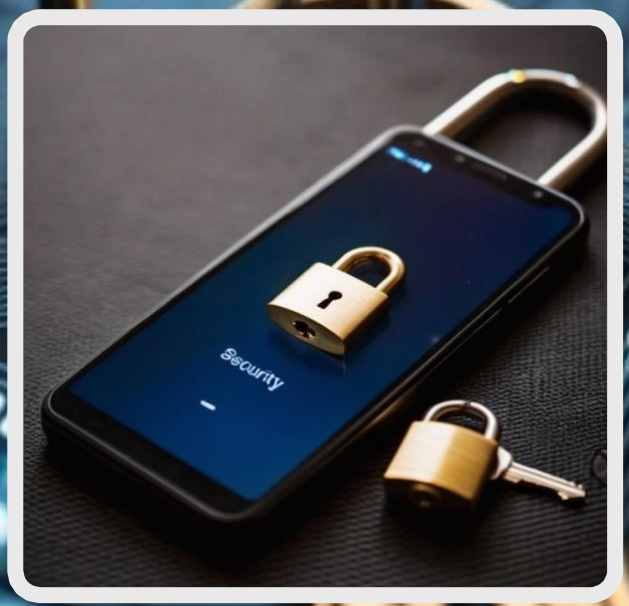
ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Τσόδουλος Ελευθέριος

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
UNIVERSITY OF WEST ATTICA

ΑΣΦΑΛΕΙΑ & ΙΔΙΩΤΙΚΟΤΗΤΑ SMARTPHON



Τίτλος Δ.Ε. : "**Ασφάλεια & ιδιωτικότητα Smartphone** "
Ονοματεπώνυμο φοιτητή: **Τσόδουλος Ελευθέριος**
Ονοματεπώνυμο επιβλέπων : **Μυριδάκης Νικόλαος,** *Επίκουρος Καθηγητής*
Ημερομηνία ανάληψης Δ.Ε. : 07/12/2023
Ημερομηνία περάτωσης Δ.Ε. : 22/07/2024

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο τμήμα "Μηχανικών Πληροφορικής και Υπολογιστών", της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής (ΠΑ.Δ.Α.) .

Η παρούσα εργασία αποτελεί πνευματική ιδιοκτησία του Τσόδουλου Ελευθέριου, φοιτητή του ΠΑ.Δ.Α. στο τμήμα Μηχανικών Πληροφορικής και Υπολογιστών που την εκπόνησε. Στο πλαίσιο της πολιτικής ανοικτής πρόσβασης, ο συγγραφέας/δημιουργός εκχωρεί στο Πανεπιστήμιο Δυτικής Αττικής άδεια χρήσης του δικαιώματος αναπαραγωγής, δανεισμού, παρουσίασης στο κοινό και ψηφιακής διάχυσης της εργασίας διεθνώς, σε ηλεκτρονική μορφή και σε οποιοδήποτε μέσο, για διδακτικούς και ερευνητικούς σκοπούς, άνευ ανταλλάγματος. Η ανοιχτή πρόσβαση στο πλήρες κείμενο της εργασίας, δεν σημαίνει καθ' οιονδήποτε τρόπο παραχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας του συγγραφέα/δημιουργού, ούτε επιτρέπει την αναπαραγωγή, αναδημοσίευση, αντιγραφή, πώληση, εμπορική χρήση, διανομή, έκδοση, μεταφόρτωση (downloading), ανάρτηση (uploading), μετάφραση, τροποποίηση με οποιονδήποτε τρόπο, τμηματικά ή περιληπτικά της εργασίας, χωρίς τη ρητή προηγούμενη έγγραφη συναίνεση του συγγραφέα/δημιουργού.

Η διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι Εξεταστική Επιτροπή:

Α/Α	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	ΥΠΟΓΡΑΦΗ
1,	Μυριδάκης Νικόλαος	Nikolaos Myridakis Digitally signed by Nikolaos Myridakis Date: 2024.07.23 20:16:14 +03'00'
2,	Καρκαζής Παναγιώτης	PANAGIOTIS KARKAZIS Digitally signed by PANAGIOTIS KARKAZIS Date: 2024.07.26 11:29:04 +03'00'
3,	Μαυρομμάτης Κωνσταντίνος	Konstantinos Mavrommatis Digitally signed by Konstantinos Mavrommatis Date: 2024.07.24 08:37:30 +03'00'

Πίνακας περιεχομένων

ΠΡΟΛΟΓΟΣ 4
ΠΕΡΙΛΗΨΗ 5
ABSTRACT 5
1. Εισαγωγή 6
1.1 Εισαγωγή στη σημασία της ασφάλειας στα smartphones 6
1.2 Ο σκοπός κι η σημασία της ιδιωτικότητας 6
2. Ασφάλεια στα Smartphones 8
2.1 Απειλές και κίνδυνοι στον κυβερνοχώρο 8
2.2 Κλοπή δεδομένων και παραβίαση απορρήτου 9
2.3 Ιοί, κακόβουλο λογισμικό, και phishing 11
2.4 Οι πρώτοι Ιοί κινητών τηλεφώνων 13
2.5 Στατιστικά απειλών στα κινητά τηλέφωνα τα τελευταία χρόνια 14
2.6 Trojans 19
2.7 Phishing 23
2.8 Στατιστικά Phishing 32
3. Ιδιωτικότητα στα Smartphones 40
3.1 Ορισμός και σημασία της ιδιωτικότητας 40
3.2 Πώς η ιδιωτικότητα προσθέτει επιπλέον επίπεδο προστασίας 42
3.3 Τεχνολογίες ιδιωτικότητας 44
3.4 Σύστημα αναγνώρισης προσώπου 47
3.5 Αισθητήρες δακτυλικού αποτυπώματος 50
3.6 Σύστημα αναγνώρισης ίριδας 52
3.7 Σύστημα αναγνώρισης φωνής 55
4. Προηγμένες Τεχνολογίες Ασφάλειας 57
4.1 Κρυπτογραφία και ασφαλείς συνδέσεις 57
4.2 Κρυπτογράφηση συμμετρικού κλειδιού 59
4.3 Κρυπτογράφηση δημοσίου κλειδιού 60

4.4 Πρωτόκολλα SSL/TLS 63
4.5 Πρωτόκολλο Ipsec 65
4.6 Εφαρμογή Κρυπτογραφίας στην Αποθήκευση και την Επικοινωνία 67
4.7 Υπηρεσίες VPN για ασφαλή περιήγηση 70
4.8 Ασφαλείς εφαρμογές και ενημερώσεις λογισμικού 73
4.9 Anti-virus 75
5. Προτεινόμενες Πρακτικές και Συμβουλές 78
5.1 Πώς να διατηρείτε το smartphone σας ασφαλές 78
5.2 Προτεινόμενες Ρυθμίσεις Ασφαλείας 79
5.3 Πώς να Αντιμετωπίζετε Περιπτώσεις Απώλειας ή Κλοπής 80
6. Συμπεράσματα 82
7. Μελλοντικές Τάσεις 83
7.1 Νέες τεχνολογίες και εξελίξεις 83
7.2 Blockchain 85
7.3 5G και Edge computing 91
7.4 Κβαντική κρυπτογραφία 93
Εικόνες 95
URLs 97
Βιβλιογραφία 99

ΠΡΟΛΟΓΟΣ

Στο σύγχρονο κόσμο, τα smartphones έχουν ενσωματώσει τεχνολογία που προσφέρει εξαιρετική συνδεσιμότητα και πρόσβαση σε πληθώρα πληροφοριών, κάτι που τα καθιστά αναπόσπαστο μέρος της καθημερινότητάς μας. Παρόλα αυτά, η ανησυχία για την ασφάλεια και την προστασία των προσωπικών δεδομένων είναι έντονη. Σε αυτό το πλαίσιο, η ιδιωτικότητα αναδεικνύεται ως κρίσιμος παράγοντας για τη διασφάλιση της ασφαλούς χρήσης και της προστασίας των δεδομένων. Η παρούσα εργασία εξετάζει εκτενώς τη σχέση μεταξύ ασφάλειας και ιδιοτικότητας στα smartphones, αναλύοντας τις προκλήσεις που αντιμετωπίζουν οι χρήστες και προτείνοντας προηγμένες λύσεις για την εξασφάλιση ενός ασφαλούς και προστατευμένου ψηφιακού περιβάλλοντος. Αναδεικνύοντας τη σημασία της προορατικής αντιμετώπισης των κινδύνων, αυτή η εργασία επιδιώκει να προσφέρει πολύτιμες εισηγήσεις για τη βελτίωση της ασφάλειας των smartphones στην εποχή της ψηφιακής επανάστασης.

Στο πλαίσιο αυτό, η συνεχής εξέλιξη της τεχνολογίας δημιουργεί νέες προκλήσεις και απαιτεί προηγμένες προσεγγίσεις για τη διατήρηση της ασφάλειας των συσκευών. Οι χρήστες συχνά αντιμετωπίζουν προβλήματα όπως ιοί, κακόβουλο λογισμικό και phishing επιθέσεις, καθώς και πιθανές παραβιάσεις της ιδιωτικότητάς τους. Ως αποτέλεσμα, η ανάγκη για αποτελεσματικά μέτρα προστασίας είναι επιτακτική. Είναι σημαντικό να είμαστε ενήμεροι για τις τελευταίες τάσεις και να εφαρμόζουμε τις κατάλληλες πρακτικές ασφαλείας, προκειμένου να διασφαλίσουμε την ακεραιότητα και την ασφάλεια των προσωπικών μας δεδομένων. Μέσω συνεχούς ενημέρωσης και επίγνωσης των απειλών που ενδέχεται να αντιμετωπίσουμε, μπορούμε να προετοιμαστούμε και να αντιδράσουμε αποτελεσματικά σε οποιαδήποτε πιθανή απειλή κατά της ασφάλειας των smartphones μας.

ΠΕΡΙΛΗΨΗ

Τα smartphones, ως αναπόσπαστο τμήμα της καθημερινότητάς μας, αντιμετωπίζουν διάφορες απειλές στον κυβερνοχώρο. Από την κλοπή δεδομένων και την παραβίαση του απορρήτου, μέχρι τον κίνδυνο από ιούς και κακόβουλο λογισμικό, οι χρήστες καλούνται να αντιμετωπίσουν ποικίλες απειλές. Σε αυτό το πλαίσιο, η ιδιωτικότητα , αναδεικνύεται ως κρίσιμος παράγοντας για την ασφαλή χρήση, προσφέροντας πρόσθετα επίπεδα προστασίας μέσω τεχνολογιών, όπως η αναγνώριση προσώπου και οι αισθητήρες δακτυλικών αποτυπωμάτων.

Η εργασία επικεντρώνεται σε προηγμένες τεχνολογίες ασφάλειας, όπως η κρυπτογραφία και οι υπηρεσίες VPN, που ενισχύουν την προστασία των δεδομένων κατά τη μετάδοση. Ταυτόχρονα, προτείνονται ασφαλείς πρακτικές για τη διατήρηση της ασφάλειας του smartphone, συμπεριλαμβανομένων των ρυθμίσεων ασφαλείας και της τακτικής ενημέρωσης του λογισμικού.

Στο σημείο των συμπερασμάτων, αναδεικνύεται η σημασία της προορατικής αντιμετώπισης κινδύνων και προτείνονται μέτρα για βελτίωση της ασφάλειας των smartphones. Εν τέλει, η εργασία εξετάζει μελλοντικές τάσεις, εστιάζοντας σε νέες τεχνολογίες που μπορούν να ενισχύσουν την ασφάλεια και την ιδιωτικότητα στον κόσμο των smartphones, προσφέροντας έτσι ένα ευρύτερο και ασφαλές ψηφιακό περιβάλλον.

ABSTRACT

In the modern world, smartphones have integrated technology that offers exceptional connectivity and access to a wealth of information, making them an integral part of our daily lives. However, concerns about smartphone security and the protection of personal data are paramount. In this context, privacy emerges as a critical factor in ensuring safe usage and data protection. This paper extensively examines the relationship between security and privacy on smartphones, analyzing the challenges users face and proposing advanced solutions to ensure a secure and protected digital environment. By highlighting the importance of proactive risk management, this work aims to provide valuable insights for enhancing smartphone security in the era of digital revolution.

Within this framework, the continuous evolution of technology presents new challenges and requires advanced approaches to maintain device security. Users often encounter issues such as viruses, malware, and phishing attacks, as well as potential breaches of their privacy. As a result, the need for effective security measures is urgent. It is important to stay informed about the latest trends and to implement appropriate security practices to ensure the integrity and security of our personal data. Through continuous education and awareness of the threats we may face, we can prepare and respond effectively to any potential security threat to our smartphones.

1. Εισαγωγή

1.1 Εισαγωγή στη σημασία της ασφάλειας στα smartphones

Η ανελέητη ενσωμάτωση των smartphones στην καθημερινότητά μας έχει φέρει αναμφίβολα πολλαπλά οφέλη, αλλά ταυτόχρονα έχει ανοίξει την πόρτα σε πολυπλοκότερες κυβερνοαπειλές. Αυτό το ψηφιακό εργαλείο, που συχνά θεωρείται ως επέκταση του εαυτού μας, αντιμετωπίζει συνεχώς απειλές που επηρεάζουν την ιδιωτικότητα μας, τα προσωπικά μας δεδομένα, και την ασφάλειά μας.

Η ευρύτερη χρήση των smartphones για ευαίσθητες δραστηριότητες, όπως τραπεζικές συναλλαγές, αγορές και επικοινωνία, καθιστά κρίσιμο το θέμα της ασφάλειας. Η απειλή κλοπής δεδομένων με σκοπό την παραβίαση της προσωπικής μας ζωής και των οικονομικών μας πόρων καθιστά την ασφάλεια πρωταρχική προτεραιότητα.

Η έλλειψη ασφάλειας στα smartphones είναι ικανή να επιφέρει σοβαρές συνέπειες, καθώς οι χρήστες εκτίθενται σε επιθέσεις κακόβουλου λογισμικού, ιών και ανεπιθύμητων εισβολών στην ιδιωτική τους ζωή. Είναι επιτακτική η ανάγκη να κατανοήσουμε όχι μόνο την ύπαρξη αυτών των κινδύνων αλλά και να αναπτύξουμε συστήματα ασφαλείας που θα προστατεύουν αποτελεσματικά τα πολυτιμότερα μας δεδομένα.

Σε αυτό το πλαίσιο, η εργασία εξετάζει τη σημασία της ασφάλειας στα smartphones και διερευνά τρόπους βελτίωσης των μέσων προστασίας για να διασφαλιστεί μια ασφαλής και αξιόπιστη εμπειρία χρήσης.

1.2 Ο σκοπός κι η σημασία της ιδιωτικότητας

Η ιδιωτικότητα αναδύεται ως ουσιαστικός παράγοντας στον κόσμο των smartphones, καθώς συνδυάζει την ταχύτητα και την άνεση της πρόσβασης με την ενίσχυση της ασφάλειας των προσωπικών δεδομένων. Ο σκοπός της ενσωμάτωσης της ιδιοτικότητας είναι να παρέχει ένα προηγμένο επίπεδο ασφαλείας, διασφαλίζοντας ότι μόνο ο εξουσιοδοτημένος χρήστης έχει πρόσβαση στη συσκευή.

Η ιδιωτικότητα εκμεταλλεύεται τα μοναδικά χαρακτηριστικά του χρήστη, όπως τα πρόσωπο, τα δακτυλικά αποτυπώματα ή άλλα βιομετρικά χαρακτηριστικά, για την αναγνώριση και την προστασία της συσκευής. Αυτό δεν διευκολύνει απλώς την πρόσβαση του χρήστη, αλλά επίσης εξασφαλίζει ότι οι προσωπικές του πληροφορίες παραμένουν προστατευμένες από την ανεπιθύμητη πρόσβαση.

Σημαντικό είναι επίσης το γεγονός ότι, η ιδιωτικότητα προσφέρει μια εναλλακτική λύση στις παραδοσιακές μεθόδους κωδικοποίησης ή προσβασιμότητας με PIN, που μπορεί να είναι ευάλωτες σε ανεξουσίαστη πρόσβαση ή επιθέσεις.

Η ιδιωτικότητα είναι ένα πολύτιμο χαρακτηριστικό που συνδυάζει την ευκολία χρήσης με την υψηλή ασφάλεια. Αντιπροσωπεύει ένα προηγμένο σύστημα προστασίας, που εξυπηρετεί τις ανάγκες άνεσης των χρηστών, ενώ ταυτόχρονα εγγυάται την αδιάβλητη προστασία των

προσωπικών τους δεδομένων. Αυτή η ισχυρή συνδυαστική προσέγγιση, δίνει τη δυνατότητα στους χρήστες, να απολαμβάνουν την πλοήγηση και τη χρήση των ψηφιακών τους υπηρεσιών, χωρίς να ανησυχούν για πιθανές απειλές στην ασφάλεια των προσωπικών τους δεδομένων.

Εικόνα 1: Σκίτσο παραβίασης ιδιωτικότητας.

2. Ασφάλεια στα Smartphones

2.1 Απειλές και κίνδυνοι στον κυβερνοχώρο

Ο κυβερνοχώρος αντιπροσωπεύει ένα πολύπλοκο οικοσύστημα, όπου οι απειλές και οι κίνδυνοι εκδηλώνονται σε ποικίλες μορφές, απαιτώντας συνεχή εποπτεία και αντιμετώπιση. Στον τομέα της ασφάλειας του κυβερνοχώρου, πολλές απειλές προκύπτουν από τη διασυνδεδεμένη φύση των συσκευών και των δικτύων.

Μία από τις κυριότερες απειλές είναι η κυβερνοασφάλεια, που περιλαμβάνει επιθέσεις που στοχεύουν τα δίκτυα, τα συστήματα, και τις πληροφορίες. Επιθέσεις όπως οι επιθέσεις DDoS (Distributed Denial of Service), μπορούν να προκαλέσουν απώλεια λειτουργικότητας, ενώ οι επιθέσεις με στόχο την απόκτηση μη εξουσιοδοτημένης πρόσβασης (hacking), μπορούν να οδηγήσουν στην παραβίαση ευαίσθητων δεδομένων.

Οι κακόβουλοι κώδικες και τα κακόβουλα λογισμικά αποτελούν μια άλλη σοβαρή απειλή. Η εμφάνιση τρογλυφικών (Trojans), ιών και άλλων επιθέσεων λογισμικού ενδέχεται να προκαλέσει ζημίες σε συστήματα και να επιτρέψει την αποστολή ευαίσθητων πληροφοριών σε εξωτερικούς εισβολείς.

Επίσης, η κλοπή ταυτότητας και η απάτη αποτελούν συνεχείς απειλές. Κακόβουλοι χρήστες μπορεί να χρησιμοποιήσουν προηγμένες τεχνικές για την παραβίαση προσωπικών πληροφοριών, με σκοπό την παραπλάνηση ή την πραγματοποίηση αναξιόπιστων συναλλαγών.

Εκτός από τις απειλές που αναφέρθηκαν, οι επιθέσεις ransomware αποτελούν μια σοβαρή ανησυχία. Αυτοί οι τύποι επιθέσεων συχνά κρυπτογραφούν τα δεδομένα του θύματος και ζητούν λύτρα για την αποκρυπτογράφησή τους. Οι επιθέσεις αυτές μπορούν να έχουν καταστροφικές επιπτώσεις σε επιχειρήσεις και οργανισμούς, καθώς μπορεί να οδηγήσουν σε απώλεια δεδομένων και οικονομικών στοιχείων. Επίσης, οι κυβερνοεπιθέσεις μπορεί να προέρχονται από κρατικά ή κρατικώς υποστηριζόμενες ομάδες, με στόχο την παραβίαση συστημάτων και την κλοπή ευαίσθητων πληροφοριών για πολιτικούς, στρατηγικούς ή οικονομικούς σκοπούς. Αυτού του είδους οι επιθέσεις μπορούν να είναι πολύ προηγμένες και να απαιτούν εξειδικευμένες μεθόδους ανίχνευσης και αντίδρασης.

Επιπλέον, η ανάπτυξη της τεχνητής νοημοσύνης και της μηχανικής μάθησης έχει οδηγήσει σε νέες μορφές κυβερνοεπιθέσεων, όπως οι επιθέσεις με χρήση εξελιγμένων αλγορίθμων για την παράγωγη καινούργιων μορφών κακόβουλου λογισμικού ή για την αποφυγή ανίχνευσης από τα συστήματα ασφαλείας. Αυτή η συνεχής εξέλιξη των τεχνολογιών απαιτεί αντίστοιχη προσαρμογή και βελτίωση των συστημάτων ασφαλείας.

Η ασφάλεια του κυβερνοχώρου, απαιτεί την υιοθέτηση προληπτικών μέτρων, όπως η χρήση προηγμένων λύσεων κυβερνοασφάλειας, την εκπαίδευση των χρηστών για τις απειλές, και τη συνεχής παρακολούθηση των νέων τάσεων στον κυβερνοχώρο για την άμεση αντίδραση σε επικίνδυνες εξελίξεις.

2.2 Κλοπή δεδομένων και παραβίαση απορρήτου

Αν και οι τεχνολογικές προόδοι έχουν φέρει πολλά οφέλη στην καθημερινότητά, έχουν επίσης δημιουργήσει νέους κινδύνους και απειλές, ιδιαίτερα όσον αφορά την ασφάλεια των προσωπικών δεδομένων. Η κλοπή δεδομένων και η παραβίαση του απορρήτου συνιστούν δύο από τις πιο σοβαρές απειλές για την ασφάλεια των smartphones, καθώς απειλούν την εμπιστευτικότητα και την ακεραιότητα των προσωπικών μας πληροφοριών.

Α. Κλοπή Δεδομένων:

1. **Μορφές κλοπής:**
   - *Ηλεκτρονική Κλοπή:* Η ηλεκτρονική κλοπή είναι μια μορφή επίθεσης που διεξάγεται μέσω του διαδικτύου, όπου κακόβουλοι χρήστες αξιοποιούν αδύναμα σημεία στην ασφάλεια των συσκευών για να αποσπάσουν προσωπικά δεδομένα.
   - *Φυσική Κλοπή:* Η φυσική κλοπή αναφέρεται στην απώλεια ή την παράνομη αφαίρεση του φυσικού κινητού τηλεφώνου από τον νόμιμο κάτοχό του. Σε αυτήν την κατάσταση, ο κίνδυνος πρόσβασης σε ευαίσθητα δεδομένα είναι πραγματικός καθώς ο εισβολέας μπορεί να έχει πρόσβαση σε προσωπικές πληροφορίες, όπως επαφές, φωτογραφίες, μηνύματα, και άλλα ευαίσθητα δεδομένα που ενδεχομένως είχε αποθηκεύσει ο νόμιμος κάτοχος στη συσκευή του.
2. **Επιπτώσεις της κλοπής:**
   - *Χρήση Προσωπικών Δεδομένων:* Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν τα κλεμμένα δεδομένα για απάτες, κλοπή ταυτότητας και άλλες απάνθρωπες ενέργειες.
   - *Επικίνδυνες Εφαρμογές:* Κακόβουλες εφαρμογές που μπορούν να εγκατασταθούν στο κλεμμένο smartphone, επιτρέποντας στους επιτιθέμενους να παρακολουθούν τις δραστηριότητες του χρήστη.

Β. Παραβίαση Απορρήτου:

1. **Κακόβουλο λογισμικό και κακόβουλες εφαρμογές:**
    - *Κρυπτογραφημένα Δεδομένα:* Οι επιτιθέμενοι επιχειρούν να αποκρυπτογραφήσουν τα αποθηκευμένα δεδομένα, απειλώντας το απόρρητο των πληροφοριών.
    - *Κακόβουλες Εφαρμογές:* Εφαρμογές που προσποιούνται να είναι αξιόπιστες, αλλά στην πραγματικότητα συλλέγουν προσωπικά δεδομένα για αμφιλεγόμενους σκοπούς.
2. **Επιπτώσεις της παραβίασης απορρήτου:**
    - *Εκθέτει τα Προσωπικά Δεδομένα:* Οι πληροφορίες που παραβιάζονται μπορεί να διαρρεύσουν σε μη εξουσιοδοτημένα μέρη, θέτοντας σε κίνδυνο την ιδιωτικότητα των χρηστών.
    - *Προσβλητική Χρήση Δεδομένων:* Οι επιτιθέμενοι μπορούν να χρησιμοποιήσουν τις παραβιάσεις για προσωπικά ή οικονομικά οφέλη, εμπλέκοντας τους χρήστες σε ανεπιθύμητες καταστάσεις.

Οι συνέπειες όλων αυτών των πράξεων είναι εξίσου σοβαρές. Οι πληροφορίες που παραβιάζονται μπορεί να διαρρεύσουν σε μη εξουσιοδοτημένα μέρη, θέτοντας σε κίνδυνο την ιδιωτικότητα των χρηστών. Επιπλέον, οι επιτιθέμενοι μπορούν να εκμεταλλευτούν αυτές τις παραβιάσεις για προσωπικό ή οικονομικό όφελος, βάζοντας τους χρήστες σε ανεπιθύμητες καταστάσεις. Επιβάλλεται, λοιπόν, η λήψη προληπτικών μέτρων για την ασφάλεια των προσωπικών δεδομένων, συμπεριλαμβανομένης της χρήσης προηγμένων τεχνολογιών ασφαλείας και της προώθησης της ευαισθητοποίησης των χρηστών.

2.3 Ιοί, κακόβουλο λογισμικό, και phishing

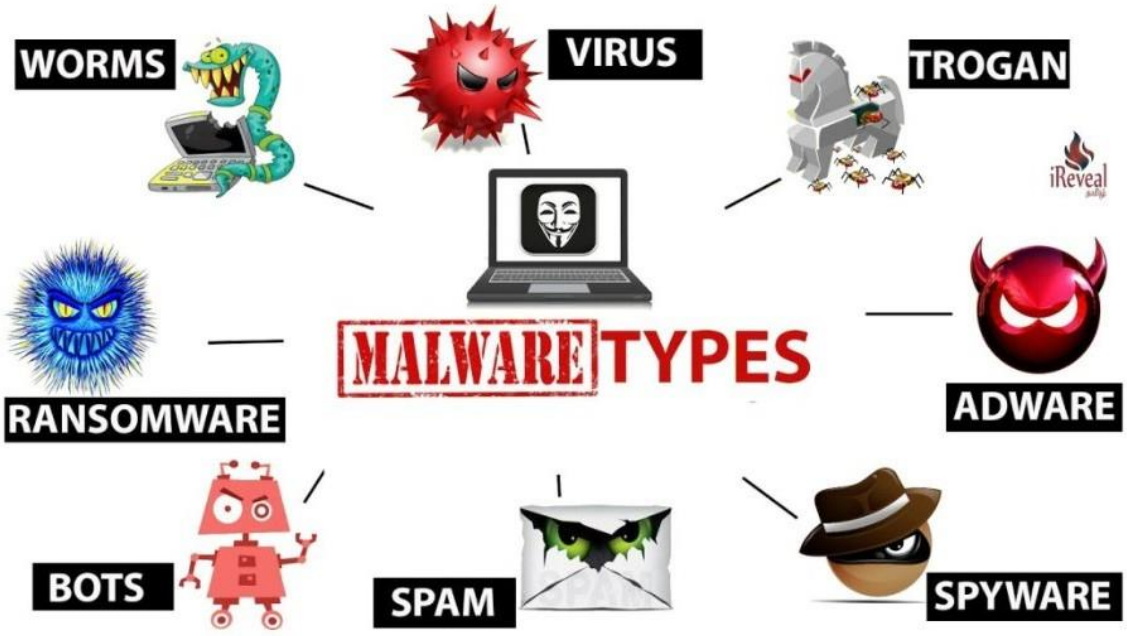
Οι ιοί, το κακόβουλο λογισμικό και το phising αποτελούν κύριες απειλές στον κυβερνοχώρο, προκαλώντας σοβαρές ανησυχίες για την ασφάλεια των πληροφοριακών συστημάτων και των χρηστών.

1. **Ιοί:**
   - Οι ιοί είναι κακόβουλοι κώδικες που επικολλώνται σε άλλα εκτελέσιμα προγράμματα επηρεάζοντας τη λειτουργία τους. Οι ιοί μπορούν επίσης να εκμεταλλευτούν τις αδυναμίες του λογισμικού για να εξαπλώσουν τον εαυτό τους, χρησιμοποιώντας τις γνωστές ως "ευπάθειες" (vulnerabilities). Εφόσον έχουν εισβάλλει σε ένα σύστημα, μπορεί να εκτελέσουν κακόβουλες ενέργειες χωρίς τη συναίνεση του χρήστη, όπως την παρακολούθηση των δραστηριοτήτων του, την παραβίαση της ιδιωτικότητάς του ή ακόμα και την υποκλοπή των προσωπικών του πληροφοριών.
   - Εκτός από την κλασική μορφή ιών που μεταδίδονται μέσω εκτελέσιμων αρχείων ή εγγράφων, οι ιοί συχνά εκμεταλλεύονται και άλλα μέσα για την εξάπλωσή τους, όπως τα ηλεκτρονικά μηνύματα ηλεκτρονικού ταχυδρομείου ή ακόμα και τα κοινωνικά δίκτυα, προσποιούμενοι αξιόπιστες πηγές ή παρουσιάζοντας αλλοίωση στα δεδομένα που αποστέλλονται. Μια αποτελεσματική προσέγγιση για την αντιμετώπιση των ιών είναι η χρήση αντιικών λογισμικών και τακτικών ενημερώσεων λογισμικού για την εξάλειψη τυχόν ευπαθειών που μπορεί να εκμεταλλευτούν οι επιθέσεις.

2. **Κακόβουλο λογισμικό:**
   - Το κακόβουλο λογισμικό περιλαμβάνει διάφορες μορφές όπως τρογλυφικά (trojans), backdoors, και rootkits. Αυτά τα επικίνδυνα προγράμματα σχεδιάζονται με σκοπό να προκαλέσουν ζημίες ή να κλέψουν πληροφορίες από τους χρήστες. Τα τρογλυφικά προσποιούνται ως αξιόπιστα προγράμματα για να αποκτήσουν πρόσβαση στο σύστημα, οι backdoors ανοίγουν κρυφές πύλες πρόσβασης για μελλοντικές επιθέσεις, ενώ τα rootkits κρύβονται βαθιά στο σύστημα, προκειμένου να αποφευχθεί η ανίχνευσή τους. Η ανάπτυξη προηγμένων ανιχνευτικών μεθόδων, όπως η συνεχής ενημέρωση και ανάλυση των υπογραφών του κακόβουλου λογισμικού, είναι ζωτικής σημασίας για τον εντοπισμό και την απομάκρυνσή του από τα συστήματα και τις δικτυακές υποδομές.

3. **Phising:**
   - Η τεχνική του phishing αποσκοπεί στο να αποκτήσει ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης, μέσω κοινωνικής εξαπάτησης. Συνήθως, πραγματοποιείται μέσω παραπλανητικών ηλεκτρονικών μηνυμάτων ή ιστοσελίδων, τα οποία φαίνονται να προέρχονται από αξιόπιστες πηγές. Οι χρήστες ενημερώνονται ότι πρέπει να παράσχουν ευαίσθητες πληροφορίες, όπως κωδικούς πρόσβασης ή προσωπικά δεδομένα, παριστάνοντας ότι πρόκειται για επείγοντα ή σημαντικά θέματα. Η εκπαίδευση των χρηστών για την αναγνώριση του phishing και η αναβάθμιση της κυβερνοασφάλειας είναι κρίσιμες για την αποτροπή τέτοιων επιθέσεων.

Η αντιμετώπιση αυτών των απειλών περιλαμβάνει τη χρήση ενημερωμένων αντιικών, τον έλεγχο των προσβάσεων, την ασφαλή περιήγηση στο διαδίκτυο, και την ενίσχυση της ευαισθητοποίησης των χρηστών σχετικά με τις τεχνικές phishing. Επίσης, η συνεχής εκπαίδευση των χρηστών για τις τελευταίες τεχνικές επιθέσεων και η προώθηση της ασφαλούς συμπεριφοράς στο διαδίκτυο είναι σημαντικά βήματα για την προστασία από το phishing.



Εικόνα 2: Τύποι κακόβουλων προγραμμάτων.

2.4 Οι πρώτοι Ιοί κινητών τηλεφώνων

Οι δυνατότητες bluetooth και internet με την πρόοδο τους είχα αυξήσει την ευπάθεια των συσκευών σε ιούς από τα πρώτα χρόνια κιόλας κυκλοφορίας τους.

Μερικοί από τους πιο γνωστούς ιούς κινητής τηλεφωνίας είναι οι παρακάτω:

- Cabir: Το cabir είναι το πρώτο παράδειγμα ιού κινητής τηλεφωνίας, όπου και δημιουργήθηκε από Τσέχους και Σλοβάκους hackers. Αν και δεν θεωρείται επικίνδυνος με την έννοια ότι μπορεί να καταστρέψει δεδομένα, η κύρια του επίπτωση ήταν η μειωμένη διάρκεια ζωής της μπαταρίας. Ο παραπάνω ιός μεταδιδόταν μέσω bluetooth και είχε την μορφή ενώ αρχείου ασφαλείας. Όταν ενεργοποιούταν η συσκευή, ξεκινούσε αυτόματη αναζήτηση άλλων συσκευών μέσω blutooth και με αυτόν τον τρόπο ο ιός μεταδιδόταν σε εμβέλεια τριάντα μέτρων.
- Commwarrior: Ο παραπάνω ιός στόχευε στην χρέωση του χρήση, χωρίς κάποιο ώφελος στον δημιουργό του ιού. Ο ιός μόλυνε τα κινητά τηλέφωνα και έστελνε σε όλες τις αποθηκευμένες επαφές του κινητού μηνύματα πολυμέσων (MMS), δημιουργώντας με αυτών τον τρόπο υψηλούς λογαριασμούς στον χρήστη.
- Trojan-SMS.AndroidOS.FakePlayer.a: Ο παραπάνω ιός ήταν ο πρώτος trojan ιός που εντοπίστηκε. Δημιουργήθηκε τον Αύγουστο του 2010 και ήταν τύπου trojan horse. Χρησιμοποιούσε το android λογισμικό σύστημα για να εγκατασταθεί και να μεταδοθεί. Εμφανιζόταν ως ένα media player και με την εγκατάστασή του, έστελνε μαζικά μηνύματα στις επαφές του κινητού τηλεφώνου, με σκοπό την υπέρογκη χρέωση του χρήστη.

Εικόνα 3: FakePlayer trojan.

2.5 Στατιστικά απειλών στα κινητά τηλέφωνα τα τελευταία χρόνια

Σύμφωνα με στατιστικά της Kaspersky Security Network για το δεύτερο τρίμηνο του 2023, έχουν βρεθεί περίπου 6 εκατομμύρια επικίνδυνα malwares κινητών συσκευών, adwares και riskwares. Η πιο κοινή απειλή με ποσοστό περίπου 30% ήταν το ανεπιθύμητο λογισμικό, ενώ εντοπίστηκαν περίπου 370 χιλιάδες κακόβουλα πακέτα εγκατάστασης, από τα οποία, τα περίπου 60 χιλιάδες ήταν Trojan για το e-banking, ενώ περίπου τα 1300 ήταν trojans για ransomware.

