Προστασία από κυβερνοαπειλές για όλους με απλές πρακτικές κυβερνοϋγιεινής

Παναγιώτης Σούλος
Μέλος ΑΛΛΗΛΟΝ
Information Security GRC Senior Manager
Panagiotis Soulos | Linkedin

Περίληψη

Η χρήση του διαδικτύου και η αλληλεπίδρασή μας με συσκευές τεχνολογίας, όπως υπολογιστές, smartphones, tablets, Internet of Things (IoTs) κ.ά., είναι πλέον μία καθημερινότητα για όλους μας. Τα οφέλη είναι πολλαπλά για κάθε ηλικία και με τα ολοένα κι αυξανόμενα επιτεύγματα στην τεχνολογία γίνεται όλο και πιο εύκολη και άμεση. Ο καθένας μας χρησιμοποιεί το διαδίκτυο και τις συσκευές για ενημέρωση, ψυχαγωγία, διαδικτυακά παιχνίδια, εκπαίδευση, απομακρυσμένη εργασία και πολλά άλλα.

Παρόλα τα οφέλη, το διαδίκτυο ελλοχεύει κινδύνους που ενδέχεται να μας βλάψουν. Μπορούμε να προστατευθούμε ενσωματώνοντας στην καθημερινότητά μας απλές και βέλτιστες πρακτικές κυβερνοασφάλειας, γνωστές ως κυβερνοϋγιεινή.

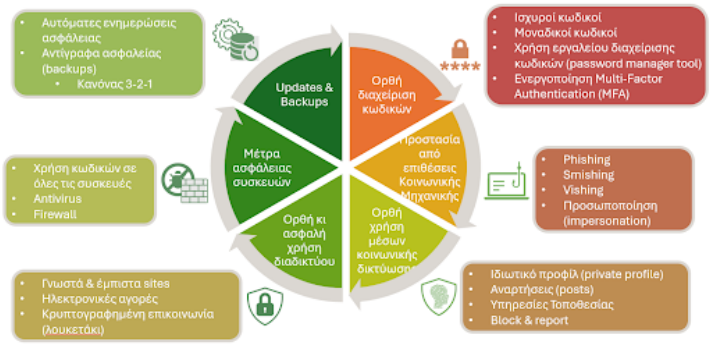
Η προστασία μας από κυβερνοαπειλές είναι πλέον απαραίτητη για όλους, καθώς η καθημερινή μας δραστηριότητα στο διαδίκτυο εκθέτει προσωπικά και επαγγελματικά δεδομένα σε πιθανούς κινδύνους. Μπορούμε να προστατευτούμε αποτελεσματικά εάν ενσωματώσουμε στην καθημερινότητά μας απλές πρακτικές κυβερνοϋγιεινής.

Ως *Κυβερνοϋγιεινή (Cyberhygiene)* αναφερόμαστε στις βέλτιστες πρακτικές ασφάλειας που οι ίδιοι λαμβάνουμε στην καθημερινότητά μας, ως συνήθεις πρακτικές, με σκοπό να προστατεύσουμε τα δεδομένα και τις συσκευές μας.

Τις πρακτικές κυβερνοϋγιεινής μπορούμε να τις εντάξουμε σε έξι χρήσιμα tips/κατηγορίες:

- Ορθή διαχείριση κωδικών (passwords)
- Προστασία από επιθέσεις Κοινωνικής Μηχανικής
- Ορθή χρήση μέσων κοινωνικής δικτύωσης
- Ορθή κι ασφαλή χρήση διαδικτύου
- Μέτρα ασφάλειας συσκευών
- Updates & Backups

Οι πρακτικές κυβερνοϋγιεινής αποτυπώνονται στο παρακάτω σχήμα.



Σχήμα 1, Βέλτιστες Πρακτικές Κυβερνοϋγιεινής

1. Ορθή διαχείριση κωδικών (passwords)

Οι κωδικοί αποτελούν ένα από τα κύρια στοιχεία που χρησιμοποιούμε στην καθημερινότητά μας ώστε να αποκτήσουμε πρόσβαση σε πληροφορίες, συστήματα και υπηρεσίες. Σε περίπτωση που οι κωδικοί μας διαρρεύσουν ή παραβιαστούν, μη εξουσιοδοτημένοι χρήστες θα αποκτήσουν πρόσβαση σε διάφορες υπηρεσίες που χρησιμοποιούμε στο διαδίκτυο. Οι υπηρεσίες αυτές είναι διαφόρων ειδών, από ένα απλό website ενημέρωσης έως το web banking μας.

