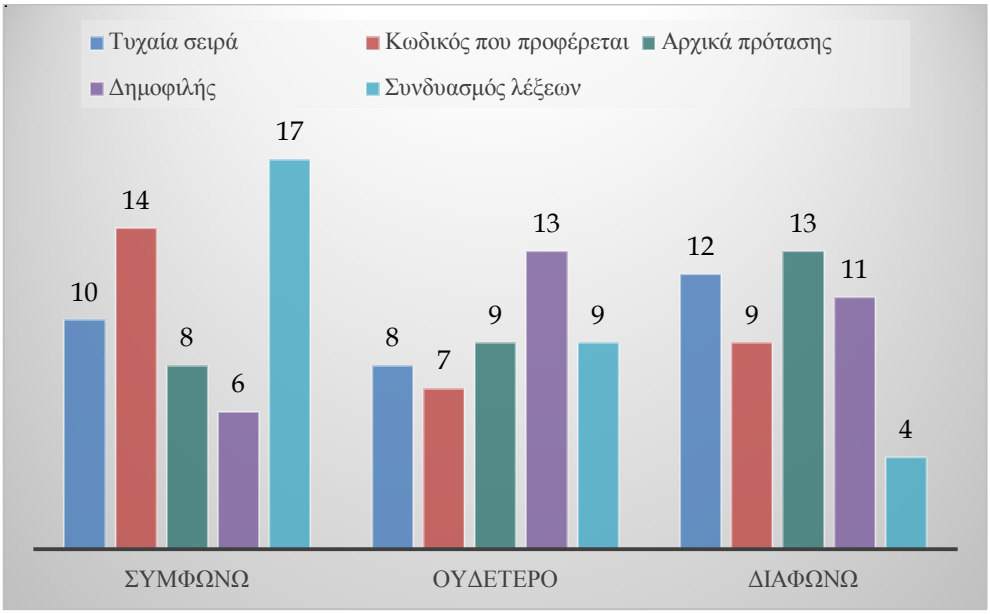
**Ερώτημα 5:** Εάν σας είχε ανατεθεί για το προσωπικό email ένας παρόμοιος κωδικός, θα ήταν πολύ ενοχλητικός;




**Γράφημα 5.14:** Αποτελέσματα ερωτήματος 5.

Εδώ όμως βλέπουμε τη δυσχέρεια των χρηστών σε μεγάλο βαθμό για όλες τις μεθόδους με το κωδικό σε τυχαία σειρά να είναι στη πρώτη θέση. Πολύ λίγοι κράτησαν ουδέτερη στάση.

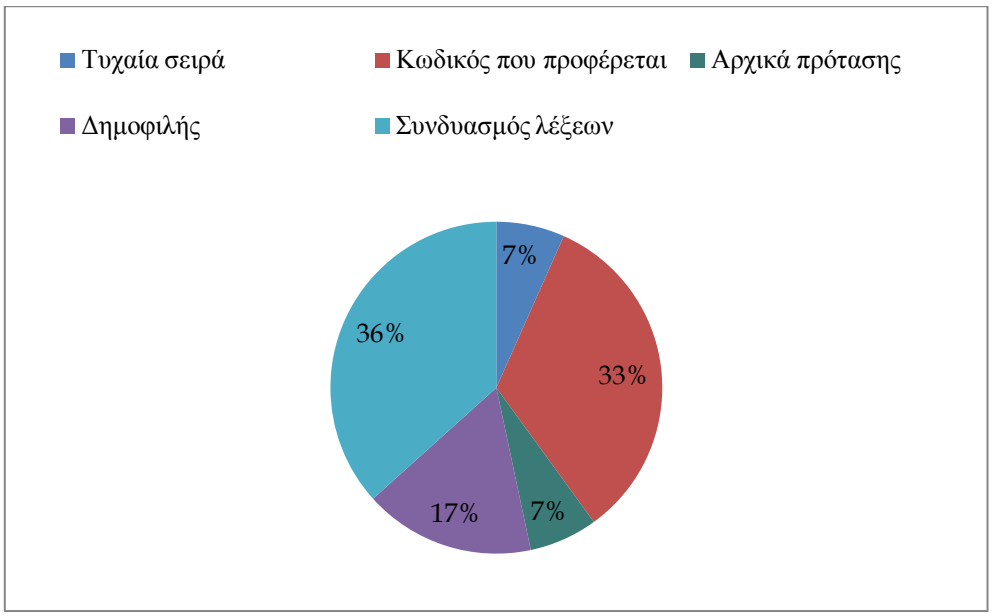
**Ερώτημα 6:** Εάν σας είχε ανατεθεί για το προσωπικό email ένας παρόμοιος κωδικός, θα ήταν πολύ πιο εύκολος;




**Γράφημα 5.15:** Αποτελέσματα ερωτήματος 6.

Εδώ οι απόψεις είναι σχεδόν κατανεμημένες στα ίσα. Οι περισσότεροι συγκλίνουν στις 2 πρώτες απαντήσεις με έμφαση το συνδυασμό λέξεων στη απάντηση Συμφωνώ. Όσοι επέλεξαν Διαφωνώ, μπορούμε να εικάσουμε ότι χρησιμοποιούν ακόμη πιο εύκολους κωδικούς.

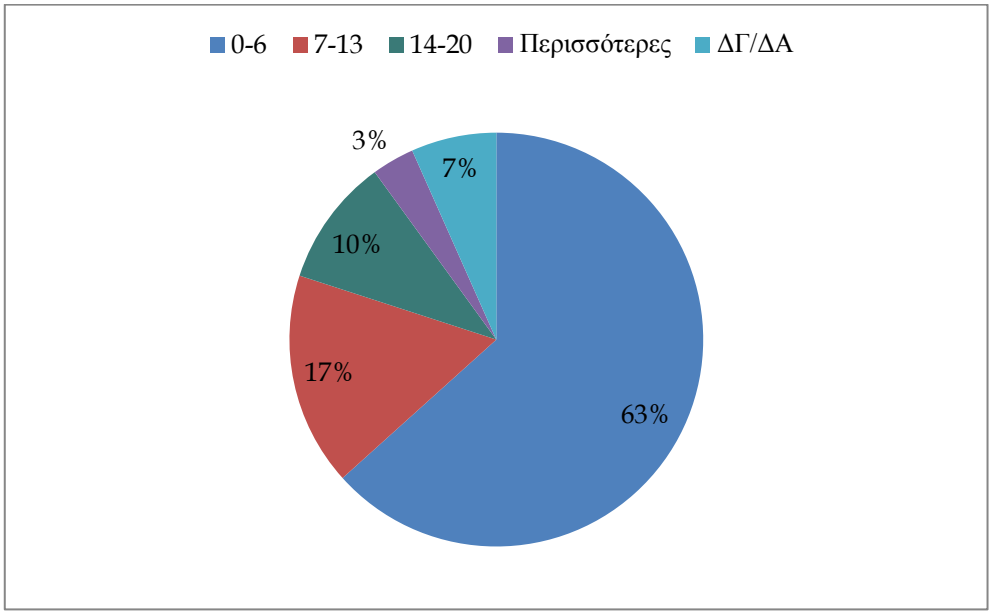
**Ερώτημα 7:** Εάν σας είχε ανατεθεί για το προσωπικό email ένας παρόμοιος κωδικός, σε ποια κατηγορία θα προτιμούσατε να ανήκει;




**Γράφημα 5.16:** Αποτελέσματα ερωτήματος 7.

Η χρήση αριθμών και ειδικών χαρακτήρων φαίνεται να δυσκόλεψε γενικά τους χρήστες δείχνοντας προτίμηση στο συνδυασμό λέξεων και στο κωδικό που προφέρεται.

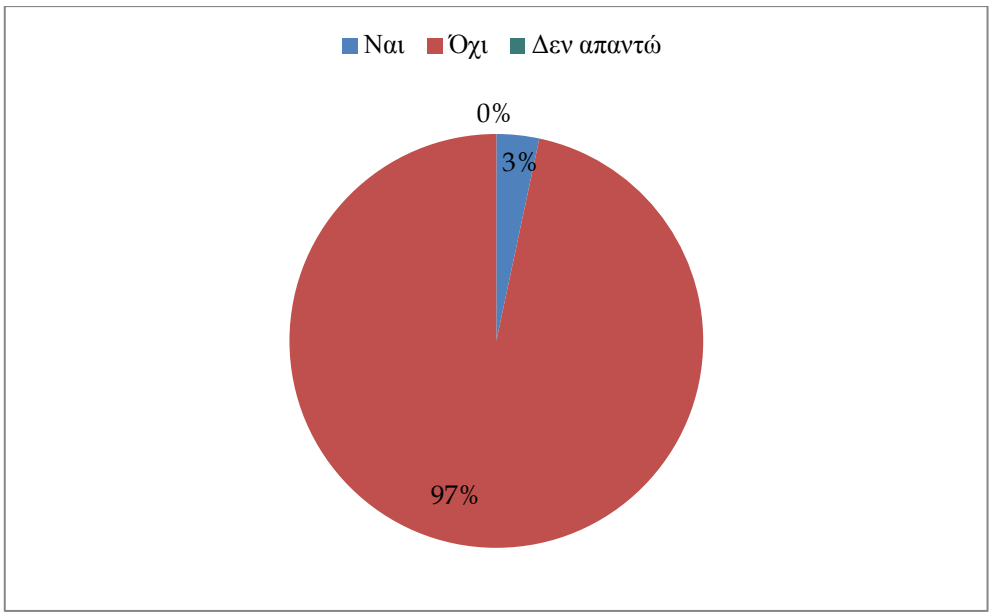
**Ερώτημα 8:** Πόσες φορές καθ' όλη τη διάρκεια των τεστ, χρειαστήκατε υπενθύμιση του κωδικού σας;




**Γράφημα 5.17:** Αποτελέσματα ερωτήματος 8.

Αρκετοί από τους χρήστες ζητούσαν υπενθύμιση κωδικού παρά επανακαθορισμό, ίσως δεν επιθυμούσαν να τους δοθεί άλλος για να μην χρειαστεί να απομνημονεύσουν νέο κωδικό.