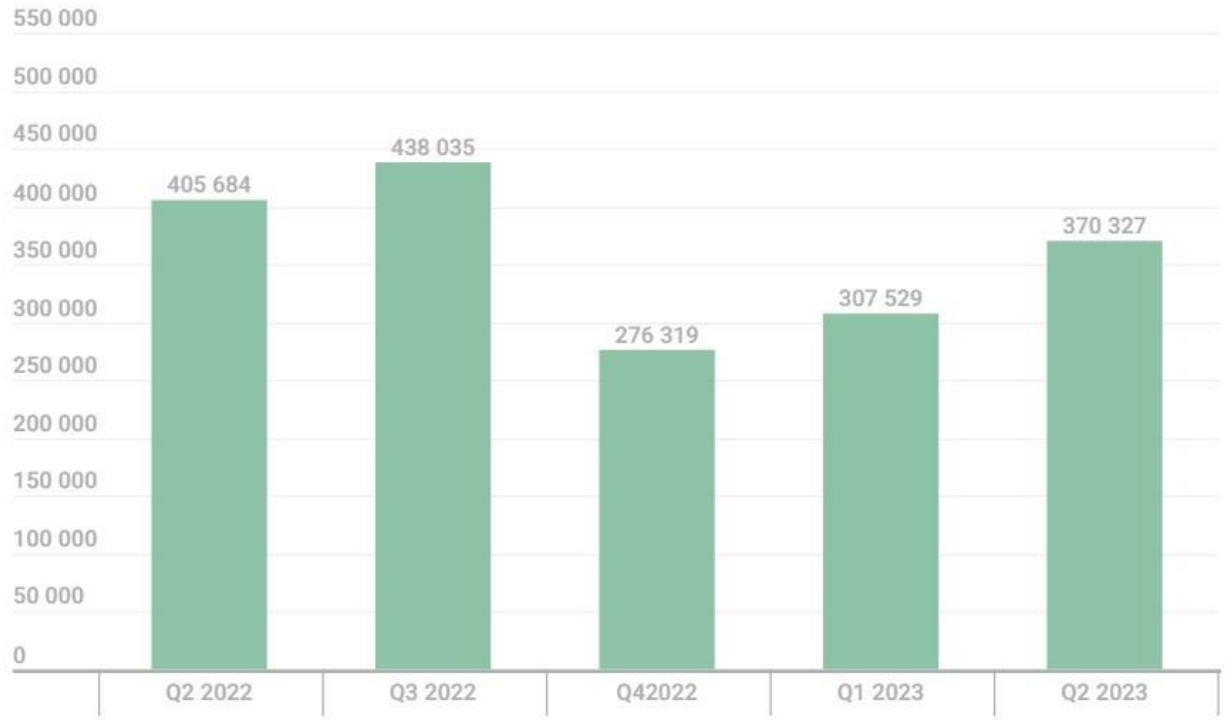
Στην παρακάτω Εικόνα φαίνονται όλες οι απειλές που εντοπίστηκαν ανά τρίμηνο των τελευταίων ετών.

Εικόνα 4: Απειλές που εντοπίστηκαν στα κινητά τηλέφωνα ανά τρίμηνο, των τελευταίων ετών.

Στην παρακάτω Εικόνα φαίνονται οι αριθμοί των εντοπισμένων κακόβουλων πακέτων εγκατάστασης στα κινητά τηλέφωνα, ανά τρίμηνο στα τελευταία χρόνια.

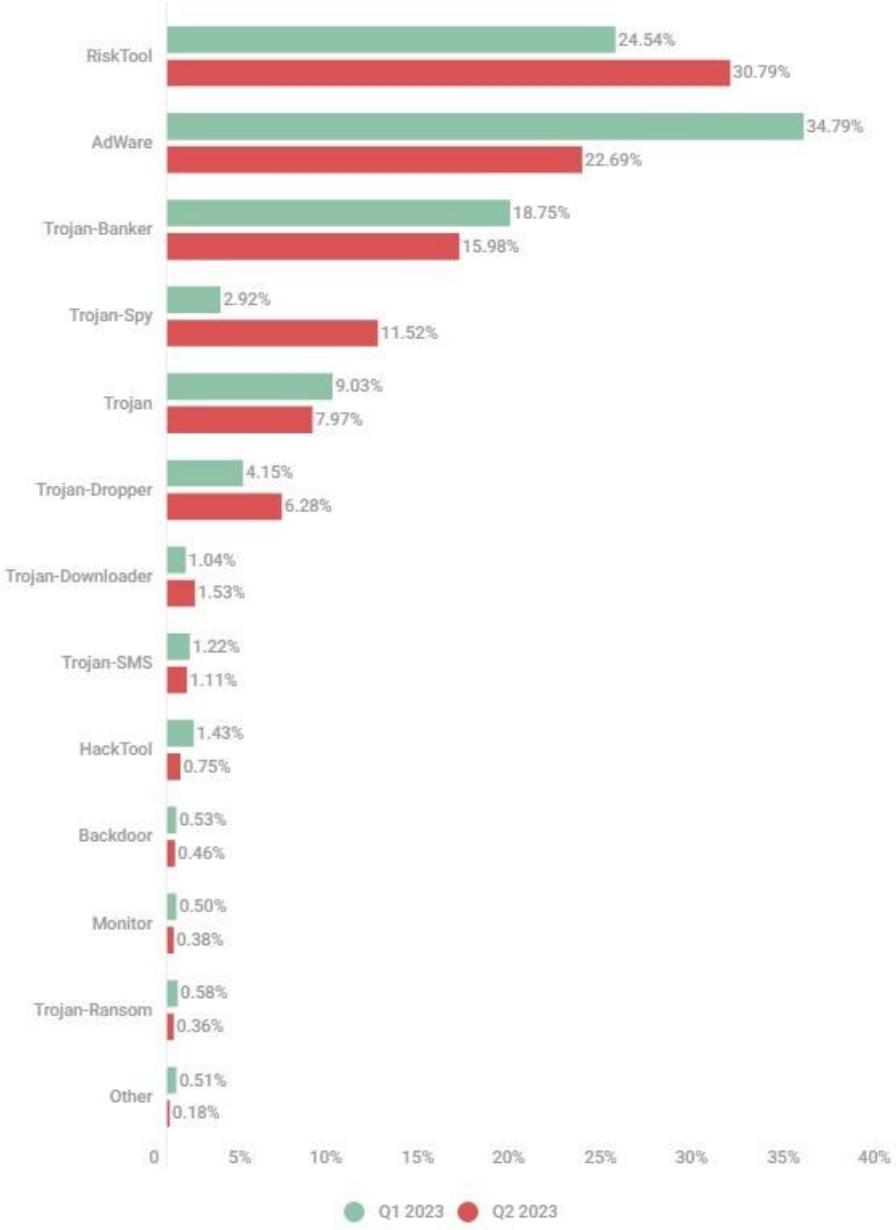
Αναλυτικότερα το τέταρτο τρίμηνο του 2022, παρατηρήθηκε μείωση στον αριθμό των κακόβουλων πακέτων εγκατάστασης, λόγω της μειωμένης δραστηριότητας του Trojan-Dropper.AndroidOS.Ingopack.

Όπως αναμενόταν, στο πρώτο τρίμηνο του 2023, παρατηρήθηκε αύξηση σε νέα πακέτα κακόβουλων λογισμικών εγκατάστασης, η οποία και συνεχίστηκε στα επόμενα τρίμηνα.



Εικόνα 5: Κακόβουλα πακέτα εγκατάστασης κινητών ανά τρίμηνω στα τελευταία έτη.

Στην παρακάτω Εικόνα φαίνονται οι τύποι των malwares που βρέθηκαν σε κινητές συσκευές, από το δεύτερο τρίμηνο του 2023, έως το δεύτερο τρίμηνο του 2023. Τα μεγαλύτερα ποσοστά είναι οι ανεπιθύμητες εφαρμογές, τα AdWares και τα πολύ επικίνδυνα Trojan-bankers.

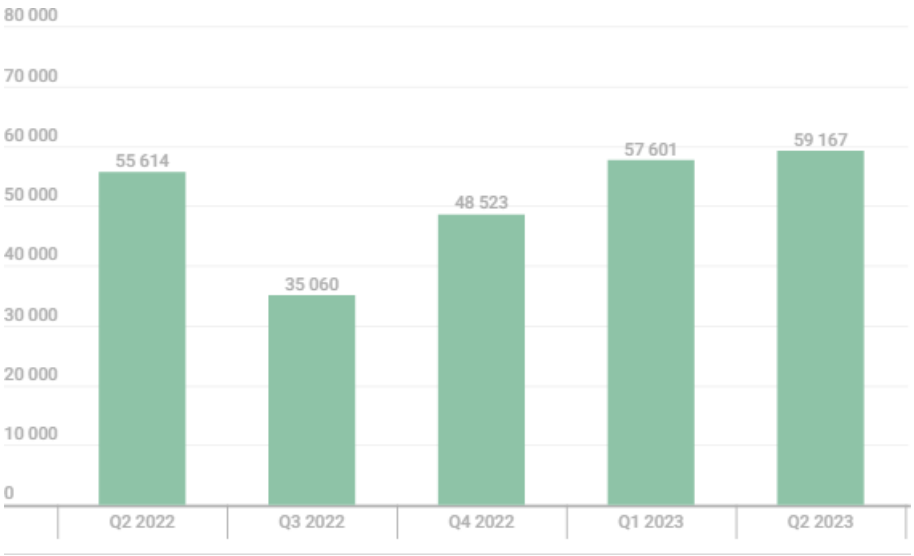


Εικόνα 6: Κατανομή των malwares που βρέθηκαν σε κινητές συσκευές μεταξύ 2022 και 2023.

Στον παρακάτω πίνακα φαίνονται τα 10 πιο κοινά malware προγράμματα των κινητών τηλεφώνων στο 2023.

Ετυμηγορία	% Q1 2023	% Q2 2023
DangerousObject.Multi.Generic.	13.27	16.79
Trojan.AndroidOS.Boogr.gsh	8.39	10.05
Trojan.AndroidOS.GriftHorse.l	6.13	8.38
Trojan.AndroidOS.Generic.	5.95	6.56
Trojan-Spy.AndroidOS.Agent.acq	8.60	6.10
Trojan.AndroidOS.Fakemoney.v	7.48	5.34
Trojan-Spy.AndroidOS.Agent.aas	3.64	3.65
DangerousObject.AndroidOS.GenericML	3.46	3.14
Trojan-Dropper.AndroidOS.Badpack.g	0.00	2.96
Trojan-Dropper.AndroidOS.Hqwar.hd	4.54	2.33

Τέλος τα επικίνδυνα Trojan-bankers διατηρούν της αυξητική τους τάση όπως φαίνεται από την παρακάτω Εικόνα.



Εικόνα 7: Αυξητική τάση των Trojan-bankers που εντοπίστηκαν από τα μέσα του 2022 ως τα μέσα του 2023.

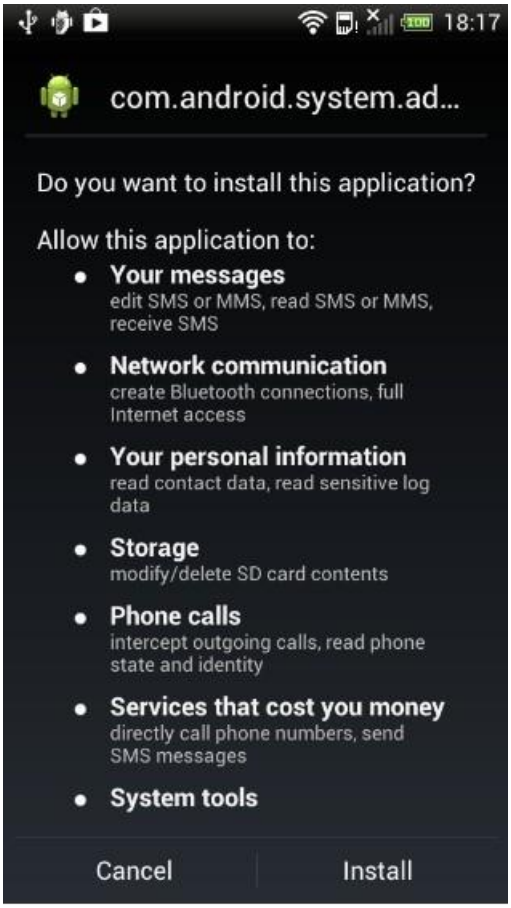
2.6 Trojans

Τα trojans είναι malwares που εγκαθίστανται στο λογισμικό android. Η ονοματολογία τους έχει τις εξής μορφές Tojan:Android/family ή Trojan.Android.Family.
Είναι εφαρμογές που τρέχουν κρυφά από τον χρήστη στο παρασκήνιο, κάνοντας πράξεις που έχουν σκοπό να υποκλέψουν προσωπικές πληροφορίες του χρήστη ή δώσουν εντολές στην συσκευή να εκτελέσει συγκεκριμένες ενέργειες.

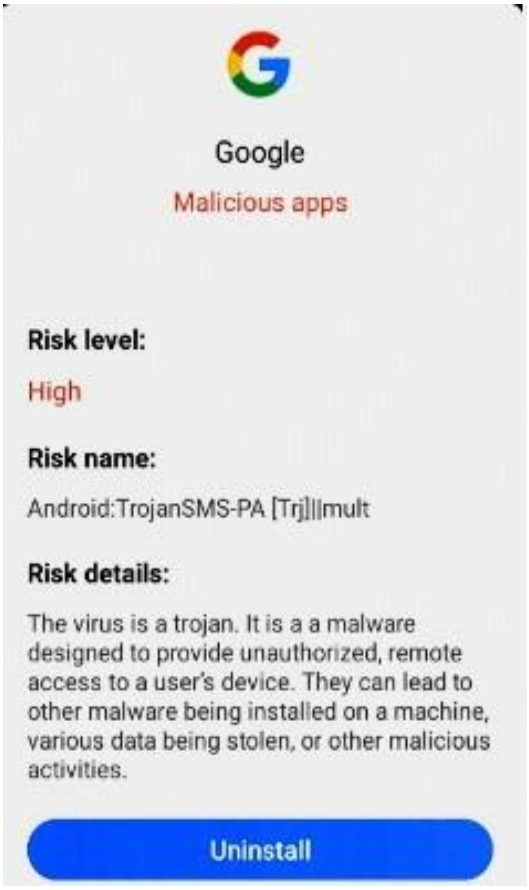
Τα trojans βασίζοντα στο γεγονός, ότι ο χρήστης λόγω του ονόματος της κακόβουλης εφαρμογής, θα μπερδευτεί και θα τα εγκαταστήσει. Δηλαδή χρησιμοποιούν παρόμοια ονόματα και κατασκευές με τις αυθεντικές εφαρμογές των marketplace, αυξάνοντας με αυτόν τον τρόπο το να παραπλανήσουν τον χρήστη.

Μερικά από τα συνήθη trojans είναι τα εξής:

- Trojan:Android/Fakeinst: εμφανίζεται σαν να είναι Installer για κάποιες αυθεντικές εφαρμογές κι εφόσον εγκατασταθεί, στέλνει μηνύματα SMS σε τηλεφωνικούς αριθμούς premium ή υπηρεσίας επί πληρωμή. Στόχος του είναι λοιπόν, η χρηματική επιβάρυνση του χρήστη.
- Trojan:Android/FakeToken: εμφανίζεται σαν να είναι μία εφαρμογή δημιουργίας token. Εφόσον εγκατασταθεί, υποκλέπτει από τα SMS τους αριθμούς ελέγχου ταυτότητας συναλλαγών, που δημιουργούνται για παράδειγμα από μία τράπεζα και στέλνονται στον χρήστη για την επιβεβαίωσή του. Το παραπάνω trojan λοιπόν, τους αριθμούς ελέγχου ταυτότητας, μαζί με αναλυτικές πληροφορίες της συσκευής, τα στέλνει σε κάποιον απομακρυσμένο χρήστη και τα μπλοκάρει από την εμφάνιση στην συσκευή.
- Trojan:Android/MarketPay.A: αυτό το trojan, μεταφέρεται μέσω μίας κακόβουλης εφαρμογής, χρησιμοποιώντας το πακέτο com.mediawoz.gotq.apk. Αφού εγκατασταθεί, κάνει παραγγελίας από κινέζικη αγορά κινητής τηλεφωνίας, χωρίς την συγκατάθεση του χρήστη, χρεώνοντας τον προς όφελος άλλων. Επίσης, αποστέλλει σε απομακρυσμένη τοποθεσία τον αριθμό τηλεφώνου του χρήστη και πληροφορίες της συσκευής, όπως για παράδειγμα το IMEI.
- Trojan:Android/Stiniter.A: το παραπάνω trojan, έχει την δυνατότητα να εγκαταστήσει στην κινητή συσκευή άλλες εφαρμογές και στοιχεία, παρά την έγκριση του χρήστη και μπορεί να συλλέξει πληροφορίες από το κινητό τηλέφωνο, όπως αριθμό τηλεφώνου, αριθμό IMEI και τα προωθεί σε απομακρυσμένη τοποθεσία.
- Trojan-Proxy:Android/NotCompatible.A: αυτό το trojan, εγκαθίσταται στην συσκευή όταν ο χρήστης μεταβεί σε μία κακόβουλη ή παραβιασμένη ιστοσελίδα και κάνει λήψη, ζητώντας από την χρήστη την επιβεβαίωση αυτής, το πακέτο update.apk. Αφου εγκατασταθεί το πακέτο, είναι εφικτή η επικοινωνία του κακόβουλου λογισμικού με ορισμένους διακομιστές εντολών και ελέγχου, για την εκτέλεση κακόβουλων δράσεων.



Εικόνα 8: Παράδειγμα αδειών σε κακόβουλη εφαρμογή.

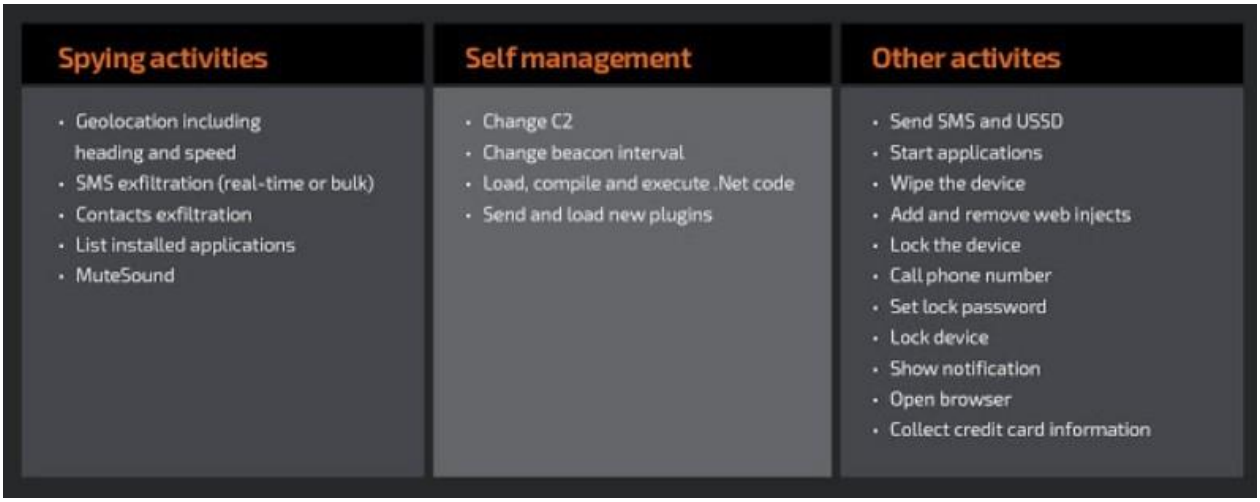


Εικόνα 9: Παράδειγμα εύρεσης κακόβουλης εφαρμογής από την google.

Ένα νέο παράδειγμα trojan είναι το Gplayed trojan, όπου τονίζεται η πολυπλοκότητα και ευελιξία του. Φαίνεται στην συσκευή ως εφαρμογή Google Store κι έχει το όνομα Google Play Marketplace. Ζητάει πολλές άδειες που αν του δωθούν έχει ουσιαστικά τον πλήρη έλεγχο της μολυσμένης συσκευής.
Η κακόβουλοι χρήστες μπορούν να προσθέσουν νέο κώδικα, επεκτείνοντας της δυνατότητες της κακόβουλης εφαρμογής, χωρίς να χρειάζεται η ενημέρωση του πακέτου στην εφαρμογή. Στέλνονται δηλαδή, κομμάτια κωδικά που εκτελούν κακόβουλες ενέργειες, τα οποία μεταγλωττίζονται κι εκτελούνται από το Gplayed, χωρίς να χρειάζεται αναβάθμιση το ίδιο, καθώς παραμένει ανεξιχνίαστο στο υπόβαθρο.

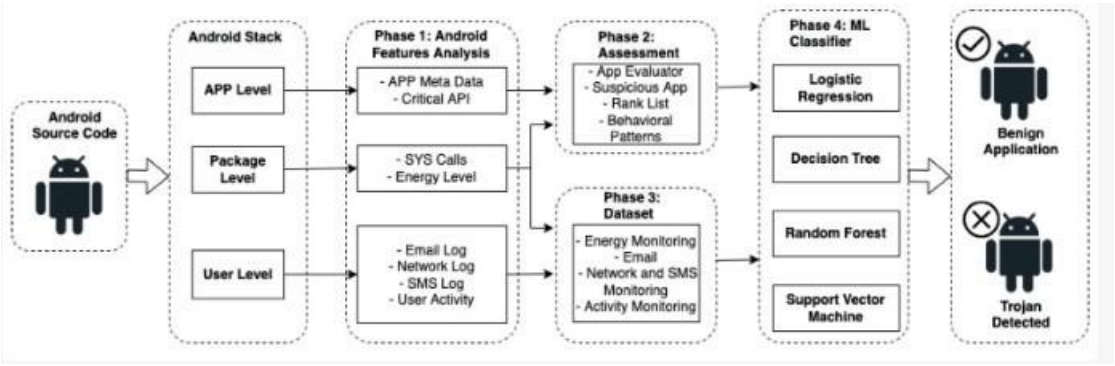
Εικόνα 10: Gplayed trojan, άδεια για ενέργειες που μπορεί να εκτελέσει.

Εκτός από τις γνωστές λειτουργίες υποκλοπής μυνημάτων, επαφών και πραγματοποίηση κλήσεων ή αποστολής SMS, το παραπάνω trojan μπορεί να ξεκινάει εφαρμογές χωρίς την άδεια του χρήστη, να προσθέτει και να αφαιρεί web injects, να υποκλέπτει πληροφορίες καρτών τραπέζης, όπως επίσης και να ορίζει νέο κωδικό κλειδώματος.
Μέσω της χρήσης κώδικα javasctript, μπορεί να προγραμματιστεί ώστε να υποκλέψει όλα τα στοιχεία που ο χρήστης γράφει σε φόρμες στο ιντερτνετ και να τα αποστείλει σε απομακρυσμένους χρήστες.



Εικόνα 11: Κακόβουλες ενέργειες του Gplayed trojan.

Από τα παραπάνω είναι φανερό πως, η εξέλιξη της τεχνολογίας δεν επιφέρει μόνο θετικά αποτελέσματα, αλλά και αρνητικές επιπτώσεις σε διάφορες πτυχές, όπως είναι η ασφάλεια του χρηστή.
Διάφορες εφαρμογές και κακόβουλα λογισμικά όπως το παραπάνω, απαιτούν και την αντίστοιχη αύξηση της ασφάλειας των συσκευών, μέσω ενημέρωσης του χρήστη πριν την εγκατάσταση κακόβουλης εφαρμογής, προστασίας του χρήστη, εφόσον έχει ήδη αντικατασταθεί η κακόβουλη εφαρμογή και η διαγραφή της.



Εικόνα 12: Εύρεση trojan μέσω multi-layer ιβριδικό σύστημα.

2.7 Phishing

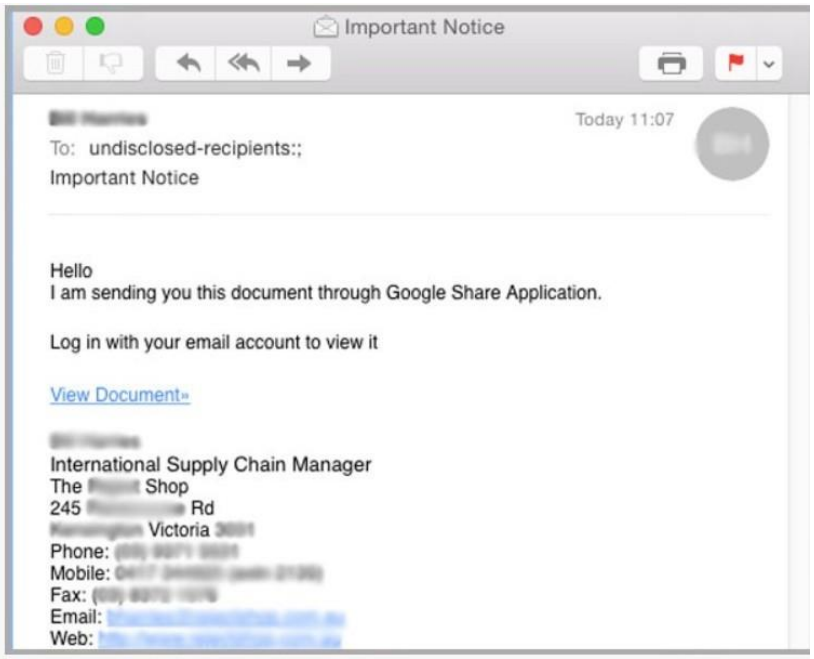
Το phising είναι τρόπος εξαπάτησης χρήστη στο διαδίκτυο. Ο θύτης δημιουργώντας ιστοσελίδες ή εφαρμογές που φαίνονται αξιόπιστες, προσπαθεί να εξαπατήσει το θύμα με σκοπό την απόκτηση προσωπικών δεδομένων, όπως κωδικών πρόσβασης σε e-mails, διάφορες ιστοσελίδες και τραπεζικές κάρτες.

Το phishing ξεκίνησε με το phone breaking, δηλαδή επιθέσεις στα τηλεφωνικά δίκτυα, ακούγοντας προσωπικές συζητήσεις και λαμβάνοντας κρίσιμες πληροφορίες για τους συμμετέχοντες. Έπειτα εμφανίστηκαν οι τεχνικές phishing μέσω e-mail και προσωπικών μνημάτων SMS. Δηλαδή, ερχόταν e-mail ή προσωπικό μήνυμα στο θύμα, στο οποίο ο θύτης φαινόταν ως αξιόπιστο στέλεχος κάποιας εταιρίας ή οργανισμού. Ζητούσε κρίσιμες πληροφορίες, όπως κωδικοί πρόσβασης ή έστελνε παραπλανητικούς συνδέσμους, όπου οδηγούσαν σε ιστοσελίδες επιφανειακά αξιόπιστες και πολλές φορές ίδιες με τις αυθεντικές και το θύμα έβαζε προσωπικούς κωδικούς πρόσβασης και λογαριασμών, οι οποίοι με την σειρά τους στέλνονταν με e-mail στο θύμα ή αποθηκεύονταν σε κάποια βάση δεδομένων όπου είχε αυτός πρόσβαση.
Έπειτα εμφανίστηκαν άλλες μέθοδοι, όπως το IDN spoofing, οι οποίες είναι πιο δύσκολες στην αναγνώρισή τους. Το IDN spoofing με χειρισμό των International Domain Names (IDN), δημιουργούνται ίδια URLs όπου οδηγούνται σε άλλες ιστοσελίδες. Με χρήση javasctript, εικόνων και flashplayer, οι hacker εξαπατούν τις anti-phishing ασφάλειες, δηλαδή καλύπτοντας το αληθινό URL, με μία εικόνα ή ένα ψεύτικο.
Τέλος άλλες μέθοδοι χρησιμοποιούν αναδυόμενα παράθυρα, πολλαπλές καρτέλες και δημιουργία ψεύτικων δημοσίων δικτύων σε κοινόχρηστους χώρους με πολλά άτομα υποκλέπτοντας στοιχεία του χρήστη που θα συνδεθεί.

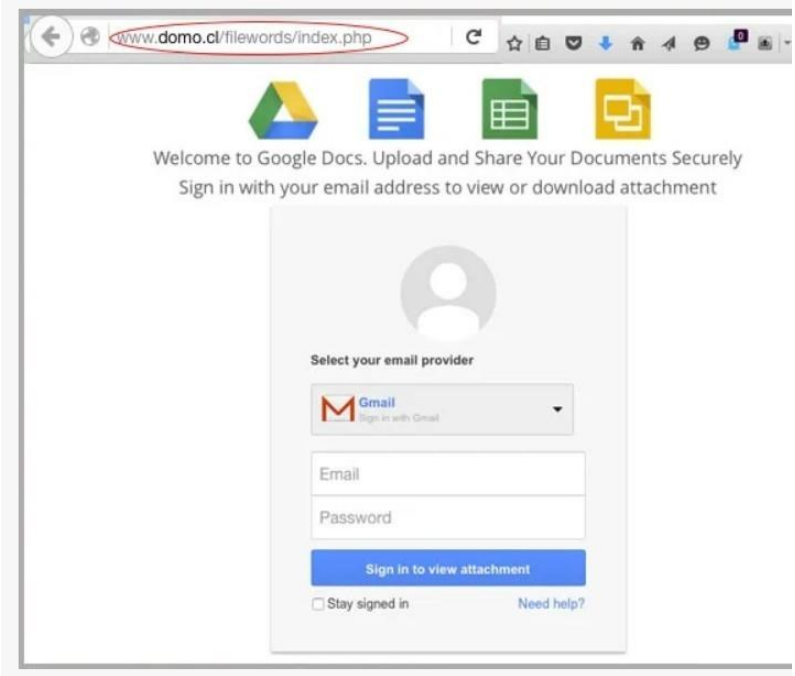
Η πρώτη περιγραφή της απάτη με τρόπο phishing καταγράφεται το 1987, στο διεθνές συνέδριο χρηστών της HP, όπου ήταν ο προάγγελος των πρώτων καταγεγραμμένων απατών (1995). Συγκεκριμένα, οι θύτες, δημιουργούσαν ψεύτικους λογαριασμούς στην υπηρεσία διαδικτυακής επικοινωνίας AOL, υποδυόμενοι τους υπάλληλους της εταιρίας, έστελναν προσωπικά μηνύματα στους χρήστες και ζητώντας κωδικούς πρόσβασης και αριθμούς τραπεζικών λογαριασμών με πρόφαση ότι υπάρχει πρόβλημα με το λογαριασμό τους. Η εταιρία τότε είχε 3.5 εκατομμύρια λογαριασμούς.

Έπειτα, άλλες απάτες phishing βρέθηκε σε εταιρίες όπως η Google Inc. η οποία έχει σήμερα πάνω από 200 εκατομμύρια χρήστες στο gmail. Η Google Inc. το 2010 κατηγόρησε την Κίνα ότι υπάρχουν hackers με βάση το Jinan της Κίνας και πραγματοποιούσαν επιθέσεις προς χρήστες της υπηρεσίας gmail, ανάμεσα στους οποίους ήταν προσωπικό από την αμερικάνικη κυβέρνηση και στρατό, εξαπατώντας τους για την κλοπή των προσωπικών κωδικών τους πρόσβασης. Η κινέζικη κυβέρνηση αρνήθηκε τις κατηγορίες και το FBI δεν μπόρεσε να δράσει παραπάνω, επειδή δεν υπήρχαν επιτυχημένες επιθέσεις απέναντι σε κυβερνητικό ή στρατιωτικό προσωπικό. Στην συνέχεια, σε τηλεοπτικό προσωπικό αναφέρθηκαν στοιχεία που ενοχοποιούν την κινέζικη κυβέρνηση και τον στρατό.

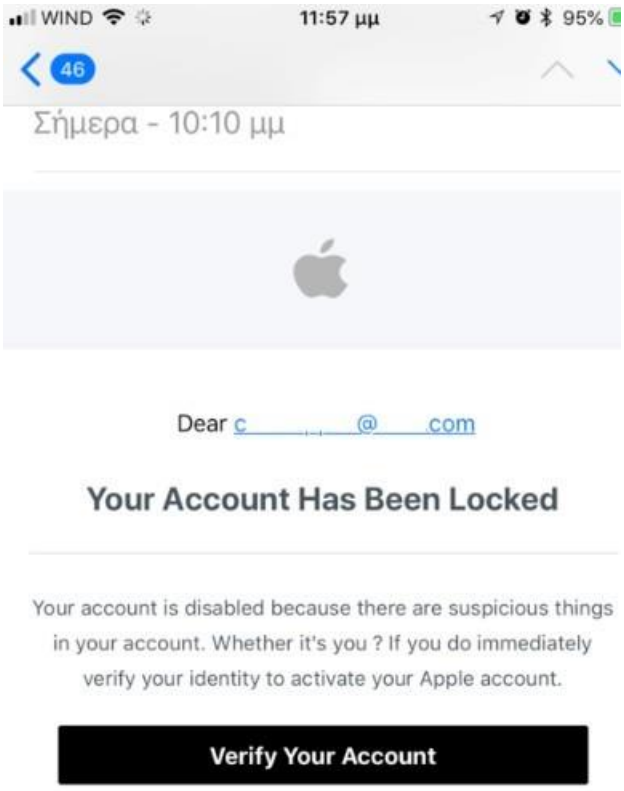
Εταιρίες όπως η Lockheed Martin, η Microsoft και η Yahoo, αν και δέχονται επιθέσεις phishing, σύμφωνα με την Google, προτιμούν να μην το δημοσιοποιήσουν, έτσι ώστε να μην υπάρξει κακή φήμη στην ασφάλεια του ονόματός τους.



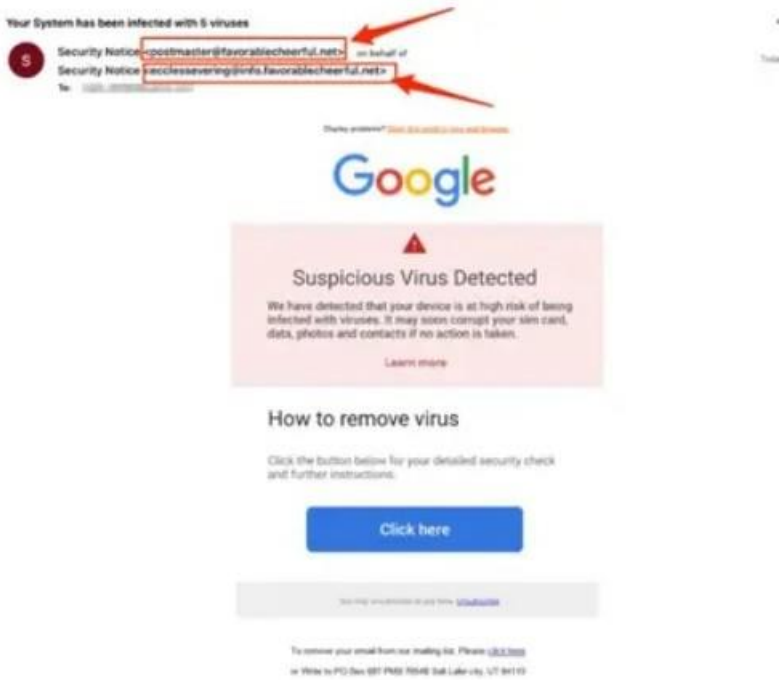
Εικόνα 13: E-mail με σκοπό την εξαπάτηση μέσω phishing (Google).



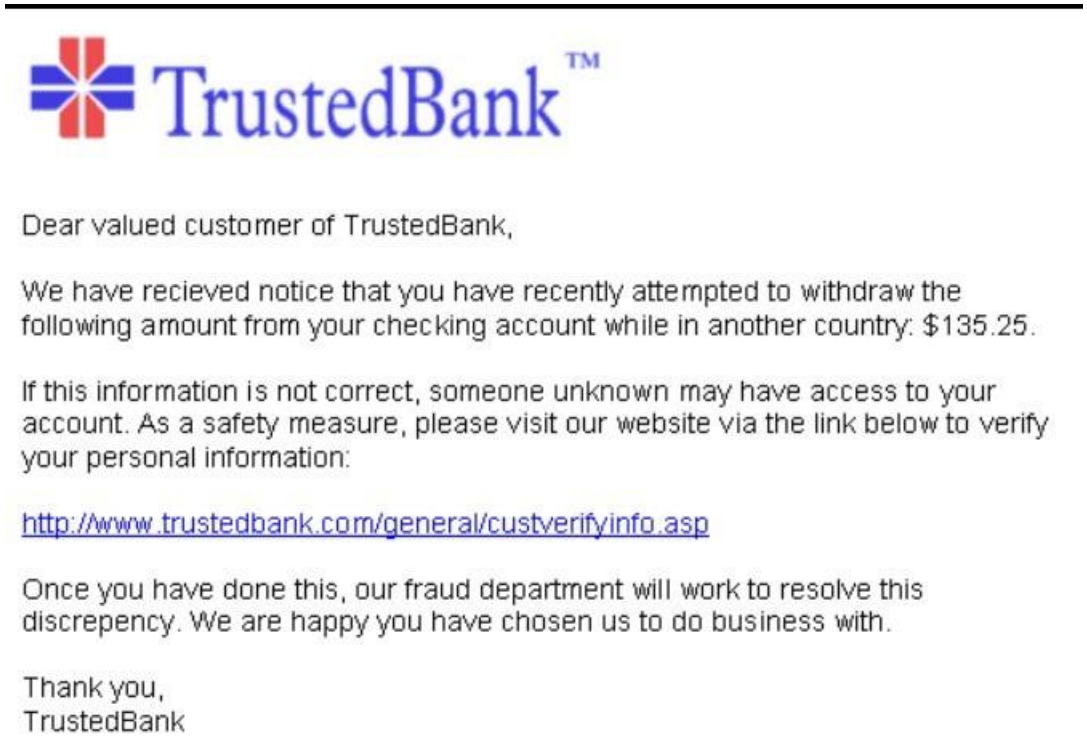
Εικόνα 14: Ψευδή είσοδος σε επίσημη ιστοσελίδα – Phishing



Εικόνα 15: Απάτη phishing (Apple).