Για να προστατεύσουμε επαρκώς τους κωδικούς μας προτείνονται οι παρακάτω βέλτιστες πρακτικές:

- Χρήση **ισχυρών κωδικών**. Ένας κωδικός θεωρείται ισχυρός:
  - Έχει μήκος τουλάχιστον 12 χαρακτήρες. Όσο μεγαλύτερος τόσο καλύτερα!
  - Αποτελείται από πεζά, κεφαλαία, αριθμούς και σύμβολα.
  - Δεν περιέχει ευρέως γνωστά στοιχεία για εμάς, όπως το όνομα και επίθετό μας, την ηλικία μας, τη διεύθυνση κατοικίας μας κ.ά.
  - Δεν περιέχει συνεχόμενους χαρακτήρες ή αριθμούς (π.χ. aaaa, 1234)
- Χρήση **μοναδικών κωδικών**. Είναι οι κωδικοί που δεν τους επαναχρησιμοποιούμε. Με τον τρόπο αυτό περιορίζουμε την επίπτωση που μπορεί να έχει η διαρροή ενός κωδικού μας σε έναν μόνο λογαριασμό/υπηρεσία.
- Χρήση **εργαλείου διαχείρισης κωδικών** (password manager tool)[1]. Τα συγκεκριμένα εργαλεία μας επιτρέπουν να:
  - Αποθηκεύουμε τους κωδικούς μας με ασφάλεια, αφού ενσωματώνουν κρυπτογράφηση επιπέδου στρατού.
  - Δημιουργούμε εύκολα και γρήγορα κωδικούς, αφού περιέχουν γεννήτρια κωδικών.
  - Αντιγράφουμε τους κωδικούς μας χωρίς να χρειάζεται να τους θυμόμαστε.
  - Θυμόμαστε μόνο έναν κωδικό, τον κύριο κωδικό (master password), για να αποκτούμε πρόσβαση στους κωδικούς μας.
  - Έχουμε τους κωδικούς μας πάντα μαζί μας και παντού, αφού μπορούν να εγκατασταθούν σε όλες μας τις συσκευές.
- Ενεργοποίηση **αυθεντικοποίηση πολλαπλών παραγόντων** (Multi-Factor Authentication - MFA). Η συγκεκριμένη ρύθμιση βρίσκεται συνήθως στις ρυθμίσεις ασφάλειας του εκάστοτε λογαριασμού μας και πλέον είναι διαθέσιμη σε όλες τις ευρέως γνωστές υπηρεσίες όπως e-mail, social media κ.ά.. Μας προσθέτει ένα επιπλέον παράγοντα αυθεντικοποίησης, όπως έναν κωδικό μίας χρήσης (One-Time Password), ένα push notification από την εφαρμογή στο κινητό μας, τα βιομετρικά μας στοιχεία (π.χ. δακτυλικό αποτύπωμα, αναγνώριση προσώπου κ.λπ.), τη στιγμή που συνδεόμαστε σε κάποια υπηρεσία. Με τον τρόπο αυτό, αποτρέπουμε τους κακόβουλους χρήστες να αποκτήσουν πρόσβαση στον λογαριασμό μας ακόμα κι αν ο κωδικός μας διαρρεύσει, αφού δεν θα έχουν στην κατοχή τους τον επιπλέον παράγοντα.

2. Προστασία από επιθέσεις Κοινωνικής Μηχανικής

Η Κοινωνική Μηχανική (Social Engineering) είναι η εκμετάλλευση ψυχολογικών ιδιοτήτων του ανθρώπινου παράγοντα, με τη χρήση κοινωνικής αλληλεπίδρασης, με σκοπό την εξαπάτησή του και την απόσπαση εμπιστευτικών πληροφοριών. Είναι η προσπάθεια εξαπάτησής μας παρουσιάζοντάς μας μία επείγουσα ανάγκη, όπου κάτι κακό πρόκειται να συμβεί και συνήθως σε πολύ σύντομο χρονικό διάστημα, εάν δεν δράσουμε άμεσα. Σύμφωνα με την πιο πρόσφατη έρευνα 2024 Verizon Data Breach Investigation Report[2], που εξετάζει ετησίως περιστατικά παραβίασης δεδομένων, το 68% των παραβιάσεων δεδομένων το 2023 οφειλόταν στον ανθρώπινο παράγοντα, συμπεριλαμβανομένου της κοινωνικής μηχανικής. Οι τρόποι με τους οποίους μπορεί να εμφανιστεί η κοινωνική μηχανική είναι οι εξής:

- **Phishing**. Απατηλά e-mails που προσπαθούν να μας εξαπατήσουν ώστε να πατήσουμε ένα σύνδεσμο, να κατεβάσουμε και να εκτελέσουμε κάποιο αρχείο, να δώσουμε τα στοιχεία σύνδεσης λογαριασμών μας κ.ά.. Θα πρέπει να είμαστε πάντα υποψιασμένοι και να επιβεβαιώνουμε τον αποστολέα και τους συνδέσμους (links) που περιέχονται, τοποθετώντας από πάνω το mouse μας - χωρίς να κάνουμε click. Εάν το αναγνωρίσουμε ως phishing, δεν απαντάμε, δεν πατάμε τους συνδέσμους, το αγνοούμε και το διαγράφουμε.
- **Smishing**. Είναι όταν μας αποστέλλουν απατηλά μηνύματα στο κινητό μας. Εάν μας αναφέρει ότι κλείνει ο λογαριασμός μας στην τράπεζά μας και πρέπει άμεσα να επιβεβαιώσουμε τα στοιχεία μας πατώντας τον σύνδεσμο στο μήνυμα, δεν πατάμε τον σύνδεσμο και καλούμε τηλεφωνικά την τράπεζά μας να το επιβεβαιώσουμε.
- **Vishing**. Είναι όταν μας καλούν στο τηλέφωνο και προσπαθούν να μας εξαπατήσουν. Δεν δίνουμε κανένα στοιχείο, όπως προσωπικά μας δεδομένα ή δεδομένα καρτών και κλείνουμε άμεσα το τηλέφωνο. Οι νέες συσκευές έχουν τη δυνατότητα αποκλεισμού τηλεφωνικών αριθμών.
- **Προσωποποίηση** (impersonation). Είναι όταν με φυσική παρουσία προσπαθούν να μας εξαπατήσουν, για να αποκτήσουν πρόσβαση σε χώρους, πληροφορίες και χρήματα. Να ρωτάμε πάντα και να μην επιτρέπουμε την πρόσβαση σε αγνώστους, ούτε

να τους δίνουμε πληροφορίες, ακόμα κι αν μας παρουσιάσουν ότι μας γνωρίζουν μέσω κάποιου γνωστού μας. Είναι πολύ πιθανό τα στοιχεία αυτά να τα άντλησαν από το διαδίκτυο!

3. Ορθή χρήση μέσων κοινωνικής δικτύωσης

Τα μέσα κοινωνικής δικτύωσης αποτελούν πλέον το βασικό μας τρόπο επικοινωνίας με την οικογένειά μας, τους φίλους μας αλλά και ενημέρωσης και ψυχαγωγίας. Για το λόγο αυτό, θα πρέπει να προστατεύσουμε τους λογαριασμούς μας σε αυτά, ώστε να αποτρέψουμε πιθανή υποκλοπή τους που θα σήμαινε την υποκλοπή της ψηφιακής μας ταυτότητας. Σε τέτοια περίπτωση, κάποιος κακόβουλος χρήστης θα μπορούσε να κάνει αναρτήσεις σαν εμάς, να δει όλα μας τα προσωπικά μας μηνύματα και να προσπαθήσει να επικοινωνήσει με τους φίλους μας με σκοπό να τους εξαπατήσει. Ένα τέτοιο περιστατικό θα είναι καταστροφικό για την ιδιωτικότητά μας. Για να προστατευτούμε, θα πρέπει να:

- Θέσουμε το προφίλ μας ως **ιδιωτικό** (private), ώστε να ελέγχουμε τα αιτήματα φιλίας και να επιλέγουμε τους φίλους μας.
- Είμαστε προσεκτικοί στις **αναρτήσεις** (posts) που κάνουμε. Οποιαδήποτε πληροφορία αναρτούμε στο διαδίκτυο παραμένει εκεί για **πάντα**. Αποφεύγουμε να αναρτούμε πότε θα πάμε διακοπές ή φωτογραφίες όταν είμαστε σε διακοπές, καθώς είναι σαν να ανακοινώνουμε ότι λείπουμε από το σπίτι μας. Επιπλέον, οι αναρτήσεις που κάνουμε μπορεί να μας επηρεάσουν στο μέλλον είτε σε προσωπικό είτε σε επαγγελματικό επίπεδο.
- Αποφεύγουμε τη χρήση **των υπηρεσιών τοποθεσίας** (location services), ιδιαίτερα όταν αφορούν σε προσωπικούς μας χώρους (π.χ. κατοικία, εξοχικό, εργασία). Μπορεί ένας κακόβουλος χρήστης να έρθει να μας συναντήσει ή να προσπαθήσει να παραβιάσει το σπίτι μας όταν εμείς θα λείπουμε.
- Ενημερωθούμε για τον τρόπο με τον οποίο μπορούμε να κάνουμε αποκλεισμό (**block**) και αναφορά (**report**). Όλα τα μέσα κοινωνικής δικτύωσης έχουν αυτή τη δυνατότητα.