**Ερώτημα 9:** Αναφέρατε τον εκάστοτε κωδικό σας σε άλλους;



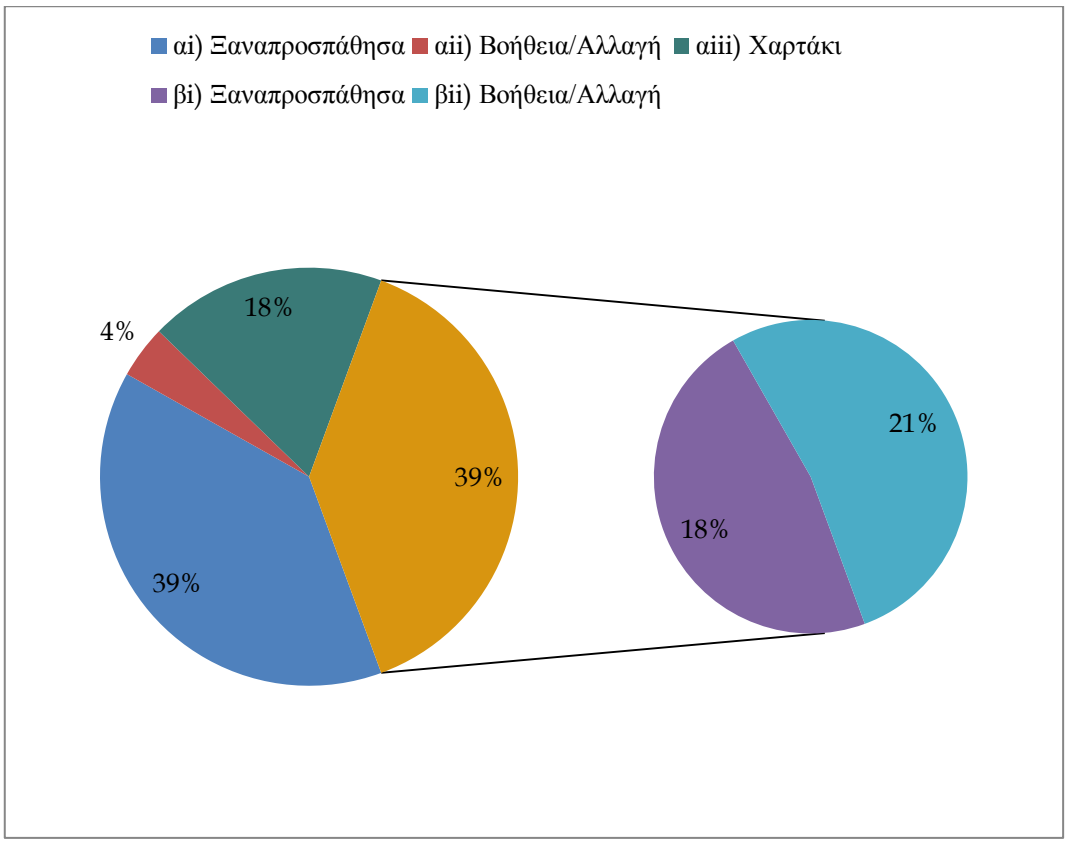

**Γράφημα 5.18:** Αποτελέσματα ερωτήματος 9.

Μόνο ένας χρήστης δήλωσε, άγνωστο για ποιο λόγο, ότι τον ανάφερε σε άλλο άτομο χωρίς ευτυχώς να παρατηρηθούν οποιαδήποτε προβλήματα.

**Ερώτημα 10:** Εάν ξεχάσατε το κωδικό σας

1. Ποιο ήταν το πρώτο βήμα που κάνατε;

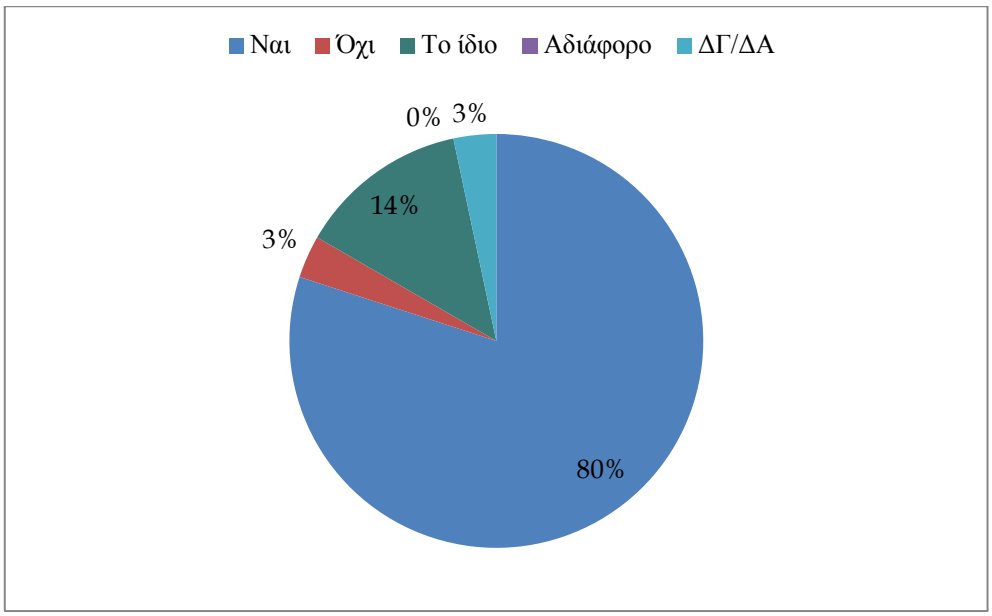
2. Εάν δεν κάνατε τις επιλογές (ii) και (iii), ποιο ήταν το δεύτερο βήμα που κάνατε;




**Γράφημα 5.19:** Αποτελέσματα ερωτήματος 10.

Θετικό μπορεί να χαρακτηριστεί το γεγονός ότι ξαναπροσπαθούσαν να εισάγουν το κωδικό τους πριν τελικά ζητήσουν βοήθεια ή αλλαγή. Υπήρχαν όμως και μερικοί που κοιτούσαν το χαρτάκι τους για βοήθεια.

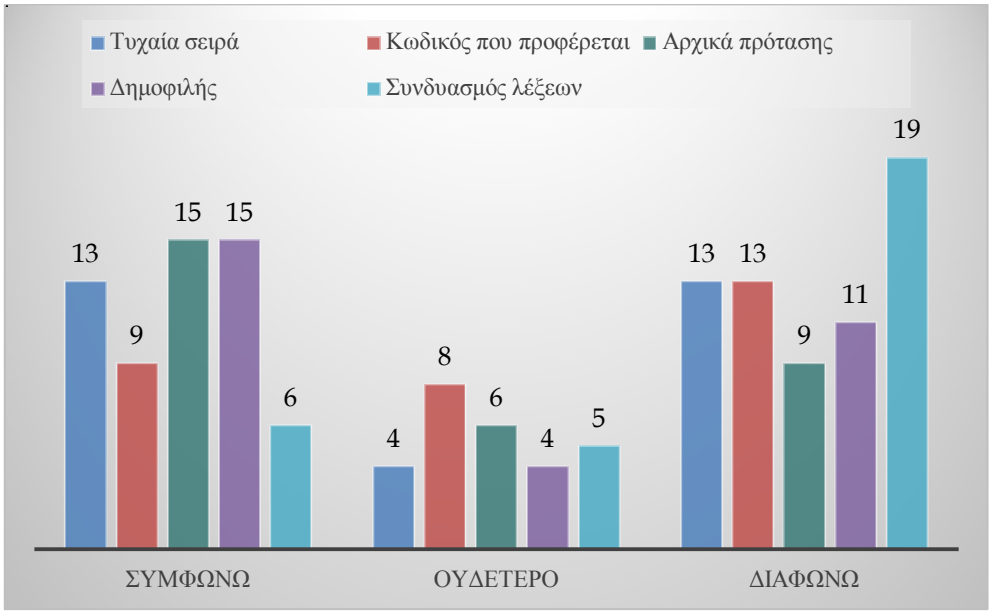
**Ερώτημα 11:** Με τη χρήση του εκάστοτε κωδικού, ο Η/Υ σας ήταν πιο ασφαλής από πριν;




**Γράφημα 5.20:** Αποτελέσματα ερωτήματος 11.

Με το ποσοστό θετικής ανταπόκρισης από τις μεθόδους να είναι πολύ μεγάλο, έγινε σκέψη για καθολική χρήση της πιο αποδεκτής μεθόδου από όλους τους συναδέλφους.

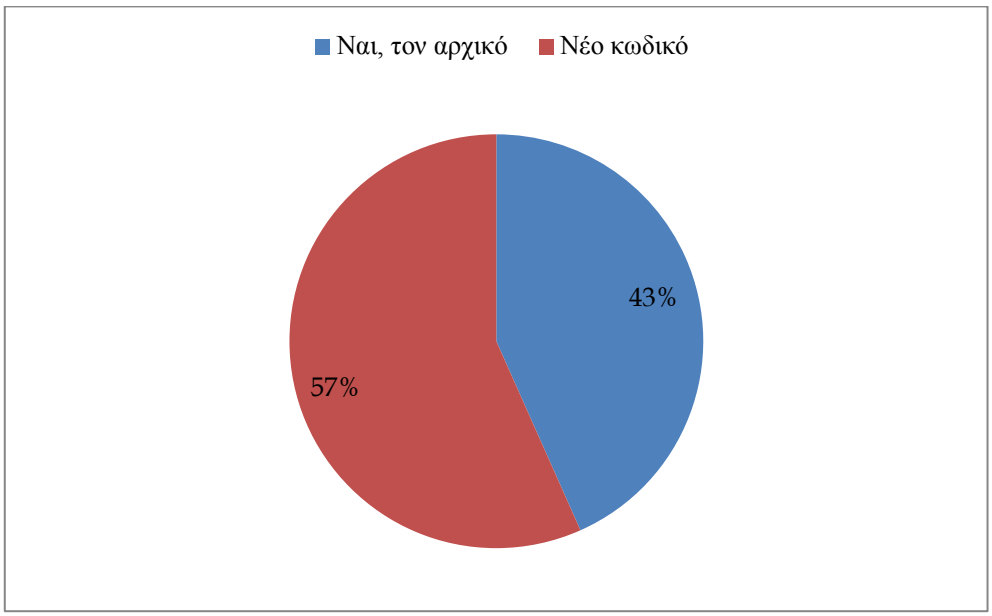
**Ερώτημα 12:** Η χρήση του εκάστοτε κωδικού, σας φάνηκε ενοχλητική;




**Γράφημα 5.21:** Αποτελέσματα ερωτήματος 12.

Οι μέθοδοι όπου ο κωδικός δεν έχει αριθμούς και ειδικούς χαρακτήρες δεν φαίνεται να ενόχλησε ιδιαίτερα τους χρήστες σε αντίθεση με τις υπόλοιπες. Ο συνδυασμός λέξεων φαίνεται να είναι η μέθοδος που ενόχλησε το λιγότερο αφού τα 2/3 των χρηστών διαφώνησαν.

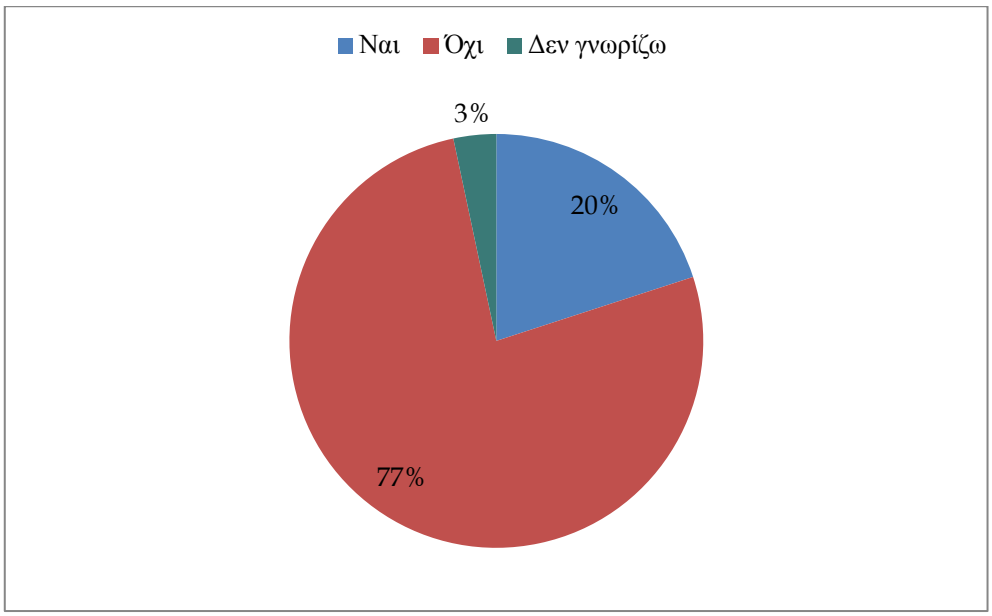
**Ερώτημα 13:** Θα θέλατε να έχετε τον αρχικό σας κωδικό ή νέο αλλά όχι τόσο δύσκολο;




**Γράφημα 5.22:** Αποτελέσματα ερωτήματος 13.

Ποσοστό λίγο πιο πάνω από τους μισούς χρήστες επέλεξε να έχει νέο κωδικό, υποθέτοντας ότι με χρήση κωδικών από τις μεθόδους μας αισθάνονται πιο ασφαλής από πριν.