Εικόνα 16: Απάτη phishing (Google).



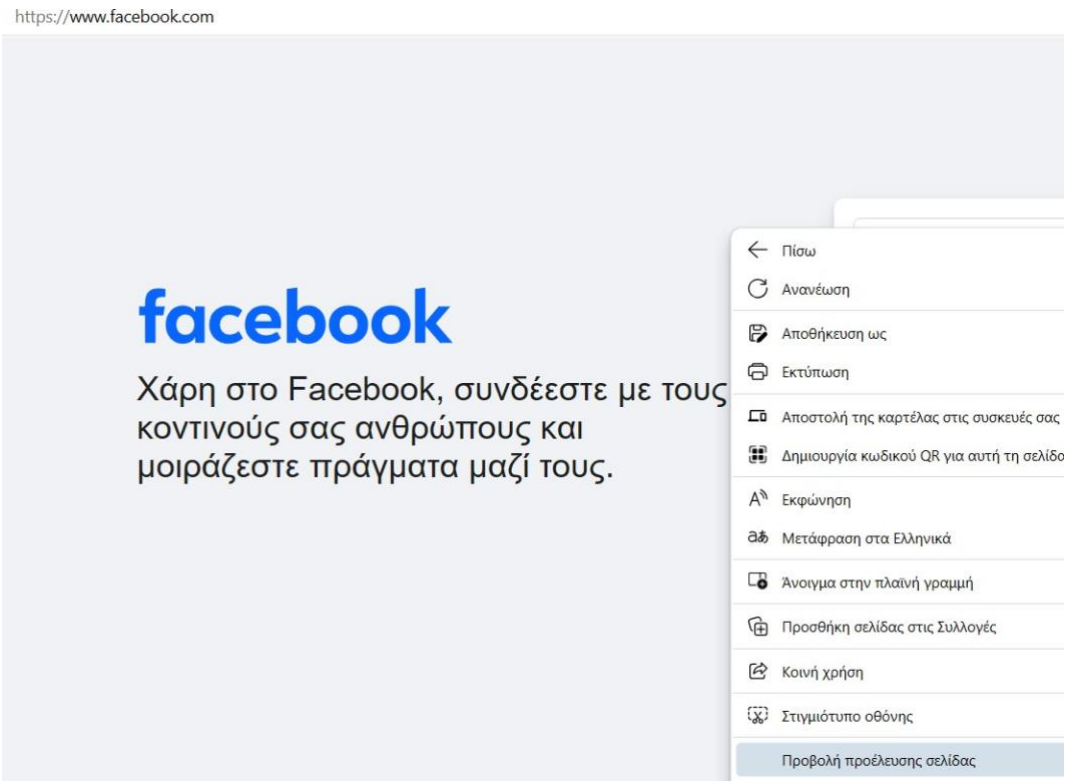
Εικόνα 17: Απάτη phishing (TrustedBank).

Η επιτυχία του Phishing στηρίζεται στην έλλειψη γνώσεων του θύματος, στην έλλειψη προσοχής του θύματος και στην οπτική εξαπάτηση, δηλαδή ομοιότητα που έχουν η ψεύτικη με την αξιόπιστη ιστοσελίδα.
Το phishing όπως προαναφέρθηκε στηρίζεται σε τεχνικές που βασίζονται σε δημιουργία ιστοσελίδων, όπου χρησιμοποιούνται γλώσσες προγραμματισμού όπως οι html,css,javasctript και php. Ο μέσος χρήστης δεν γνωρίζει πως λειτουργούν αυτές ή γενικά πως λειτουργεί μία ιστοσελίδα και δεν μπορεί να αντιληφθεί πότε πέφτει θύμα εξαπάτησης.
Ακόμη όμως κι αν έχει γνώση, πολλές φορές δεν θα προσέχει τα σημάδια, λόγω κεκτημένης ταχύτητας ή μπορεί να είναι απασχολημένος με άλλες εργασίες.

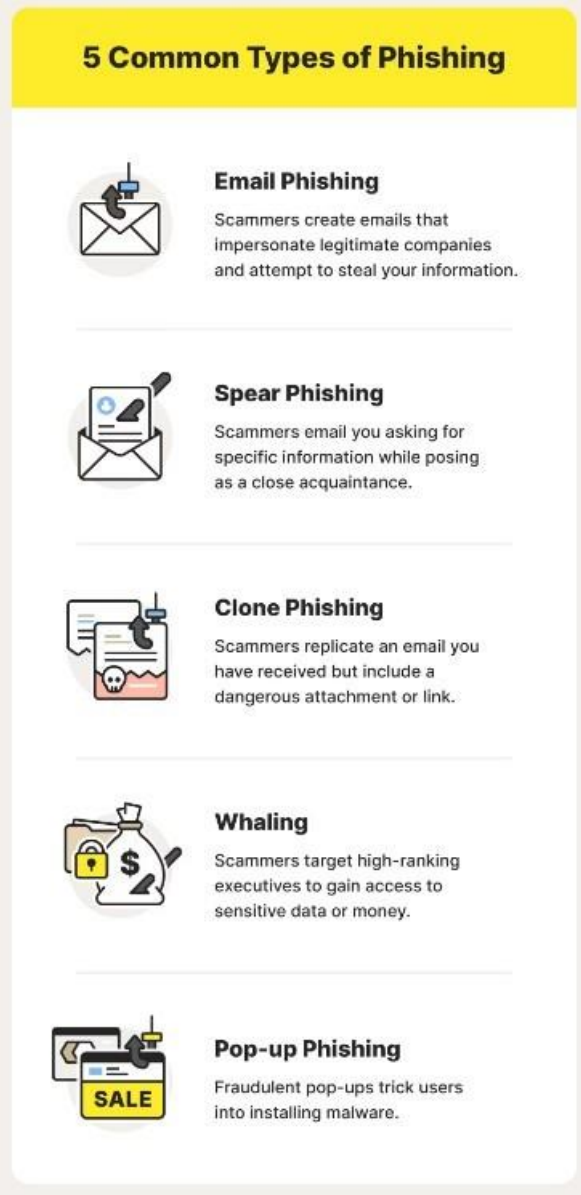
Οι κύριες παραπλανητικές περιέχουν:

- Παραπλανητικό κείμενο: Χρησιμοποιείται διαφορετική σύνταξη λέξεων facebook – fasebook, αναγραμματισμός λέξεων youtube – yutoube ή χρήση διαφορετικών γραμμάτων που είναι ίδια μικρό L με κεφαλαίο i. Έτσι ο θύτης μπορεί να μπερδέψει το θύμα να εισέρθει στο ψεύτικο URL.
- Παραπλανητικές εικόνες και design: Χρησιμοποιούνται οι ίδιες εικόνες που έχουν τα αξιόπιστα σάιτ, το οποίο είναι αρκετά εύκολα με την χρήση των Html και javasctript, όπως επίσης και το ακριβώς ίδιο design, το οποίο μπορεί να γίνει με μία αντιγραφή του κώδικα της ιστοσελίδας που έχει πρόσβαση ο οποιοδήποτε μέσω του browser.
- Παραπλανητικά μηνύματα: Αυτά τα μηνύματα περιέχουν εντολές πληρωμής ή εισόδου σε μία ιστοσελίδα με την πρόφαση κάποιου προβλήματος στον λογαριασμό του χρήστη ή κάποιας ποινής εις βάρος του χρήστη.

Με χρήση των παραπάνω, ο θύτης αναγκάζει το θύμα να εισέρθει στην ψεύτικη και επικίνδυνη ιστοσελίδα, να δώσει τα προσωπικά του στοιχεία (πχ κωδικοί πρόσβασης μέσων κοινωνικής δικτύωσης, emails, τραπεζικών λογαριασμών) και να γίνει κλοπή αυτών.


https://www.facebook.com
facebook
Χάρη στο Facebook, συνδέεστε με τους κοντινούς σας ανθρώπους και μοιράζεστε πράγματα μαζί τους.
Πίσω
Ανανέωση
Αποθήκευση ως
Εκτύπωση
Αποστολή της καρτέλας στις συσκευές σας
Δημιουργία κωδικού QR για αυτή τη σελίδο
Εκφώνηση
Μετάφραση στα Ελληνικά
Άνοιγμα στην πλαϊνή γραμμή
Προσθήκη σελίδας στις Συλλογές
Κοινή χρήση
Στιγμιότυπο οθόνης
Προβολή προέλευσης σελίδας


view-source:https://www.facebook.com
Αναδίπλωση γραμμών
<!DOCTYPE html>
<html lang="el" id="facebook" class="no_js">
<head><meta charset="utf-8" /><meta name="referrer" content="origin-when-crossorigin" id="meta_refer
<link type="text/css" rel="stylesheet" href="https://static.xx.fbcdn.net/rsrc.php/v3/ye/l/0,cross/LO
<link type="text/css" rel="stylesheet" href="https://static.xx.fbcdn.net/rsrc.php/v3/yy/l/0,cross/Li
<link type="text/css" rel="stylesheet" href="https://static.xx.fbcdn.net/rsrc.php/v3/yV/l/0,cross/Bm
<link type="text/css" rel="stylesheet" href="https://static.xx.fbcdn.net/rsrc.php/v3/y6/l/0,cross/sL
<script src="https://static.xx.fbcdn.net/rsrc.php/v3/yJ/r/sGcGGNWA3Bv.js?_nc_x=Ij3Wp8lg5Kz" data-boo
<script nonce="vb7uyX4O">requireLazy(["HasteSupportData"],function(m){m.handle({"clpData":{"1744178"
<script>requireLazy(["HasteSupportData"],function(m){m.handle({"bxData":{"875231":{"uri":"https:\/\/
<script>requireLazy(["InitialJSLoader"], function(InitialJSLoader) {InitialJSLoader.loadOnDOMContent
<script>requireLazy(["TimeSliceImpl","ServerJS"],function(TimeSlice,ServerJS){var s=(new ServerJS())
<script>now_inl=(function(){var p=window.performance;return p&&p.now&&p.timing&&p.timing.navigationS
<link rel="preload" href="https://static.xx.fbcdn.net/rsrc.php/v3/y8/l/0,cross/NTGX1ZDE_he.css?_nc_x
<link rel="preload" href="https://static.xx.fbcdn.net/rsrc.php/v3/ye/l/0,cross/LOZiXEdsFNx.css?_nc_x
<link rel="preload" href="https://static.xx.fbcdn.net/rsrc.php/v3/yy/l/0,cross/LiHTRP8uipK.css?_nc_x
<link rel="preload" href="https://static.xx.fbcdn.net/rsrc.php/v3/yV/l/0,cross/Bm4uCSyRllh.css?_nc_x
<link rel="preload" href="https://static.xx.fbcdn.net/rsrc.php/v3/y6/l/0,cross/sLmoPVxkk8Z.css?_nc_x
<link rel="preload" href="https://static.xx.fbcdn.net/rsrc.php/v3ir-O4/y1/l/el_GR/NYVXZdZ4Ltt.js?_nc
<link rel="preload" href="https://static.xx.fbcdn.net/rsrc.php/v3/yt/r/0mE-_d-u_Zw.js?_nc_x=Ij3Wp8lg
<link rel="preload" href="https://static.xx.fbcdn.net/rsrc.php/v3/yQ/r/3s0oqSI3NLx.js?_nc_x=Ij3Wp8lg
<link rel="preload" href="https://static.xx.fbcdn.net/rsrc.php/v3/yX/r/Q1COZ4Pa6TU.js?_nc_x=Ij3Wp8lg
<script>window.__bigPipeCtor=now_inl();requireLazy(["BigPipe"],function(BigPipe){define("__bigPipe",
<script nonce="vb7uyX4O">(function(){var n=now_inl();requireLazy(["__bigPipe"],function(bigPipe){big
<script nonce="vb7uyX4O">requireLazy(["__bigPipe"],(function(bigPipe){bigPipe.onPageletArrive({displ
<script>requireLazy(["__bigPipe"],function(bigPipe){bigPipe.setPageID("7341018319216363159")});</scr
<script nonce="vb7uyX4O">requireLazy(["__bigPipe"],(function(bigPipe){bigPipe.onPageletArrive({displ



Εικόνα 20: Οι πέντε πιο κοινές επιθέσεις phishing.

Οι κύριες τεχνικές αντιμετώπισης του phishing περιλαμβάνουν:

- Ενημέρωση: Ο κάθε χρήστης πρέπει αρχικά από μόνος του να ενημερώνεται για αυτές τις τεχνικές εξαπάτησης και να μάθει να προστατεύει τον εαυτό του, αναγνωρίζοντας τις ψεύτικες ιστοσελίδες και τεχνικές εξαπάτησης. Υπάρχουν διάφορες ιστοσελίδες που περιέχουν πληροφορίες γι αυτές τις κακόβουλες τεχνικές και πως να αναγνωριστούν.
- Προσοχή: Ο κάθε χρήστης πρέπει να είναι προσεκτικός όταν χρησιμοποιεί τους κωδικούς πρόσβασής του και να γνωρίζει που πρόκυτε να συνδεθεί. Επίσης, πρέπει να βλέπει ποιες ιστοσελίδες χρησιμοποιούν https:// πρωτόκολλα και ποια είναι η προέλευση τους.
- Προγράμματα περιήγησης: Υπάρχουν διάφορα προγράμματα περιήγησης που μπορούν να εγκατασταθούν, τα οποία αναγνωρίζουν παραπλανητικά μηνύματα και ιστοσελίδες και ενημερώνουν τον χρήστη.
- Λογισμικά προστασίας: Υπάρχουν επίσης διάφορα λογισμικά προστασίας από ιούς και προγράμματα κατασκοπίας. Επίσης, υπάρχουν anti-spam λογισμικά, ώστε να μην λαμβάνονται από τον χρήστη e-mails που στέλνονται μαζικά κι έχουν σκοπό την εξαπάτησή του.
- Πρόσθετα προστασίας: Υπάρχουν adds-in σε κάθε browser, όπου εντοπίζουν phishing scripts στις ιστοσελίδες προστατεύοντας κι ενημερώνοντας τον χρήστη.
- Safe browsing advisor: Διάφορα anti-virus έχουν αυτήν την επιλογή, όπου ενημερώνουν τον χρήστη με τις αξιολογήσεις που υπάρχουν για κάθε σάιτ που θέλει να επισκεφτεί.

Εικόνα 21: Τρόποι αντίδρασης σε phishing e-mail.

Εικόνα 22: Οι 10 καλύτερες συμβολές ενάντια στο phishing.

2.8 Στατιστικά Phishing

Οι επιθέσεις τύπου phishing λόγω της ευκολίας δημιουργίας τους κι αποφυγής αναγνώρισής τους, αυξάνονται τα τελευταία χρόνια. Στην παρακάτω εικόνα, φαίνεται σε μόλις 3 χρόνια ότι παρατηρήθηκε εφταπλασιασμός των επιθέσεων phishing.
Οι κύριες λέξεις κλειδιά των επιθέσεων μέσω E-mail περιέχουν τιμολόγιο, μήνυμα, απαιτείται, αρχείο, αίτηση, έγγραφο, επαλήθευση, δράση, eFax.

YEAR	NUMBER OF ATTACKS OBSERVED
2019	779,200
2020	1,845,814
2021	2,847,773
2022	4,744,699

Εικόνα 23: Παρατηρούμενες επιθέσεις Phishing.

Τα μεγαλύτερα ποσοστά αυτών των επιθέσεων αφορούν τομείς/οργανισμούς εκπαίδευσης, οικονομικών και τεχνολογίες πληροφόρησης.

SECTOR	CLICK RATE
Education	27.6%
Finance & Insurance	26.6%
Information Technology	25.6%
Agriculture & Food	21.2%
Service Providers	20.2%
Not-for-profit	16.3%
Energy	14.8%
Manufacturing	13.4%
Public Sector	10.4%
Transport	7.5%
Retail	7.2%
Healthcare	5.6%

Εικόνα 24: Ποσοστά επιθέσεων ανά οργανισμό.

Το πρώτο εξάμηνο του 2022 παρατηρήθηκε ότι οι επιθέσεις έχουν στόχο την κλοπή χρημάτων, αφού επικεντρώνονται κυρίως σε τράπεζες και διαδικτυακές συναλλαγές.

INDUSTRY	PERCENTAGE OF PHISHING ATTACKS
Banks	27.7%
Online Shops	17.2%
NGOs	10.7%
Educational Institutions	9.3%
Healthcare	9.1%
Governmental Organizations	8.2%
Telecom	7.5%
IT Services	6.6%
Insurance	2.4%
Others	1.3%

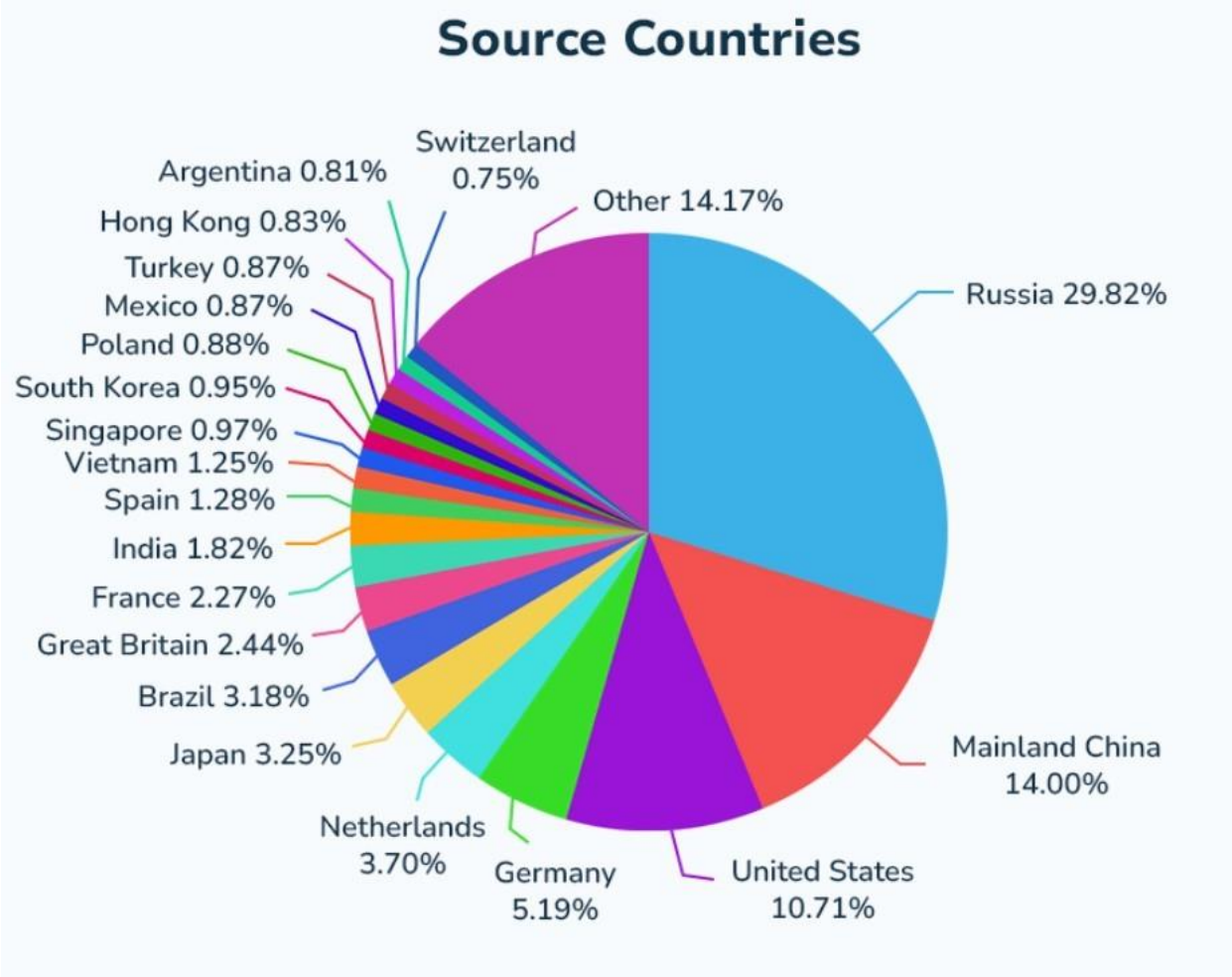
Εικόνα 25: Ποσοστιαίες επιθέσεις το πρώτο εξάμηνο του 2022.

Οι κύριες χώρες επιθέσεων ήταν οι βόριες χώρες όπως Ολλανδία,Ρωσία και Μολδαβία, ενώ μικρότερα ποσοστά παρατηρούνται σε Ευρωπαϊκές χώρες. Στις πρώτες θέσεις ήταν η Γερμανία και η Αγγλία.

Country	Number of Emails	Percentage
Netherlands	68,908,098	17.6777%
Russia	53,211,482	13.6509%
Moldova	27,192,790	6.9760%
USA	24,135,668	6.1918%
Thailand	21,935,110	5.6272%
China	14,574,632	3.7390%
Germany	13,486,816	3.4599%
Great Britain	11,394,190	2.9231%
India	11,311,772	2.9019%
Vietnam	11,231,432	2.8813%
Other Countries	2,157,990	0.5536%

Εικόνα 26: Επιθέσεις phishing ανά χώρα.

Το παραπάνω εξηγείται από την παρατήρηση των χωρών που επιτίθονται μέσω phishing. Στην πρώτη θέση αυτών είναι η Ρωσία, οπότε και οι το μεγαλύτερο ποσοστό επιθέσεων θα αφορά τις Βόρειες χώρες, ενώ ακολουθούν οι Κίνα και η ΗΠΑ.



Εικόνα 27: Χώρες όπου οι Hackers ξεκινούν phishing attacks.

Οι hackers μιμούνται κυρίως τις εταιρίες Linkedln, DHL και Google, ενώ ακολουθεί η Microsoft. Η προτίμηση αυτών των εταιριών προκύπτει λόγω των χρηστών που χρησιμοποιούν αυτές.

COMPANY	PERCENTAGE OF ALL BRANDED PHISHING ATTEMPTS GLOBALLY
LinkedIn	52%
DHL	14%
Google	7%
Microsoft	6%
FedEx	6%
WhatsApp	4%
Amazon	2%
Maersk	1%
AliExpress	0.8%
Apple	0.8%

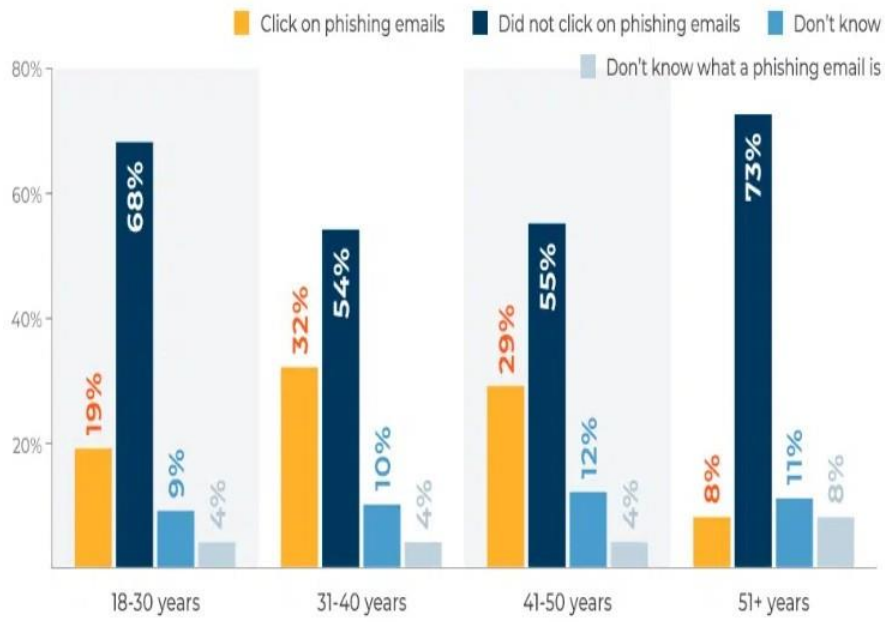
Εικόνα 28: Εταιρίες που μιμούνται οι hackers για phishing.

Οι κύριες συνέπειες υψηλόβαθμων στελεχών που δέχτηκαν Phishing είναι η υποκλοπή προσωπικών δεδομένων, δεδομένων τραπεζικών λογαριασμών και η εγκατάσταση κακόβουλων ransoware.

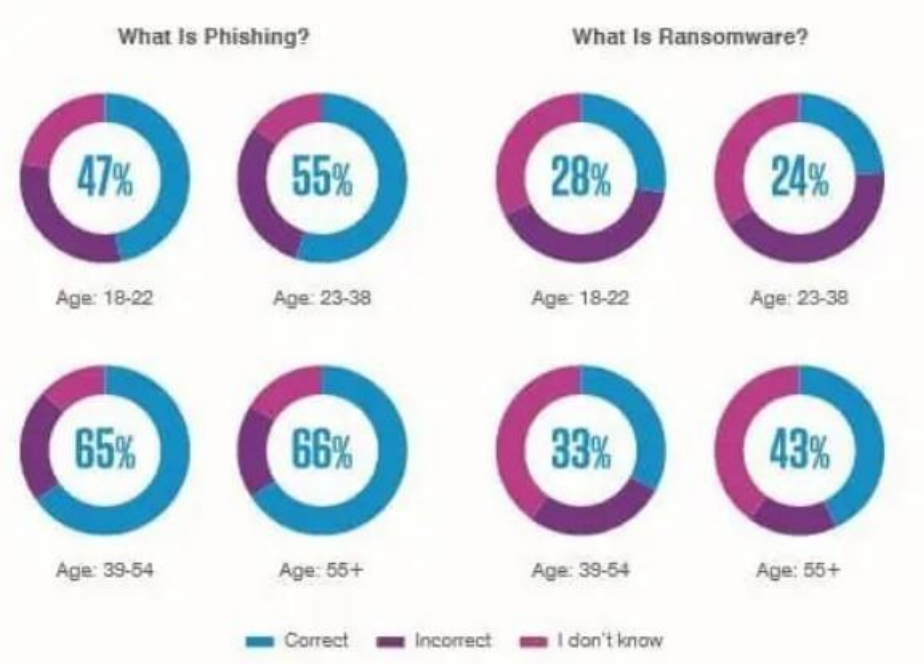
CONSEQUENCE OF PHISHING	PERCENTAGE OF SECURITY LEADERS WHO EXPERIENCE IT
Lost/stolen data	60%
Compromised credentials and accounts	50%
Ransomware	45%
Other malware	30%
Direct financial loss	20%

Εικόνα 29: Κύριες συνέπειες phishing.

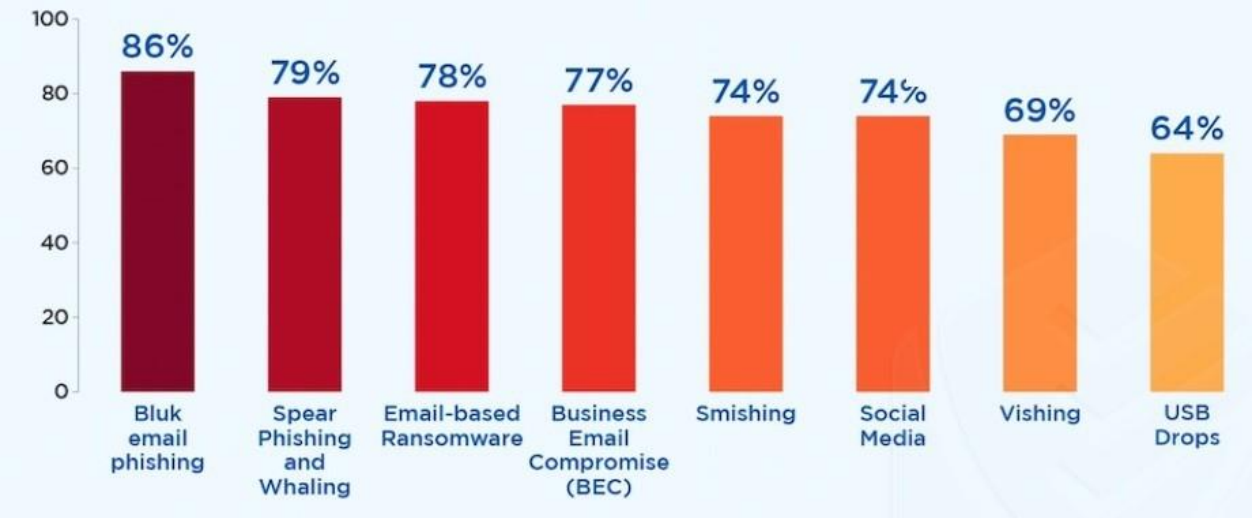
Το μεγαλύτερο ποσοστό που δεν γνωρίζουν από επιθέσεις phishing και μπαίνουν σε κακόβουλους συνδέσμους είναι 31-40 χρονών, ενώ οι ηλικίες που δεν μπαίνουν είναι 18-30 ετώνκαι 51+ ετών λόγω γνώσης του phishing.



Εικόνα 30: Ποσοστά αντίδρασης σε διάφορες ηλικίες σε επιθέσεις phishing.



Εικόνα 31: Ποσοστά ανά ηλικία για την γνώση περί phishing και ransomware.



Εικόνα 32: Τύποι phishing επιθέσεων το 2021.

Στην παρακάτω εικόνα φαίνονται την περίοδο 2018 έως 2022 τα χρήματα που έκλεψαν hackers μέσω επιθέσεων phishing στις USA.

Εικόνα 33: Επιθέσεις phishing και ποσά χρημάτων που εκλάπηκαν στις ΗΠΑ τα έτη 2018-2022.

3. Ιδιωτικότητα στα Smartphones

3.1 Ορισμός και σημασία της ιδιωτικότητας

Η ιδιωτικότητα αναφέρεται στην ικανότητα ενός συστήματος ή ενός προγράμματος να αναγνωρίζει τους χρήστες και να παρέχει πρόσβαση βάσει των διακριτικών χαρακτηριστικών και των δικαιωμάτων που τους έχουν ανατεθεί. Στο πλαίσιο των smartphones, η ιδιωτικότητα παίζει έναν ζωτικό ρόλο στη διασφάλιση της ασφάλειας και της προστασίας των προσωπικών δεδομένων. Η διατήρηση της ιδιοτικότητας στα smartphones εξασφαλίζει ότι μόνο εξουσιοδοτημένοι χρήστες έχουν πρόσβαση σε προσωπικές πληροφορίες και επιτρέπει στους χρήστες να διαχειρίζονται τις ρυθμίσεις απορρήτου, σύμφωνα με τις προτιμήσεις τους. Επιπλέον, η διασφάλιση της ιδιοτικότητας, εμποδίζει την ανεπιθύμητη πρόσβαση ή χρήση των προσωπικών δεδομένων από μη εξουσιοδοτημένα πρόσωπα ή εφαρμογές. Ως εκ τούτου, η ιδιωτικότητα στα smartphones είναι κρίσιμη για τη διατήρηση της ασφάλειας και της εμπιστοσύνης των χρηστών στη χρήση των συσκευών τους.

1. **Αναγνώριση χρηστών:**
    - Η χρήση της ιδιοτικότητας, επιτρέπει την αναγνώριση αυθεντικών χρηστών, μέσω διαφόρων μεθόδων, όπως οι κωδικοί πρόσβασης, τα αναγνωριστικά δακτυλικών αποτυπωμάτων και η αναγνώριση προσώπου.
    - Η εφαρμογή πολυεπίπεδων μεθόδων αυθεντικοποίησης ενισχύει την ασφάλεια των smartphones και εμποδίζει την παράνομη πρόσβαση σε προσωπικά δεδομένα.
    - Κάθε μέθοδος αυθεντικοποίησης έχει τα πλεονεκτήματά της και τις ιδιαιτερότητές της, μεριμνώντας για την αποτελεσματική προστασία των πληροφοριών των χρηστών.
    - Ωστόσο, η σωστή εφαρμογή και διαχείριση αυτών των μεθόδων απαιτεί προσοχή, καθώς μια αδύναμη αυθεντικοποίηση, μπορεί να διακινδυνεύσει την ασφάλεια του συστήματος και των προσωπικών δεδομένων των χρηστών.
2. **Περιορισμός δικαιωμάτων πρόσβασης:**
    - Μέσω της ιδιοτικότητας, είναι δυνατός ο καθορισμός και ο περιορισμός των δικαιωμάτων πρόσβασης για κάθε χρήστη, ανάλογα με τις ανάγκες του και τον ρόλο του.
    - Αυτό επιτυγχάνεται μέσω της διαχείρισης των δικαιωμάτων πρόσβασης και της οριοθέτησης των επιπέδων πρόσβασης σε διάφορες λειτουργίες και πληροφορίες του συστήματος.
    - Με την εφαρμογή αυτής της αρχής, οι διαχειριστές μπορούν να ελέγχουν ποιοι χρήστες έχουν πρόσβαση σε ποιες πληροφορίες, προστατεύοντας έτσι την εμπιστευτικότητα και την ασφάλεια των δεδομένων.
    - Επιπλέον, η διαχείριση των δικαιωμάτων πρόσβασης επιτρέπει την προσαρμογή των δικαιωμάτων και των επιπέδων πρόσβασης σε περιβάλλοντα με πολλαπλούς χρήστες, προσφέροντας έτσι ευελιξία και προστασία σε διαφορετικές ανάγκες και σενάρια χρήσης..

3. **Διαχείριση προσωπικών δεδομένων:**
    - Η ιδιωτικότητα διευκολύνει τη διαχείριση των προσωπικών δεδομένων, ελέγχοντας ποιος έχει πρόσβαση σε ευαίσθητες πληροφορίες και διασφαλίζοντας τη συμμόρφωση προς τις νομικές απαιτήσεις.
    - Αυτό σημαίνει ότι οι οργανισμοί και οι χρήστες, μπορούν να διαχειρίζονται τα προσωπικά δεδομένα με πιο αποτελεσματικό τρόπο, προστατεύοντάς τα από ανεπιθύμητη πρόσβαση και χρήση.
    - Επιπλέον, η συμμόρφωση με τις νομικές απαιτήσεις, όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων της Ευρωπαϊκής Ένωσης (GDPR) και άλλες νομοθεσίες περί προστασίας δεδομένων, είναι ζωτικής σημασίας για τη διατήρηση της εμπιστοσύνης των χρηστών και την αποφυγή πιθανών κυρώσεων ή κινδύνων για την οργάνωση.
    - Έτσι, η ιδιωτικότητα συμβάλλει στη διασφάλιση, όχι μόνο της ασφάλειας των δεδομένων, αλλά και της νομικής συμμόρφωσης και της επιχειρησιακής ακεραιότητας.
4. **Αυξημένη ασφάλεια:**
    - Με τη χρήση πολυεπίπεδων μεθόδων ιδιοτικότητας, όπως η διπλή πιστοποίηση και η αναγνώριση προσώπου, επιτυγχάνεται αυξημένο επίπεδο ασφάλειας.
    - Η συνδυασμένη χρήση πολλών τεχνικών αυθεντικοποίησης και πιστοποίησης ενισχύει την προστασία από ανεπιθύμητη πρόσβαση, καθιστώντας πιο δύσκολη την παραβίαση των συστημάτων και την αντιγραφή των δεδομένων.
    - Αυτό επιφέρει ένα αίσθημα ασφάλειας, τόσο στους χρήστες όσο και στους οργανισμούς, ενισχύοντας την εμπιστοσύνη στα πληροφοριακά συστήματα και τις υπηρεσίες.
5. **Αντίδραση σε καταστάσεις κινδύνου:**
    - Η ιδιωτικότητα επιτρέπει την άμεση αντίδραση σε καταστάσεις κινδύνου, όπως απώλεια του smartphone, μέσω αντικλεπτικών λειτουργιών.
    - Η δυνατότητα απομακρυσμένης διαγραφής δεδομένων ή η απενεργοποίηση της συσκευής από απόσταση αποτελούν σημαντικά μέσα για την προστασία των προσωπικών δεδομένων και την αποτροπή μη εξουσιοδοτημένης πρόσβασης στις πληροφορίες.

