

# ΨΗΦΙΑΚΗ ΑΣΦΑΛΕΙΑ & ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΗΛΕΚΤΡΟΝΙΚΕΣ ΑΠΑΤΕΣ



ΕΚΔΟΣΗ 1.0 | ΦΕΒΡΟΥΑΡΙΟΣ 2023

[datamix.gr](http://datamix.gr) & [limeframe.gr](http://limeframe.gr)

# ΕΙΣΑΓΩΓΗ

Το παρόν ενημερωτικό έγγραφο προέκυψε από την συνεργασία των εταιρειών DATAMIX και LIMEFRAME και αποτελεί την πρώτη έκδοση ενός συνοπτικού οδηγού για την ψηφιακή ασφάλεια και προστασία από ηλεκτρονικές απάτες.

## **DATAMIX**

Καθαβρύτων 19, Τρίπολη  
info@datamix.gr  
www.datamix.gr

## **limeframe**

Αγίου Δημητρίου 3, Τρίπολη  
info@limeframe.gr  
www.limeframe.gr

## ΤΗΛΕΦΩΝΙΚΕΣ ΚΛΗΣΕΙΣ

- 1 Πριν από οποιαδήποτε επικοινωνία οφείλουμε να εξακριβώσουμε την ταυτότητα του ατόμου που κάνουμε συναλλαγή.
- 2 Δεν δίνουμε **KANENA** κωδικό σε τρίτους ( π.χ. κωδικούς ebanking, email, κωδικούς OTP κ.λπ.)
- 3 Δεν δίνουμε ποτέ τον τριψήφιο κωδικό της χρεωστικής ή της πιστωτικής μας κάρτας.

# ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ

- 1 Πριν από οποιαδήποτε επικοινωνία οφείλουμε να εξακριβώσουμε την ταυτότητα του ατόμου που κάνουμε συναλλαγή.
- 2 Δεν δίνουμε σε κανέναν κωδικούς e-banking και pin μέσω email.
- 3 Δεν δίνουμε ποτέ τον τριψήφιο κωδικό της χρεωστικής ή της πιστωτικής μας κάρτας.
- 4 Δεν κοινοποιούμε ούτε κωδικούς με email, ούτε καν στους εταιρικούς μας λογαριασμούς αλληλογραφίας. (υπάρχει πιθανότητα να παρεμβάλλετε κάποιος στην επικοινωνία και να αποκτήσει πρόσβαση στους κωδικούς μας).
- 5 Όταν με email μας κοινοποιούν IBAN και τραπεζικούς λογαριασμούς, πριν την συναλλαγή επιβεβαιώνουμε τηλεφωνικώς την ορθότητα του λογαριασμού (είναι κοινή πρακτική να παρεμβάλλεται κάποιος στην αλληλογραφία και να αλληλιώνει τα email).

# ΗΛΕΚΤΡΟΝΙΚΕΣ ΣΥΝΑΛΛΑΓΕΣ

1

Δεν εισάγουμε κωδικούς e-banking, καρτών, ούτε στοιχεία ταυτοποίησης, σε ιστοσελίδες που έχουμε επισκεφτεί μέσω (link), αν πρώτα δεν έχουμε επιβεβαιώσει την ασφάλεια της σελίδας που επισκεφτήκαμε. (αν το link είναι με οποιαδήποτε τρόπο αμφιβόλου προελεύσεως τότε δεν πρέπει να ολοκληρώσουμε την συναλλαγή).

2

Κατά την διάρκεια της συναλλαγής δεν δίνουμε την κάρτα (πιστωτική ή χρεωστική) στο κατάστημα για να ολοκληρώσουν μόνοι τους την συναλλαγή. (υπάρχει μεγάλος κίνδυνος κάποιος να κρατήσει τα στοιχεία της κάρτας)

3

Επιβεβαιώνουμε ότι για την ολοκλήρωση μιας συναλλαγής θα μας ζητείτε πάντα κωδικός OTP και φυσικά ότι έχουμε στον έλεγχο μας την συσκευή που λαμβάνουμε το OTP. (ο έλεγχος πρέπει να γίνει για όλους τους λογαριασμούς και κάρτες που έχουμε)

4

## ΔΙΑΧΕΙΡΙΣΗ ΚΩΔΙΚΩΝ (PASSWORD)

1

**Δεν αποθηκεύουμε ποτέ κωδικούς στους browser.**

(chrome, mozilla, edge κλπ)

(αν κάποιος αποκτήσει πρόσβαση στον υπολογιστή μας, τοπικά ή απομακρυσμένα, θα έχει αυτομάτως και πρόσβαση στους κωδικούς μας)

2

**Δεν χρησιμοποιούμε ποτέ το ίδιο password σε πάνω από μία εφαρμογές.**

3

**Αλλάζουμε συχνά τους κωδικούς μας.** (μπορεί οι τράπεζες και άλλες εφαρμογές να μας υποχρεώνουν να αλλάζουμε τους κωδικούς ανά τακτά χρονικά διαστήματα αλλά δεν πρέπει να ξεχνάμε τους λογαριασμού αλληλογραφίας)

## ΕΠΙΠΛΕΟΝ ΚΑΝΟΝΕΣ

- 1 Όλοι οι υπολογιστές και Server's του δικτύου μας, πρέπει να έχουν antivirus, το οποίο να είναι ενημερωμένο στην τελευταία του έκδοση.
- 2 Το δίκτυο μας, θα πρέπει να προστατεύεται με Firewall για την αποτροπή μη επιθυμητής απομακρυσμένης πρόσβασης.
- 3 Σε περίπτωση που παρέχουμε WiFi στους επισκέπτες/πελάτες της επιχείρησής μας τότε αυτό θα πρέπει να είναι ξεχωριστό από το δίκτυο της επιχείρησής μας.
- 4 Οι υπολογιστές θα πρέπει να έχουν ισχυρό κωδικό ασφαλείας, ο οποίος μάλιστα θα πρέπει να αλλάζει σε τακτικά διαστήματα.

## ΧΡΗΣΙΜΕΣ ΙΣΤΟΣΕΛΙΔΕΣ

1

CyberScams

<https://cyberalert.gr/start/cyberscams/>

2

Απάτες μέσω διαδικτύου

<https://cyberalert.gr/apates-meso-diadiktiou/>

3

Mobile Malware

<https://cyberalert.gr/mobile-malware/>



# Κοινωνική

## μηχανική (social engineering)

**Είναι η πράξη της προφορικής χειραγώγησης ατόμων με σκοπό την απόσπαση πληροφοριών.**

Αν και είναι παρόμοια με το τέχνασμα ή την απλή απάτη, ο όρος είναι κυρίως συνδεδεμένος με την εξαπάτηση ατόμων με σκοπό την απόσπαση εμπιστευτικών πληροφοριών που είναι απαραίτητες για την πρόσβαση σε κάποιο υπολογιστικό σύστημα.

Συνήθως αυτός που την εφαρμόζει δεν έρχεται ποτέ πρόσωπο με πρόσωπο με το άτομο που εξαπατά ή παραπλανά.

## Ιστορικά

Ο πρώην εγκληματίας υπολογιστών και αργότερα σύμβουλος ασφαλείας πληροφορικών συστημάτων Κέβιν Μίτνικ διέδωσε τον όρο «κοινωνική μηχανική», επισημαίνοντας ότι **είναι πολύ ευκολότερο να ξεγελάσεις κάποιον να δώσει έναν κωδικό πρόσβασης για ένα σύστημα από το να προσπαθήσεις να τον σπάσεις.**

Πηγή: Wikipedia