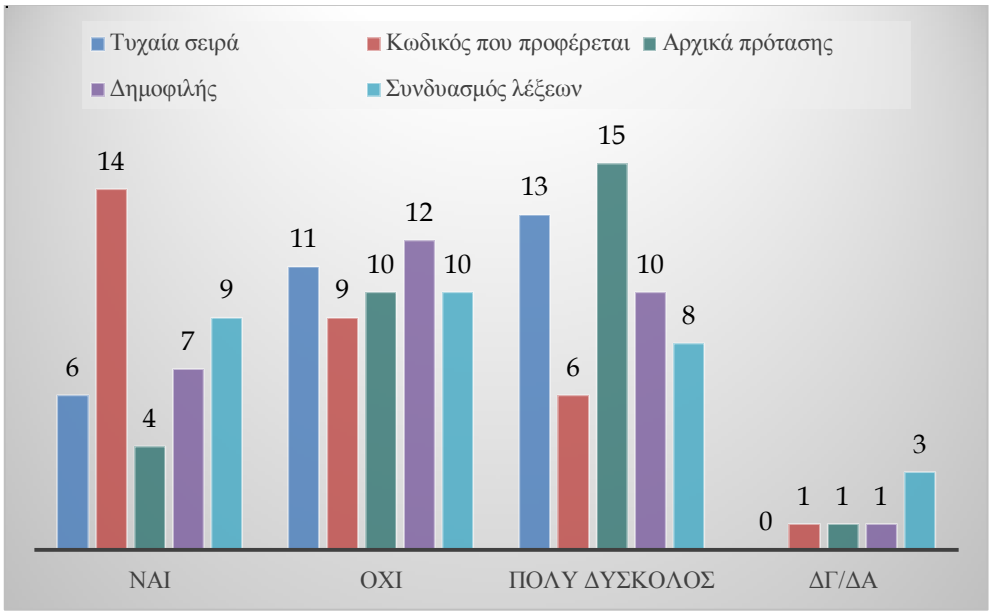
**Ερώτημα 14:** Είχατε ποτέ καθοδήγηση για τη δημιουργία ενός ασφαλούς κωδικού;




**Γράφημα 5.23:** Αποτελέσματα ερωτήματος 14.

Εδώ παρατηρούμε ότι ένα ποσοστό της τάξης του 77% δεν είχε καθοδήγηση για ασφαλή κωδικό και αυτό μπορεί να έχει επιπτώσεις εάν το άτομο διαχειρίζεται κρίσιμες και σημαντικές πληροφορίες.

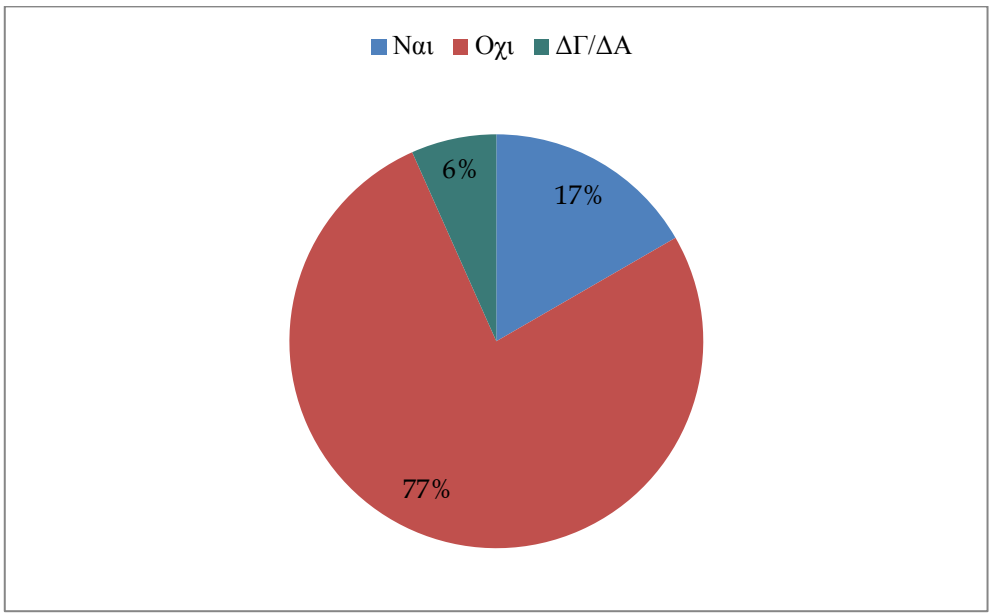
**Ερώτημα 15:** Ο εκάστοτε κωδικός που σας δόθηκε, είναι κοντά στο δικό σας τρόπο σκέψης και επιλογής ενός ασφαλούς κωδικού;




**Γράφημα 5.24:** Αποτελέσματα ερωτήματος 15.

Οι περισσότεροι έδωσαν αρνητική απάντηση εδώ γιατί οι κωδικοί που δόθηκαν ήταν κάπως πρωτόγνωροι γι' αυτούς. Ο κωδικός που προφέρεται ήταν η πιο θετική απάντηση που πήραμε (συγκεκριμένα, συνάδελφος είχε σαν κωδικό το πρώτο μισό από τα παιδιά του.)

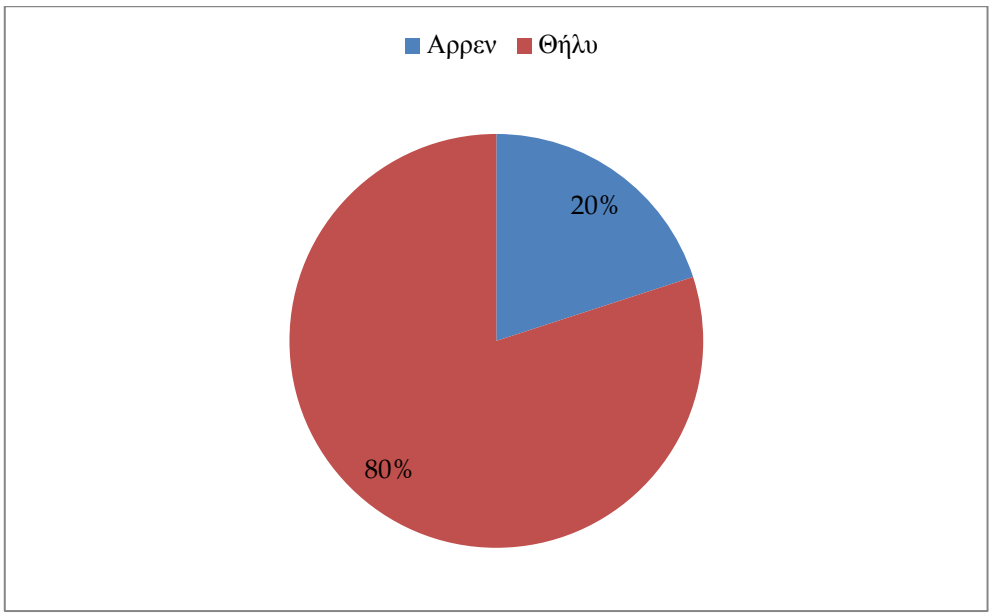
**Ερώτημα 16:** Έτυχε ποτέ να σας παραβιάσουν κάποιο προσωπικό κωδικό / λογαριασμό;




**Γράφημα 5.25:** Αποτελέσματα ερωτήματος 16.

Παρά τους εύκολους κωδικούς που υποθέτουμε ότι έχουν οι χρήστες, αρκετοί δήλωσαν ότι δεν τους είχαν παραβιάσει κάποιο λογαριασμό ενώ πολύ λίγοι ήταν αυτοί που απάντησαν θετικά.

**Ερώτημα 17:** Δηλώστε το φύλο σας.




**Γράφημα 5.26:** Αποτελέσματα ερωτήματος 17.

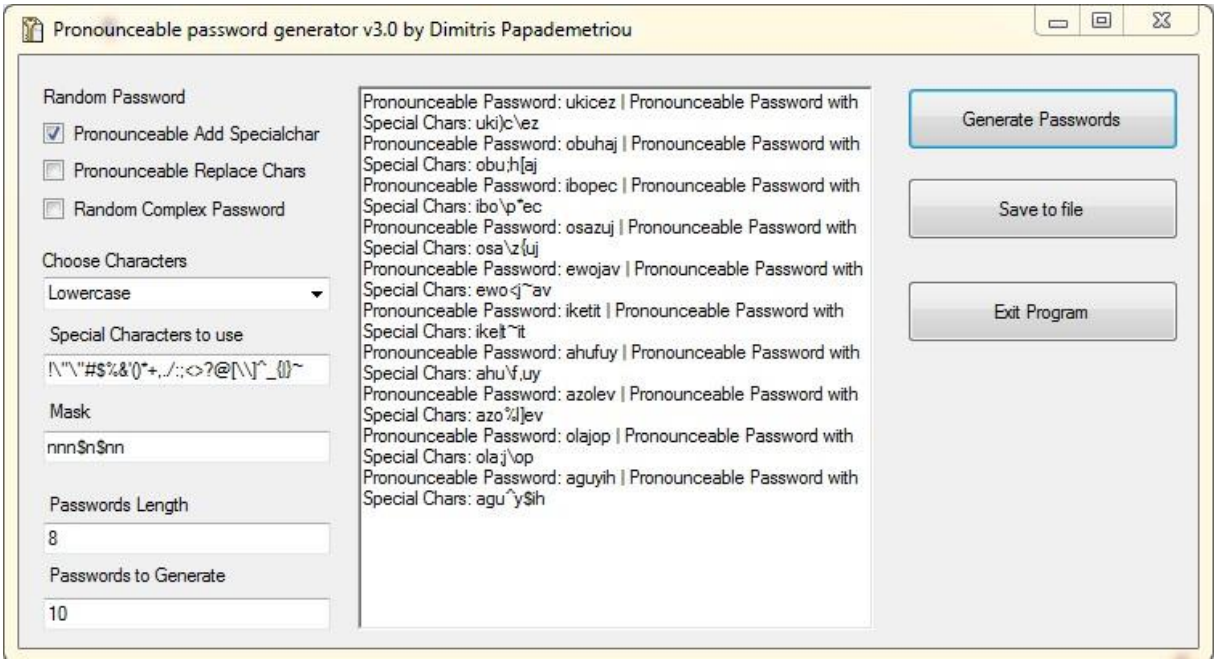
Το ποσοστό που αναλογεί στους χρήστες μας ανά φύλο.