Συνολικά, η ιδιωτικότητα αντιπροσωπεύει ένα κρίσιμο κομμάτι των μέτρων ασφαλείας στα smartphones, διασφαλίζοντας όχι μόνο την αυθεντικότητα του χρήστη αλλά και την αποτελεσματική προστασία των προσωπικών του δεδομένων. Από την εφαρμογή τεχνολογικών μεθόδων ασφαλείας όπως η διπλή πιστοποίηση και η αναγνώριση προσώπου μέχρι την ενίσχυση της ευαισθητοποίησης των χρηστών, η ιδιωτικότητα ,διασφαλίζει την αποτελεσματική προστασία του ατόμου και των προσωπικών του πληροφοριών.

3.2 Πώς η ιδιωτικότητα προσθέτει επιπλέον επίπεδο προστασίας

Η ενσωμάτωση της ιδιοτικότητας στα smartphones, αποτελεί κρίσιμο στοιχείο που προσθέτει επιπλέον επίπεδο προστασίας, ενισχύοντας την ασφάλεια των συσκευών και των προσωπικών δεδομένων των χρηστών. Οι παρακάτω πτυχές αναδεικνύουν πώς η ιδιωτικότητα συνεισφέρει σημαντικά στην ενίσχυση της ασφάλειας:

1. **Αναγνώριση χρηστών με υψηλή ακρίβεια:**
    - Η ιδιωτικότητα επιτρέπει τη χρήση προηγμένων μεθόδων αναγνώρισης, όπως οι αισθητήρες δακτυλικών αποτυπωμάτων, οι τεχνολογίες αναγνώρισης προσώπου, και οι αισθητήρες ιριδίων.
    - Αυτές οι τεχνολογίες παρέχουν υψηλό επίπεδο ακρίβειας, εμποδίζοντας αποτελεσματικά την πρόσβαση από μη εξουσιοδοτημένα άτομα.
    - Μέσω αυτών των προηγμένων μεθόδων αναγνώρισης, εξασφαλίζεται ότι μόνο οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στις συσκευές και τα προσωπικά δεδομένα τους.
2. **Διπλή πιστοποίηση για επιπλέον ασφάλεια:**
    - Η ιδιωτικότητα επιτρέπει τη χρήση της διπλής πιστοποίησης, συνδυάζοντας διάφορες μεθόδους αναγνώρισης όπως δακτυλικά αποτυπώματα και κωδικούς πρόσβασης.
    - Αυτό δημιουργεί ένα επιπρόσθετο εμπόδιο για πιθανούς εισβολείς. Η συνδυασμένη χρήση πολλαπλών μεθόδων επιβεβαίωσης αυξάνει το επίπεδο ασφάλειας και δυσκολεύει τους ανεπιθύμητους χρήστες να προσπεράσουν την προστασία του συστήματος.
3. **Προστασία από καταπάτηση δεδομένων:**
    - Μέσω της ιδιοτικότητας, τα προσωπικά χαρακτηριστικά του χρήστη αποτελούν έναν ασφαλή τρόπο αναγνώρισης.
    - Αυτό εμποδίζει την πρόσβαση σε πληροφορίες ακόμη και σε περίπτωση απώλειας ή κλοπής της συσκευής.
    - Οι τεχνολογίες αναγνώρισης προσώπου, δακτυλικών αποτυπωμάτων και άλλες βιομετρικές μεθόδοι, εξασφαλίζουν ότι μόνο ο αυθεντικός χρήστης μπορεί να αποκτήσει πρόσβαση στις ευαίσθητες πληροφορίες της συσκευής.
4. **Αντίδραση σε κακόβουλες προσπάθειες:**
    - Οι προηγμένοι αισθητήρες ιδιοτικότητας, μπορούν να ανιχνεύουν κακόβουλες προσπάθειες, όπως η χρήση απομιμήσεων δακτυλικών αποτυπωμάτων.
    - Αυτή η δυνατότητα, αυξάνει το επίπεδο προστασίας, καθώς επιτρέπει την ανίχνευση πιθανών προσπαθειών απάτης ή παραβίασης της ασφάλειας.
    - Μέσω της τεχνολογίας αυτής, οι συσκευές είναι σε θέση να αναγνωρίζουν τις γνήσιες αποτυπώσεις και να αντιλαμβάνονται εάν πραγματοποιείται προσπάθεια πρόσβασης από μη εξουσιοδοτημένο χρήστη.

5. **Εξατομίκευση Προστασίας:**
    - Η ιδιωτικότητα επιτρέπει την εξατομίκευση των μεθόδων ασφαλείας, λαμβάνοντας υπόψη τις προτιμήσεις και τις ανάγκες του κάθε χρήστη.
    - Αυτό σημαίνει ότι οι χρήστες μπορούν να επιλέξουν τις μεθόδους ασφαλείας που τους ταιριάζουν καλύτερα, όπως η χρήση δακτυλικών αποτυπωμάτων, η αναγνώριση προσώπου ή η χρήση κωδικών πρόσβασης, και να τις προσαρμόσουν σύμφωνα με τις προτιμήσεις τους για μεγαλύτερη ασφάλεια και άνεση.

Συνολικά, η ιδιωτικότητα προσδίδει στα smartphones, επιπλέον επίπεδο προστασίας μέσω προηγμένων μεθόδων αναγνώρισης και εξειδικευμένων τεχνολογιών, διασφαλίζοντας την ασφάλεια των συσκευών και την προστασία των δεδομένων.

Η συνδυασμένη χρήση διαφόρων μεθόδων αναγνώρισης, όπως οι αισθητήρες δακτυλικών αποτυπωμάτων και η αναγνώριση προσώπου, ενισχύει την αυθεντικότητα των χρηστών και μειώνει τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης.

Αυτό οδηγεί σε μια ολοκληρωμένη προσέγγιση της ασφάλειας, βοηθώντας στην προστασία των συσκευών και των προσωπικών δεδομένων των χρηστών από πιθανούς κινδύνους κι επιθέσεις.

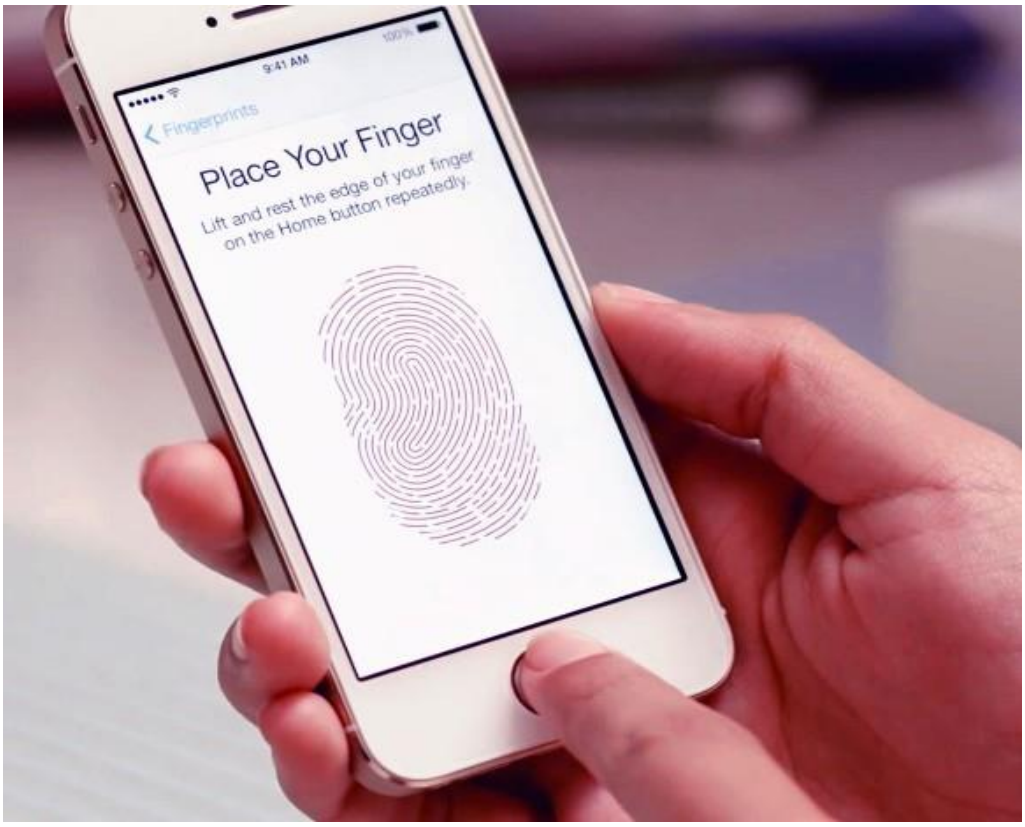
3.3 Τεχνολογίες ιδιωτικότητας

Οι τεχνολογίες ιδιοτικότητας αποτελούν κρίσιμο κομμάτι των μέτρων ασφαλείας στα smartphones, προσφέροντας προηγμένες μεθόδους αναγνώρισης και επιβεβαίωσης της ταυτότητας του χρήστη. Ανάμεσα σε αυτές, ξεχωρίζουν οι εξής:

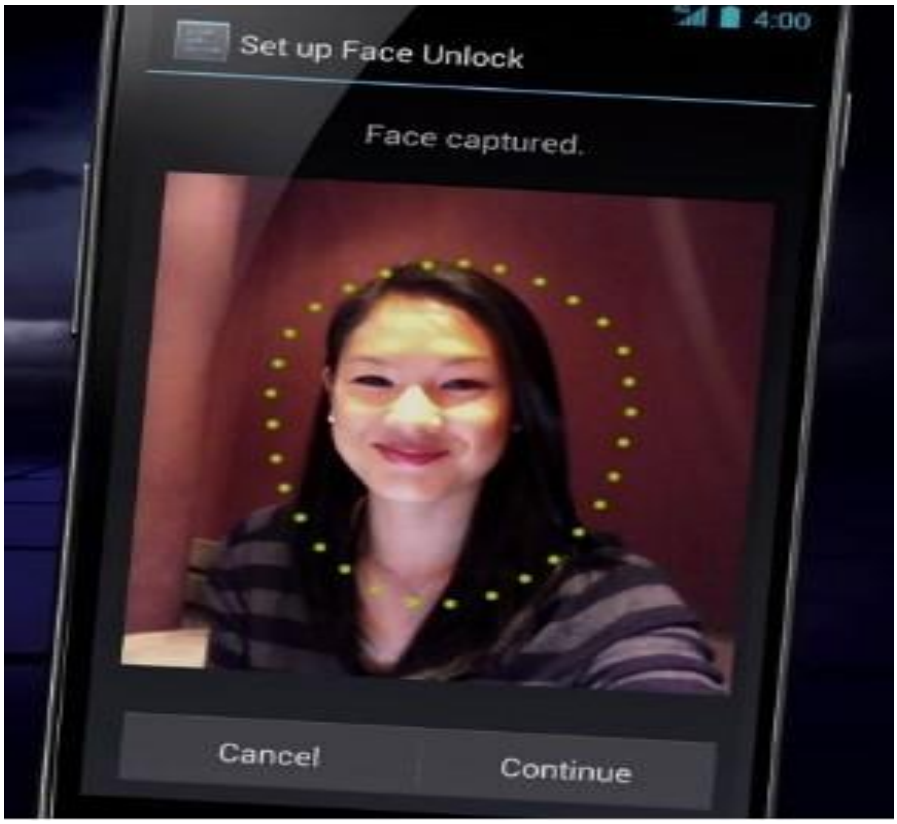
1. **Αναγνώριση προσώπου:**
    - Η τεχνολογία αναγνώρισης προσώπου χρησιμοποιεί αλγόριθμους που αναγνωρίζουν μοναδικά χαρακτηριστικά του προσώπου του χρήστη, όπως η διάταξη των ματιών, της μύτης και του στόματος.
    - Είναι γρήγορη και άνετη, ενώ η συνδυασμένη χρήση 3D αισθητήρων μειώνει τον κίνδυνο απάτης με φωτογραφίες.
    - Η αξιοπιστία της αναγνώρισης προσώπου σε διαφορετικές συνθήκες φωτισμού και γωνίες προβολής συμβάλλει στην αποτροπή μη εξουσιοδοτημένης πρόσβασης.
2. **Αισθητήρες δακτυλικών αποτυπωμάτων:**
    - Οι αισθητήρες δακτυλικών αποτυπωμάτων εγγράφουν και αναλύουν τα μοναδικά χαρακτηριστικά του δακτυλικού αποτυπώματος του χρήστη.
    - Είναι γρήγοροι, αξιόπιστοι και διαθέσιμοι σε πολλές σύγχρονες συσκευές, προσφέροντας υψηλή ασφάλεια.
    - Η χρήση αισθητήρων δακτυλικών αποτυπωμάτων εξασφαλίζει την ταυτοποίηση του χρήστη με μεγάλη ακρίβεια και αποτελεσματικότητα, επιβεβαιώνοντας την ταυτότητά του και εμποδίζοντας την πρόσβαση από μη εξουσιοδοτημένα άτομα.
3. **Αναγνώριση ιριδίων:**
    - Η αναγνώριση ιριδίων βασίζεται στα μοναδικά χαρακτηριστικά του ιριδίου του ματιού. Είναι μια ασφαλής μέθοδος που απαιτεί εξειδικευμένο εξοπλισμό, παρέχοντας υψηλό βαθμό ακρίβειας.
4. **Αναγνώριση φωνής:**
    - Η τεχνολογία αναγνώρισης φωνής, χρησιμοποιεί τα μοναδικά χαρακτηριστικά της φωνής του χρήστη, όπως τον τόνο, το ρυθμό, και τις συχνότητες.
    - Παρέχει μια εναλλακτική λύση για την αναγνώριση ταυτότητας, επιτρέποντας στον χρήστη να αποκτήσει πρόσβαση στη συσκευή του μέσω της φωνητικής του εντολής, προσφέροντας έτσι ευκολία και ασφάλεια.
5. **Τεχνολογία ανίχνευσης κινήσεων:**
    - Οι αισθητήρες κίνησης όπως το επιταχυνσιόμετρο και το γυροσκόπιο, χρησιμοποιούνται για τον ανιχνευτή κινήσεων.
    - Αυτή η τεχνολογία μπορεί να χρησιμοποιηθεί για επιπλέον επιβεβαίωση της ταυτότητας, όπως πατώντας συγκεκριμένα σημεία ή κινώντας το smartphone με έναν προκαθορισμένο τρόπο.
    - Αυτή η διπλή επιβεβαίωση μπορεί να προσθέσει ένα επιπλέον επίπεδο ασφάλειας, καθιστώντας πιο δύσκολη την πρόσβαση στη συσκευή από μη εξουσιοδοτημένα άτομα.

Ο συνδυασμός αυτών των τεχνολογιών παρέχει ολοκληρωμένες λύσεις για την ασφαλή και αποτελεσματική προστασία των smartphones και των προσωπικών δεδομένων των χρηστών. Με την αξιοποίηση ποικίλων μεθόδων αναγνώρισης, όπως η αναγνώριση προσώπου, οι αισθητήρες δακτυλικών αποτυπωμάτων και οι αισθητήρες κίνησης, επιτυγχάνεται ένα υψηλό επίπεδο ασφάλειας που δυσκολεύει την παράβαση από μη εξουσιοδοτημένα άτομα.

Με τη συνεχή εξέλιξη και την εφαρμογή προηγμένων τεχνολογιών, η προστασία των smartphones γίνεται όλο και πιο αποτελεσματική, εξασφαλίζοντας την ακεραιότητα των δεδομένων και την ιδιωτικότητα των χρηστών.



Εικόνα 34: Τεχνολογία δακτυλικού αποτυπώματος.



Εικόνα 35: Τεχνολογία αναγνώρισης προσώπου.

Εικόνα 36: Τεχνολογία αναγνώρισης φωνής.

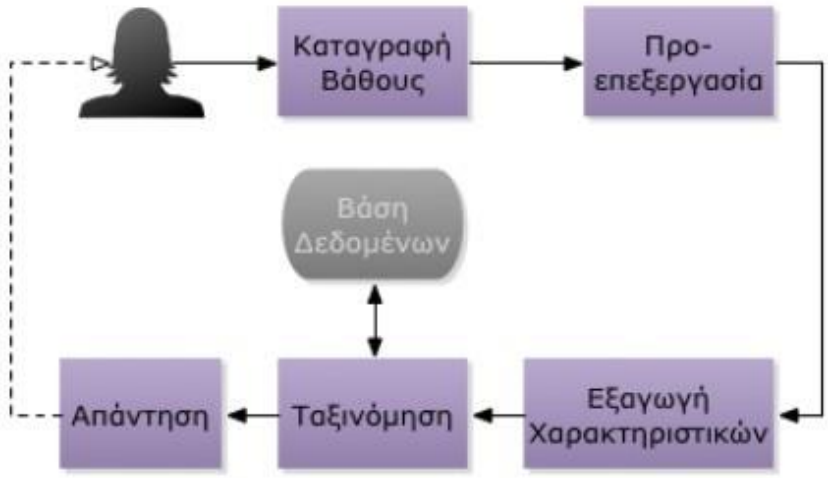
3.4 Σύστημα αναγνώρισης προσώπου

Το σύστημα αναγνώρισης προσώπου είναι εφαρμογή που χρησιμοποιείται σε διάφορες συσκευές, για την σωστή αναγνώριση και ταυτοποίηση του χρήστη. Αυτό επιτυγχάνεται μέσω της σύγκρισης των δεδομένων που υπάρχουν σε μία βάση δεδομένων και των δεδομένων όπου δίνονται ως είσοδο στην εφαρμογής

Οι τεχνικές που χρησιμοποιούνται είναι οι εξής:

- Λήψη μετρήσεων για διάφορες ιδιότητες από το πρόσωπο του χρήστη.
- Μείωση του θορύβου και κανονικοποίηση αυτών των μετρήσεων.
- Εξαγωγή των κύριων χαρακτηριστικών από τις μετρήσεις με βάση των οποίων θα γίνει η σύγκριση.
- Σύγκριση των κύριων χαρακτηριστικών που εξήχθησαν από την λήψη μετρήσεων με τα κύρια χαρακτηριστικά που είναι αποθηκευμένα στην βάση δεδομένων και χρησιμοποιούνται ως αυθεντικά.

Οι βασικές μέθοδοι επιλογής δεδομένων είναι η γεωμετρική, όπου βασίζεται στην επιλογή δεδομένων των χαρακτηριστικών του προσώπου, ενώ η δεύτερη είναι η φωτομετρική, όπου βασίζεται σε επιλογή δεδομένων που αφορούν την όψη του προσώπου.



Εικόνα 37: Ενδεικτική διαδικασία αναγνώρισης προσώπου.

Υπάρχουν δύο κύριοι αλγόριθμοι που χρησιμοποιούνται για την αναγνώριση προσώπου. Ο ένας ονομάζεται αλγόριθμος δύο διαστάσεων, ενώ ο δεύτερος ονομάζεται αλγόριθμος τριών διαστάσεων.

Αλγόριθμος 2D - δύο διαστάσεων
Τα κύρια χαρακτηριστικά επιλογής σε αυτήν την περίπτωση είναι χαρακτηριστικά που κάνουν μοναδικό το πρόσωπο κάθε ανθρώπου σε σχέση με άλλα. Υπάρχουν πάνω από 80 τέτοια χαρακτηριστικά και ονομάζονται κομβικά σημεία.
Ενδεικτικά μερικά από αυτά είναι:

- Απόσταση μεταξύ των ματιών
- Βάθος ματιών
- Πλάτος μύτης
- Σχήμα ζυγωματικών
- Μήκος σαγονιού

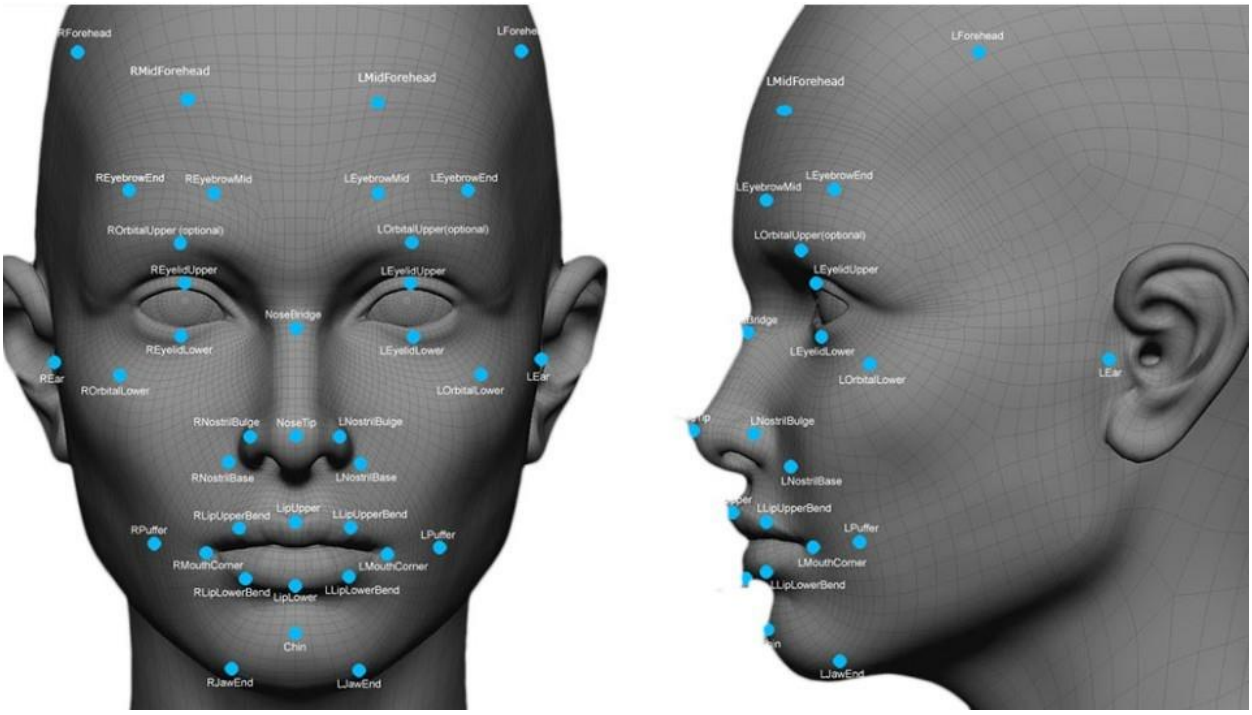
Για την εξαγωγή κυρίων χαρακτηριστικών από όλα αυτά που θα μετρήσει ο αλγόριθμος, μπορούν να χρησιμοποιηθούν μεθόδοι όπως το PCA (Principal Component Analysis), ο οποίος επιλέγει από έναν πίνακα μετρήσεων χαρακτηριστικών αυτά που έχουν μεγαλύτερη διασπορά τιμών. Τέτοιο παράδειγμα είναι το γνωστό παράδειγμα δημιουργείας eigenfaces. Άλλη μία μέθοδος επιλογής κύριων χαρακτηριστικών είναι η LDA (Linear Discriminant Analysis).

Αλγόριθμος 3D – τριών διαστάσεων
Σε αυτήν την περίπτωση χρησιμοποιείται η τρισδιάστατη γεωμετρία του προσώπου για την εξαγωγή των κυρίων χαρακτηριστικών, αυξάνοντας έτσι την σωστή αναγνώριση, πλησιάζοντας σε ακρίβεια την ταυτοποίηση του δακτυλικού αποτυπώματος.
Για την δημιουργία χαρακτηριστικών από τρισδιάστατη λήψη, χρειάζονται ειδικά συστήματα λήψεων, τα οποία αυξάνον μεν την ασφάλεια και ακρίβεια όπως ειπώθηκε προηγουμένως, αυξάνουν όμως δε και το κόστος της συσκευής που θα περιέχει τέτοιο σύστημα αναγνώρισης προσώπου.

Βιομετρική αναγνώριση
Σύγχρονες τεχνολογίες, μαζί με την εξαγωγή κυριών χαρακτηριστικών από το πρόσωπο, χρησιμοποιούν την διαδικασία της ανάλυσης υφής επιφάνειας, όπου η υφή του προσώπου μετατρέπεται σε μαθηματικές ακολουθίες. Οι ακολουθίες ουσιαστικά, περιέχουν διάφορους πόρους και γραμμές που έχει το κάθε συγκεκριμένο πρόσωπο μεταφρασμένα σε μαθηματικές ακολουθίες, αυξάνοντας έτσι την σωστή αναγνώριση του προσώπου, αλλά αυξάνοντας επίσης το κόστος της συνολικής διαδικασίας αναγνώρισης.

Αδυναμίες

Οι αδυναμίες τέτοιων συστημάτων αναγνώρισης προσώπου, δεν γίνονται εμφανής στον μέσο χρήστη. Για του λόγου το αληθές, όταν ικανοποιούνται οι ευνοϊκές συνθήκες που ορίζει ο δημιουργός, τα ποσοστό λάθους είναι σχεδόν μηδαμινά. Όταν όμως αυτές οι συνθήκες δεν ικανοποιούνται πλήρως (πχ χαμηλός φωτισμός, γωνία λήψης μεγαλύτερης των 20 μοιρών, χρήση γυαλιών ηλίου, τα μαλλιά εμπλέκονται στο πρόσωπο), τότε τα σφάλματα αναγνώρισης αυξάνονται.



Εικόνα 38: Μετρήσεις χαρακτηριστικών στην αναγνώριση προσώπου.

3.5 Αισθητήρες δακτυλικού αποτυπώματος

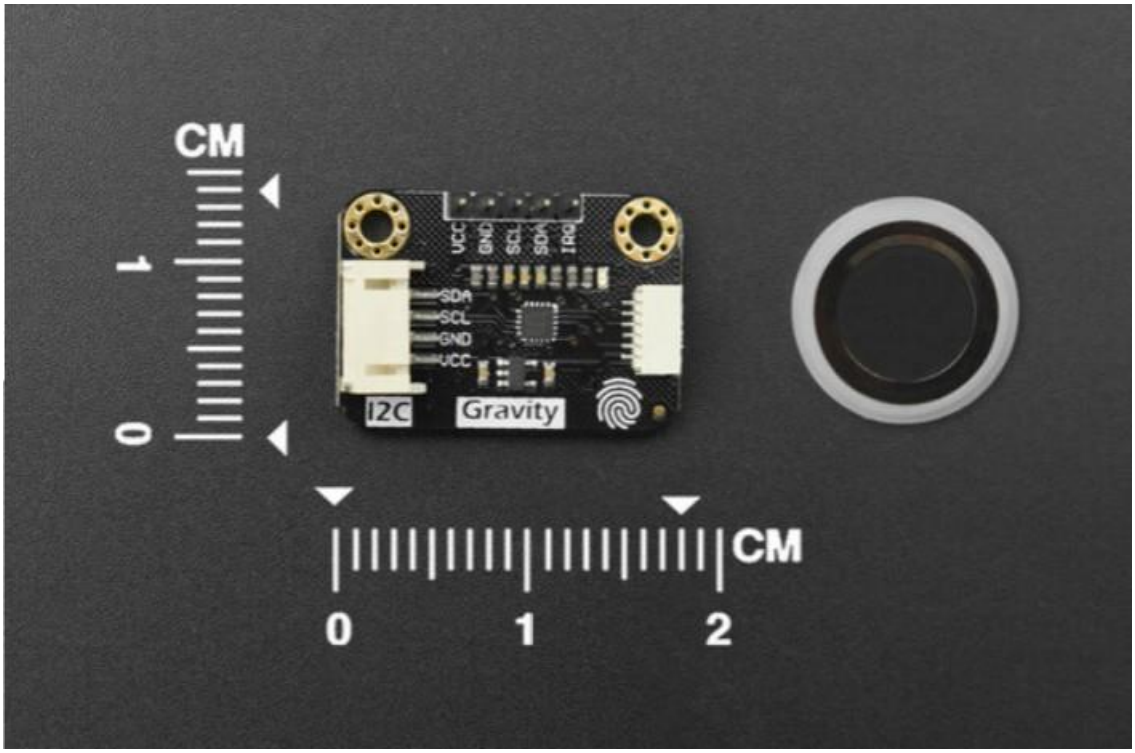
Οι αισθητήρες δακτυλικού αποτυπώματος έκαναν την εμφάνισή τους πρώτα σε κινητές συσκευές υψηλού κόστους και πλέον μπορούν να βρεθούν σχεδόν σε κάθε smartphone. Πληροφοριακά εμφανίστηκαν πρώτα στο κινητό τηλέφωνο Motorola Atrix, όμως η χρήση τους καθιερώθηκε με την εισαγωγή τους στο κινητό τηλέφωνο Iphone 5s.

Οι κύριοι αισθητήρες που χρησιμοποιούνται στις σύγχρονες συσκευές είναι οι παρακάτω:

- **Οπτικοί αισθητήρες**. Είναι η παλαιότερη τεχνολογία που χρησιμοποιείται στην αναγνώριση του δακτυλικού αποτυπώματος. Στηρίζεται στην λήψη μίας φωτογραφίας του δακτυλικού αποτυπώματος κι έπειτα αναλύονται έτσι ώστε να βρεθούν μοναδικά πρότυπα. Οι ειδική αλγόριθμοι αναλύουν φωτεινές και σκοτεινές περιοχές και μπορούν να βρουν τις μοναδικές γραμμές και σημάδια του δακτυλικού αποτυπώματος. Διαθέτουν φώτα led και μεγάλο αριθμό διόδων, όπου αυξάνουν και το μέγεθος του αισθητήρα, οπότε αποφεύγονται στις περισσότερες σύγχρονες, λεπτές συσκευές. Τέλος, μία εικόνα πολύς καλής ανάλυσης, μπορεί να τους ξεγελάσει, διότι βασίζονται σε δισδιάστατη ανάλυση του δακτυλικού αποτυπώματος. Γενικά χρησιμοποιούνται σε συσκευές χαμηλού κόστους, όμως αναμένεται μελλοντικά να αυξηθεί η χρήση τους, αφού μπορούν να τοποθετηθούν κάτω από την οθόνη.
- **Χωρητικοί αισθητήρες**. Χρησιμοποιούν μια σειρά πυκνωτών για την συλλογή δεδομένων και είναι ευρεία η χρήση τους, αφού βρίσκονται στις περισσότερες σύγχρονες συσκευές. Όταν τα δάκτυλο ακουμπά τον αισθητήρα, η μορφή του δακτύλου, προκαλεί αλλαγές στο ηλεκτρικό ρεύμα που βρίσκεται αποθηκευμένο στους πυκνωτές. Συγκεκριμένα, οι αυλακώσεις δεν αλλάζουν το ρεύμα, ενώ οι πτυχώσεις το επηρεάζουν. Αυτές οι αλλαγές καταγράφομαι και αποθηκεύονται, ενώ έπειτα αναλύονται για την εξαγωγή κυρίων χαρακτηριστικών του δακτύλου του χρήστη. Είναι πάρα πολύ ασφαλείς, εφόσον δεν μπορούν να ξεγελαστούν ούτε με εικόνα, ούτε με ομοίωμα.
- **Αισθητήρες με υπέρηχους**. Λειτουργούν μέσω ηχητικών κυμάτων. Καθώς το δάκτυλο ακουμπάει τον αισθητήρα, μεταδίδεται ένα υπερηχητικό σήμα, όπου κάποιο μέρος του απορροφάται από το δάκτυλο, ενώ το υπόλοιπο ανακλάται. Η απορρόφηση εξαρτάται από τα μοναδικά χαρακτηριστικά του δακτύλου (πχ πτυχώσεις, πόρους). Άρα δημιουργείται ένας χάρτης από το ανακλώμενο κύμα που επιστρέφει στον αισθητήρα κι εξαρτάται από τα μοναδικά χαρακτηριστικά του δακτύλου. Αυτοί οι αισθητήρες μπορούν να τοποθετηθούν κάτω από την οθόνη, οπότε αναμένεται αύξηση στην χρήση τους στο μέλλον.

Τα πλεονεκτήματα των δακτυλικών αποτυπωμάτων είναι η ταχύτητα αναγνώρισής τους και η ασφάλεια, αφού δεν γίνεται να κλαπεί το χέρι ή να ξεχαστεί το χέρι κάπου όπως ένας κωδικός. Το κύριο μειονέκτημα τους είναι το πόσο καλά κρυπτογραφούνται τα δεδομένα που αναλύονται από το δάκτυλο. Επίσης, προβλήματα μπορεί να δημιουργηθούν από χτυπήματα στο δάκτυλο, βρωμιά, υγρασία ή χρήση γαντιών.

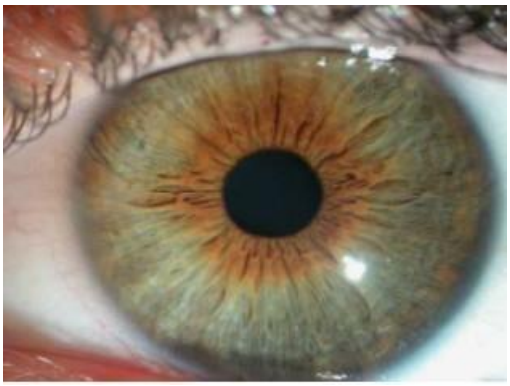
Εικόνα 39: Αισθητήρας δακτυλικού αποτυπώματος.



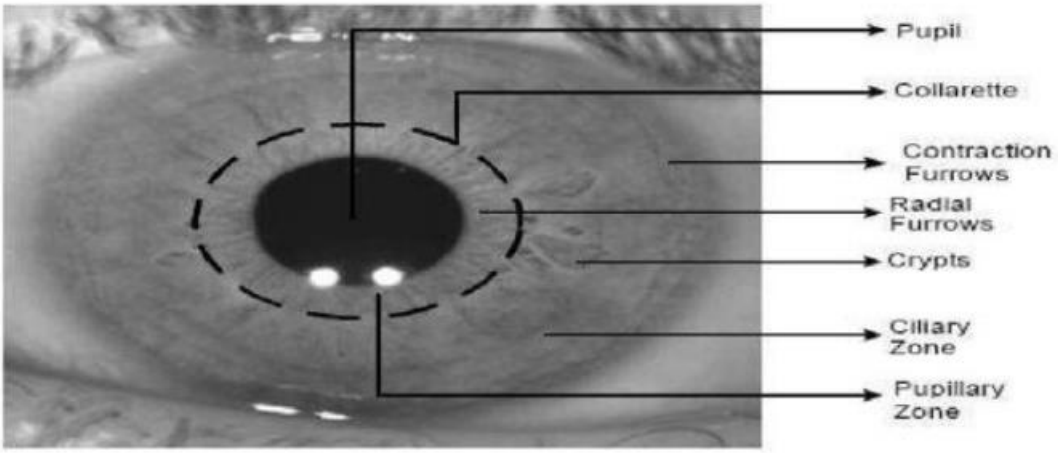
Εικόνα 40: Μέγεθος αισθητήρα δακτυλικού απότυπώματος.