4. Ορθή κι ασφαλή χρήση διαδικτύου

Για να προστατευτούμε στο διαδίκτυο, θα πρέπει να:

- Επισκεπτόμαστε μόνο **γνωστά** κι **έμπιστα websites**. Είναι αυτά που είναι ευρέως γνωστά.
- Προσέχουμε ιδιαίτερα όσον αφορά στις **ηλεκτρονικές πληρωμές**. Δεν κάνουμε αγορές από άγνωστα websites και δεν δίνουμε τα στοιχεία της κάρτας μας σε κανέναν!
- Επιβιώνουμε ότι η **επικοινωνία** είναι **κρυπτογραφημένη** όταν παρέχουμε ευαίσθητα δεδομένα, όπως τα προσωπικά μας δεδομένα, τους κωδικούς μας και τα στοιχεία της κάρτας μας. Κοιτάμε στη μπάρα διεύθυνσης ότι εμφανίζεται το «λουκετάκι» κι ότι δεν εμφανίζεται κάποιο μήνυμα για μη ασφαλή σύνδεση.

5. Μέτρα ασφάλειας συσκευών

Οι συσκευές μας ενδέχεται να χαθούν ή κλαπούν κι ακόμα να μολυνθούν από κακόβουλο λογισμικό. Γι' αυτό θα πρέπει να λάβουμε βασικά μέτρα ασφάλειας, όπως:

- **Χρήση κωδικών** σε όλες τις συσκευές, ώστε να αποτραπεί η πρόσβαση στα δεδομένα των συσκευών μας σε όσους έχουν φυσική πρόσβαση σε αυτές.
- **Antivirus**[3], το οποίο θα προστατεύσει τη συσκευή μας από πιθανή μόλυνση κακόβουλου λογισμικού. Θα πρέπει να το συντηρούμε πάντα ενημερωμένο και με τις τελευταίες ενημερώσεις κακόβουλων λογισμικών.
- **Firewall**, το οποίο θα μας προστατεύσει από πιθανές κυβερνοεπιθέσεις.

6. Updates & Backups

Τα λογισμικά που έχουμε εγκατεστημένα στις συσκευές μας ενδέχεται να έχουν ευπάθειες ασφαλείας και οι συσκευές μας ενδέχεται να χαλάσουν για οποιοδήποτε λόγο. Γι' αυτό θα πρέπει να:

- Ενεργοποιήσουμε τις **αυτόματες ενημερώσεις ασφάλειας** σε οποιοδήποτε λογισμικό έχουμε στις συσκευές μας.
- Λαμβάνουμε περιοδικά **αντίγραφα ασφάλειας** (backup), ώστε να διατηρήσουμε τα δεδομένα μας σε περίπτωση κλοπής ή απώλειας της συσκευής μας. Οι βέλτιστες πρακτικές προτείνουν τον κανόνα 3-2-1, δηλαδή:
  - 3 αντίγραφα ασφάλειας
  - 2 σε διαφορετικά μέσα, π.χ. εξωτερικό σκληρό δίσκο και usb
  - 1 σε διαφορετική τοποθεσία, π.χ. cloud

Συνοψίζοντας, οι παραπάνω βέλτιστες πρακτικές κυβερνοϋγιεινής με όλο και πιο συχνή χρήση μπορούν να μας γίνουν καθημερινές συνήθειες για την προστασία των δεδομένων μας στην σύγχρονη εποχή.

Παραπομπές

1 Ενδεικτικά παραδείγματα password manager tools: BitWarden, 1Password

2 Verizon Data Breach Investigation Report

3 Σύγκριση ευρέων γνωστών λύσεων antivirus: https://www.av-test.org/en/