Οι απαντήσεις που συλλέξαμε στα 2 ερωτηματολόγια μας δίνουν μια ξεκάθαρη εικόνα όσον αφορά τη συνήθεια να χρησιμοποιούν όσο πιο απλούς και εύκολους κωδικούς γίνεται για τη δική τους ευκολία. Έτσι αγνοούν τους κινδύνους παραβίασης του λογαριασμού τους και κατ' επέκταση διείσδυση σε περισσότερους Η/Υ και μηχανήματα στο εταιρικό δίκτυο. Η χρήση αριθμών και ειδικών χαρακτήρων φαίνεται να προκαλεί σύγχυση όταν πρέπει να χρησιμοποιηθούν πλην της περίπτωσης όπου οι αριθμοί ακολουθούν αυξητική σειρά, για παράδειγμα κωδικός1, κωδικός2 κτλ. Οι ερωτήσεις 1 και 2 του προσωπικού ερωτηματολογίου μας δίνουν μια ξεκάθαρη εικόνα της επαναχρησιμοποίησης των κωδικών έστω και αν προβαίνουν σε μικροαλλαγές, που αυτό μεταφράζεται στο γεγονός ο κυβερνοεγκληματίας να πετύχει πρόσβαση σχεδόν σε όλους τους λογαριασμούς του χρήστη μόλις αποκτήσει ένα κωδικό του. Αιτία που συμβάλει σε αυτό είναι η έλλειψη καθοδήγησης του χρήστη ώστε να δημιουργεί και να χρησιμοποιεί ισχυρούς κωδικούς. Αναλύοντας τα αποτελέσματα των ερωτήσεων 4 και 6 από το τελικό ερωτηματολόγιο, συμπεραίνουμε ότι σε προσωπικό επίπεδο οι χρήστες προτιμούν και αποδέχονται να έχουν δύσκολο κωδικό (χρήση αριθμών και ειδικών χαρακτήρων σε τυχαία σειρά) αλλά τους φαντάζει αρκετά ενοχλητικό στο να τον χρησιμοποιούν σε καθημερινή βάση. Η γενική ιδέα που αποκομίσαμε από τα ερωτηματολόγια είναι πως όσο πιο απλός ο κωδικός τόσο το καλύτερο για να τον απομνημονεύσει ο χρήστης, σε διαφορετική περίπτωση θα δυσκολευτεί.

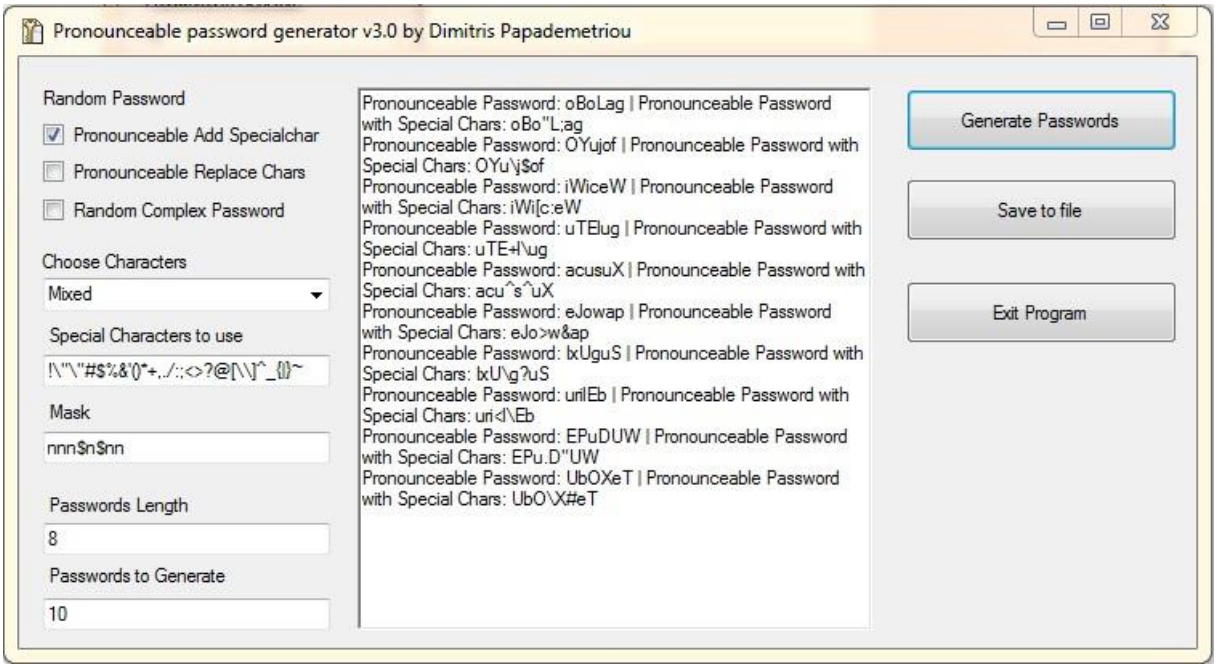
## 5.2 Δημιουργία Προγράμματος Παραγωγής Κωδικών

Αναλύοντας τα αποτελέσματα και την ανατροφοδότηση που πήραμε από τους χρήστες, καταλήξαμε ότι η μέθοδος η οποία είχε τη πιο θετική επιρροή ήταν ο κωδικός που προφέρεται. Ενθαρρυντικά ήταν τα αποτελέσματα της συγκεκριμένης μεθόδου αφού σε σύντομο χρονικό διάστημα καταφέραμε να τους αλλάξουμε τρόπο σκέψης καθώς επίσης παρατηρήθηκε το γεγονός όταν ο κωδικός τους φαινότανε αστείος, ο χρήστης μπορούσε να τον απομνημονεύσει πολύ πιο εύκολα και είχε περισσότερη αποδοχή σε σχέση με κωδικούς που δόθηκαν σε άλλους χρήστες. Παράδειγμα τέτοιων αστείων κωδικών είναι: iFUTaLAL, TutIfiBi, YeYUkENi, LonaTEWE και XIRAtoYi.

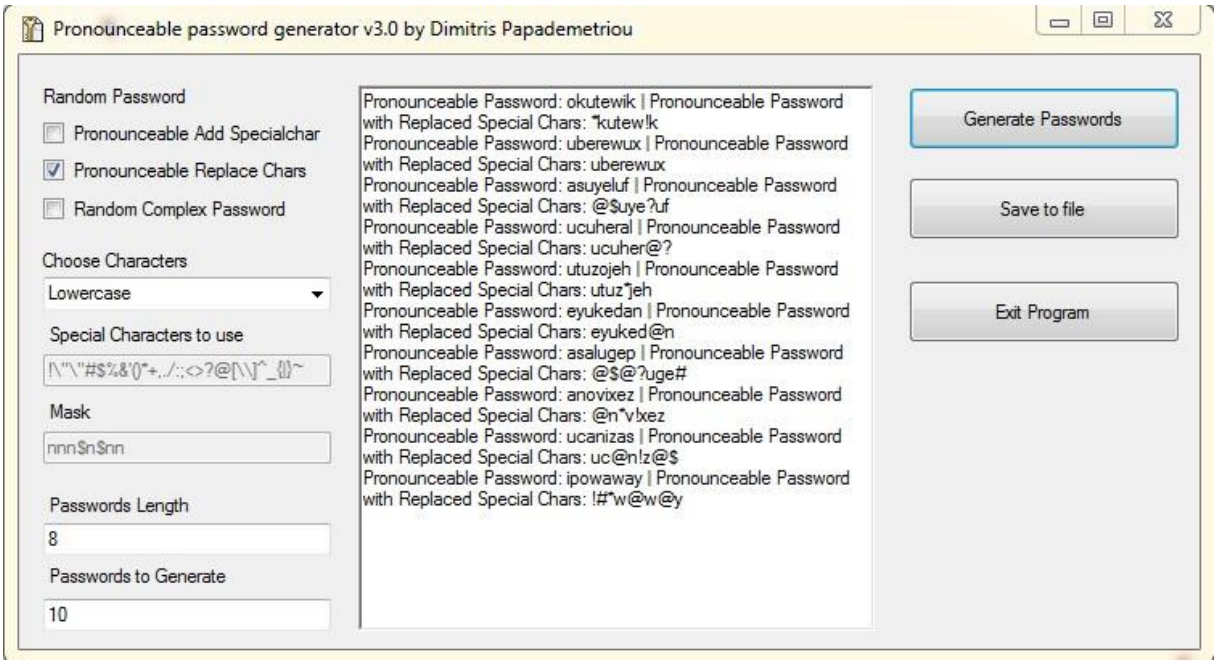
Στηριζόμενοι στα pronounceable passwords, προχωρήσαμε στη δημιουργία ενός προγράμματος που παράγει τέτοιους κωδικούς. Το πρόγραμμα σου δίνει την δυνατότητα να επιλέξεις δύο τύπους pronounceable password και αντίστοιχα τρείς επιλογές για τον κάθε τύπο που είναι πεζά (Lowercase), κεφαλαία (Uppercase) και ανάμεικτα (Lowercase και Uppercase) γράμματα. Στις εικόνες που ακολουθούν φαίνεται η παραγωγή κωδικών 8 χαρακτήρων pronounceable τόσο με χρήση μόνο πεζών γραμμάτων όσο και με χρήση πεζών και κεφαλαίων.



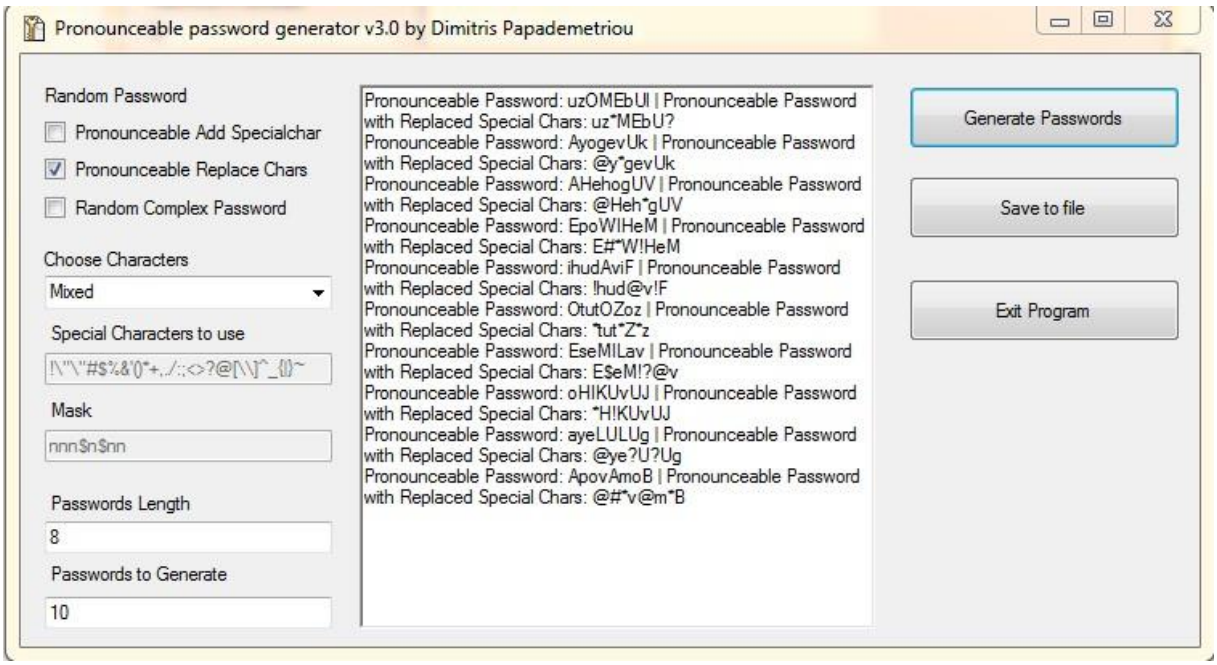

**Εικόνα 5.1:** Παραγωγή pronounceable κωδικών με προσθήκη ειδικών χαρακτήρων σε καθορισμένες θέσεις και χρήση πεζών γραμμάτων μόνο.