3.6 Σύστημα αναγνώρισης ίριδας

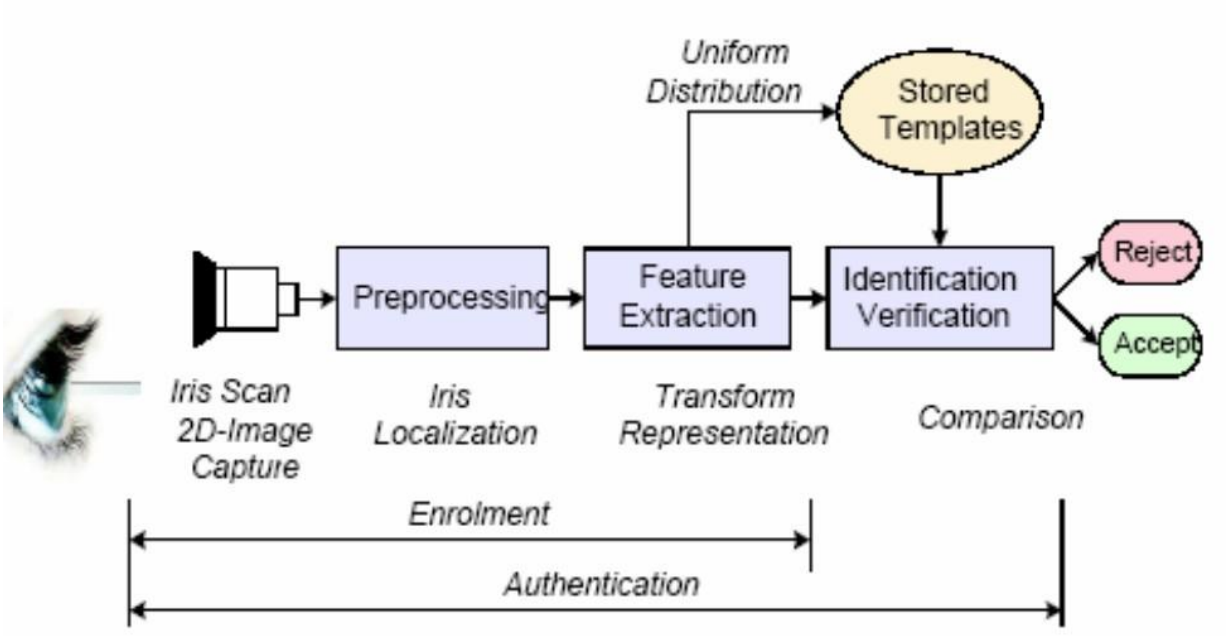
Η ίριδα παρουσιάζει σημαντικά πλεονεκτήματα στην βιομετρική αναγνώριση λόγω μοναδικότητας, μονιμότητας και λεπτομερής υφής.



Εικόνα 41: Ίριδα του ματιού.



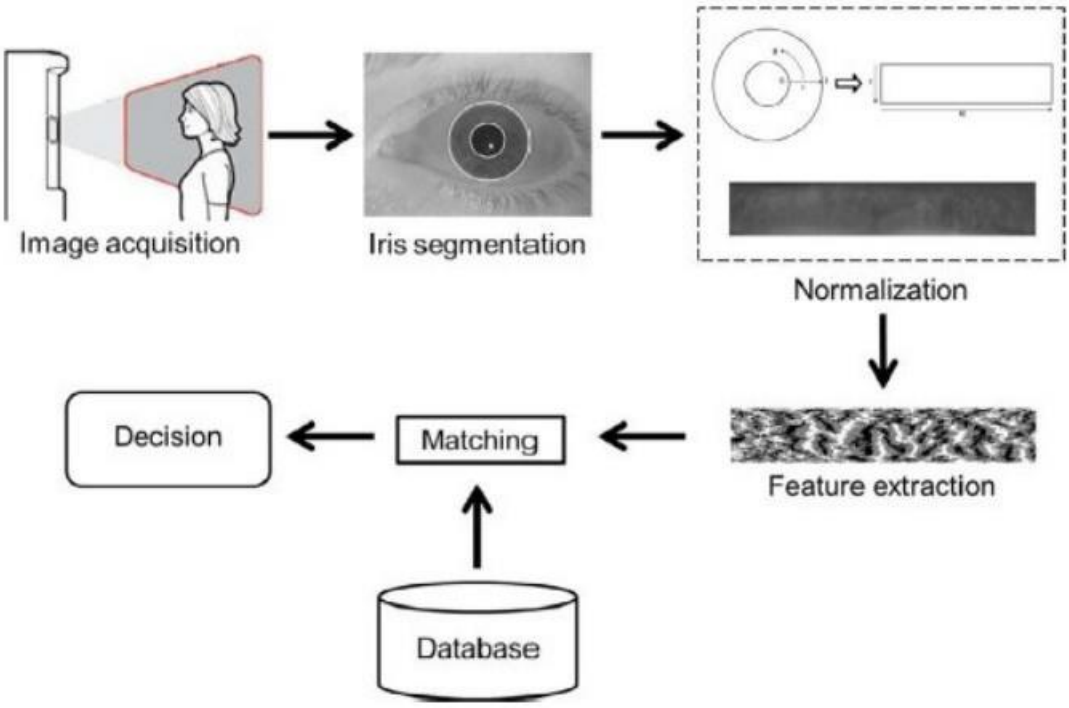
Εικόνα 42: Μέρη της ίριδας.



Εικόνα 43: Το σύστημα αναγνώρισης της Ίριδας.

Το σύστημα αναγνώρισης της ίριδας περιλαμβάνει τα εξής βήματα:

- Λήψη εικόνας του ματιού.
- Εύρεση της εικόνας ίριδας στην εικόνα του ματιού, εύρεση της ακτίνας της κόρης και υπολογισμός του πάχους δακτυλίου της.
- Κανονικοποίηση της εικόνας της ίριδας.
- Ξετύγλιμα σε ορθογώνιο παράθυρο της εικόνας.
- Επιλογή κυρίων χαρακτηριστικών της ίριδας και κωδικοποίηση τους, όπου θα χρησιμοποιηθούν για αναγνώριση.
- Τέλος, αποθήκευση των δεδομένων σε βάση δεδομένων (αν πρόκειται για εισαγωγή ίριδας) ή έλεγχος/σύγκριση των δεδομένων με δεδομένα της βάσης δεδομένων (αν πρόκειται για ταυτοποίηση του χρήστη).



Εικόνα 44: Βήματα επεξεργασίας εικόνας ματιού.

Τα κύρια πλεονεκτήματα που προσφέρει το σύστημα αναγνώρισης ίριδας είναι τα εξής:

- Υψηλή ασφάλεια, αφού η ίριδα είναι μοναδικό χαρακτηριστικό του ματιού για κάθε άνθρωπο.
- Υψηλή ακρίβεια.
- Σταθερότητα, εφόσον η ίριδα του ανθρώπου δεν αλλάζει.

Τα κύρια μειονεκτήματα είναι τα εξής:

- Υψηλό κόστος σε σχέση με άλλες μεθόδους αναγνώρισης.
- Δεδομένες συνθήκες όπως χαμηλός φωτισμός και διαφορετική γωνία θέασης επηρεάζουν την απόδοση.

3.7 Σύστημα αναγνώρισης φωνής

Οι κύριες αρχές λειτουργίας του συστήματος αναγνώρισης φωνής είναι:

- Ακουστική καταγραφή: ο χρήστης καταγραφή στην συσκευή την εντολή ξεκλειδώματος και η συσκευή την ψηφιοποιεί.
- Εξάγονται τα κύρια χαρακτηριστικά του μηνύματος, τα οποία μπορεί να είναι μήκος, τόνος, ένταση, ταχύτητα και ρυθμός κωδικοποιουνται και αποθηκεύονται στην βάση δεδομένων.
- Κατά την αναγνώρισης τα κωδικοποιημένα χαρακτηριστικά συγκρίνονται με τα αποθηκευμένα και γίνεται έλεγχος για την εγκυρότητα του χρήστη.

Τα κύρια χαρακτηριστικά της παραπάνω μεθόδου είναι τα εξής:

- Μεγάλη απόδοση: Η τεχνολογία αναγνώρισης φωνής βασίζεται σε μοναδικά χαρακτηριστικά της φωνής του χρήστη όπως τόνο, ένταση και ρυθμό.
- Μεγάλη ασφάλεια: Είναι αρκετά δύσκολο να αντιγράψει κανείς τα παραπάνω ώστε να ξεγελάσει το σύστημα αναγνώρισης φωνής.
- Επικοινωνία σε πραγματικό χρόνο: σε αντίθεση με άλλες μεθόδους αυθεντικοποίησης, η παραπάνω μέθοδος γίνεται σε πραγματικό χρόνο, κάνοντάς την πιο ευέλικτη και βολική.
- Συνδυασμό με άλλες μεθόδους: η αναγνώριση φωνής μπορεί να συνδυαστεί με άλλες μεθόδους για την αυθεντικοποίηση του χρήστη προσφέροντας έξτρα ασφάλεια.

Τα κύρια μειονεκτήματα της είναι:

- Μείωσης απόδοσης από ήχους τους περιβάλλοντος.
- Απαιτείται επαρκής εκπαίδευση για την διατήρηση της απόδοσης σε υψηλά ποσοστά.
- Αν δεν είναι επαρκώς εκπαιδευμένη, μειώνεται η απόδοσή της σε εσφαλμένη θετική αναγνώριση.
- Πολλές φορές το σύστημα δεν μπορεί να ξεχωρίσει διαφορετικά άτομα που έχουν παρόμοιες φωνές κι έτσι δίνει πρόσβαση σε μη εξουσιοδοτημένους χρήστες.
- Η φωνή του χρήστη δεν είναι σταθερή όπως η ίριδα και μπορεί να αλλάξει λόγω κάποιας ασθένειας ή τραυματισμών κι άρα αποκλείεται η πρόσβαση στην συσκευή.

Εικόνα 45: Απλός αισθητήρας αναγνώρισης φωνής του εμπορίου.

4. Προηγμένες Τεχνολογίες Ασφάλειας

4.1 Κρυπτογραφία και ασφαλείς συνδέσεις

Η Κρυπτογραφία και οι ασφαλείς συνδέσεις, αποτελούν την πρώτη γραμμή άμυνας για τα smartphones, εξασφαλίζοντας την προστασία των προσωπικών δεδομένων και των επικοινωνιών. Ας εξετάσουμε λεπτομερέστερα τις βασικές τους πτυχές:

1. **Συμμετρική και δημόσια κρυπτογραφία:**
    - **Συμμετρική κρυπτογραφία:** Η χρήση κοινού κλειδιού για κρυπτογράφηση και αποκρυπτογράφηση, προσφέρει αποτελεσματική προστασία. Ωστόσο, η πρόκληση είναι η ασφαλής διανομή του κλειδιού, καθώς κάθε εμπλεκόμενο μέρος, πρέπει να έχει πρόσβαση σε αυτό χωρίς να αποκαλύπτεται σε μη εξουσιοδοτημένους.
    - **Δημόσια κρυπτογραφία:** Η χρήση ζεύγους δημόσιου και ιδιωτικού κλειδιού, επιτρέπει ασφαλή ανταλλαγή πληροφοριών, χωρίς την ανάγκη κοινού κλειδιού. Το δημόσιο κλειδί χρησιμοποιείται για την κρυπτογράφηση των δεδομένων, ενώ το ιδιωτικό κλειδί χρησιμοποιείται για την αποκρυπτογράφηση τους. Αυτό επιτρέπει την ασφαλή ανταλλαγή ευαίσθητων πληροφοριών, χωρίς τον κίνδυνο αποκάλυψης του ιδιωτικού κλειδιού.
2. **Πρωτόκολλα ασφαλούς συνδεσιμότητας:**
    - **SSL/TLS:** Χρησιμοποιείται για την ασφαλή επικοινωνία μεταξύ πελάτη και εξυπηρετητή στο διαδίκτυο. Η εμφάνιση του "https://" στις διευθύνσεις ιστοσελίδων δείχνει τη χρήση αυτού του πρωτοκόλλου.
    - **IPsec:** Η τεχνολογία IPsec (Internet Protocol Security) αναλαμβάνει τον ρόλο του φρουρού στο επίπεδο δικτύου, προσφέροντας ασφάλεια και προστασία από διάφορες απειλές. Μέσω της κρυπτογράφησης και των μηχανισμών αυθεντικοποίησης, το IPsec διασφαλίζει ότι οι δεδομένες πληροφορίες παραμένουν ακέραιες και εμπιστευτικές κατά τη διαμετακόμιση μέσω δικτύων. Είναι ιδιαίτερα χρήσιμο σε επικοινωνίες μεταξύ απομακρυσμένων τοποθεσιών, όπου η ασφάλεια και το απόρρητο των δεδομένων αποτελούν κρίσιμα θέματα.
3. **Εφαρμογή κρυπτογραφίας στην αποθήκευση και την επικοινωνία:**
   Η εφαρμογή της κρυπτογραφίας στην αποθήκευση και την επικοινωνία, αποτελεί κρίσιμο μέρος των προληπτικών μέτρων ασφαλείας στις συσκευές και στις διαδικασίες επικοινωνίας στο διαδίκτυο.
    - **Κρυπτογράφηση δεδομένων κατά την αποθήκευση:** Αυτή η πρακτική προστατεύει τα αρχεία και τις εφαρμογές που αποθηκεύονται στη συσκευή. Χρησιμοποιείται για να αποτρέψει την ανεπιθύμητη πρόσβαση σε ευαίσθητα δεδομένα σε περίπτωση απώλειας ή κλοπής της συσκευής.
    - **Κρυπτογράφηση επικοινωνίας με HTTPS:** Το πρωτόκολλο HTTPS (Hypertext Transfer Protocol Secure) εξασφαλίζει την ασφαλή μεταφορά πληροφοριών μεταξύ της συσκευής του χρήστη και των εξυπηρετητών στο διαδίκτυο. Η χρήση κρυπτογράφησης με HTTPS προστατεύει τις επικοινωνίες από πιθανούς

εισβολείς και διασφαλίζει την ακεραιότητα και το απόρρητο των δεδομένων που ανταλλάσσονται.

4. **Ασφαλείς συνδέσεις σε δημόσια δίκτυα:**
    - **Εικονικές ιδιωτικές δικτυώσεις (VPN):** Οι VPN προσφέρουν έναν ασφαλή τρόπο σύνδεσης στο διαδίκτυο μέσω κρυπτογραφημένων συνδέσεων. Με τη χρήση ενός VPN, η πραγματική διεύθυνση IP του χρήστη κρύβεται, προσφέροντας προστασία από πιθανούς εισβολείς και παρέχοντας ανωνυμία στο διαδίκτυο.
    - **Πρωτόκολλο WPA3 στα ασύρματα δίκτυα:** Το πρωτόκολλο WPA3 είναι η τελευταία έκδοση του πρωτοκόλλου ασφαλείας Wi-Fi Protected Access. Παρέχει επιπλέον ασφάλεια στις ασύρματες συνδέσεις, καθιστώντας δυσκολότερη την ανεπιθύμητη πρόσβαση στο δίκτυο. Με τη χρήση του WPA3, οι επικοινωνίες στα ασύρματα δίκτυα προστατεύονται από επιθέσεις και αυξάνεται η ασφάλεια των δικτύων Wi-Fi.
5. **Κρυπτογραφία τηλεφωνικών κλήσεων/μηνυμάτων:**
    - **Κρυπτογράφηση VoIP:** Η κρυπτογράφηση των τηλεφωνικών κλήσεων VoIP προστατεύει το απορρήτου των συνομιλιών, μέσω προηγμένων πρωτοκόλλων. Με τη χρήση κρυπτογράφησης στις VoIP κλήσεις, τα δεδομένα που μεταδίδονται μέσω του δικτύου προστατεύονται από ανεπιθύμητη παρακολούθηση και ασφαλίζεται η εμπιστευτικότητα των συνομιλιών.
    - **Κρυπτογράφηση μηνυμάτων:** Η κρυπτογράφηση των μηνυμάτων εξασφαλίζει την ασφαλή ανταλλαγή μηνυμάτων μεταξύ των χρηστών. Μέσω προηγμένων αλγορίθμων κρυπτογράφησης, τα μηνύματα που μεταδίδονται μέσω διαφόρων πλατφορμών επικοινωνίας, όπως τα μηνύματα ηλεκτρονικού ταχυδρομείου ή οι συνομιλίες σε εφαρμογές μηνυμάτων, προστατεύονται από την ανεπιθύμητη πρόσβαση τρίτων.

Ο συνδυασμός αυτών των τεχνολογιών, δημιουργεί ένα ανθεκτικό περιβάλλον ασφαλείας για τα smartphones, προσφέροντας ολοκληρωμένη προστασία σε διάφορα επίπεδα. Η συνεργασία μεταξύ προηγμένων μεθόδων αναγνώρισης χρηστών, κρυπτογράφησης δεδομένων και προστασίας δικτύου, διασφαλίζει την ασφάλεια, την ιδιωτικότητα και την ακεραιότητα των προσωπικών δεδομένων των χρηστών. Με αυτόν τον τρόπο, οι χρήστες μπορούν να αισθάνονται ασφαλείς όταν χρησιμοποιούν τις συσκευές τους και να εμπιστεύονται ότι οι προσωπικές τους πληροφορίες παραμένουν προστατευμένες.

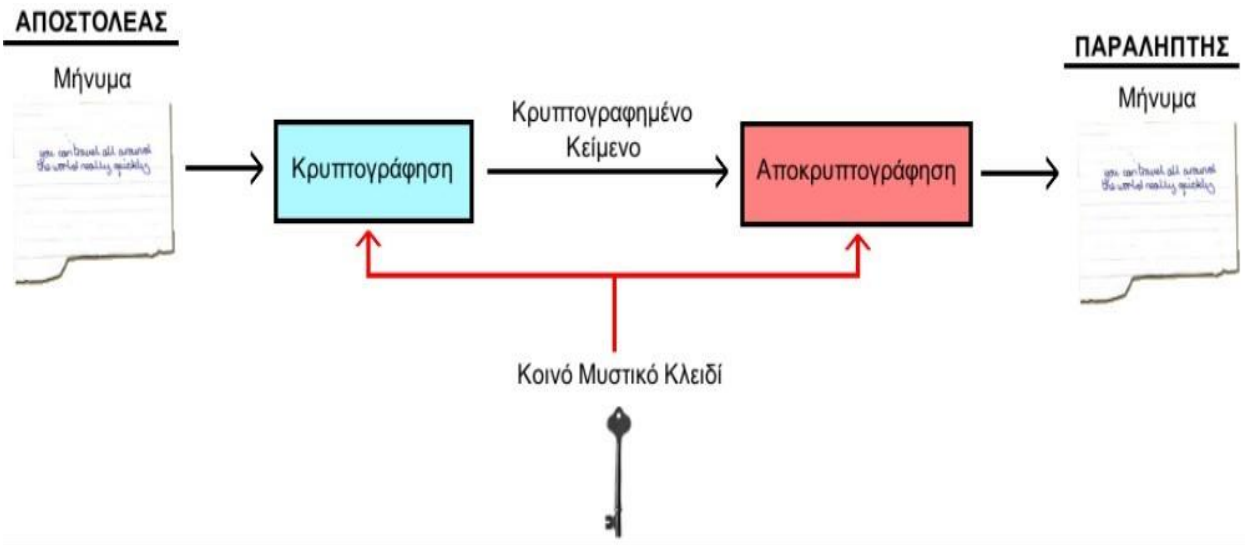
4.2 Κρυπτογράφηση συμμετρικού κλειδιού

Η κρυπτογράφηση συμμετρικού κλειδιού βασίζεται στην ύπαρξη μόνο ενός κλειδιού, το οποίο χρησιμοποιείται και για την κρυπρογράφηση αλλά και για την αποκρυπρογράφηση του κωδικοποιημένου μηνύματος.

Το κλειδί αυτό πρέπει να είναι γνωστό μόνο στα εξουσιοδοτημένα άτομα κι από αυτό ξεκινάει η αδυναμία του παραπάνω μοντέλου.
Δεν υπάρχει δηλαδή, ασφαλείς τρόπος μετάδοσης του κλειδιού κωδικοποίησης παρά μόνο της εξ επαφής ανταλλαγής. Πολλές φορές ο αποστολέας κι ο παραλήπτης όμως δεν γνωρίζονται και για την ασφαλή ανταλλαγή του κλειδιού πρέπει να υπάρχει κάποιο ασφαλές κανάλι επικοινωνίας. Το διαδίκτυο όμως δεν μπορεί να αποτελέσει ασφαλές κανάλι επικοινωνίας κι αυτός είναι ο λόγος που η παραπάνω μέθοδος είναι αρκετά περιορισμένη στην χρήση της.

Το θετικό που προσφέρει η παραπάνω μέθοδος είναι η γρήγορη κρυπρογράφηση κι αποκρυπρογράφηση του μηνύματος, η οποία δεν καταναλώνει μεγάλη υπολογιστική ισχύς.

Πιο γνωστοί αλγόριθμοι για την παραπάνω μέθοδο είναι οι DES, Triple Des και IDEA.



Εικόνα 46: Διαδικασία κρυπτογράφησης συμμετρικού κλειδίου.

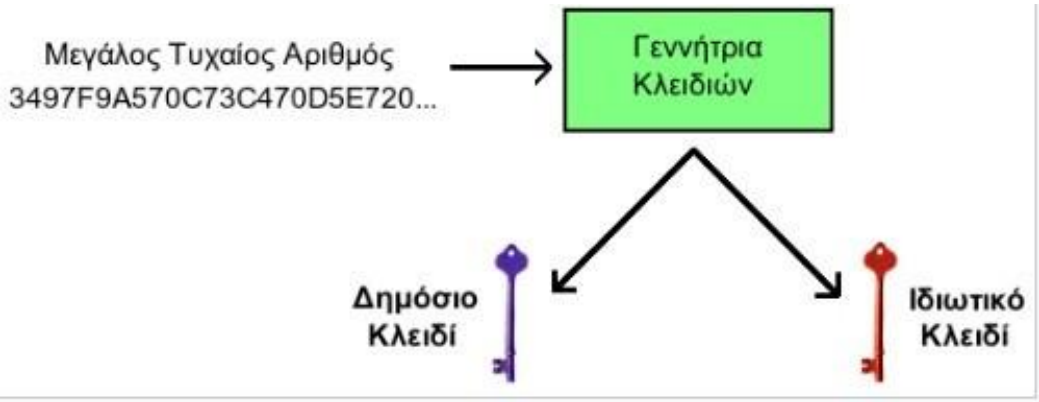
4.3 Κρυπτογράφηση δημοσίου κλειδιού

Αρχές λειτουργίας

Η κρυπτογράφηση δημοσίου κλειδιού ή ασύμμετρου κλειδιού χρησιμοποιεί δύο κλειδιά για κάθε χρήστη. Το ένα είναι το ιδιωτικό κλειδί και το άλλο είναι το δημόσιο κλειδί.
Το ιδιωτικό κλειδί πρέπει να παραμένει κρυφό για κάθε χρήστη και να μην το μοιράζεται, ενώ το δημόσιο κλειδί δεν είναι απαραίτητη η προφύλαξή του.
Τα δύο κλειδιά αυτά συσχετίζονται μεταξύ τους μαθηματικά, έτσι ώστε το ιδιωτικό κλειδί να μπορέσει να αποκρυπτογραφήσει το κωδικοποιημένο μήνυμα που προήλθε μέσω κρυπτογράφησης από το δημόσιο κλειδί.
Σημειώνεται πως, από την γνώση του δημοσίου κλειδιού δεν είναι εφικτή η κατασκευή του ιδιωτικού κλειδιού κι άρα δεν καθίσταται εφικτή η αποκοδικοποίηση του μηνύματος σε λογικά πλαίσια χρόνου.
Αυτό σημαίνει πως ακόμα κι αν κάποιος υποκλέψει το κωδικοποιημένο μήνυμα και γνωρίζει το δημόσιο κλειδί, δεν μπορεί με κανέναν τρόπο να αποκωδικοποιήσει το μήνυμα σε άμεσο χρόνο με την χρήση των σύγχρονων υπολογιστών.

Δημιουργία κλειδιών

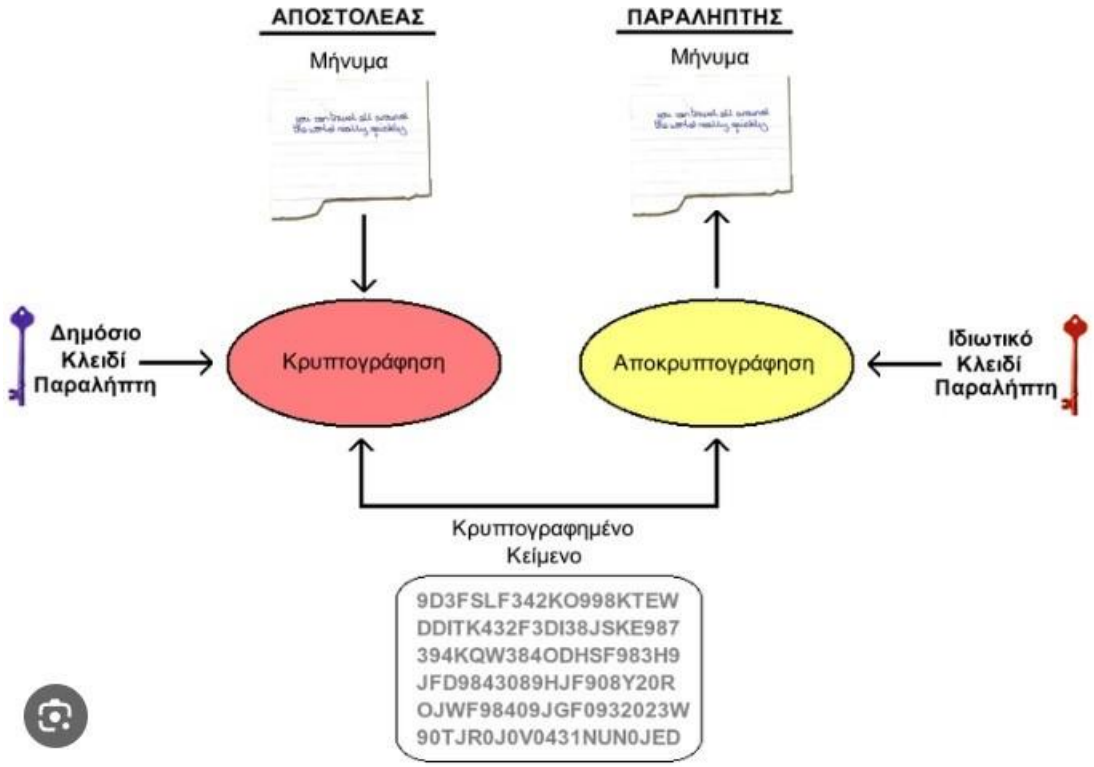
Η δημιουργία των δύο κλειδιών γίνεται από ειδικές συναρτήσεις, οι οποίες χρησιμοποιούν έναν αριθμό ως είσοδο και παράγουν ως έξοδο τα δύο κλειδιά.
Όσο πιο τυχαίος (και μεγάλος) είναι ο αριθμός εισόδου τόσο πιο ασφαλή είναι τα δύο κλειδιά, γιατί ακόμα κι αν έχει κάποιον την συνάρτηση δημιουργίας κλειδιών, δεν θα μπορέσει ποτέ να τα αναπαραγάγει.



Εικόνα 47: Γεννήτρια συνάρτηση παραγωγής δημοσίου και ιδιωτικού κλειδιού.

Μέθοδος επικοινωνίας

Ο αποστολέας χρησιμοποιόντας το δημόσιο κλειδί κωδικοποιεί το μήνυμα που θέλει να στείλει και το στέλνει στον παραλήπτη μέσω κάποιου καναλιού επικοινωνίας.
Ο παραλήπτης στην συνέχεια χρησιμοποιεί το ιδιωτικό του κλειδί και αποκωδικοποιεί το μήνυμα.
Τέλος ο παραλήπτης μπορεί να κωδικοποιήσει το δικό του μήνυμα και να το στείλει πίσω στον αποστολέα, ο οποίος με την σειρά του θα το αποκωδικοποιήσει με το ιδιωτικό του κλειδί.
Εφόσον κανένας άλλος δεν γνωρίζει τα ιδιωτικά κλειδιά, τότε κανένας δεν μπορεί να αποκωδικοποιήσει το μήνυμα ακόμα κι αν το υποκλέψει.

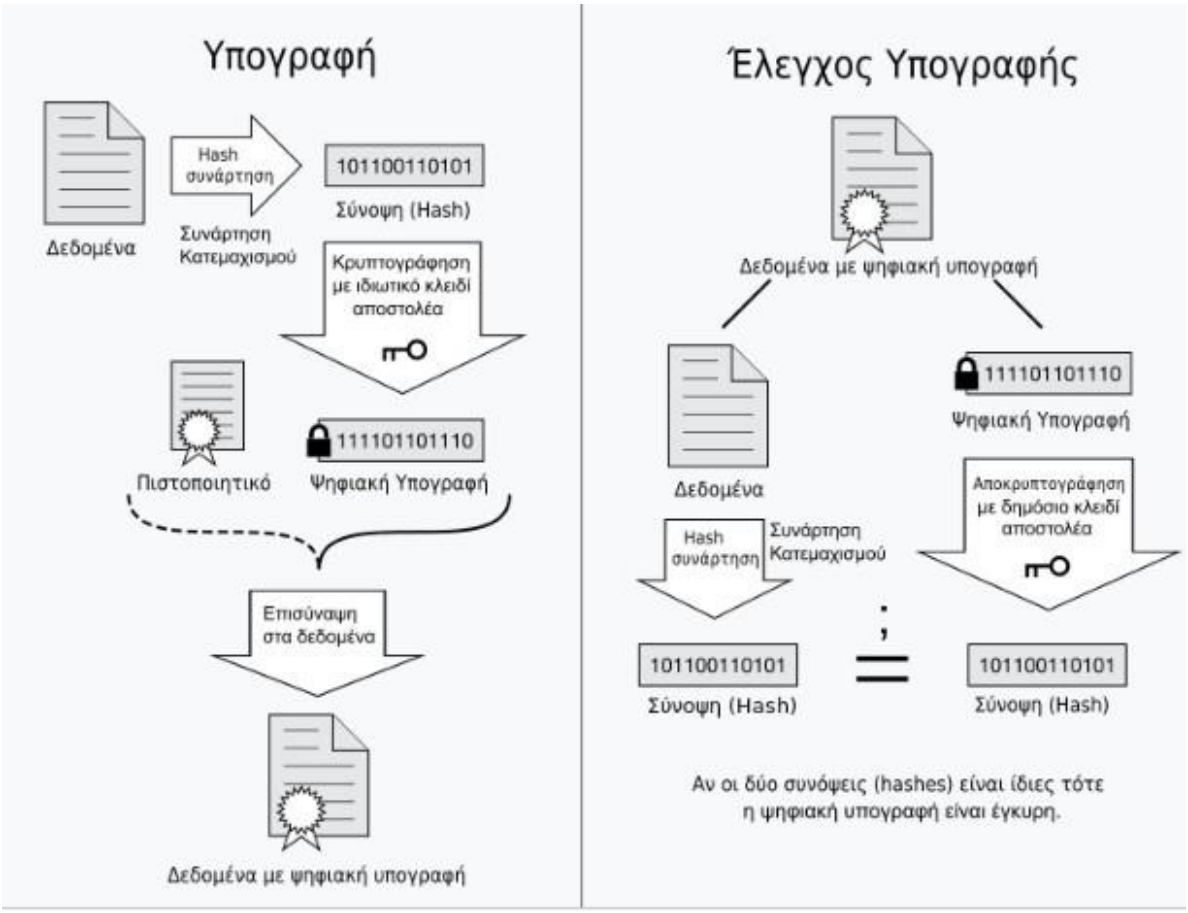


Εικόνα 48: Κρυπτογράφηση δημόσιου κλειδίου.

Σημαντικό μειονέκτημα της μεθόδου είναι πως δεν μπορεί να εξασφαλίσει την πιστοποίηση του αποστολέα. Δηλάδη, οποιοσδήποτε έχει το δημόσιο κλειδί μπορεί να κωδικοποιήσει κάποιο μήνυμα, να το αποστείλει χρησιμοποιόντας ψευδή ταυτότητα και να εξαπατήσει τον παραλήπτη.
Το παραπάνω πρόβλημα μπορεί να λυθεί, χρησιμοποιόντας ο κάθε ένας για κρυπτογράφηση το ιδιωτικό κλειδί, ενώ για αποκρυπτογράφηση το δημόσιο κλειδί κι άρα είναι εφικτή η γνώση ότι το κωδικοποιημένο μήνυμα ήρθε από έμπιστο αποστολέα.

Ψηφιακή υπογραφή

Η ψηφιακή υπογραφή είναι ένας μηχανισμός που χρησιμοποιείται για να επιβεβαιώσει την αυθεντικότητα του αποστολέα ενός μηνύματος.
Είναι δηλαδή, το αντίστοιχο της χειρόγραφης υπογραφής.
Γίνεται χρήση κρυπτογραφικών αλγορίθμων για τη δημιουργία ενός μοναδικού ψηφίου που δηλώνει ότι το μήνυμα εστάλη από συγκεκριμένο αποστολέα.
Αυτό το ψηφίο, γνωστό ως ψηφιακή υπογραφή, συνήθως προστίθεται στο μήνυμα για την εγκυροποίηση του μηνύματος.
Γίνεται έλεγχος εγκυρότητας του ψηφίου αυτού, μέσω ενός δημόσιου κλειδιού.
Δηλαδή μόνο αυτός που διαθέτει το ιδιωτικό κλειδί μπορεί να παράγει έγκυρες ψηφιακές υπογραφές και η επιβαιβεώνεται μέσω της αποκωδικοποίησεις αυτού με το δημόσιο κλειδί.



Εικόνα 49: Παράδειγμα χρήσης της ψηφιακής υπογραφής.

4.4 Πρωτόκολλα SSL/TLS

Τα πρωτόκολλα TLS (Transport Layer Security) και SSL (Secure Sockets Layer) είναι πρωτόκολλα κρυπτογράφησης που παρέχουν ασφάλεια επικοινωνίας σε δίκτυα υπολογιστών. Επίσης, οι ιστοσελίδες χρησιμοποιούν αυτά τα πρωτόκολλα (κυρίως το νεότερο TLS) για να παρέχουν ασφάλεια μεταξύ του περιηγητή και των εξυπηρετητών.

Η σύνδεση μεταξύ περιηγητή και εξυπηρετητή ή μεταξύ δύο χρηστών, έχει τις εξής ιδιότητες:

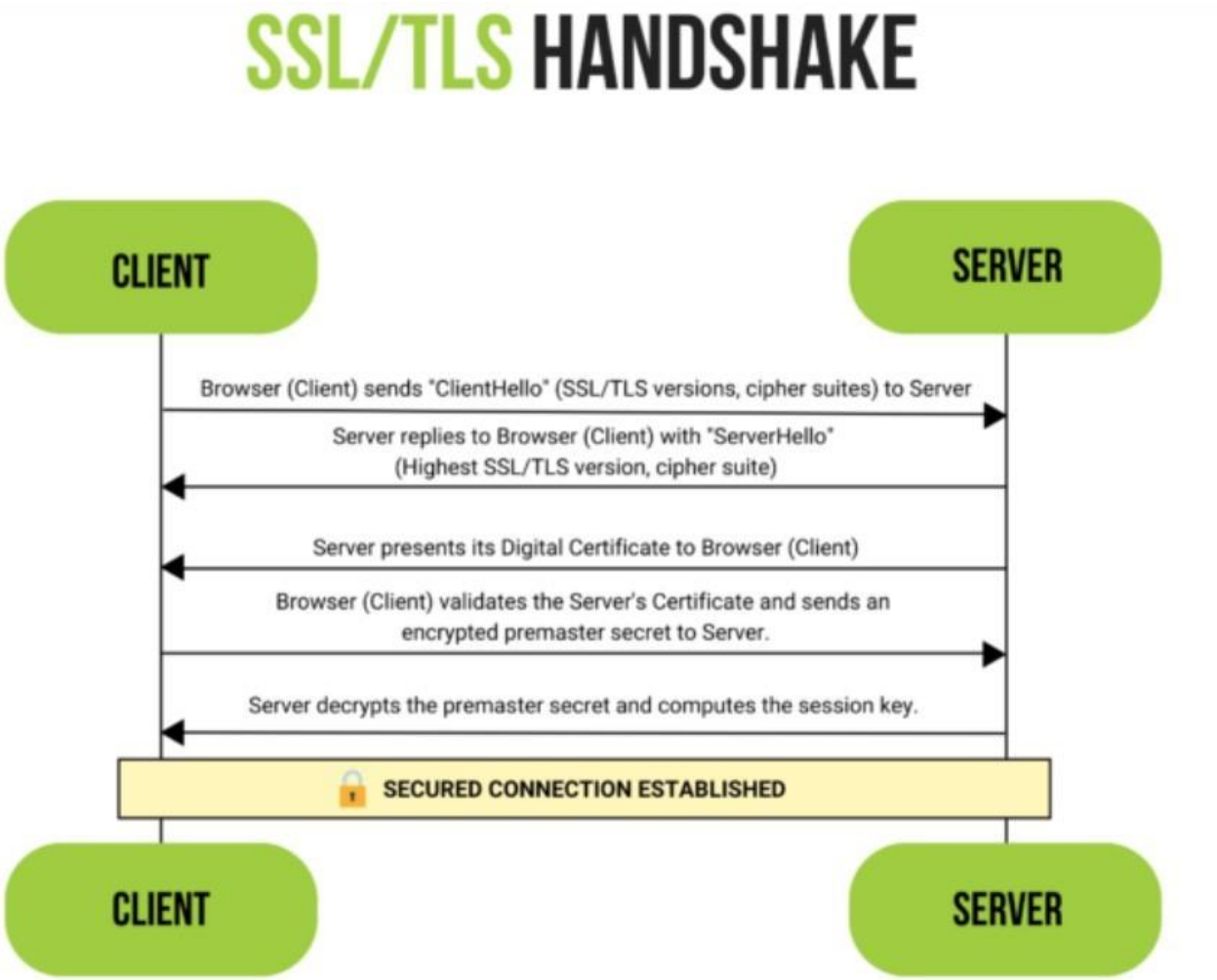
- Ιδιωτική σύνδεση. Χρησιμοποιείται συμμετρική κρυπτογραφία για τα δεδομένα που στέλνονται και λαμβάνονται από τον χρήστη. Τα κλειδιά όπου δημιουργούνται είναι μοναδικά για κάθε σύνδεση, και διασφαλίζονται πριν μεταδοθεί το πρώτο byte πληροφορίας. Τα κλειδιά δεν εμφανίζονται σε κανέναν τρίτο κι ακόμη κι αν κάποιον επιτεθεί δεν γίνεται να περάσει απαρατήρητος.
- Η ταυτότητα των δύο χρηστών κωδικοποιείται με κρυπτογραφία δημοσίου κλειδιού.
- Η σύνδεση εγγυάται ακεραιότητα δεδομένων, διότι κάθε μήνυμα που αποστέλλεται ελέγχεται για την ακεραιότητά του και περιλαμβάνει έναν κωδικό αυθεντικότητας μηνύματος, έτσι ώστε να μπορεί να βρεθεί η κλοπή δεδομένων.

Το πρωτόκολλο TLS συνεχίζει να αναβαθμίζει την ασφάλειά του, με αλλαγές που αποτρέπουν επιτυχημένες επιθέσεις, όπως επίσης και για κενά ασφαλείας που μπορεί να προκύψουν.

Διάφορες εφαρμογές χρησιμοποιούν το μοντέλο πελάτη-διακοσμητή. Αυτές οι εφαρμογές χρησιμοποιούν για την επικοινωνία μέσω δικτύου το πρωτόκολλο TLS.
Μόλις ο πελάτης κι ο διακοσμητής συμφωνήσουν να χρησιμοποιηθεί το πρωτόκολλο TLS, τότε χρησιμοποιείται η διαδικασία της χειραψίας.
Αυτή η διαδικασία περιλαμβάνει:

- Ξεκινάει όταν ο πελάτης συνδέεται σε διακοσμητή που υποστηρίζει πρωτόκολλο TLS και απαιτεί ασφαλής σύνδεση. Παρουσιάζεται μία λίστα με κρυπτογραφήματα και μία λίστα με κρυπτογραφικές συναρτήσεις κατακερματισμού.
- Από αυτές τις λίστες, ο διακοσμητής επιλέγει έναν αλγόριθμο κρυπτογράφησης κι μία κρυπτογραφική συνάρτηση και ενημερώνεται ο πελάτης.
- Ο διακοσμητής στέλνει επιβεβαίωση ταυτότητας σε μορφή ψηφιακού πιστοποιητικού, το οποίο περιέχει όνομα διακοσμητή, αρχή πιστοποίησης και δημόσιο κλειδί για την κρυπτογραφία δημοσίου κλειδιού.
- Ο πελάτης πρέπει να επιβεβαιώσει το ψηφιακό πιστοποιητικό έτσι ώστε να ξεκινήσει η διαδικασία.
- Για την δημιουργία κλειδιού συνεδρίας, πρέπει ο πελάτης είτε να κρυπτογραφήσει έναν τυχαίο αριθμό με το δημόσιο κλειδί του διακοσμητή και γίνεται χρήση αυτού του τυχαίου αριθμού ως κλειδί συνεδρίας, είτε χρησιμοποιεί ανταλλαγή κλειδιών Diffle-Hellman για την δημιουργία μοναδικού κλειδιού συνεδρίας.

Έτσι τελειώνει η χειραψία και αρχίζει η ασφαλής σύνδεση, τα δεδομένα της οποίας κρυπτογραφούνται κι αποκρυπτογραφούνται με το κλειδί συνεδρίας.



Εικόνα 50: Χειραψία σε πρωτόκολα TLS και SSL.

4.5 Πρωτόκολλο Ipsec

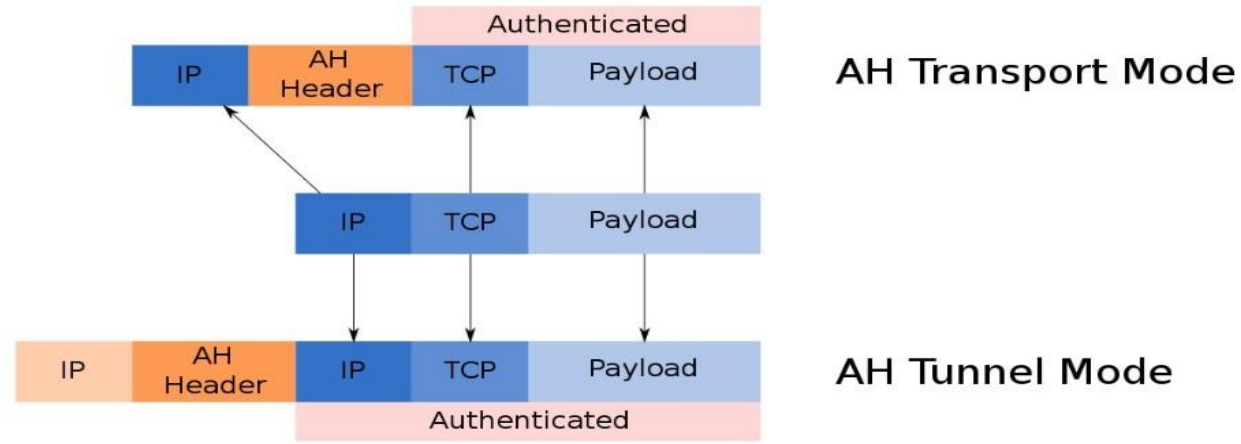
Το Ipsec (Internet Protocol Security) είναι ένα ασφαλές πρωτόκολλο, που κρυπτογραφεί πακέτα δεδομένων για να παρέχει ασφαλή επικοινωνία μεταξύ δύο υπολογιστών, μέσω ενός δικτύου Internet Protocol.
Το Ipsec προστατεύει τη ροή δεδομένων μεταξύ, δύο υπολογιστών (host-to-host), ενός δύο πυλών ασφαλείας (δίκτυο-προς-δίκτυο), κι μιας πύλης ασφαλείας και ενός υπολογιστή (δίκτυο-προς-χρήστη).

Το Ipsec είναι πρότυπο ανοιχτού κώδικα της IPv4 και χρησιμοποιεί τα εξής:

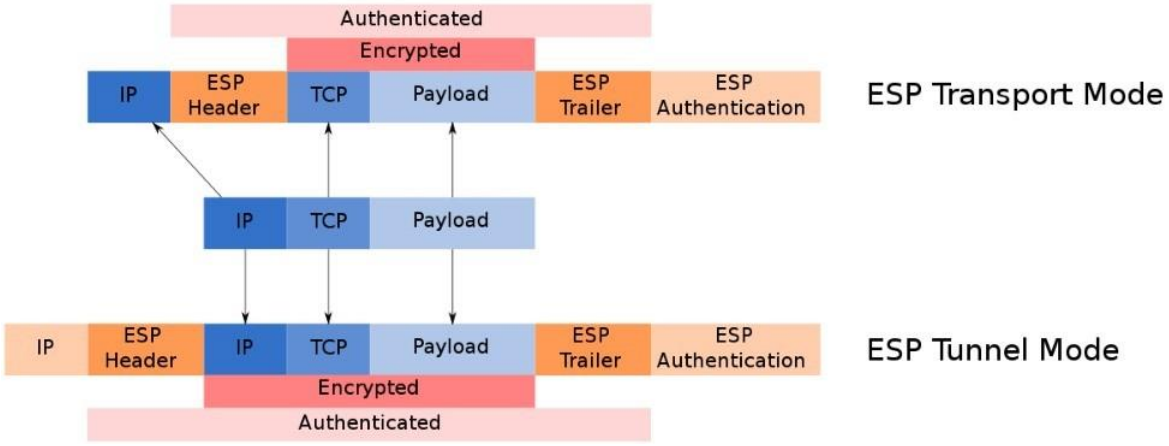
- Authentication header: παρέχει προστασία δεδομένων ένταντι επιθέσεων και την ακεραιότητά τους χωρίς σύνδεση και αντικειμενικοποίηση δεδομένων για IP δεδομένα.
- Encapsulating security payload (ESP): παρέχει ακεραιότητα δεδομένων χωρίς σύνδεση, αυθεντικοποίησης δεδομένων και περιορισμένη εμπιστευτικότητα ροής κίνησης.
- Internet security association and key management protocol: παρέχει το πλαίσιο που γίνεται η ανταλλαγή κλειδιών και η αυθεντικοποίηση. Ο σκοπός του είναι να δημιουργήσει συνδέσεις ασφαλείας για τις λειτουργείες ESP και authentication header.

Authentication header (AH).
Είναι μέρος της σουίτας πρωτοκόλλων Ipsec και εξασφαλίζει την ακεραιότητα χωρίς σύνδεση με την χρήση ενός μυστικού κλειδιού και μίας συνάρτησης κατακερματισμού, και αυθεντικοποιεί τα πακέτα IP. Λειτουργεί απευθείας πάνω από το IP, χρησιμοποιώντας τον αριθμό πρωτοκόλλου IP 51.

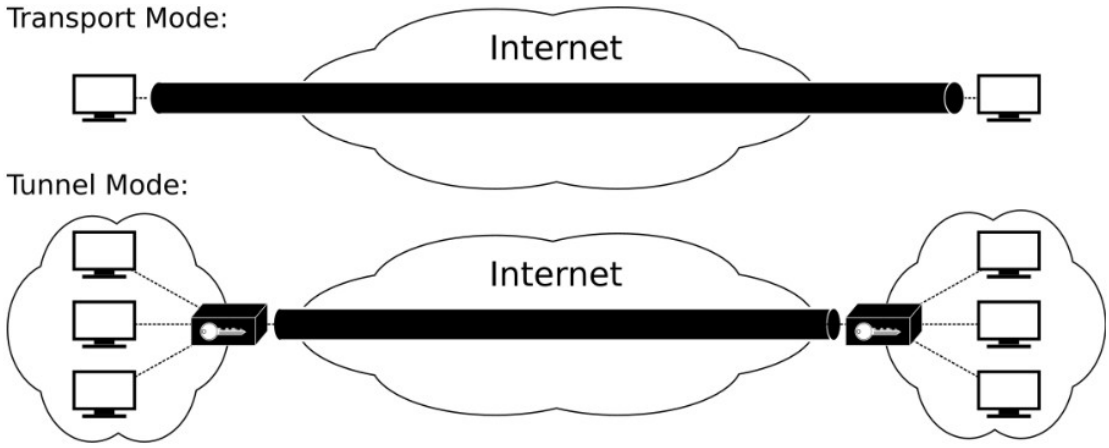
Encapsulating security payload (ESP).
Το ESP είναι κι αυτό μέρος της σουίτας πρωτοκόλλων Ipsec και παρέχει αυθεντικότητα προέλευσης και πιστοποίησης για ολόκληρο το πακέτο IP. Λειτουργεί απευθείας πάνω από το IP, χρησιμοποιώντας τον αριθμό πρωτοκόλλου IP 50.



Εικόνα 51: Authentication header transport και tunnel modes.



Εικόνα 52: ESP transport και tunnel modes.



Εικόνα 53: Transport και Tunnel modes.

4.6 Εφαρμογή Κρυπτογραφίας στην Αποθήκευση και την Επικοινωνία

Πρωτόκολλο HTTPS

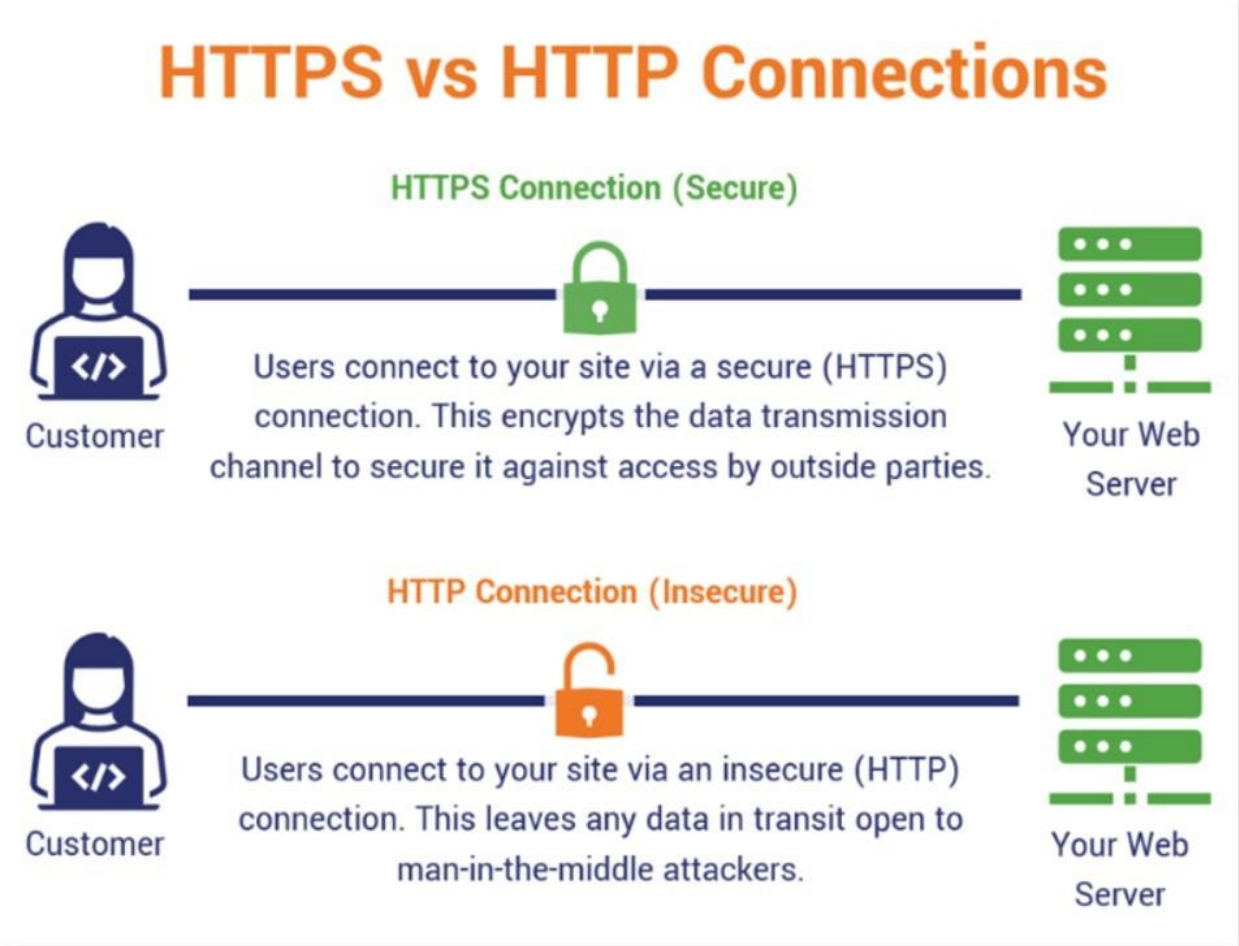
Το παραπάνω πρωτόκολλο ονομάζεται και πρωτόκολλο μεταφοράς υπερκειμένου ασφαλούς επικοινωνίας υποκείμενου HTTP και είναι η ασφαλής έκδοση του πρωτοκόλλου HTTP, το οποίο χρησιμοποιεί το προαναφερόμενο SSL/TSL πρωτόκολλο για κρυπτογράφηση και ελέγχους ταυτότητας.

Το πρωτόκολλο HTTPS επιτρέπει στους χρήστες να μεταδίδουν ευαίσθητα δεδομένα στο διαδίκτυο. Τέτοια δεδομένα είναι αριθμοί τραπεζικών καρτών, κωδικών πρόσβασης. Γι αυτόν τον λόγο είναι ευρέος χρησιμοποιούμενο στους περισσότερους ιστότοπους που χειρίζονται ευαίσθητα δεδομένα.

Η χρήση του SSL/TSL πρωτοκόλλου κρυπτογράφησης αυξάνει την ασφάλεια του πρωτοκόλλου HTTP, το οποίο είναι ευάλωτο σε υποκλοπές, και με την χρήση δημοσίου κλειδιού εξασφαλίζει την ασφαλή μεταφορά δεδομένων. Επίσης, το πρωτόκολλο HTTPS, χρησιμοποιείται συχνά για έλεγχο ταυτότητας (αυθεντικοποίησης) στον οποίο παρουσιάζεται ένα πιστοποιητικό πελάτη που προσδιορίζει τον χρήστη. Τέλος, κάθε έγγραφο ή δεδομένο που αποστέλλεται μέσω ιστοσελίδας που χρησιμοποιεί HTTPS πρωτόκολλο, περιλαμβάνει μία ψηφιακή υπογραφή, η οποία προσδιορίζει ότι το έγγραφο είναι αυθεντικό και δεν έχει τροποποιηθεί από τρίτο.

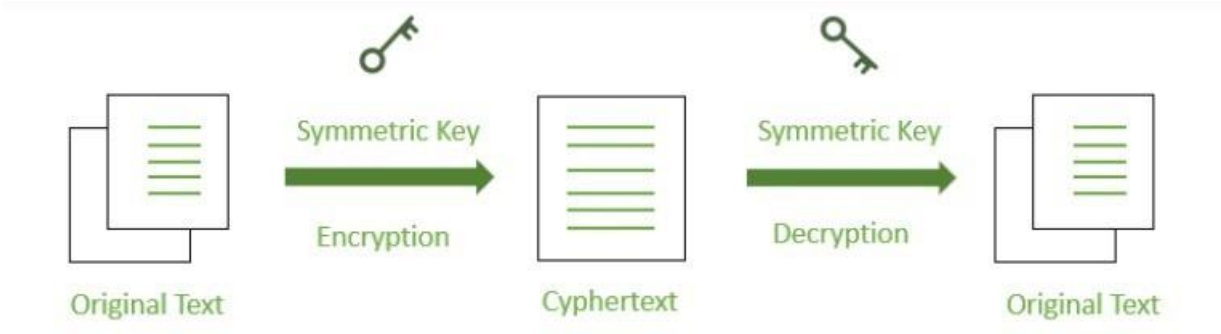
Data encryption

Η κρυπτογράφηση δεδομένων βοηθάει στην προστασία των δεδομένων που αποθηκεύονται, στέλνονται ή λαμβάνονται από υποκλοπές, ενώ χρησιμοποιείται μία συσκευή.
Τέτοια παραδείγματα είναι κωδικοί, μηνύματα, τραπεζικές συναλλαγές και οποιοδήποτε άλλη πληροφορία κειμένου.
Συγκεκριμένα, κάθε πληροφορία κειμένου, αλλάζει μορφή και αποθηκεύεται ή μεταδίδεται ως αδιάβαστη μορφή, η οποία ονομάζεται ciphertext. Για να επιστροφή στην αρχική της μορφή, χρειάζεται αποκρυπρογράφηση και μπορεί να γίνεται με διάφορους τρόπους, οι οποίοι ποικίλουν σε ασφάλεια, ταχύτητα και ευκολία.

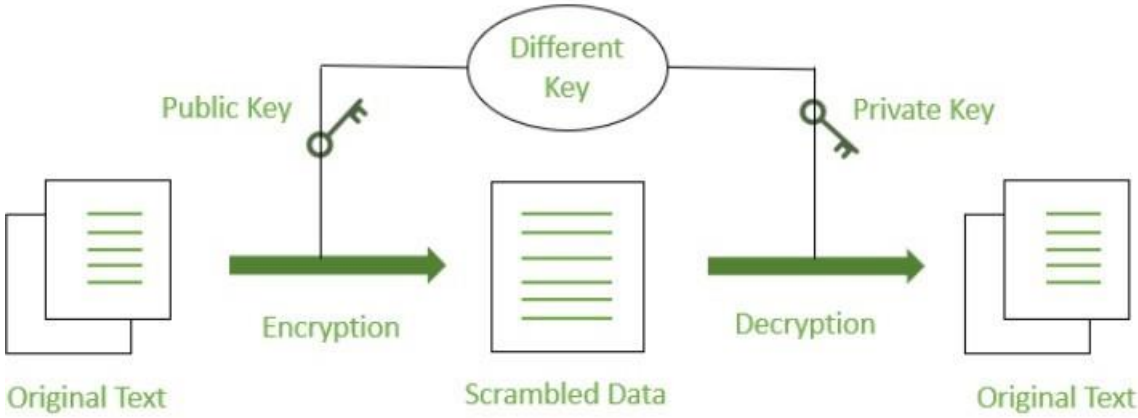


Εικόνα 54: HTTPS και HTTP.

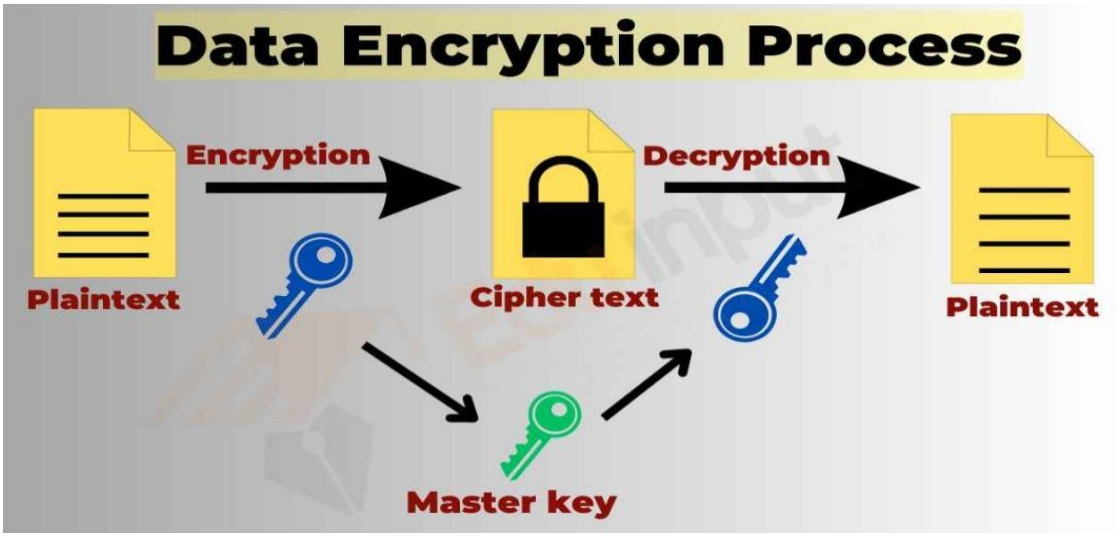
Εικόνα 55: Δημιουργία του HTTPS.



Εικόνα 56: Συμμετρική data encryption.



Εικόνα 57: Ασύμμετρη data encrytion.



Εικόνα 58: Γενική διαδικασία data encryption.

4.7 Υπηρεσίες VPN για ασφαλή περιήγηση

Οι υπηρεσίες Virtual Private Network (VPN) αναδεικνύονται ως ουσιώδες εργαλείο για τη διασφάλιση της ασφαλούς περιήγησης στα smartphones, αντιμετωπίζοντας ουσιαστικούς κινδύνους που απειλούν την ασφάλεια των προσωπικών δεδομένων και την εμπιστευτικότητα των επικοινωνιών. Ας εξετάσουμε πιο λεπτομερώς τα οφέλη και τις λειτουργίες των υπηρεσιών VPN:

1. **Απόκρυψη της διεύθυνσης IP:**
   Η υπηρεσία VPN (Virtual Private Network) λειτουργεί ως ενδιάμεσος μεταξύ της συσκευής του χρήστη και του διαδικτυακού κόσμου, παρέχοντας ένα ασφαλές τούνελ από τη συσκευή προς τον VPN εξυπηρετητή. Κατά τη σύνδεση σε έναν VPN εξυπηρετητή, η πραγματική διεύθυνση IP του χρήστη αντικαθίσταται με μια διεύθυνση που ανήκει στον εξυπηρετητή VPN. Αυτό δημιουργεί ένα επίπεδο ανωνυμίας και απορρύθμισης, καθώς οι ιστότοποι και οι επιθέτοντες δεν μπορούν να παρακολουθήσουν την πραγματική προέλευση της σύνδεσης.
2. **Ασφαλής σύνδεση σε δημόσια δίκτυα:**
   Σε ανοικτά και δημόσια Wi-Fi δίκτυα, όπου η ασφάλεια είναι ευάλωτη λόγω του ανοικτού χαρακτήρα τους, η χρήση μιας υπηρεσίας VPN είναι ιδιαίτερα χρήσιμη. Η VPN προσφέρει έναν ασφαλή τούνελ επικοινωνίας μεταξύ της συσκευής του χρήστη και του εξυπηρετητή VPN.
   Κατά τη χρήση του VPN, όλη η επικοινωνία κρυπτογραφείται, προστατεύοντας έτσι τα δεδομένα του χρήστη από επιθέσεις και παρακολούθηση.
   Αυτό εξασφαλίζει ότι ακόμη και όταν χρησιμοποιείτε δημόσιο Wi-Fi, η επικοινωνία παραμένει ιδιωτική και ασφαλής.
3. **Κρυπτογράφηση δεδομένων:**
   Η κρυπτογράφηση της διακίνησης δεδομένων μεταξύ της συσκευής και του VPN εξυπηρετητή, δημιουργεί ένα ασφαλές και προστατευτικό περιβάλλον.
   Αυτό σημαίνει ότι ακόμη και αν κάποιος προσπαθήσει να παρακολουθήσει τη σύνδεση ή να παραβιάσει την ασφάλεια, τα δεδομένα που μεταφέρονται παραμένουν ασφαλή. Η κρυπτογράφηση εξασφαλίζει ότι τα δεδομένα είναι μη αναγνώσιμα για οποιονδήποτε δεν διαθέτει το κατάλληλο κλειδί πρόσβασης, προσφέροντας έτσι ένα επιπρόσθετο επίπεδο ασφάλειας κατά τη μετάδοση των δεδομένων.
4. **Πρόσβαση σε περιορισμένο περιεχόμενο:**
   Οι χρήστες μπορούν να χρησιμοποιήσουν υπηρεσίες VPN για να παρακάμψουν γεωγραφικούς περιορισμούς και να έχουν πρόσβαση σε περιορισμένο περιεχόμενο, που ίσως είναι απροσπέλαστο σε συγκεκριμένες περιοχές.
   Με τη χρήση ενός VPN, η σύνδεση του χρήστη δρομολογείται μέσω ενός εξυπηρετητή σε άλλη τοποθεσία, η οποία μπορεί να επιτρέπει την πρόσβαση σε περιεχόμενο που διαφορετικά θα ήταν μη διαθέσιμο στην περιοχή του χρήστη. Αυτό μπορεί να περιλαμβάνει πρόσβαση σε ορισμένες υπηρεσίες streaming, ιστοσελίδες ή πλατφόρμες που είναι περιορισμένες μόνο σε συγκεκριμένες περιοχές ή χώρες.

5. **Προστασία από επιθέσεις μεσάζοντα:**

   Οι επιτιθέμενοι που δρουν σε μεσάζοντα, όπως ακόμη και σε ανοικτά δίκτυα, έχουν περιορισμένη πρόσβαση στις δραστηριότητες των χρηστών που χρησιμοποιούν VPN.

   Η κρυπτογραφία που παρέχεται από την υπηρεσία VPN δυσκολεύει τους επιτιθέμενους να παρακολουθήσουν και να παρεμβαίνουν στην επικοινωνία του χρήστη, καθιστώντας την πιο ασφαλή.

   Αυτό προστατεύει τους χρήστες από διάφορες μορφές επιθέσεων, όπως την παρακολούθηση της δικτυακής τους κίνησης ή την κατάχρηση ευαίσθητων δεδομένων.

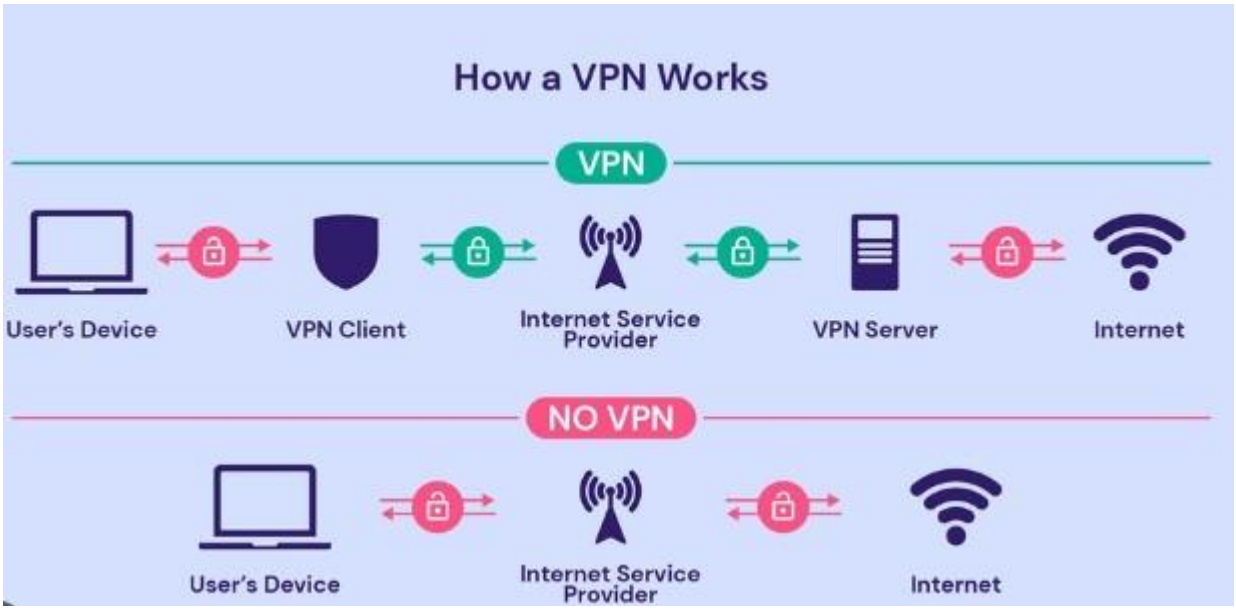
6. **Ανωνυμία κατά την περιήγηση:**

   Η χρήση VPN παρέχει ένα επίπεδο ανωνυμίας, καθώς η πραγματική διεύθυνση IP και άλλες πληροφορίες παραμένουν κρυφές, δίνοντας στους χρήστες την ελευθερία να περιηγούνται ανώνυμα.

   Αυτό σημαίνει ότι οι δραστηριότητες περιήγησης τους δεν μπορούν εύκολα να συσχετιστούν με την πραγματική τους ταυτότητα ή την τοποθεσία τους.

   Η ανωνυμία αυτή μπορεί να είναι χρήσιμη για πολλούς λόγους, συμπεριλαμβανομένης της προστασίας της ιδιωτικής ζωής και της αποφυγής της παρακολούθησης από διάφορους φορείς.

Οι υπηρεσίες VPN αντιπροσωπεύουν έναν αποτελεσματικό μηχανισμό προστασίας για την ασφαλή περιήγηση στο διαδίκτυο μέσω smartphones, εξασφαλίζοντας την εμπιστευτικότητα και την ασφάλεια των επικοινωνιών και των προσωπικών δεδομένων. Με την κρυπτογράφηση της σύνδεσης και την αλλαγή της διεύθυνσης IP, οι VPN προσφέρουν μια επιπλέον στρώση προστασίας, εμποδίζοντας τους κακόβουλους από το να παρακολουθήσουν την δραστηριότητα του χρήστη και να αποκτήσουν πρόσβαση σε προσωπικές πληροφορίες. Με αυτόν τον τρόπο, οι χρήστες μπορούν να περιηγούνται στο διαδίκτυο με ασφάλεια και ανωνυμία, ανεμπόδιστα από περιορισμούς και επιθέσεις.



Εικόνα 59: Λειτουργία VPN.

4.8 Ασφαλείς εφαρμογές και ενημερώσεις λογισμικού

Η ασφάλεια των smartphones δεν είναι μόνο ευθύνη του δικτύου και της σύνδεσης, αλλά και των εφαρμογών που εκτελούνται σε αυτά και των ενημερώσεων λογισμικού. Οι ασφαλείς εφαρμογές και τα ενημερωμένα λογισμικά συνιστούν κρίσιμο στοιχείο για την προστασία από επιθέσεις και απώλεια δεδομένων. Ας εξετάσουμε πιο λεπτομερώς τα ζητήματα αυτά:

1. **Ασφαλείς εφαρμογές:**
    - Η ασφάλεια των smartphones εξαρτάται σε μεγάλο βαθμό από τις εφαρμογές που χρησιμοποιούνται σε αυτά. Η επιλογή εφαρμογών από αξιόπιστες πηγές, όπως τα επίσημα καταστήματα λήψης (Google Play Store, Apple App Store), είναι κρίσιμη. Οι χρήστες πρέπει να διαβάζουν κριτικές, να ελέγχουν τις άδειες πρόσβασης και να ανανεώνουν τις εφαρμογές τους μόνο από τις επίσημες πηγές, προκειμένου να μειώσουν τον κίνδυνο κακόβουλων εφαρμογών που μπορεί να απειλήσουν την ασφάλεια των δεδομένων τους.
2. **Δικαιώματα πρόσβασης:**
    - Οι χρήστες πρέπει να είναι προσεκτικοί όταν χορηγούν δικαιώματα πρόσβασης στις εφαρμογές τους. Οι αδικαιολόγητες απαιτήσεις δικαιωμάτων είναι σημάδι ανησυχίας και μπορεί να υποδεικνύουν ότι η εφαρμογή επιδιώκει πρόσβαση σε προσωπικά δεδομένα χωρίς να υπάρχει πραγματικός λόγος γι' αυτό. Είναι σημαντικό να ελέγχουν οι χρήστες προσεκτικά τις αδειοδοτήσεις που ζητούν οι εφαρμογές πριν τις εγκαταστήσουν, προκειμένου να διασφαλίσουν την ιδιωτικότητα και την ασφάλεια των δεδομένων τους.
3. **Ενημερώσεις λογισμικού:**
    - Η συχνή ενημέρωση του λειτουργικού συστήματος και των εφαρμογών είναι ουσιαστική για τη διατήρηση της ασφάλειας του smartphone. Οι ενημερώσεις συνήθως περιλαμβάνουν διορθώσεις ασφαλείας που αντιμετωπίζουν ενδεχόμενες ευπάθειες στο λογισμικό, βελτιώνοντας την προστασία ενάντια σε διάφορες μορφές επιθέσεων. Επιπλέον, οι ενημερώσεις μπορεί να προσθέτουν νέες λειτουργίες και βελτιώσεις στην εμπειρία χρήστη, κάνοντας το smartphone πιο αποτελεσματικό και ασφαλές.
4. **Κατασκευαστικές ασφάλειας:**
    - Οι κατασκευαστικές πρακτικές ασφαλείας είναι κρίσιμες για την προστασία των smartphones. Μεταξύ αυτών, ο κώδικας πηγαίου κώδικα, η ανάλυση ασφάλειας και ο έλεγχος των εφαρμογών πριν από τη δημοσίευσή τους έχουν ιδιαίτερη σημασία. Με αυτόν τον τρόπο, μπορούν να ανιχνευθούν πιθανές ευπάθειες και να διορθωθούν πριν η εφαρμογή φτάσει στα χέρια των χρηστών, προστατεύοντας έτσι τα προσωπικά δεδομένα και την ασφάλεια των συσκευών.
5. **Διαχείριση αναγνωριστικών:**
    - Η διαχείριση των αναγνωριστικών είναι κρίσιμη για την ασφάλεια των smartphones. Οι εφαρμογές πρέπει να είναι προσεκτικές στον τρόπο που διαχειρίζονται τα προσωπικά δεδομένα των χρηστών, προσφέροντας τη δυνατότητα ελέγχου και την επιλογή των δεδομένων που μοιράζονται. Τα απαραίτητα δεδομένα πρέπει να παρέχονται μόνο όταν είναι απαραίτητα για τη

λειτουργία της εφαρμογής, προστατεύοντας έτσι την ιδιωτικότητα και την ασφάλεια των χρηστών

6. **Αντι-Malware εφαρμογές:**
    - Η εγκατάσταση αντι-Malware εφαρμογών στα smartphones αποτελεί σημαντική προφυλάξη ενάντια σε πιθανές απειλές από κακόβουλο λογισμικό και ιούς. Αυτές οι εφαρμογές μπορούν να σαρώσουν τις συσκευές για εντοπισμό και αφαίρεση ενδεχόμενων απειλών, παρέχοντας έτσι ένα επιπλέον επίπεδο προστασίας για τα προσωπικά δεδομένα των χρηστών και τη σταθερή λειτουργία της συσκευής.