**Εικόνα 5.2:** Παραγωγή pronounceable κωδικών με προσθήκη ειδικών χαρακτήρων σε καθορισμένες θέσεις και χρήση πεζών και κεφαλαίων γραμμάτων.




**Εικόνα 5.3:** Παραγωγή pronounceable κωδικών με αντικατάσταση χαρακτήρων και χρήση πεζών γραμμάτων μόνο.




**Εικόνα 5.4:** Παραγωγή pronounceable κωδικών με αντικατάσταση χαρακτήρων και χρήση πεζών και κεφαλαίων γραμμάτων.

Το συγκεκριμένο πρόγραμμα ζητήθηκε από αρκετούς χρήστες που πήραν μέρος στην έρευνα (περίπου 85%) και τους δόθηκε να το αξιοποιήσουν για ιδιωτική χρήση στους προσωπικούς τους λογαριασμούς.

# Κεφάλαιο 6
# Επίλογος

Στη παρούσα μελέτη μελετήσαμε θέματα που αφορούν την ασφάλεια των χρηστών και πιο συγκεκριμένα τους κωδικούς πρόσβασης τους με κύριο άξονα τους χρήστες που υπάγονται σε εταιρικά περιβάλλοντα. Παρά τα μέτρα ασφαλείας που χρησιμοποιούν πολλές εταιρείες, η κακή ενημέρωση των χρηστών και ο λάθος τρόπος αντιμετώπισης, τους οδηγούν να χρησιμοποιούν κωδικούς που είναι πολύ εύκολα να βρεθούν μηδενίζοντας και τα πιο ακριβά συστήματα περιμετρικής ασφάλειας. Επίσης η ύπαρξη ίδιων κωδικών σε πολλούς λογαριασμούς θέτει σε μεγαλύτερο κίνδυνο τους χρήστες. Η χρήση διαφόρων προγραμμάτων ανάκτησης και εύρεσης κωδικών βοηθούν τους διαχειριστές συστημάτων για καλύτερο έλεγχο του επιπέδου ασφαλείας κωδικών στα συστήματα και τα μηχανήματα που επιτηρούν, όπως επίσης και για ανίχνευση αδύναμων κωδικών χρηστών. Με τη ίδια ευκολία όμως, αυτά τα προγράμματα μπορούν να αξιοποιηθούν και από κυβερνοεγκληματίες και να ανακτήσουν κρυπτογραφημένους και μη κωδικούς.

Πρωταρχικός στόχος της μελέτης ήταν η διερεύνηση των αδυναμιών που διακρίνουν τους χρήστες στη διαχείριση και δημιουργία ισχυρών κωδικών με βάση τη σχετική βιβλιογραφία. Η διενέργεια των πέντε (5) τεστ είχε σαν σκοπό να μελετήσει από κοντά τις αντιδράσεις των χρηστών που ανήκουν σε εταιρικό περιβάλλον όταν θα τους δίνεται ένας πολύπλοκος κωδικός,

με στόχο τη ανάδειξη της καλύτερης και πιο προσιτής μεθόδου. Όπως φάνηκε από τα αποτελέσματα, οι χρήστες αντιμετώπισαν δυσκολίες καθ' όλη τη διάρκεια, κυρίως με τη μέθοδο πολύπλοκων κωδικών (complex passwords) που περιείχε αριθμούς και ειδικούς χαρακτήρες σε εντελώς τυχαία σειρά. Σε κάθε περίπτωση, ανάλογα με τη προτίμηση του χρήστη, γινόταν υπενθύμιση ή επανακαθορισμός του κωδικού. Οι χρήστες, μετά την ολοκλήρωση των πειραμάτων, έδειξαν σημάδια ευαισθητοποίησης όσον αφορά θέματα ασφαλείας, στο προσωπικό και εργασιακό τους περιβάλλον, καθώς επίσης ήταν σε θέση να δημιουργήσουν πλέον ισχυρούς κωδικούς και να τους εφαρμόσουν σε προσωπικά ηλεκτρονικά ταχυδρομεία και λογαριασμούς που διατηρούσαν σε ιστοσελίδες κοινωνικής δικτύωσης.

Η μελέτη είχε μεγάλο αντίκτυπο για τη εσωτερική πολιτική ασφαλείας της εταιρείας. Τα αποτελέσματα αφού κρίθηκαν ως ικανοποιητικά και αποδεκτά από το διοικητικό συμβούλιο, αποφασίστηκε η καθολική εφαρμογή του pronounceable κωδικού με αντικατάσταση χαρακτήρων όπως φαίνεται στην εικόνα 5.4.

## 6.1 Μελλοντική Δουλειά

Κατά τη διάρκεια εκπλήρωσης της διατριβής και πιο συγκεκριμένα των τεστ, πήραμε αρκετές απαντήσεις αλλά ταυτόχρονα δημιουργήθηκαν νέες ερωτήσεις. Για παράδειγμα, αναρωτηθήκαμε για ποιο λόγο οι χρήστες δεν ήταν ικανοί να προτείνουν οι ίδιοι ένα κωδικό της αρεσκείας τους για τα τεστ κωδικός από πρόταση και κωδικός από δημοφιλή φράση. Τι είναι αυτό που τους αποτρέπει - δυσκολεύει ώστε να δημιουργήσουν ένα κωδικό από μια φράση, χρησιμοποιώντας προτάσεις από τη καθημερινότητά τους, αριθμούς και ειδικούς χαρακτήρες; Γιατί μπέρδευαν τα πεζά με τα κεφαλαία γράμματα στα τεστ κωδικός που προφέρεται εύκολα και συνδυασμός λέξεων; Αυτά τα δυο ερωτήματα χρήζουν περαιτέρω μελέτης για να βρεθεί η βέλτιστη λύση στο πρόβλημα και μέσω αυτού, οι χρήστες να γίνουν πιο ικανοί στη δημιουργία ισχυρών κωδικών.

Η τελική μας πρόταση έχει δύο (2) παραλλαγές της μεθόδου «κωδικός που προφέρεται εύκολα» (pronounceable password). Η μια παραλλαγή περιλαμβάνει προσθήκη σε προκαθορισμένη θέση ειδικών χαρακτήρων ενώ η δεύτερη περιλαμβάνει αντικατάσταση γραμμάτων με σύμβολα ή αριθμούς. Για παράδειγμα το γράμμα Α ή a με το @, το γράμμα Ε ή e με το 3 συμβάλλοντας έτσι στη αύξηση της ασφάλειας των κωδικών και θέτοντας το πήχη της προστασίας προσωπικών δεδομένων ακόμη πιο ψηλά.

Μελλοντική δουλεία θα ήτανε να δοκιμάσουμε τις δύο (2) αυτές μεθόδους που προτείναμε με μήκος κωδικών μεγαλύτερων των οκτώ (8) χαρακτήρων που προτείνει η βιβλιογραφία και να δούμε πώς συμπεριφέρονται οι ηλικίες καθώς και το φύλο των ατόμων που παίρνουν μέρος στα πειράματα. Επίσης το δείγμα των ατόμων θα ήτανε καλύτερο να είναι σε μεγαλύτερο βαθμό (πχ 60 άτομα ομοιόμορφα χωρισμένα ανά φύλο και ηλικία) και να μπορέσουμε να χρησιμοποιήσουμε τρείς (3) ή περισσότερες διαφορετικές εταιρίες, με διαφορετικό τομέα απασχόλησης. Τέλος η προσθήκη κινήτρων θα ήτανε ένα ακόμη πιθανό σενάριο που μπορεί να προστεθεί σε αυτά τα πειράματα.

# Βιβλιογραφία


[01] Ablon, L., Libicki, M.C. and Golay, A.A. 2014, Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar, Rand Corporation.

[02] Aldeid Security 2013, November 23, 2013-last update, Medusa Wiki. Available: http://www.aldeid.com/wiki/Medusa [2015, February, 21].

[03] Christian Thöing 2015, PWGen for Windows - Generator of cryptographically-strong passwords, 2.5.4 edn, SourceForge.

[04] Computer Hope 2015, 2015-last update, Brute-force attack. Available: http://www.computerhope.com/jargon/b/brutforc.htm [2015, February, 24].

[05] Dudhade, S. 2013, 2013-last update, Wfuzz - Web application bruteforcer. Available: http://santoshdudhade.blogspot.com/2012/05/wfuzz-web-application-bruteforcer.html [2015, February, 23].

[06] Florêncio, D., Herley, C. and Coskun, B. 2007, "Do strong web passwords accomplish anything?", HotSec, vol. 7, pp. 6.

[07] Foofus 2012, Medusa Parallel Network Login Auditor, 2.1.1 edn, Foofus.

[08] Gordon, W. 2014, October 09, 2014-last update, 5 Million Online Passwords Leaked, Check Yours. Available: http://lifehacker.com/5-million-gmail-passwords-leaked-check-yours-now-1632983265 [2015, February, 20].

[09] Graham Cluley 2012, August 02, 2015-last update, Outlook webmail passwords restricted to 16 chars - how does that compare with Yahoo and Gmail?. Available: https://nakedsecurity.sophos.com/2012/08/02/maximum-password-length-outlook-yahoo-gmail-compared/ [2015, March 24, 2015].

[10] Helkala, K. and Hoddø Bakås, T. 2014, "Extended results of Norwegian password security survey", Information Management and Computer Security, vol. 22, no. 4, pp. 346-357.

[11] Inside-Logger.com 2010, Inside Keylogger , 4.7th edn, Inside-Logger.com.

[12] Janssen, C. -, --last update, Dictionary Attack. Available: http://www.techopedia.com/definition/1774/dictionary-attack [2015, February, 23].

[13] Keelog.com 2015, February 25, 2015-last update, KeyGrabber Hardware Keylogger. Available: https://www.keelog.com/wireless_keylogger.html [2015, February, 24].

[14] Kelsey, J., Schneier, B., Wagner, D. and Hall, C. 1998, "Cryptanalytic attacks on pseudorandom number generators", Fast Software EncryptionSpringer, , pp. 168.

[15] Klosowski, T. 2015, January 30, 2015-last update, The Best Password Managers, Compared. Available: http://lifehacker.com/lifehacker-faceoff-the-best-password-managers-compare-1682443320 [2015, February, 24].

[16] Kottke, J. 2012, June 04, 2012-last update, The world's worst password requirements list. Available: http://kottke.org/12/06/the-worlds-worst-password-requirements-list [2015, February, 24].

[17] Kuliukas, K. 2006, December 11, 2006-last update, How Rainbow tables work. Available: http://kestas.kuliukas.com/RainbowTables/ [2015, February, 24].

[18] Kuo, C., Romanosky, S. and Cranor, L.F. 2006, "Human selection of mnemonic phrase-based passwords", Proceedings of the second symposium on Usable privacy and securityACM, , pp. 67.

[19] L0pht Holdings, L. 2009, L0phtcrack Password Auditing and Recovery, 6th edn, L0phtcrack.

[20] Lampe, J. 2014, January 6, 2014-last update, Beyond Password Length and Complexity. Available: http://resources.infosecinstitute.com/beyond-password-length-complexity/ [2015, February, 24].