Συνολικά, ο σωστός συνδυασμός ασφαλών εφαρμογών και συχνών ενημερώσεων λογισμικού αποτελεί κρίσιμο παράγοντα για τη διασφάλιση της ασφαλούς και αξιόπιστης λειτουργίας των smartphones. Οι ασφαλείς εφαρμογές που προέρχονται από αξιόπιστες πηγές και οι ενημερώσεις λογισμικού που περιλαμβάνουν διορθώσεις ασφαλείας συνιστούν καίριους παράγοντες για την προστασία των προσωπικών δεδομένων και την αποτροπή ενδεχόμενων απειλών από κακόβουλο λογισμικό και άλλες απειλές στο διαδίκτυο.

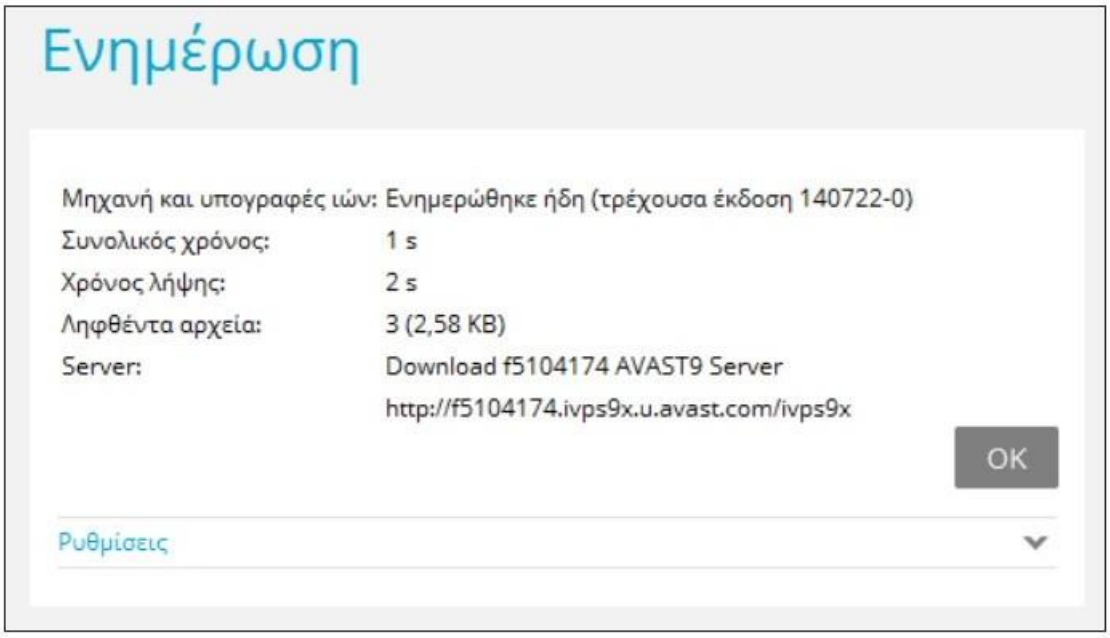
4.9 Anti-virus

Το anti-virus ήταν ένα λογισμικό προστασίας από ιούς, ονομάζεται αλλιώς και anti-malware. Ο σκοπός του είναι η απαγόρευση ιών το σύστημα, ο εντοπισμός τους σε περίπτωση που υπάρχουν και η αφαίρεσή τους.
Τα τελευταία χρόνια, με την αύξηση διάφορων κακόβουλων ενεργειών, ο σκοπός του έχει αλλάξει και συμπεριλαμβάνει προστασία από spyware, trojan horses, ransoware, keylogers, backdoor rootkits και άλλα.

Σε αντίθεση με διάφορες εφαρμογές, το anti-virus πρέπει να είναι ενεργεί καθ' όλη την διάρκεια λειτουργίας της συσκευής, δηλαδή να ανοίγει με την ενεργοποίησή της και να παραμένει ανοιχτή στο παρασκήνιο.
Προσφέρει προστασία σε πραγματικό χρόνο, ελέγχοντας οποιοδήποτε αρχείο εισέρχεται ή χρησιμοποιείται από την συσκευή, είτε με την θέληση του χρήση είτε χωρίς.

Τα anti-virus διαθέτουν πρόσβαση σε μία βάση δεδομένων όπου περιέχει τα χαρακτηριστικά διάφορων ιών, trojans και malware που έχουν βρεθεί στο παρελθόν, σε διάφορες συσκευές στον κόσμο. Αυτά χαρακτηριστικά ονομάζονται υπογραφές ιών.

Κατά την σάρωση των αρχείων από το anti-virus, το πρόγραμμα προσπαθεί να βρει και να συγκρίνει τέτοια χαρακτηριστικά με τα χαρακτηριστικά της βάσης δεδομένων, έτσι ώστε να καταλάβει ότι έχει υπάρξει ιός.
Αναγκαία προϋπόθεση είναι λοιπόν, η συχνή ανανέωση των anti-virus, ώστε να μπορούν να ελέγχουν για χαρακτηριστικά νέων ιών, οι οποίοι παράγονται καθημερινώς.

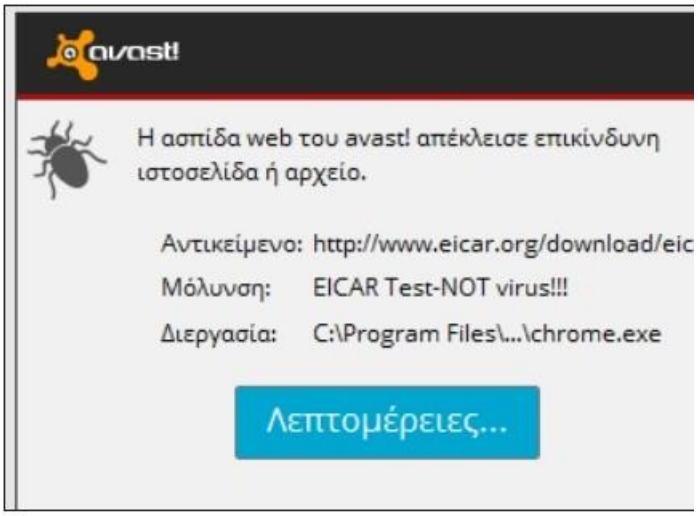


Εικόνα 60: Παράδειγμα ενημέρωσης anti-virus.

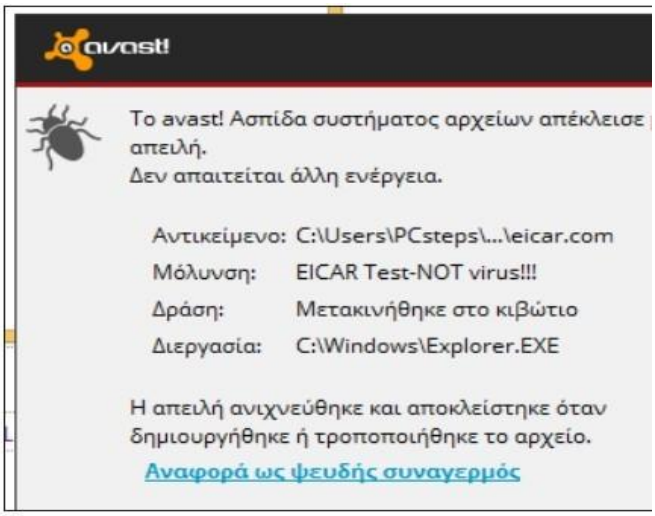
Ακόμα ένας έλεγχος που περιλαμβάνουν ταν anti-viurs, είναι ο έλεγχος των heuristics των αρχείων. Δηλαδή ο έλεγχος του κώδικα των εφαρμογών για περίεργες συμπεριφορές.

Ο έλεγχος αυτός δεν πρέπει να είναι πολύ αυστηρός, γιατί θα βγάζει συνεχώς false positive ενδείξεις, αλλά ούτε και πολύ χαλαρός γιατί κακόβουλες εφαρμογές θα μπορούν να ξεγελάσουν τον έλεγχο και να περάσουν malware στο σύστημά.

Ο έλεγχος των αρχείων από το anti-virus γίνεται μόλις αλληλεπιδράσει η συσκευή με αυτό το αρχείο. Είτε δηλαδή στο άνοιγμα, είτε στο κατέβασμα, είτε κατά την χρήση το από άλλη εφαρμογή.Επίσης ελέγχονται αυτόματα από το anti-virus αρχεία περίεργων καταλήξεων, αλλά και αρχεία που συνήθως μεταβιβάζουν ιούς όπως τα .zip αρχεία.



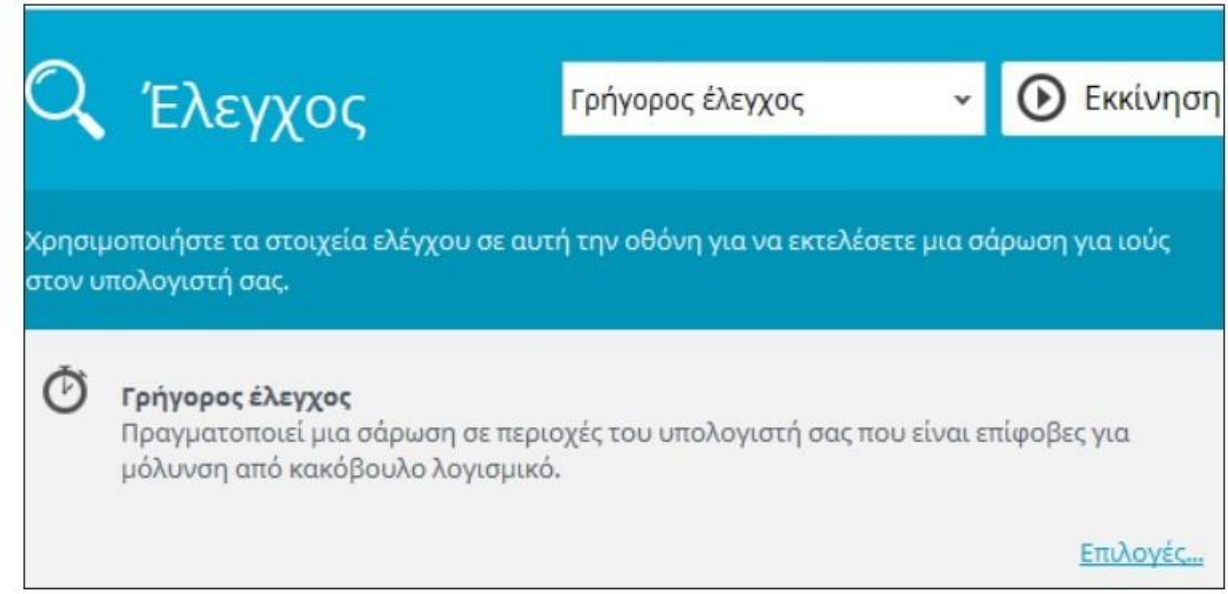
Εικόνα 61: Παράδειγμα εύρεσης κακόβουλης



Εικόνα 62: Παράδειγμα εύρεσης κακόβουλης εφαρμογής από anti-virus.

Το κύριο μειονέκτημα των anti-virus προκύπτει από την συνεχή εργασία της εφαρμογής και είναι η κατανάλωση πόρων, σε μέγεθος ανάλογα με τις επιλογές ασφαλείας που υπάρχουν.

Οι εταιρίες βέβαια προσπαθούν να κρατούν ελαφριά τα προγράμματά τους, διατηρώντας τον έλεγχο σε λογικά αλλά ασφαλή πλαίσια και να δίνεται μεγαλύτερη βαρύτητα στους χειροκίνητους ελέγχους.
Ο χειροκίνητος έλεγχος προσφέρει διάφορες επιλογές λειτουργίας, κάποιες πιο γρήγορες, αλλά και κάποιες σε μεγαλύτερο βάθος και πιο χρονοβόρες. Προτείνεται εβδομαδιαία να γίνεται ένας γρήγορος έλεγχος της συσκευής και μηνιαία ένα πλήρες έλεγχος της συσκευής.



Εικόνα 63: Γρήγορος έλεγχος συστήματος.

Εικόνα 64: Πλήρες έλεγχος συστήματος.

5. Προτεινόμενες Πρακτικές και Συμβουλές

Για την ασφαλή χρήση των smartphones, είναι ουσιώδες να ακολουθούνται προτεινόμενες πρακτικές και συμβουλές που ενισχύουν την προστασία των προσωπικών δεδομένων και την αποτροπή πιθανών κινδύνων. Κρίσιμα βήματα περιλαμβάνουν τον προσεκτικό χειρισμό των προσωπικών πληροφοριών, την αποφυγή επικίνδυνων συνδέσεων και την ενίσχυση της ασφάλειας της συσκευής.

5.1 Πώς να διατηρείτε το smartphone σας ασφαλές

Η διατήρηση της ασφάλειας του smartphone, είναι ένας ζωτικός παράγοντας για την προστασία των προσωπικών σας δεδομένων και την αποφυγή ενδεχόμενων απειλών. Ορισμένες σημαντικές πρακτικές που μπορείτε να ακολουθήσετε περιλαμβάνουν:

1. **Κλειδώστε τη συσκευή σας:**
   Για να διασφαλίσετε την ασφάλεια των προσωπικών σας δεδομένων, ενεργοποιήστε τις επιλογές κλειδώματος οθόνης, όπως κωδικός πρόσβασης, κωδικός PIN ή αναγνώριση προσώπου στη συσκευή σας.
   Αυτό θα αποτρέψει την ανεπιθύμητη πρόσβαση σε προσωπικά σας δεδομένα σε περίπτωση απώλειας ή κλοπής του smartphone.
2. **Ενημερώσεις λογισμικού:**
   Είναι σημαντικό να βεβαιωθείτε ότι το λειτουργικό σύστημα και οι εφαρμογές σας είναι πάντα ενημερωμένα.
   Οι ενημερώσεις συχνά περιλαμβάνουν βελτιώσεις ασφαλείας που είναι ουσιώδους σημασίας για την προστασία των δεδομένων σας.
3. **Αξιόπιστες εφαρμογές:**
   Κατεβάστε εφαρμογές μόνο από αξιόπιστες πηγές όπως τα επίσημα καταστήματα λήψης εφαρμογών (App Stores).
   Προσέξτε τις κριτικές και τις αξιολογήσεις προτού εγκαταστήσετε οποιαδήποτε εφαρμογή.
4. **Σύνδεση σε ασφαλή δίκτυα:**
   Αποφύγετε τη σύνδεση σε μη ασφαλή δίκτυα Wi-Fi. Χρησιμοποιήστε επίσης εφαρμογές VPN για επιπλέον επίπεδο ασφαλείας κατά τη σύνδεση σε δημόσια δίκτυα.
5. **Εφαρμογές Ασφαλείας:**
   Εγκαταστήστε αξιόπιστες εφαρμογές ασφαλείας και αντι-Malware που μπορούν να προστατεύσουν τη συσκευή σας από επιθέσεις.
6. **Αντίγραφα Ασφαλείας:**
   Κάντε τακτικά αντίγραφα ασφαλείας των δεδομένων σας. Αυτό εξασφαλίζει ότι αν τυχόν χαθεί ή κλαπεί το smartphone, δεν θα χάσετε σημαντικές πληροφορίες.

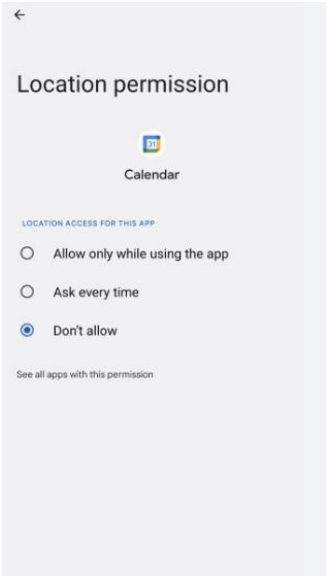
Ακολουθώντας αυτές τις πρακτικές, μπορείτε να διασφαλίσετε ότι το smartphone σας παραμένει ασφαλές και οι προσωπικές σας πληροφορίες παραμένουν προστατευμένες.

5.2 Προτεινόμενες Ρυθμίσεις Ασφαλείας

Η επιτυχημένη χρήση ενός smartphone, συνδέεται σημαντικά με τις σωστές ρυθμίσεις ασφαλείας. Η εφαρμογή κατάλληλων ρυθμίσεων μπορεί να προστατεύσει τα προσωπικά δεδομένα και να αποτρέψει απειλές ασφαλείας. Παρακάτω παρουσιάζονται ορισμένες σημαντικές προτεινόμενες ρυθμίσεις:

1. **Ενημερώσεις εφαρμογών:**
   Ρυθμίστε τις εφαρμογές να ενημερώνονται αυτόματα για να επιτρέψετε την άμεση εγκατάσταση ενημερώσεων ασφαλείας.
2. **Έλεγχος εφαρμογών:**
   Ενεργοποιήστε τον έλεγχο εφαρμογών, επιτρέποντας την πρόσβαση μόνο σε αναγκαίες άδειες και αποφεύγοντας ύποπτες εφαρμογές.
3. **Έλεγχος τοποθεσίας:**
   Ρυθμίστε τις ρυθμίσεις τοποθεσίας για κάθε εφαρμογή, παρέχοντας πρόσβαση μόνο όταν είναι απαραίτητο.
4. **Διαχείριση συσκευής:**
   Ενεργοποιήστε τις ρυθμίσεις διαχείρισης συσκευής για απομακρυσμένο εντοπισμό, κλείδωμα ή διαγραφή δεδομένων σε περίπτωση απώλειας.
5. **Κρυπτογράφηση δεδομένων:**
   Ενεργοποιήστε την κρυπτογράφηση δεδομένων για προστασία των αποθηκευμένων πληροφοριών από ανεπιθύμητη πρόσβαση.

Η σωστή ρύθμιση αυτών των παραμέτρων ενισχύει την ασφάλεια του smartphone, παρέχοντας την απαραίτητη προστασία από διάφορες απειλές και εξασφαλίζοντας την ιδιωτικότητα των χρηστών.



Εικόνα 65: Απόρριψη αιτημάτων μη αναγκαίων αδειών.

5.3 Πώς να Αντιμετωπίζετε Περιπτώσεις Απώλειας ή Κλοπής

Η απώλεια ή η κλοπή ενός smartphone μπορεί να είναι επιβλαβής για την ασφάλεια των προσωπικών δεδομένων. Για να αντιμετωπίσετε αποτελεσματικά αυτές τις καταστάσεις, πρέπει να λάβετε συγκεκριμένα μέτρα:

1. **Ενεργοποίηση δυνατότητας εντοπισμού:**
   Μια άλλη σημαντική πτυχή της ασφάλειας των smartphones είναι η δυνατότητα εντοπισμού και απομακρυσμένης διαγραφής δεδομένων σε περίπτωση απώλειας ή κλοπής της συσκευής.
   Οι χρήστες μπορούν να χρησιμοποιήσουν λειτουργίες όπως το "Find My iPhone" ή το "Find My Device" για να εντοπίσουν τη συσκευή τους σε περίπτωση απώλειας και να προστατεύσουν τα προσωπικά τους δεδομένα απομακρύνοντάς τα από την κλεμμένη συσκευή.
2. **Απομακρυσμένο κλείδωμα και διαγραφή δεδομένων:**
   Σε περίπτωση απώλειας του smartphone σας, είναι ουσιώδους σημασίας να αντιδράσετε άμεσα, για να προστατεύσετε τα προσωπικά σας δεδομένα από τυχόν ανεπιθύμητη πρόσβαση.
   Μια αποτελεσματική προσέγγιση είναι η χρήση της δυνατότητας απομακρυσμένου κλειδώματος ή διαγραφής δεδομένων.
   Αυτή η λειτουργία σάς επιτρέπει να κλειδώσετε τη συσκευή σας από απόσταση ή ακόμη και να διαγράψετε τα δεδομένα της εντελώς, εξασφαλίζοντας έτσι ότι κανείς άλλος δεν θα έχει πρόσβαση σε ευαίσθητες πληροφορίες.
3. **Ενημέρωση του παρόχου υπηρεσιών:**
   Σε περίπτωση απώλειας της συσκευής σας, είναι σημαντικό να επικοινωνήσετε αμέσως με τον πάροχο των υπηρεσιών σας. Ζητήστε να απενεργοποιήσετε την κάρτα SIM που χρησιμοποιείτε στην χαμμένη συσκευή.
   Αυτό μπορεί να αποτρέψει την ανεπιθύμητη χρήση της συσκευής από τρίτους. Επιπλέον, ο πάροχος υπηρεσιών μπορεί να σας παρέχει πληροφορίες σχετικά με τα επόμενα βήματα που πρέπει να ακολουθήσετε.
   Αυτή η άμεση αντίδραση μπορεί να συμβάλει στην προστασία των προσωπικών σας δεδομένων και στην αποτροπή πιθανής κατάχρησης της συσκευής.
4. **Καταγγελία στις αρχές:**
   Σε περίπτωση απώλειας ή κλοπής της συσκευής σας, είναι σημαντικό να καταγγείλετε το περιστατικό στις τοπικές αστυνομικές αρχές. Κατά την καταγγελία, παρέχετε λεπτομερείς πληροφορίες σχετικά με το πώς χάθηκε ή κλάπηκε η συσκευή σας.
   Αυτό μπορεί να βοηθήσει τις αρχές να δράσουν γρήγορα και να προσπαθήσουν να εντοπίσουν τη συσκευή σας, ενώ ταυτόχρονα δημιουργεί μια επίσημη ηχογραφημένη αναφορά για το περιστατικό.
5. **Επικοινωνία με επαφές έκτακτης ανάγκης:**
   Σε περίπτωση απώλειας ή κλοπής της συσκευής σας, είναι σημαντικό να ενημερώσετε τους ανθρώπους έκτακτης ανάγκης που σας αποθηκευμένους στη συσκευή σας, για το περιστατικό και για τυχόν αλλαγές στις επαφές σας. Αυτό μπορεί να συμπεριλαμβάνει μέλη της οικογένειάς σας, φίλους ή άλλα άτομα που

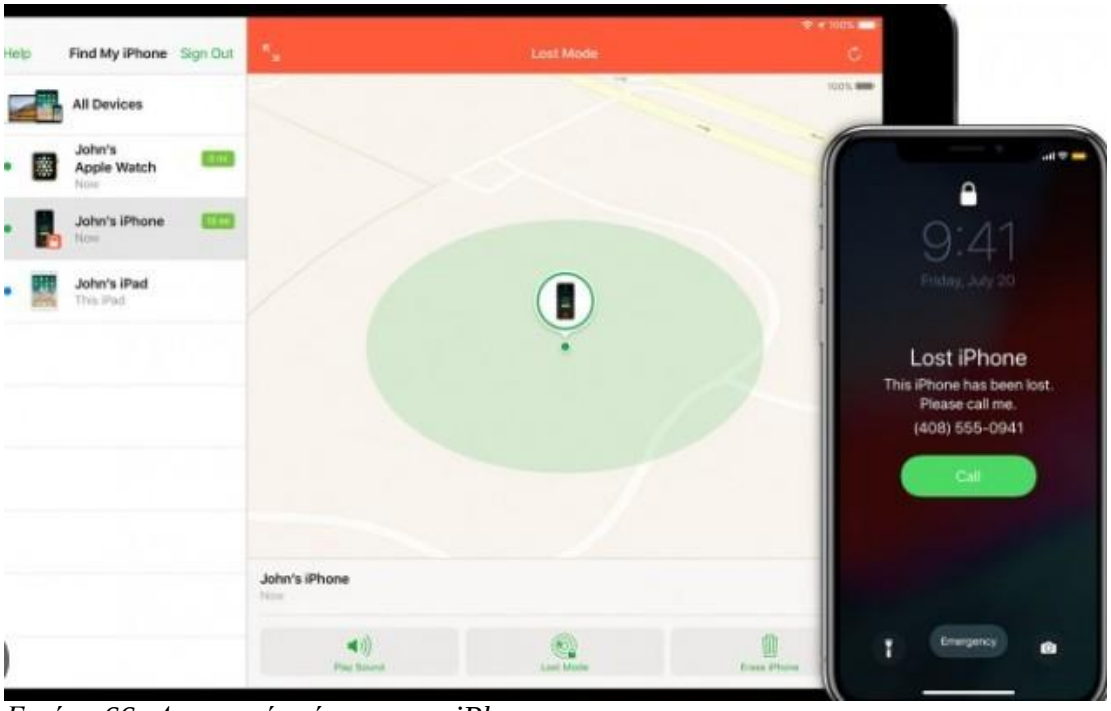
μπορεί να χρειαστεί να ενημερωθούν για την κατάστασή σας. Η ενημέρωσή τους μπορεί να βοηθήσει στην αντιμετώπιση της κατάστασης και στην παροχή υποστήριξης εάν απαιτηθεί.

6. **Αλλαγή κωδικού πρόσβασης:**

   Σε περίπτωση που υπάρχει η πιθανότητα ότι ο κωδικός πρόσβασής σας έχει διαρρεύσει, είναι σημαντικό να αλλάξετε τον κωδικό άμεσα για επιπλέον ασφάλεια

   Επιλέξτε έναν ισχυρό κωδικό που να περιλαμβάνει συνδυασμούς αριθμών, γραμμάτων και ειδικών χαρακτήρων για να ενισχύσετε την ασφάλειά σας.

Τα παραπάνω μέτρα σας επιτρέπουν να αντιδράσετε άμεσα σε καταστάσεις απώλειας ή κλοπής, διασφαλίζοντας παράλληλα την προστασία των προσωπικών σας δεδομένων και μειώνοντας τους κινδύνους ανεπιθύμητης πρόσβασης στις πληροφορίες σας. Με την άμεση αντίδραση και την εφαρμογή των παραπάνω μέτρων, μπορείτε να ελέγχετε την κατάσταση και να προστατεύετε τα προσωπικά σας δεδομένα από ανεπιθύμητη πρόσβαση.



Εικόνα 66: Λειτουργία εύρεσης του iPhone μου.

6. Συμπεράσματα

Στον σύγχρονο ψηφιακό κόσμο, η ασφάλεια των smartphones αποτελεί πρωταρχική προτεραιότητα για την προστασία των προσωπικών δεδομένων και την αποτροπή ανεπιθύμητης πρόσβασης σε ευαίσθητες πληροφορίες. Η εργασία αυτή εξετάζει τη σημασία της ασφάλειας στα smartphones, επικεντρώνοντας την προσοχή στην ιδιωτικότητα ως κρίσιμο παράγοντα προστασίας.

Στο πλαίσιο της ασφάλειας, η ιδιωτικότητα αναδεικνύεται ως ουσιώδης διαδικασία για την εξασφάλιση των προσωπικών δεδομένων. Οι χρήστες έχουν την ευκαιρία να προστατεύουν τις συσκευές τους μέσω της χρήσης ασφαλών κωδικών πρόσβασης, της διπλής επαλήθευσης, και άλλων τεχνολογιών ιδιοτικότητας.

Επιπλέον, αναλύθηκαν οι απειλές και οι κίνδυνοι στον κυβερνοχώρο, με έμφαση σε ιούς, κακόβουλο λογισμικό και phishing επιθέσεις. Η αντιμετώπιση αυτών των κινδύνων απαιτεί τη συνειδητοποίηση των χρηστών και την εφαρμογή αποτελεσματικών μέτρων προστασίας.

Τέλος, παρουσιάστηκαν προτεινόμενες πρακτικές και συμβουλές για τη διατήρηση ασφαλούς smartphone, περιλαμβάνοντας τη σημασία της ενημέρωσης του λογισμικού, τη χρήση υπηρεσιών VPN, και τη διαχείριση περιπτώσεων απώλειας ή κλοπής.

Συνοψίζοντας, η ασφάλεια στα smartphones είναι εντονότερα επίκαιρη στην εποχή της ψηφιακής επανάστασης. Η ιδιωτικότητα αποτελεί βασικό πυλώνα προστασίας, και η προαγωγή ευαισθητοποίησης και εφαρμογής ασφαλών πρακτικών είναι απαραίτητη για τη διατήρηση της ασφάλειας και της ιδιοτικότητας των χρηστών.

7. Μελλοντικές Τάσεις

7.1 Νέες τεχνολογίες και εξελίξεις

Καθώς η τεχνολογία συνεχίζει να εξελίσσεται με ραγδαίους ρυθμούς, ο τομέας της ασφάλειας και ιδιοτικότητας στα smartphones αναμένεται να υιοθετήσει καινοτόμες λύσεις και τεχνολογίες για την προστασία των χρηστών. Ορισμένες μελλοντικές τάσεις περιλαμβάνουν:

1. **Βελτιωμένη βιομετρική αναγνώριση:**
   Η βιομετρική αναγνώριση αναμένεται να εξελιχθεί περαιτέρω με την εφαρμογή προηγμένων τεχνολογιών και προσεγμένων αλγορίθμων. Μελλοντικά, ενδέχεται να δούμε επίσης την ενσωμάτωση νέων μεθόδων βιομετρικής αναγνώρισης ή η αναγνώριση βαθμού κινδύνου με βάση το μοτίβο περιπάτου.
   Αυτές οι καινοτομίες αναμένεται να δώσουν έμφαση στην ασφάλεια και την ακρίβεια της αναγνώρισης, καθιστώντας τα συστήματα βιομετρικής αναγνώρισης ακόμη πιο αξιόπιστα και αποτελεσματικά.
2. **Blockchain για προστασία δεδομένων:**
   Η τεχνολογία blockchain, διαθέτει το δυναμικό να επανασχεδιάσει τον τρόπο που αποθηκεύονται και επεξεργάζονται τα προσωπικά δεδομένα. Με τη χρήση blockchain, τα δεδομένα αποθηκεύονται σε αλυσίδες μπλοκ που είναι κρυπτογραφημένες και αδιαλλάκτιστες, επιτρέποντας την ασφαλή αποθήκευση και επεξεργασία των πληροφοριών.
   Κάθε νέο δεδομένο που προστίθεται στην αλυσίδα επαληθεύεται και επιβεβαιώνεται από το σύνολο της δικτυακής κοινότητας, ενισχύοντας την ασφάλεια και την εμπιστοσύνη στα δεδομένα.
   Επιπλέον, η αδιαλλάκτη φύση της blockchain δυσκολεύει την τροποποίηση ή την αλλοίωση των δεδομένων, προσφέροντας ένα υψηλό επίπεδο ασφάλειας και ακεραιότητας .
3. **Ενίσχυση της τεχνητής νοημοσύνης:**
   Η ενσωμάτωση της τεχνητής νοημοσύνης στην ασφάλεια των smartphones έχει τη δυνατότητα να αναβαθμίσει το επίπεδο προστασίας και ανίχνευσης κινδύνων σε πραγματικό χρόνο.
   Η τεχνητή νοημοσύνη μπορεί να αναλύσει μεγάλους όγκους δεδομένων από διάφορες πηγές, όπως αλγόριθμους συμπερασμού και μοτίβων, για να αναγνωρίσει ανωμαλίες και ανεπιθύμητη συμπεριφορά.
   Με την επίγνωση των τρεχουσών απειλών και των τελευταίων τάσεων στον κυβερνοχώρο, η τεχνητή νοημοσύνη μπορεί να αντιμετωπίσει απειλές, όπως τα malware, τις phishing επιθέσεις και άλλες μορφές κυβερνοεγκλήματος με μεγαλύτερη αποτελεσματικότητα και ταχύτητα.
   Επιπλέον, η συνεχής εκπαίδευση και εξέλιξη των αλγορίθμων μπορεί να επιτρέψει την αντίδραση σε νέες απειλές που εμφανίζονται στον ψηφιακό χώρο, διατηρώντας ένα υψηλό επίπεδο προστασίας των συσκευών και των δεδομένων τους.

4. 5G και Edge computing:

Η συνδεσιμότητα 5G και η χρήση της υπολογιστικής επεξεργασίας στο Edge, ανοίγουν το δρόμο για πιο αποτελεσματικά μέτρα ασφαλείας στον κυβερνοχώρο των smartphones.

Η ταχεία ανταπόκριση της τεχνολογίας 5G συνδυασμένη με τη δυνατότητα χρήσης της υπολογιστικής ισχύος στην άκρη του δικτύου (Edge computing), επιτρέπει την εκτέλεση προηγμένων αλγορίθμων ανίχνευσης και αντίδρασης σε επιθέσεις απευθείας στη συσκευή ή σε πολύ κοντινές απομακρυσμένες τοποθεσίες.

Αυτό σημαίνει ότι ο χρόνος αντίδρασης σε επιθέσεις μπορεί να μειωθεί σημαντικά, καθιστώντας το σύστημα ασφαλέστερο και πιο αποτελεσματικό στην αντιμετώπιση κυβερνοεπιθέσεων.

Επιπλέον, η ανάπτυξη προηγμένων αλγορίθμων εκμάθησης, που λειτουργούν σε πραγματικό χρόνο μπορεί να ενισχύσει την αυτόματη ανίχνευση και απόκριση σε επιθέσεις, προστατεύοντας τα δεδομένα και την ιδιωτικότητα των χρηστών.

5. **Κβαντική κρυπτογραφία:**

   Η κβαντική ασφάλεια αντιπροσωπεύει μια καινοτόμο προσέγγιση στην κρυπτογραφία, η οποία μπορεί να αντιμετωπίσει τις προκλήσεις που θα αντιμετωπίζουν τα μελλοντικά υπολογιστικά συστήματα.

   Η κβαντική τεχνολογία εκμεταλλεύεται τις ιδιότητες της κβαντικής μηχανικής για τη δημιουργία ανθεκτικών μηχανισμών κρυπτογράφησης.

   Αντίθετα με τις κλασικές μεθόδους κρυπτογράφησης που βασίζονται σε προβλήματα υπολογιστικής δυσκολίας, οι αλγόριθμοι κβαντικής κρυπτογραφίας βασίζονται σε μαθηματικά προβλήματα που είναι αδύνατο να λυθούν ακόμα και από τους πιο ισχυρούς κβαντικούς υπολογιστές.

   Με αυτόν τον τρόπο, η κβαντική ασφάλεια προσφέρει ένα υψηλό επίπεδο προστασίας από επιθέσεις και παραβιάσεις της ασφάλειας δεδομένων, ενισχύοντας την ασφάλεια των μελλοντικών ψηφιακών συστημάτων.

Αυτές οι εξελίξεις αναμένεται να οδηγήσουν στη δημιουργία πιο ασφαλών, έξυπνων και προστατευμένων smartphones, ενισχύοντας έτσι την ασφάλεια και την ιδιωτικότητα των συσκευών και των δεδομένων τους.

Η υιοθέτηση προηγμένων τεχνολογιών όπως η βιομετρική αναγνώριση, η κρυπτογράφηση δεδομένων με τη χρήση blockchain, η τεχνητή νοημοσύνη για τον εντοπισμό κινδύνων και οι ταχείες συνδέσεις 5G σε συνδυασμό με την υπολογιστική επεξεργασία στο Edge, αναμένεται να ενισχύσουν την ασφάλεια των smartphones και να προστατεύσουν τα προσωπικά δεδομένα των χρηστών από πιθανές απειλές και επιθέσεις.