[21] Li, Z., He, W., Akhawe, D. and Song, D. 2014, "The Emperor's new password manager: Security analysis of web-based password managers", 23rd USENIX Security Symposium (USENIX Security 14).

[22] Manasa, C. "Password Authentication using Click based Graphical passwords and Color-Login".

[23] Mihailowitsch, F. 2010, Detecting Hardware Keyloggers, Hack.lu.

[24] Miller, G.A. 1956, "The magical number seven, plus or minus two: some limits on our capacity for processing information.", Psychological review, vol. 63, no. 2, pp. 81.

[25] Openwall 30 May 2013, John the Ripper password cracker , 1.8.0 edn, Openwall.

[26] Oxid.it 2014, Cain and Abel, 4.5.96 edn, Oxid.it.

[27] Saita, A. 2013, May 29, 2013-last update, Drupal.org Resets Passwords After Data Breach. Available: http://threatpost.com/drupal-org-resets-passwords-after-data-breach/100816 [2015, February, 20].

[28] Schneier, B. 2014, March 3, 2014-last update, Choosing Secure Password. Available: https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html [2015, February 19].

[29] Schneier, B. 2005, June 17, 2005-last update, Write down your password. Available: https://www.schneier.com/blog/archives/2005/06/write_down_your.html [2015, February 19].

[30] Schweitzer, D., Boleng, J., Hughes, C. and Murphy, L. 2009, "Visualizing keyboard pattern passwords", Visualization for Cyber Security, 2009. VizSec 2009. 6th International Workshop onIEEE, , pp. 69.

[31] Security Training Share 2013, October 15, 2013-last update, What is a hybrid attack?. Available: https://www.facebook.com/haking.cracking.tutorial/posts/649808981716275 [2015, February, 24].

[32] Spencer, W. 2011, January 3, 2011-last update, Cajun Slang Words and Phrases. Available: http://www.tech-faq.com/cajun-slang.html [2015, February, 24].

[33] thc.org 2015, May 2012-last update, Comparison of features and Services Coverage. Available: https://www.thc.org/thc-hydra/network_password_cracker_comparison.html [2015, February, 23].

[34] Tomes, T. 2011, February 28, 2011-last update, Creating Complex Password lists with John the Ripper. Available: http://www.lanmaster53.com/2011/02/creating-complex-password-lists-with-john-the-ripper/ [2015, February, 20].

[35] Tony Bradley 2015, 2015-last update, Introduction to Packet Sniffing [Homepage of About.com], [Online]. Available: http://netsecurity.about.com/cs/hackertools/a/aa121403.htm [2015, March 24, 2015].

[36] van Hauser 2014, THC-Hydra , 8.1st edn, Github.

[37] W3Schools 2015, 2015-last update, HTTP Methods: GET vs. POST. Available: http://www.w3schools.com/tags/ref_httpmethods.asp [2015, February, 23].

[38] Weir, M. 2009, December 19, 2009-last update, The RockYou 32 Million Password List Top 100. Available: http://reusablesec.blogspot.com/2009/12/rockyou-32-million-password-list-top.html [2015, February 19].

[39] Weiss, R. and De Luca, A. 2008, "PassShapes: utilizing stroke based authentication to increase password memorability", Proceedings of the 5th Nordic conference on Human-computer interaction: building bridgesACM, , pp. 383.

[40] Williams, O. 2014, October 14, 2014-last update, Hundreds of Dropbox passwords leaked online. Available: http://thenextweb.com/apps/2014/10/14/dropbox-passwords-leak-online-alleged-hack/> [2015, February, 20].

[41] Xavier Mendez 2015, Wfuzz – The Web Application Bruteforcer, 2.1.3 edn, Github.

[42] Yan, J. 2004, "Password memorability and security: Empirical results", IEEE Security and privacy, , no. 5, pp. 25-31.

[43] Yibico 2015, 2015-last update, Yubikey standard and Nano. Available: https://www.yubico.com/products/yubikey-hardware/yubikey-2/ [2015, February, 24]

# Παραρτήματα

## Α-1 Προσωπικό ερωτηματολόγιο

**Παρακαλώ σημειώστε αυτό που ισχύει σε κάθε περίπτωση.**

1. Έχετε κωδικό ή κωδικούς που τους χρησιμοποιείτε **σε περισσότερες από μια περιπτώσεις;**

    1. Ναι

    2. Όχι

    3. Προτιμώ να μην αναφέρω

2. Έχετε κάποιο κωδικό που χρησιμοποιείτε σε περισσότερες από μια περιπτώσεις **κάνοντας μικροαλλαγές κάθε φορά**;

    1. Ναι

    2. Όχι

3. Προτιμώ να μην αναφέρω

3. Κάθε πόσο αλλάζετε κάποιο προσωπικό σας κωδικό;

    1. Μια φορά το δίμηνο
    2. Μια φορά το τρίμηνο
    3. Μια φορά το εξάμηνο
    4. Μια φορά το χρόνο
    5. Ποτέ
    6. Δεν γνωρίζω
    7. Προτιμώ να μην αναφέρω

Οι ερωτήσεις 4 έως 8 αφορούν τη χρήση κωδικού στο προσωπικό σας email.

4. Στη περίπτωση του κωδικού για προσωπικό email, ο παροχέας σας ζητάει να αλλάζετε το κωδικό σας σε τακτά διαστήματα;

    1. Ναι
    2. Όχι
    3. Δεν γνωρίζω
    4. Προτιμώ να μην αναφέρω

5. Όταν πρέπει να χρησιμοποιήσετε ένα κωδικό, τι κάνετε για **να τον θυμάστε**;

    1. Τον απομνημονεύω καλά
    2. Τον έχω αποθηκευμένο στον περιηγητή μου

3. Κάνω αντιγραφή και επικόλληση από ένα αρχείο κειμένου
4. Κοιτάζω το χαρτάκι όπου τον έχω αναγράψει
5. Χρησιμοποιώ λογισμικό απομνημόνευσης κωδικών
6. Προτιμώ να μην αναφέρω

6. Εάν είχατε γραμμένο κάπου το κωδικό σας, πώς τον προστατεύσατε;
    1. Δεν τον προστατεύω καθόλου
    2. Ήταν κρυμμένος
    3. Ήταν γραμμένος στο κινητό μου
    4. Κλείδωσα το χαρτάκι σε ένα συρτάρι
    5. Τον είχα πάντα μαζί μου (πορτοφόλι/τσάντα)
    6. Έγραψα κάτι άλλο για να μου το θυμίζει
    7. Δεν τον αναγράφω πότε
7. Συνδυάσατε το κωδικό σας με κάποια φράση ώστε να τον θυμάστε;
    1. Ναι
    2. Όχι
8. Πόσο συχνά πληκτρολογείτε το κωδικό σας;
    1. Μερικές φορές τη μέρα
    2. Μια φορά τη μέρα
    3. Μερικές φορές την εβδομάδα

4. Μια φορά την εβδομάδα

5. Μερικές φορές το μήνα

9. Όταν θέλετε να δημιουργήσετε ένα καινούργιο κωδικό, με ποιο σκεπτικό το κάνετε;

    1. Σκέφτομαι μια εικόνα

    2. Συνδυάζω ημερομηνίες με ονόματα

    3. Συνδυάζω χρώματα με αγαπημένα πρόσωπα

    4. Συνδυάζω λέξεις

    5. Συνδυάζω φρούτα με χρώματα

    6. Βάζω ένα αφηρημένο κωδικό αλλά το γράφω σε ένα χαρτί

10. Συμπληρώστε τους αντίστοιχους ελληνικούς και αγγλικούς στίχους των τραγουδιών.

| | |
|---|---|
| Σε είχα ερωτευτεί πολύ μαζί σου είχα _____ μα ξαφνικά μου λες εγώ πως θέλεις να σε παντρευτώ | i. Φίλους<br>ii. Παίζεις<br>iii. Αγάπη<br>iv. Μέλλον<br>v. Φοράει<br>vi. Τρελαθεί<br>vii. Μαύρα |
| _____ είναι να λες στον άλλον όπως είσαι μείνε και όχι να του λες για μένα γίνε ρούχο δανεικό | |
| Και σου γράφω τραγούδια σου στέλνω λουλούδια με σπρέι στους τοίχους καρδιές ζωγραφίζω για σένα τους _____ συνέχεια ζαλίζω | |
| Κι η μουσική το σώμα της διαπερνάει και προκαλεί όλους μ' αυτά που _____ οπλοφορεί κι άμα της αντισταθείς πυροβολεί εξ' επαφής | |
| Τελευταία πράξη _____ πράξη πιο δραματική και μου υπόσχεσαι πως θα 'χω ρόλο πρωταγωνιστή | |
| Είναι τα βράδια μου μακριά σου πιο μαύρα απ' τα μαλλιά σου τα _____ σου μαλλιά είσαι δροσούλα στα όνειρά μου φωτιά μες την καρδιά μου κι ο κόσμος μια σταλιά | |
| Θα του λέει λόγια αγάπης που πε σ' εμένα μα δεν ξέρει το _____τι της φυλάει.. για ψεύτικα φιλιά και προδωμένα σ' αγαπώ προτίμησε αυτόν και ας πάω εγώ να τρελαθώ.. | |

| | |
|---|---|
| Ακόμα κι αν με _____ να σε βρω μέσα από χιλιάδες ακόμα κι αν γίνουν τα όνειρά μου φρικτοί εφιάλτες θα σ' αγαπάω, εγώ θα σ' αγαπάω | i. Αντισταθεί<br>ii. Φτάνει<br>iii. Ψευδαίσθηση<br>iv. Τελειώσαμε<br>v. Δυνατή<br>vi. Προδόθηκα<br>vii. Πληγώσεις<br>viii. Καρδιά<br>ix. Βάλουν<br>x. Ερωτευμένη<br>xi. Κλείνομαι<br>xii. Νοιάζομαι |
| Μα δεν τελειώσαμε δε γίνεται σου λέω, δεν _____ το χρόνο απλά για λίγο τον παγώσαμε αυτό θυμάμαι, αυτό είπες πριν χαθείς | |
| Τρελή καρδιά που δεν μπορεί σε αμαρτίες ν' _____ και ψάχνεται μες στον βοριά και στα δίχτυα του έρωτα | |
| Κράτα τα μάτια σου κλειστά, τρέμει το σώμα κι η καρδιά δε _____ μόνο μια φορά, κράτα τα μάτια σου κλειστά | |
| Έλεγα πως το φεγγάρι μου'χε κάνει πια τη χάρη και μου έδειξε επιτέλους έναν από τους αγγέλους μα ήσουν μια _____ κι εσύ που έμοιαζες με άγγελο κι ήσουν καταστροφή | |
| Παραμυθιάζομαι, ξέρω πολύ καλά τι θα συμβεί Κι ούτε που_____ , θέλω μαζί να μας βρει το πρωί Παραμυθιάζομαι, μιας νύχτας όνειρα εγώ κι εσύ | |
| Με έχεις τρελάνει κι όμως σε θέλω επειγόντως είναι η αγάπη μου για σένα _____ Μ έχεις τρελάνει κι όμως άγραφος είσαι νόμος με εξουσιάζεις και μ' αφήνεις στη στιγμή | |
| Παραλίγο να σ' ερωτευτώ, μα σώθηκα, λίγο πριν μαζί σου τρελαθώ, _____ , παραλίγο να σ' ερωτευτώ, Θεέ μου, πόσο θα 'θελα ένα ψέμα να σου πω. | |
| Έχω πετάξει μαζί σου σε κάθε φιλί σου, σε κάθε σου λέξη, σ' αγαπώ μη με _____ θυμήσου πως ήμουν μαζί σου και τώρα μονάχος μου ζω. | |
| Έχεις φύγει κι έχεις φέρει, συννεφιά και τρικυμία δεν τη θέλω τη ζωή μου, να τη ζω χωρίς ουσία με τη σκέψη πως σε χάνω, καίγομαι, στην τρέλα φτάνω _____στον εαυτό μου, και δε σκέφτομαι τι κάνω | |
| Νιώσε την καρδιά φωνάζει σ' αγαπώ και λέει ψιθυριστά, για σένα είμαι εδώ. Νιώσε την _____και έλα πιο κοντά. Δεν ένιωσα ποτέ, ποτέ πιο δυνατά. | |
| Αλυσίδα στην καρδιά μου περασμένη Αλυσίδα μου τρελά _____ Να σε σπάσει πια κανένας δεν μπορεί Με 'χεις δέσει για μια ολόκληρη ζωή... | |

| | |
|---|---|
| Μες στο μυαλό γυρνάς, όλο εκεί τριγυρνάς συνέχεια κάτι γυρεύεις, συνέχεια κάτι ζητάς μες στο δωμάτιο_____ , εκεί περπατάς καθώς τα ρούχα σου ψάχνεις, γυρνάς, μου χαμογελάς τι κάνουμε με ρωτάς, σου απαντώ ότι θες λιγάκι αδιαφορώ, γιατί σε είχα και χθες | i. Σώματα<br>ii. Καρδιά<br>iii. Φίλησέ<br>iv. Άχρηστα<br>v. Ανέμελη<br>vi. Κανένας<br>vii. Χρόνος<br>viii. Κοσμήματα<br>ix. Ακολουθώ<br>x. Ταιριάζετε |
| Τίποτα δε θα ‘πρεπε να θες, οι ζωές μας διαφορετικές όμως όταν με κοιτάς, πάω όπου με πας Τίποτα δε φαίνεται σωστό, όμως την καρδιά μου _____ φίλα με, μη σταματάς, πάω όπου με πας | |
| Δεν _____ σου λέω τόσο αντικειμενικά στο λέω και άσε τις φίλες σου να λένε το αντίθετο, ξέρεις μάτια μου που μένω και όσο δίνεσαι θα περιμένω από αντίδραση το ξέρω το έκανες και αυτό. | |
| Άσε με πάλι να ρωτώ ο _____ τι θα φέρει ο ήλιος και ο κεραυνός μου στήσανε καρτέρι | |
| Δεν άξιζα, μου λες δεν άξιζες, θα πω οι λέξεις μας στα _____ χτυπάνε Να μάθεις ν’ αγαπάς Να μάθω ν’ αγαπώ Να ξέραμε τα λόγια να μετράμε | |
| Έτσι νομίζεις, γιατί έτσι δανείζεις το άδειο σου σώμα, _____ σε όλους τα ίδια σκορπάς αντικλείδια κι αλλάζεις απλά κλειδαριά | |
| Κάνε μια στροφή, κοίταξέ με, δίπλα σου περνώ μια ζωή. Δίπλα σου από πάρτι σε πάρτι, δίπλα σου να λιώνω από αγάπη. Πιάσε το ρυθμό και _____με στη στροφή. | |
| Όλα μου φαίνονται _____όταν μ’ εγκαταλείπεις και γίνομαι στη μοναξιά ένα παιδί της λύπης | |
| Μα εκείνη θέλει ακριβά ρούχα, αμάξια και____, ξέρεις δεν έχω τίποτα απ’ αυτά, κι’ έχω πάθει ζημιά | |
| Ώρες ώρες κι εγώ απορώ με τι μοιάζω Είμαι τόσο ψυχρός που ο ίδιος τρομάζω Και _____ αυτό δεν μπορεί να το νιώσει Μόνο εσύ το μπορείς που με έχεις σκοτώσει | |

| | |
|---|---|
| Upside, _____ out she's living la vida loca She'll push and pull you down, living la vida loca Her lips are devil red and her skin's the color mocha She will wear you out living la vida loca Come On! | i. Came<br>ii. Block<br>iii. Concentrate<br>iv. Claims<br>v. Dough<br>vi. Inside<br>vii. Heart<br>viii. Stealing<br>ix. Innocent<br>x. Stronger<br>xi. Once<br>xii. Loneliness |
| Young man, there's a place you can go. I said, young man, when you're short on your_____ .You can stay there, and I'm sure you will find Many ways to have a good time | |
| And we could be together baby As long as skies are blue You act so _____ now But you lied so soon When I met you in the summer | |
| Hey ma I know you like the game come out and play now cause my _____ is yours take care now got a winning hand so come on and play now, play now | |
| Billie Jean is not my lover She's just a girl who _____ that I am the one But the kid is not my son She says I am the one, but the kid is not my son | |
| Never made it as a wise man I couldn't cut it as a poor man _____Tired of living like a blind man I'm sick of sight without a sense of feeling | |
| My, my, I tried to hold you back but you were _____ Oh yeah, and now it seems my only chance is giving up the fight And how could I ever refuse I feel like I win when I lose | |
| Near, far, wherever you are I believe that the heart does go on _____ more you open the door And you're here in my heart And my heart will go on and on | |
| My _____is killing me I must confess, I still believe When I'm not with you I lose my mind Give me a sign Hit me baby one more time | |
| I heard he sang a good song, I heard he had a style, and so I ____ to see him and listen for a while. And there he was this young boy, a stranger to my eyes | |
| Don't be fooled by the rocks that I got I'm still, I'm still Jenny from the ____ Used to have a little, now I have a lot No matter where I go, I know where I came from | |
| I stop and stare at you Walking on the shore I try to _____ My mind wants to explore The tropical scent of you Takes me up above And girl when I look at you | |

# Α-2 Τελικό ερωτηματολόγιο

**Παρακαλώ σημειώστε αυτό που ισχύει σε κάθε περίπτωση.**

1) Μπορέσατε να απομνημονεύσετε πλήρως το κωδικό σας;

| *Μέθοδος* / *Απάντηση* | Τυχαία σειρά | Κωδικός που προφέρεται στα αγγλικά | Αρχικά από μια μεγάλη πρόταση | Χρήση δημοφιλών φράσεων και ποιημάτων | Συνδυασμός λέξεων |
|---|---|---|---|---|---|
| Ναι | | | | | |
| Εύκολα | | | | | |
| Δύσκολα | | | | | |
| Όχι | | | | | |

2) Είχατε αναγραμμένο κάπου το κωδικό σας;

| *Μέθοδος* / *Απάντηση* | Τυχαία σειρά | Κωδικός που προφέρεται στα αγγλικά | Αρχικά από μια μεγάλη πρόταση | Χρήση δημοφιλών φράσεων και ποιημάτων | Συνδυασμός λέξεων |
|---|---|---|---|---|---|
| Ναι | | | | | |
| Όχι | | | | | |

3) Πώς σας φάνηκε ο κωδικός;

| *Μέθοδος* / *Απάντηση* | Τυχαία σειρά | Κωδικός που προφέρεται στα αγγλικά | Αρχικά από μια μεγάλη πρόταση | Χρήση δημοφιλών φράσεων και ποιημάτων | Συνδυασμός λέξεων |
|---|---|---|---|---|---|
| Πολύ εύκολος | | | | | |
| Εύκολος | | | | | |
| Δύσκολος | | | | | |
| Πολύ δύσκολος | | | | | |

4) Εάν σας είχε ανατεθεί για το **προσωπικό email** ένας παρόμοιος κωδικός, θα ήταν πολύ **πιο ασφαλής**;

| Μέθοδος / Απάντηση | Τυχαία σειρά | Κωδικός που προφέρεται στα αγγλικά | Αρχικά από μια μεγάλη πρόταση | Χρήση δημοφιλών φράσεων και ποιημάτων | Συνδυασμός λέξεων |
|---|---|---|---|---|---|
| Συμφωνώ | | | | | |
| Ουδέτερο | | | | | |
| Διαφωνώ | | | | | |

5) Εάν σας είχε ανατεθεί για το **προσωπικό email** ένας παρόμοιος κωδικός, θα ήταν **πολύ ενοχλητικός**;

| Μέθοδος / Απάντηση | Τυχαία σειρά | Κωδικός που προφέρεται στα αγγλικά | Αρχικά από μια μεγάλη πρόταση | Χρήση δημοφιλών φράσεων και ποιημάτων | Συνδυασμός λέξεων |
|---|---|---|---|---|---|
| Συμφωνώ | | | | | |
| Ουδέτερο | | | | | |
| Διαφωνώ | | | | | |

6) Εάν σας είχε ανατεθεί για το **προσωπικό email** ένας παρόμοιος κωδικός, θα ήταν πολύ **πιο εύκολος**;

| Μέθοδος / Απάντηση | Τυχαία σειρά | Κωδικός που προφέρεται στα αγγλικά | Αρχικά από μια μεγάλη πρόταση | Χρήση δημοφιλών φράσεων και ποιημάτων | Συνδυασμός λέξεων |
|---|---|---|---|---|---|
| Συμφωνώ | | | | | |
| Ουδέτερο | | | | | |
| Διαφωνώ | | | | | |

7) Εάν σας είχε ανατεθεί για το **προσωπικό email** ένας παρόμοιος κωδικός, σε ποια κατηγορία θα προτιμούσατε να ανήκει;

1. κωδικός με τυχαία σειρά χαρακτήρων
2. κωδικός που προφέρεται στα αγγλικά
3. κωδικός παρμένος από μια πρόταση
4. κωδικός από δημοφιλή φράση / ποίημα / σλόγκαν / στίχους / βιβλία / ταινίες

5. κωδικός που συνδυάζει λέξεις για μια νέα λέξη

8) Πόσες φορές καθ' όλη τη διάρκεια των τεστ, χρειαστήκατε υπενθύμιση του κωδικού σας;

1. 0 – 6
2. 7 – 13
3. 14 – 20
4. Περισσότερες
5. Δεν γνωρίζω / δεν απαντώ

9) Αναφέρατε τον εκάστοτε σας κωδικό σε άλλους;

1. Ναι
2. Όχι
3. Δεν απαντώ

10) Εάν ξεχάσατε το κωδικό σας

1. Ποιο ήταν το **πρώτο βήμα** που κάνατε;
   i. Ξαναπροσπάθησα
   ii. Ζήτησα βοήθεια / αλλαγή κωδικού με νέο
   iii. Συμβουλεύτηκα το χαρτάκι που είχα κάπου κρυφά
2. Εάν δεν κάνατε τις επιλογές (ii) και (iii), ποιο ήταν το **δεύτερο βήμα** που κάνατε;
   i. Ξαναπροσπάθησα
   ii. Ζήτησα βοήθεια / αλλαγή κωδικού με νέο

11) Με τη χρήση του εκάστοτε κωδικού, ο Η/Υ σας είναι πιο ασφαλής από πριν;

1. Ναι
2. Όχι
3. Είναι το ίδιο
4. Μου είναι αδιάφορο
5. Δεν γνωρίζω / δεν απαντώ

12) Σε γενικές γραμμές, η χρήση του νέου εκάστοτε σας φάνηκε ενοχλητική;

| *Μέθοδος* / *Απάντηση* | Τυχαία σειρά | Κωδικός που προφέρεται στα αγγλικά | Αρχικά από μια μεγάλη πρόταση | Χρήση δημοφιλών φράσεων και ποιημάτων | Συνδυασμός λέξεων |
|---|---|---|---|---|---|
| Συμφωνώ | | | | | |
| Ουδέτερο | | | | | |
| Διαφωνώ | | | | | |

13) Θα θέλατε να έχετε τον αρχικό σας κωδικό ή νέο αλλά όχι τόσο δύσκολο;

1. Ναι
2. Νέο κωδικό

14) Είχατε ποτέ καθοδήγηση για τη δημιουργία ενός ασφαλούς κωδικού;

1. Ναι
2. Όχι
3. Δεν γνωρίζω

15) Ο εκάστοτε κωδικός που σας δόθηκε, είναι κοντά στο δικό σας τρόπο σκέψης και επιλογής ενός ασφαλούς κωδικού;

| Μέθοδος / Απάντηση | Τυχαία σειρά | Κωδικός που προφέρεται στα αγγλικά | Αρχικά από μια μεγάλη πρόταση | Χρήση δημοφιλών φράσεων και ποιημάτων | Συνδυασμός λέξεων |
|---|---|---|---|---|---|
| Ναι | | | | | |
| Όχι | | | | | |
| Πολύ δύσκολος σε σχέση με αυτούς που χρησιμοποιώ | | | | | |
| Δεν γνωρίζω / δεν απαντώ | | | | | |

16) Έτυχε ποτέ να σας παραβιάσουν κάποιο προσωπικό κωδικό;

1. Ναι
2. Όχι
3. Δεν γνωρίζω / δεν απαντώ

17) Δηλώστε το φύλο σας.