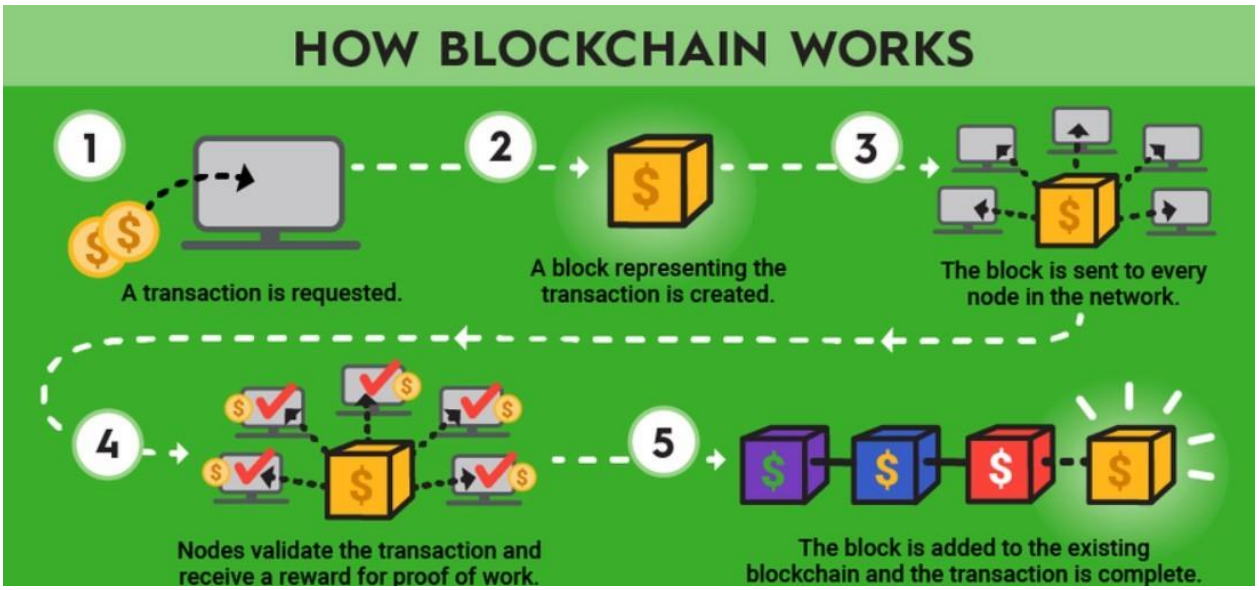
7.2 Blockchain

Το blockchain είναι ένα είδος βάσης δεδομένων όπου ονομάζεται και αποκεντρωμένο ψηφιακό καθολικό. Τα δεδομένα αυτής της βάσης δεδομένων οργανώνονται σε block, χρονολογικά διατεταγμένα και κρυπτογραφημένα.

Σε ένα δίκτυο blockchain δεν υπάρχει μεσάζον που να ελέγχει την ροή των δεδομένων κι αυτά ελέγχονται από ένα κατανεμημένο δίκτυο υπολογιστών και διατηρούν την ακεραιότητα του δικτύου. Δηλαδή η κύρια αρχή του blockchain είναι πως η ισχύς ελέγχου δεν καθορίζεται από συγκεκριμένη οντότητα, αλλά από τους χρήστες του.

Λειτουργία

Στον πυρήνα καταγράφονται με ασφάλεια οι συναλλαγές μεταξύ δύο χρηστών παρέχοντας προστασία. Αυτά τα δεδομένα καταγράφονται από ένα παγκόσμιο κατανεμημένο δίκτυο ειδικών υπολογιστών που ονομάζονται κόμβοι. Όταν ξεκινάει μία συναλλαγή, τότε μεταδίδεται στο δίκτυο και κάθε κόμβος την ταυτοποιεί, ελέγχοντας τις ψηφιακές υπογραφές κι άλλα δεδομένα. Εφόσον όλοι οι κόμβοι ταυτοποιήσουν αυτήν την συνναλαγή, τότε θα αποθηκευτεί σε έναν κόμβο, μαζί με άλλες ταυτοποιημένες συνναλαγές.
Η σύνδεση των blocks μεταξύ τους γίνεται με κρυπτογραφικές μεθόδους κι έτσι σχηματίζεται το blockchain.
Μία σημαντική κρυπτογραφική μέθοδος που χρησιμοποιείται είναι το hashing, η οποία μετατρέπει μία εισροή σε μία σειρά χαρακτήρων (εκροή). Οι συναρτήσεις hash σπάνια θα παράγουν εκροές όμοιες μεταξύ τους, όσο μικρές κι αν είναι οι δύο διαφορετικές εισροές. Επίσης οι συναρτήσεις hash είναι μίας κατεύθυνσης, όπως σημαίνει δεν είναι αντιστρεπτές και δεν είναι εφικτό να βρεθούν οι εισροές με την γνώση των εκροών.



Εικόνα 67: Λειτουργία του blockchain.

Κάθε block του blockchain έχει το hash του προηγούμενου bock κι έτσι δημιουργείται μία αλυσίδα από blocks, η οποία για να αλλάξει σε κάποιο block, πρέπει να αλλαχτούν κι όλα τα επόμενα blocks.

Χρησιμοποιείται επίσης, η κωδικοποίηση δημοσίου κλειδιού στα blockchain, όπου κάθε χρήστης μέσω του ιδιωτικού του κλειδιού, δημιουργεί την ψηφιακή του υπογραφή στην συναλλαγή, ενώ οι υπόλοιποι χρήστες την επαληθεύουν μέσω του δημοσίου κλειδιού. Αυτό επίσης, προσδίδει ασφάλεια στις συναλλαγές, αφού μόνο ο εκάστοτε χρήστης εξουσιοδοτεί μία συναλλαγή, ενώ οι υπόλοιποι επαληθεύουν την ψηφιακή υπογραφή του.

Τέλος, άλλο ένα χαρακτηριστικό είναι η διαφάνεια, όπου οποιοσδήποτε χρήστης μπορεί να κάνει έλεγχο στα δεδομένα ενός δημόσιου blockchain.

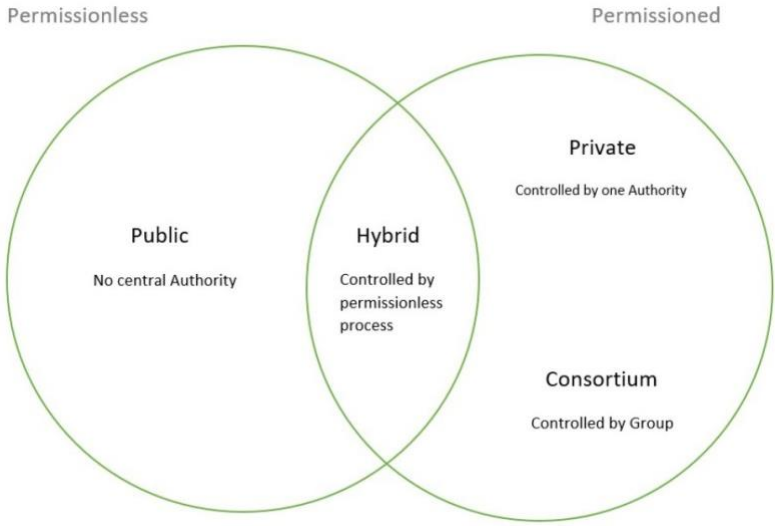
Μηχανισμός ομοφωνίας
Ο μηχανισμός ομοφωνίας επιτρέπει την επιβεβαίωση εγκυρότητας οποιασδήποτε συναλλαγής, μέσω ομοφωνίας διάφορων παραγόντων, ακόμη κι αν μερικοί αποτύχουν, αφού δεν υπάρχει κάποιος μεζάσον. Δηλαδή, εξασφαλίζεται ότι οι κόμβοι έχουν το ίδιο αντίγραφο του καθολικού. Αυτό σημαίνει πως, ακόμη κι αν υπάρχουν κακόβουλοι κόμβοι, πρέπει να υπάρχει ένα αντίγραφο των δεδομένων σε κάθε κόμβο για την σωστή και ασφαλή λειτουργία του blockchain. Δύο ευρέος χρησιμοποιούμενοι μηχανισμοί ομοφωνίας είναι το proof of stake (PoS) και το proof of work (PoW). Το πρώτο είναι ουσιαστικά μία βελτίωση του proof of work.
Το proof of work χρησιμοποιείται για την επαλήθευση και διατήρηση της ακεραιότητας των συναλλαγών στο blockchain. Οι εξορύκτες προσπαθούν να λύσουν το δύσκολο μαθηματικό πρόβλημα για την εισαγωγή ενός block στο blockchain, ο πρώτος εξορυκτής που θα λύση το πρόβλημα ανταμείβεται χρηματικά. Σε αυτήν την μέθοδο απαιτείται σημαντική υπολογιστική ισχύς και ενέργειας.
Στο proof of stake, οι επικυρωτές δηλώνουν το ποσό εγγύησης σε περίπτωση προβλήματος στην προσθήκη του επόμενου block στο blockchain, επιλέγονται τυχαία και ανταμείβονται με κάποιο ποσοστό της συναλλαγής, εφόσον η προσθήκη του block είναι επιτυχής.
Άλλοι μηχανισμοί ομοφωνίας είναι υβριδικοί μηχανισμοί των δύο παραπάνω ή τελείως διαφορετικοί μηχανισμοί όπως, το proof of authority.

Πλεονεκτήματα του blockchain

- Αποκέντρωση: δεν υπάρχουν μεμονωμένα σημεία αποτυχίας ή ελέγχου κι άρα είναι ασφαλή σε επιθέσεις και κακόβουλους χρήστες.
- Διαφάνεια: οι συναλλαγές εφόσον είναι ορατές σε όλους, επαληθεύονται πιο εύκολα και κρίνεται η ακρίβειά τους.
- Αποδοτικότητα: παρά την αρκετή υπολογιστική ισχύς που έχει η λειτουργία του, οι συναλλαγές μέσω blockchain είναι πολύ πιο γρήγορες από τις συνήθεις συναλλαγές, αφού δεν απαιτείται η χρήση μεζάσοντα.
- Χαμηλές προμήθειες: εφόσον δεν υπάρχει μεσάζοντας κι αρκετές λειτουργίες είναι αυτοματοποιημένες, ο χρήστης πληρώνει χαμηλότερη προμήθεια για την εκτέλεση της συναλλαγής του.

Το blockchain χρησιμοποιείται κυρίως σε συναλλαγές κρυπτονομισμάτν, αλλά επίσης και στην δημιουργία ψηφιακών ταυτοτήτων, ψηφοφοριών και σε διαχειρίσεις εφοδιαστικών αλυσίδων.

Υπάρχουν τρεις τύποι blockchain, το δημόσιο, το ιδιωτικό και ένα υβριδικό με όνομα κοινοπραξία blockchain.
Το δημόσιο blockchain είναι αποκεντρωμένο δίκτυο, ανοιχτό σε όλους. Χαρακτηρίζονται από διαφάνεια και είναι ανοιχτού κώδικα. Το ιδιωτικό blockchain, δεν είναι ανοιχτό σε όλους. Διευθύνεται από κάποιο συγκεκριμένο χρήστη (πχ μία εταιρία) και χρησιμοποιείται για εσωτερικούς σκοπούς αυτού. Δεν έχουν διαφάνεια, αφού δεν έχουν όλα τα μέλη πρόσβαση στην δημιουργία block ή έλεγχο των υπολοίπων blocks.
Τέλος τα υβριδικά block, αποτελούνται από συνδυασμό ιδιωτικών και δημοσίων blockchain και δίνεται πρόσβαση σε μέρος των μελών για κάποιες διεργασίες, ενώ κάποιες διεργασία είναι ελεύθερες προς όλους. Για παράδειγμα, αν μερικές εταιρίες δημιουργήσουν ένα κοινό blockchain, όλα τα μέλη μπορούν τα δουν τις συναλλαγές, όμως η κάθε εταιρία είναι υπεύθυνη για εισαγωγή block στον τομέα της.



Εικόνα 68: Τύποι blockchain.

	Permissioned	Permissionless
Preferred Purpose	Popular among industry-level firms and enterprises	Popular for public use
Decentralization	Limited decentralization	Broad decentralization
Development	Generally proprietary	Generally open source
Transparency	Less transparent	More transparent
Use cases	Manage supply chains Create contracts Verify payment between parties	Cryptocurrency blockchains

Εικόνα 69: Ανοιχτά blockchain και blockchain με περιορισμό.

	Public	Private	Hybrid	Consortium
Permissioned/ Permissionless	Permissionless	Permissioned	Permissioned & Permissionless	Permissioned
Control	No control by a central authority	Control by a central authority	Control by a central authority	Control by multiple central authorities
Main Advantages	✓ Independence ✓ Transparency	✓ Performance ✓ Scalability	✓ Performance ✓ Low Cost	✓ Performance ✓ Security
Main Disadvantages	✗ Performance ✗ Scalability Issues	✗ Security ✗ Trust	✗ Transparency ✗ Upgrading	✗ Transparency
Examples	Bitcoin Litecoin	Hyperledger Fabric	XRP token	Corda Quorum

Εικόνα 70: 4 κύριοι τύποι των blockchain.

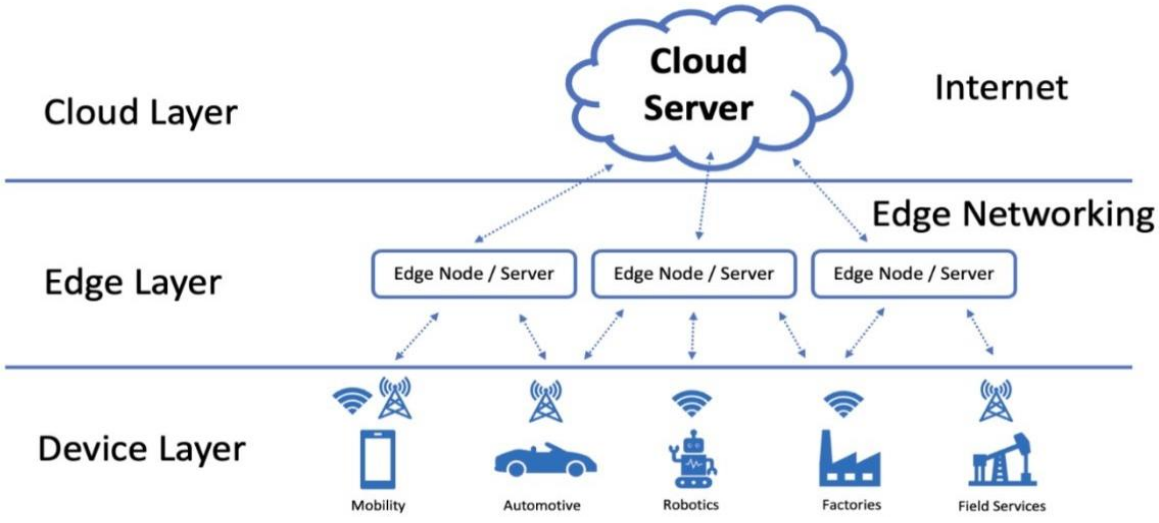
7.3 5G και Edge computing

Το edge computing ονομάζεται υπολογιστική περιφέρειας. Τοποθετείται η πηγή υπολογιστική ισχύς και τα αποθηκευτικά μέσα κοντά στις συσκευές που γίνεται η χρήση και παραγωγή δεδομένων. Τα δεδομένα δηλαδή, δεν στέλνονται στις κεντρικές μονάδες υπολογιστών για επεξεργασία και ανάλυση, παραμένουν όμως κοντά στην συσκευή. Επίσης, χρεισιμοποιείται αρκετά συχνά σε περιπτώσεις που δεν απαιτείται είσοδος στο διαδίκτυο ή αυτή η σύνδεση είναι ασταθής. Όλα τα παραπάνω, συμβάλουν στην αύξηση της απόδοσης, της ταχύτητας και της ασφάλειας.

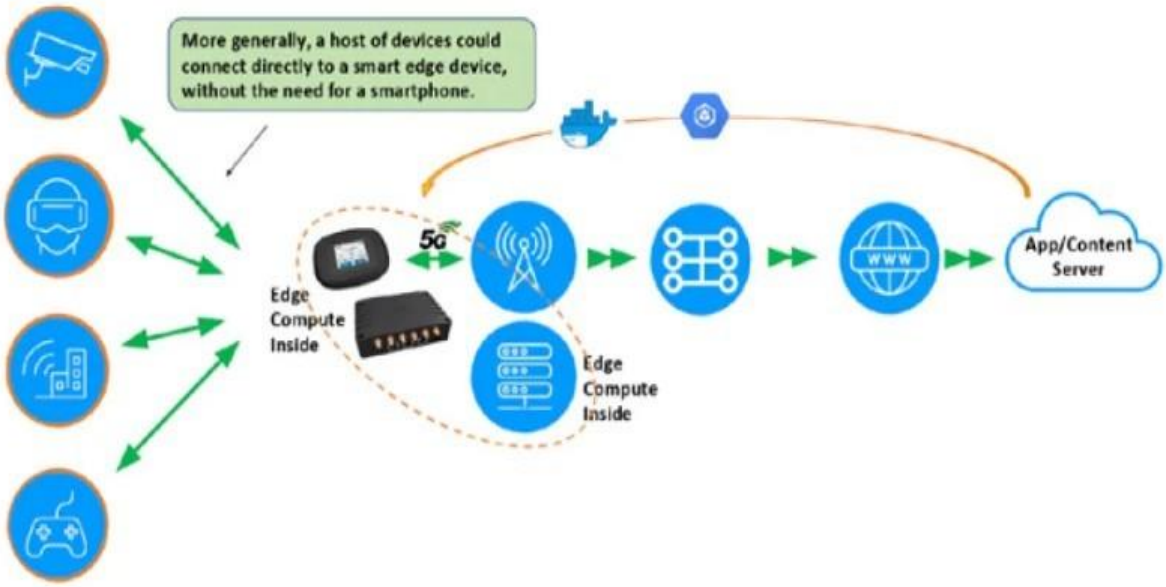
Το 5G έχει ταχύτητα έως και 10 φορές μεγαλύτερες από τον προκάτοχό του 4G. Η σύνδεση του 5G με το edge computing αυξάνουν σημαντικά την ταχύτητα επεξεργασίας κι ανάλυσης δεδομένων σε πραγματικό χρόνο, όπως επίσης μπορούν να αυξήσουν την απόδοση των εφαρμογών.

Το 5G χρειάζεται το edge computing, γιατί για τον μέσο χρήστη οι ταχύτητες που υπόσχεται δεν είναι εφικτές (αν και στο εργαστήριο -ιδανικές συνθήκες- υπήρχαν ταχύτητες με καθυστέρηση της τάξης του 1msec). Κι επίσης, νέες εφαρμογές δεν μπορούν να ξεκινήσουν να παράγονται πριν καθιερωθεί ευρέος το 5G (κάνει που ακόμα καθυστερεί), όμως αυτές οι εφαρμογές μπορούν να λειτουργήσουν σταδιακά με την υποστήριξη του edge computing.

Παρ’ όλα αυτά το 5G, προσφέρει βελτιωμένες τεχνικές κωδικοποίησης δεδομένων εκτός από την ταχύτητα και σε συνδυασμό με την τοπική ανάλυση δεδομένων από το edge computing, αυξάνεται η ασφάλεια σημαντικά. Τέλος, το edge computing επιτρέπει αυθεντικοποίηση και εξουσιοδότηση από κοντινά σημεία στο δίκτυο, όπου και μειώνεται η απομακρυσμένη μη εξουσιοδοτημένη πρόσβαση.



Εικόνα 71: Απλή αρχιτεκτονική Edge computing.



Εικόνα 72: Συνδιασμός Edge computing και 5G.

7.4 Κβαντική κρυπτογραφία

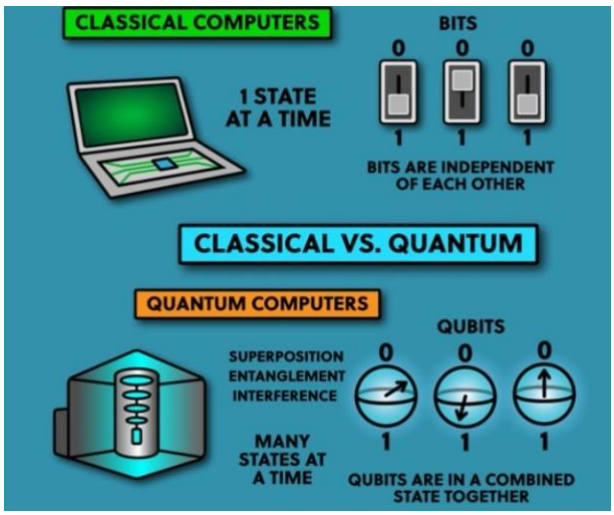
Η κβαντική κρυπτογραφία βασίζεται στις κβαντομηχανικές ιδιότητες κάποιου συστήματος καταστάσεων, όπως την κατάρρευση της κυμματοσυνάρτησης με την μέτρηση της κατάστασης του συστήματος (από έναν υποκλοπέα) και της κβαντική αερομεταφοράς, για την δημιουργία κλειδιού κρυπτογράφησης.

Η κύρια διαφορά με την κλασική κρυπτογραφία είναι η δυνατότητα να βρεθεί αν και πότε υπάρχει υποκλοπέας, καθώς η παρακολούθηση ενός κβαντικού συστήματος, το διαταράσσει και το σύστημα καταρρέει, δηλαδή η κατάστασή του γίνεται δεδομένη.

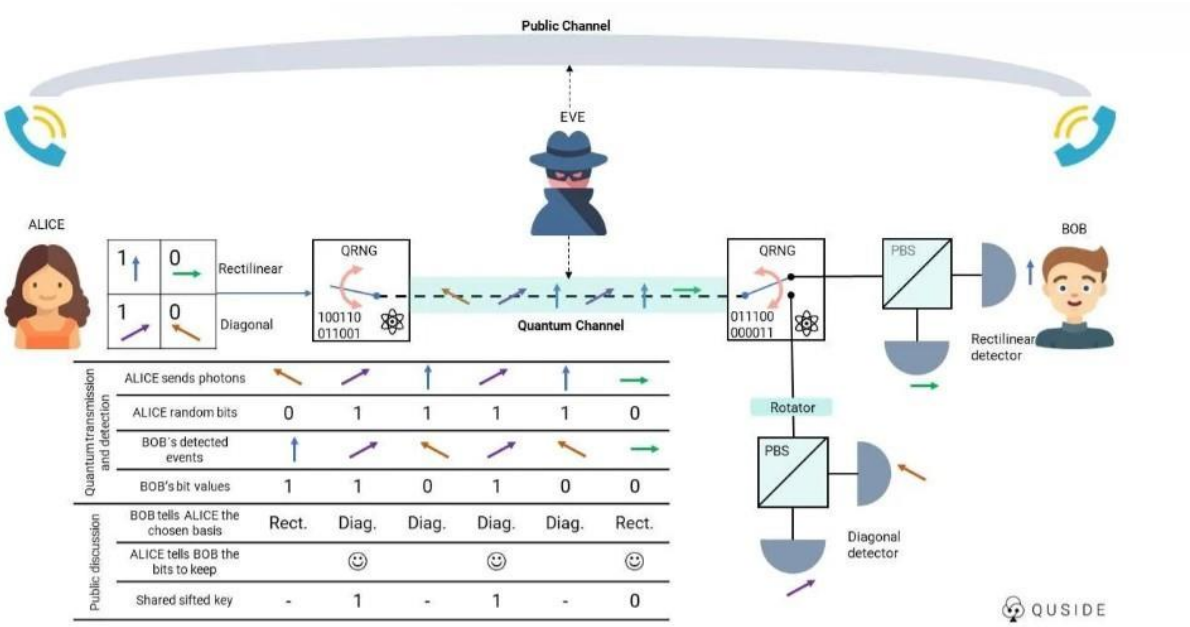
Ο κύριος αλγόριθμος που χρησιμοποιείται στην κβαντική κρυπτογραφία είναι ο αλγόριθμος του Shor, σύμφωνα με τον οποίο αναλύεται ένας αριθμός σε γινόμενο δύο πρώτων αριθμών, υπολογίζεται η περίοδος τ μιας συνάρτηση f(x) με κβαντικό τρόπο, μειώνοντας έτσι την υπολογιστική ισχύς που απαιτείται. Δηλαδή, ένας κλασικός υπολογιστής τον ίδιο υπολογισμό θα τον έκανε σε δεκάδες χρόνια.

Επίσης, ακόμη κι αν υπάρχει υποκλοπέας, ακόμη κι αν βρεθεί να υποκλέβει το μήνυμα, δεν είναι εφικτή η αντιστροφή του κλειδιού με κλασικούς υπολογιστές, πράγμα που σημαίνει πως ακόμη κι αν το καταφέρει, θα έχουν περάσει αρκετά χρόνια και θα είναι άχρηστο.

Στην κβαντική κρυπτογραφία η πληροφορία μεταδίδεται με τα λεγόμενα qubits, που είναι καταστάσεις κβαντικού συστήματος. Δηλαδή είναι διανύσματα (μονοδιάστατοι πίνακες) που το άθροισμα των μέτρων του δηλώνει πιθανότητα κι άρα οι συντελεστές τους πρέπει να ισούνται με την μονάδα. Κατά την υποκλοπή, το σύστημα καταρρέει σε μία από αυτές τις καταστάσεις και αναγνωρίζεται ότι κάποιος μέτρησε την κατάσταση του συστήματος κι αυτή κατέρρευσε (υποκλοπέας)



Εικόνα 73: Κβαντική και κλασική κρυπτογραφία.



Εικόνα 74: Κβαντική κρυπτογραφία σενάρια.

Εικόνες

1. https://www.uniwa.gr/to-panepistimio/optiki-taytotita/meros-2o/
2. https://blogs.sch.gr/nsamaras/2021/01/08/ioi-ypologiston-kakovoylo-logismiko-malware/?repeat=w3tc
3. https://popaganda.gr/life/xeklidoma-me-daktiliko-apotipoma/
4. https://www.secnews.gr/364671/pws-rythisete-anagnwrish-proswpou-kinhta-samsung-galaxy/
5. https://www.hostinger.com/tutorials/what-is-vpn
6. https://www.gsmarena.com/find_my_iphone_and_find_my_friends_will_merge_into_a_single_app_apple_planning_to_add_offline_tracki-news-36659.php
7. https://www.uscybersecurity.net/mobile-security/
8. https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%B4%CE%B7%CE%BC%CF%8C%CF%83%CE%B9%CE%BF%CF%85_%CE%BA%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D
9. https://www.androidauthority.com/app-permissions-886758/
10. https://www.helpnetsecurity.com/2010/08/11/first-sms-android-trojan/
11. https://medicoengineer.com/remove-google-trojan-virus-warning-in-android-mobiles/
12. https://www.google.com/imgres?imgurl=https%3A%2F%2Fmedia.kasperskycontenthub.com%2Fwp-content%2Fuploads%2Fsites%2F43%2F2013%2F06%2F07205001%2Fandroid_trojan_011.png&tbnid=D9BJeRmVKgR0OM&vet=12ahUKEwj26L3whLqEAxUl7LsIHY_aD90QMygAegQIARBP..i&imgrefurl=https%3A%2F%2Fsecurelist.com%2Fthe-most-sophisticated-android-trojan%2F35929%2F&docid=Ey0o9lYXd-MbLM&w=540&h=960&q=trojans%20on%20androids&ved=2ahUKEwj26L3whLqEAxUl7LsIHY_aD90QMygAegQIARBP
13. https://www.bleepingcomputer.com/news/security/new-android-trojan-gplayed-adapts-to-attackers-needs/
14. https://www.mdpi.com/2076-3417/12/21/10755
15. https://hellenicstation.gr/facial-recognition-what-you-should-know/
16. https://www.hellasdigital.gr/electronics/sensors/gravity-capacitive-fingerprint-sensor-sen0359/
17. https://www.researchgate.net/publication/349073977_A_Brief_Survey_on_Modern_Iris_Feature_Extraction_Methods/figures?lo=1&utm_source=google&utm_medium=organic
18. https://grobotronics.com/voice-recognition-module.html
19. https://energyartweb.gr/2018/12/19/hello-world/
20. https://www.geeksforgeeks.org/what-is-data-encryption/
21. https://eduinput.com/data-encryption-in-the-cloud/
22. https://www.thesslstore.com/blog/http-vs-https-difference-between-http-https-protocols/
23. https://www.fool.com/terms/b/blockchain/
24. https://blog.cfte.education/types-of-blockchain-networks/
25. https://www.geeksforgeeks.org/types-of-blockchain/

26. https://www.wipro.com/infrastructure/edge-computing-understanding-the-user-experience/
27. https://www.a10networks.com/blog/5g-deployment-and-edge-computing-monetization-strategies/
28. https://physicsgg.me/2023/03/28/%CE%BA%CE%B2%CE%B1%CE%BD%CF%84%CE%B9%CE%BA%CF%8C-%CE%AC%CE%BB%CE%BC%CE%B1-%CF%83%CF%84%CE%BF%CE%BD-%CE%B4%CE%B7%CE%BC%CF%8C%CE%BA%CF%81%CE%B9%CF%84%CE%BF/
29. https://quside.com/how-does-quantum-key-distribution-qkd-work/
30. https://commons.wikimedia.org/wiki/File:Phishing_attempt.png
31. https://www.foxnews.com/tech/beware-this-latest-phishing-attack-disguised-official-email-sent-google
32. https://itsnews.uncg.edu/2023/03/24/alert-google-doc-phishing/
33. https://www.mailguard.com.au/blog/another-google-phishing-email-scam
34. https://www.antivirusguide.com/cybersecurity/phishing-statistics/
35. https://truelist.co/blog/phishing-statistics/
36. https://www.techopedia.com/phishing-statistics
37. https://news.nau.edu/phishing-attacks-2021/
38. https://us.norton.com/blog/online-scams/what-is-phishing
39. https://www.wallarm.com/what/phishing-attack-prevention-how-to-spot-what-should-do
40. https://us.norton.com/blog/online-scams/what-is-phishing
41. Οι υπόλοιπες εικόνες εξωφύλλου δημιουργήθηκαν με προγράμματα AI όπως το Dale-e & Lensgo.

URLs

1. https://el.theastrologypage.com/mobile-phone-virus
2. https://securelist.com/it-threat-evolution-q2-2023-mobile-statistics/110427/
3. https://www.f-secure.com/v-descs/trojan-android.shtml
4. https://el.wikipedia.org/wiki/%CE%A3%CF%8D%CF%83%CF%84%CE%B7%CE%BC%CE%B1_%CE%91%CE%BD%CE%B1%CE%B3%CE%BD%CF%8E%CF%81%CE%B9%CF%83%CE%B7%CF%82_%CE%A0%CF%81%CE%BF%CF%83%CF%8E%CF%80%CE%BF%CF%85
5. https://www.lab.com.gr/%CE%B1%CE%B9%CF%83%CE%B8%CE%B7%CF%84%CE%AE%CF%81%CE%B1%CF%82-%CE%B4%CE%B1%CE%BA%CF%84%CF%85%CE%BB%CE%B9%CE%BA%CE%BF%CF%8D-%CE%B1%CF%80%CE%BF%CF%84%CF%85%CF%80%CF%8E%CE%BC%CE%B1%CF%84%CE%BF%CF%82/
6. http://www.hep.upatras.gr/research/download/2005/Mixopoulou_IrisRecognition.pdf
7. https://el.wikipedia.org/wiki/%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7_%CE%A3%CF%85%CE%BC%CE%BC%CE%B5%CF%84%CF%81%CE%B9%CE%BA%CE%BF%CF%8D_%CE%9A%CE%BB%CE%B5%CE%B9%CE%B4%CE%B9%CE%BF%CF%8D
8. https://www.ssl.com/article/ssl-tls-handshake-ensuring-secure-online-interactions/
9. https://el.wikipedia.org/wiki/TLS
10. https://en.wikipedia.org/wiki/IPsec
11. https://www.ssl.com/el/%CE%A3%CF%85%CF%87%CE%BD%CE%AD%CF%82-%CE%B5%CF%81%CF%89%CF%84%CE%AE%CF%83%CE%B5%CE%B9%CF%82/%CF%84%CE%B9-%CE%B5%CE%AF%CE%BD%CE%B1%CE%B9-https/
12. https://www.intersys.gr/ti-einai-data-encryption/
13. https://academy.binance.com/el/articles/what-is-blockchain-and-how-does-it-work
14. https://stlpartners.com/articles/edge-computing/5g-edge-computing/
15. https://el.wikipedia.org/wiki/%CE%91%CE%BD%CF%84%CE%B9%CE%B9%CE%B9%CE%BA%CF%8C_%CF%80%CF%81%CF%8C%CE%B3%CF%81%CE%B1%CE%BC%CE%BC%CE%B1

16. https://www.pcsteps.gr/1391-%CF%80%CF%8E%CF%82-%CE%BB%CE%B5%CE%B9%CF%84%CE%BF%CF%85%CF%81%CE%B3%CE%B5%CE%AF-%CF%84%CE%BF-antivirus/
17. https://www.gasimakis.gr/p/blog-page_11.html?m=1
18. https://el.wikipedia.org/wiki/Phishing
19. https://www.stationx.net/phishing-statistics/

Βιβλιογραφία

1. **Ασφάλεια Συστημάτων Κινητών Συσκευών:**
   - Dacosta, I., & Guedes, L. A. (2018). Mobile Device Security: A Comprehensive Review. In 2018 IEEE 9th Latin American Symposium on Circuits & Systems (LASCAS) (pp. 1-4). IEEE.
2. **ιδιωτικότητα και Βιομετρία:**
   - Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20.
3. **Προκλήσεις στην Ασφάλεια των Smartphones:**
   - Enck, W., Ongtang, M., & McDaniel, P. (2009). On Lightweight Mobile Phone Application Certification. In Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09), 235-245.
4. **Προηγμένες Τεχνολογίες Ασφάλειας στα Smartphones:**
   - Choudhury, O., Das, A. K., & Roy, N. (2014). A survey on security issues in mobile computing. In 2014 IEEE Calcutta Conference (CALCON) (pp. 1-6). IEEE.
5. **Κυβερνοασφάλεια και Επίθεση DDoS:**
   - Douligeris, C., Mitrokotsa, A., & Nassis, V. (2004). DDoS attacks and defense mechanisms: Classification and state-of-the-art. Computer Networks, 44(5), 643-666.
6. **Κακόβουλος Κώδικας και Κακόβουλο Λογισμικό:**
   - Skowyra, R., & Kotulski, Z. (2014). Detection of malicious software using machine learning methods. Procedia Computer Science, 35, 965-972.
7. **Κλοπή Ταυτότητας και Απάτη:**
   - Furnell, S. (2007). Insider threat prediction tool. Computers & Security, 26(1), 35-39.
8. Anderson, R., & Moore, T. (2006). Information Security Economics—And Beyond. In Advances in Information Security (Vol. 19). Springer.
9. Stallings, W. (2017). Network Security Essentials: Applications and Standards. Pearson.
10. Jakobsson, M. (2007). Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. Wiley.
11. Rachael Lininger & Russell Dean Vines(2005). Phishing: Cutting the Identity Theft Line 1rst edition.Wiley.
12. Christopher Hadnagy (2010). Social Engineering 1st Edition. Wiley.
13. Kevin D. Mitnick & William L. Simon (2001).The Art of Deception: Controlling the Human Element of Security. Wiley.
14. George A. Akerlof & Robert J. Shiller (2005). Phishing for Phools: The Economics of Manipulation and Deception". Princeton University Press.

15. Christopher Hadnagy & Michele Fincher (2015). Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. Wiley.
16. Neil Bergman, Mike Stanfield, & Jason Rouse (2013). Hacking Exposed Mobile: Security Secrets & Solutions. McGraw Hill.
17. Dominic Chell, Tyrone Erasmus, Shaun Colley, & Ollie Whitehouse (2015). The Mobile Application Hacker's Handbook. Wiley.
18. Iosif I. Androulidakis & Kim-Kwang Raymond Choo (2012). Smartphone Security and Forensics: A Practical Approach. Springer New York, NY.