1. Άρρεν
2. Θήλυ

# B-1 Ενημερωτικό email

Αγαπητοί συνάδελφοι,

Σαν μέρος για τη επιτυχή ολοκλήρωση της μεταπτυχιακής μου διατριβής και κατόπιν συνεννόησης με τον υπεύθυνο του IT Dept. Δώρο Θεοδώρου, σας επιλέξαμε **τυχαία** ώστε να διεξάγουμε μερικά tests αναφορικά με τη χρήση των κωδικών. Σκοπός της διατριβής είναι η εξαγωγή συμπερασμάτων για την ικανότητα απομνημόνευσης του κωδικού **ενός χρήστη σε εταιρικό περιβάλλον**. Συνολικά θα χρησιμοποιηθούν **5 tests/μέθοδοι** με διάρκεια το **μέγιστο 3 εβδομάδες** το καθένα.

Οι κωδικοί που θα χρησιμοποιείτε θα σας δίνονται απευθείας από μένα **μόνο**. Το μήκος του νέου κωδικού που θα σας ανατίθεται κάθε φορά είναι **8 χαρακτήρες**. Ο κωδικός αυτός θα αντικαταστήσει τον ήδη υπάρχων που κάνετε login το πρωί, ισχύει επίσης για το Outlook και τα αρχεία σας που είναι αποθηκευμένα σε κοινόχρηστους δίσκους.

**Οι συνδυασμοί θα περιλαμβάνουν γράμματα ( πεζά και κεφαλαία ), αριθμούς και ειδικούς χαρακτήρες ( !,._*+-/ )**

Παρακαλώ όπως αφιερώσετε λίγη ώρα να διαβάσετε μια μικρή περιγραφή για το κάθε test, θα είμαι πάντοτε σε επικοινωνία μαζί σας για την όποια επεξήγηση ή βοήθεια χρειαστείτε καθ' όλη τη διάρκεια.

1. Τυχαίος κωδικός: **σύνολο 8 χαρακτήρων** σε τυχαία σειρά που θα περιλαμβάνει όλους τους προαναφερθέντες συνδυασμούς. Δεν θα είναι λέξη αλλά αλληλουχία διαφορετικών χαρακτήρων, ίσως η μοναδική μέθοδος που θα έχει κάποιο βαθμό δυσκολίας (για παράδειγμα → ejD-UOo, k6ec0TTk).

2. Κωδικός που προφέρεται στα αγγλικά: **σύνολο 8 χαρακτήρων** θα περιέχει μόνο γράμματα. Δεν θα είναι λέξεις που χρησιμοποιούνται, δεν είναι υπαρκτές αλλά μπορούν να προφέρονται (για παράδειγμα → baBEtEWA, esuSOKAX ).

3. Κωδικός παρμένος από μια πρόταση: **σύνολο 8 χαρακτήρων** με βασική ιδέα να είναι η χρήση οποιουδήποτε γράμματος κάθε λέξης και εδώ μπορείτε να αφήσετε ελεύθερη τη φαντασία σας και να σχεδιάσετε όπως σας βολεύει εσάς καλύτερα το κωδικό φτάνει να συνάδει με τους προαναφερθέντες συνδυασμούς. Θα φροντίσω να δημιουργήσω αρκετούς κωδικούς (για παράδειγμα → The manager appoints the adhesive mass θα γίνει tM@aTAdm, Can the dumped carrier strike across the freeze? θα γίνει CTdCs@tF ).

4. Δημοφιλής φράσεις/ποιήματα/σλόγκαν/στίχοι/βιβλία/ταινίες: **σύνολο 8 χαρακτήρων** που είναι παρόμοιο με το προηγούμενο απλά η διαφορά είναι στο ότι θα περιοριστούμε στις κατηγορίες που αναφέρονται. Μπορείτε να προτείνετε και δικά σας. (για παράδειγμα → Good to the last drop θα γίνει Gud2T1d+ (maxwell house coffee), Don't leave home without it θα γίνει dN'1h0Wi (american express card)).

5. Συνδυασμός λέξεων για νέα λέξη: **σύνολο 8 χαρακτήρων** ίσως η πιο εύκολη και διασκεδαστική μέθοδος μιας και θα συνδυάζουμε λέξεις για να προκύπτει μια νέα λέξη. Και εδώ θα έχετε τη ευχέρεια να δημιουργήσετε τη δική σας λέξη (για παράδειγμα → BaReBacK, ZoopHile ).

Είναι μια πρωτοποριακή μελέτη και δεν υπάρχει παρόμοια καταγεγραμμένη πουθενά μέχρι στιγμής που συνδυάζει τις πιο πάνω μεθόδους και να διεξάγεται σε εταιρικό περιβάλλον.

Για λόγους στατιστικών δεδομένων, το μοναδικό προσωπικό δεδομένο που θα χρειαστώ από εσάς **και θα το διαχειριστώ με άκρα εχεμύθεια** είναι η ηλικία σας.

Τα tests θα ξεκινήσουν **από την ερχόμενη Δευτέρα 24/11/2014**. Για τις μεθόδους 1-2-5, οι κωδικοί θα δημιουργούνται από μένα ενώ στις μεθόδους 3-4 θα μπορείτε να προτείνετε και σεις για δική σας ευκολία. Για την οποιανδήποτε απορία ή διευκρίνιση, παρακαλώ όπως επικοινωνήσετε μαζί μου. Σας ευχαριστώ εκ των προτέρων για τη συνεργασία και τη βοήθεια σας.

Με εκτίμηση

Δημήτρης Παπαδημητρίου

Assistant, Information Technology Dept.

# B-2 Επιστολή γνωστοποίησης

Παρασκευή, 14 Νοεμβρίου 2014

**Προς:** Υπεύθυνο Τμήματος Πληροφορικής της [redacted]

Αγαπητέ κ. Θεοδώρου,

Σαν μέρος για τη επιτυχή ολοκλήρωση της μεταπτυχιακής μου διατριβής, παρακαλώ όπως έχω τη γραπτή έγκρισή σας να διαχειρίζομαι και να προβαίνω στις αναγκαίες αλλαγές στο Active Directory τη εταιρείας για τριάντα (30) συναδέλφους.

Σκοπός της διατριβής είναι η εξαγωγή συμπερασμάτων για την ικανότητα απομνημόνευσης του κωδικού **ενός χρήστη σε εταιρικό περιβάλλον**. Συνολικά θα χρησιμοποιηθούν **5 tests/μέθοδοι** με διάρκεια το **μέγιστο 3 εβδομάδες** το καθένα.

Παρακαλώ όπως αφιερώσετε λίγη ώρα να διαβάσετε μια μικρή περιγραφή για το κάθε test.

1. *Κωδικός σε τυχαία σειρά*: **σύνολο 8 χαρακτήρων** σε τυχαία σειρά που θα περιλαμβάνει όλους τους προαναφερθέντες συνδυασμούς. Δεν θα είναι λέξη αλλά αλληλουχία διαφορετικών χαρακτήρων, ίσως η μοναδική μέθοδος που θα έχει κάποιο βαθμό δυσκολίας (για παράδειγμα → ejD-UOo, k6ec0TTk).

2. *Κωδικός που προφέρεται στα αγγλικά*: **σύνολο 8 χαρακτήρων** θα περιέχει μόνο γράμματα. Δεν θα είναι λέξεις που χρησιμοποιούνται, δεν είναι υπαρκτές αλλά μπορούν να προφέρονται (για παράδειγμα → baBEtEWA, esuSOKAX ).

3. *Κωδικός με αρχικά από μια μεγάλη πρόταση*: **σύνολο 8 χαρακτήρων** με βασική ιδέα να είναι η χρήση οποιουδήποτε γράμματος κάθε λέξης και εδώ μπορείτε να αφήσετε ελεύθερη τη φαντασία σας και να σχεδιάσετε όπως σας βολεύει εσάς καλύτερα το κωδικό φτάνει να συνάδει με τους προαναφερθέντες συνδυασμούς. Θα φροντίσω να δημιουργήσω αρκετούς κωδικούς (για παράδειγμα → The manager appoints the adhesive mass θα γίνει tM@aTAdm, Can the dumped carrier strike across the freeze? θα γίνει CTdCs@tF ).

4. *Κωδικός με χρήση δημοφιλών προτάσεων και φράσεων*: **σύνολο 8 χαρακτήρων** που είναι παρόμοιο με το προηγούμενο απλά η διαφορά είναι στο ότι θα περιοριστούμε στις κατηγορίες που αναφέρονται. Μπορείτε να προτείνετε και δικά σας. (για παράδειγμα → Good to the last drop θα γίνει Gud2T1d+ (maxwell house coffee), Don't leave home without it θα γίνει dN'1h0Wi (american express card)).

5. *Συνδυασμός λέξεων*: **σύνολο 8 χαρακτήρων** ίσως η πιο εύκολη και διασκεδαστική μέθοδος μιας και θα συνδυάζουμε λέξεις για να προκύπτει μια νέα λέξη. Και εδώ θα έχετε τη ευχέρεια να δημιουργήσετε τη δική σας λέξη (για παράδειγμα → BaReBacK, ZoopHile ).

Τα tests θα ξεκινήσουν **από την ερχόμενη Δευτέρα 24/11/2014** και θα τελειώσουν τη **Παρασκευή 06/03/2015**. Σας ευχαριστώ εκ των προτέρων για τη συνεργασία και τη βοήθεια σας.

Με εκτίμηση

**Δημήτρης Παπαδημητρίου**
Assistant, Information Technology Dept

# Β-3 Επιστολή αποδοχής

[redacted]

**To:** Papademetriou Demetris

November 16, 2014

Dear Demetris,

Thank you for your initiative finding a policy that will lead in results how uses behave with passwords and I am sure that results of your survey will assist in improving our internal password policies and the overall company security.

I will be glad to share the results of this survey and we can together monitor your effort in the various stages to share conclusions on users' behavior.

Our firm and my department will do the best to assist you in your task.

Regards,

[redacted]

Head of Information Technology Dept

[redacted]