Συνοπτικός Οδηγός Κυβερνοασφάλειας ΣΔΕΕ

Πώς να προστατεύσετε αποτελεσματικά τις πληροφορίες σας με απλά και πρακτικά βήματα

I. Κωδικοί

Τι να κάνετε:

- Οι κωδικοί πρόσβασης που χρησιμοποιούμε σε επαγγελματικούς λογαριασμούς (email, web-banking, e-justice, taxisnet, ΟΠΣ Ολομέλειας κ.λπ.) να είναι **ισχυροί και μοναδικοί για κάθε εφαρμογή**. Οι κωδικοί καλόν είναι:
  - να έχουν **τουλάχιστον 12 χαρακτήρες**
  - να περιλαμβάνουν **γράμματα (πεζά–κεφαλαία), αριθμούς και σύμβολα,**
  - ιδανικά, να είναι με τη μορφή **passphrase**, δηλαδή μίας μικρής φράσης-κωδικού. Ένα **passphrase** μπορεί να είναι, για παράδειγμα:
    - ToSpitiExei4Gates, ή
    - VazwDyskoloKwdiko@1285

  Αυτοί οι κωδικοί είναι **αρκετά μακροί**, **εύκολοι να τους θυμάστε**, αλλά **πολύ δύσκολο να τους μαντέψει άλλος**.
- **Να αποφεύγετε** κωδικούς που κάποιος μπορεί εύκολα να μαντέψει, όπως:
  - Ονόματα (δικά σας, παιδιών, συζύγου)
  - Ημερομηνίες γέννησης
  - Απλές παραλλαγές, π.χ. Manos123!@#
- **Ποτέ μην χρησιμοποιείτε τον ίδιο κωδικό** σε προσωπικές εφαρμογές (π.χ. social media, streaming, e-shops) και σε επαγγελματικούς λογαριασμούς που σχετίζονται με υποθέσεις πελατών.
- **Να χρησιμοποιήστε password manager**

  Αντί να θυμάστε 15 κωδικούς, θυμάστε **έναν πολύ δυνατό master password**.
  Όλα τα υπόλοιπα μπορούν να είναι τυχαία και ακόμη πιο σύνθετα.
- **Να μην μοιράζεστε κωδικούς με συνεργάτες/γραμματεία**

  Αν χρειάζεται πρόσβαση άλλος, προτιμήστε ξεχωριστό λογαριασμό χρήστη

- **Να αλλάζετε κωδικούς όταν:**
  - Υπάρχει υποψία παραβίασης
  - Έγινε λάθος αποστολή σε τρίτο
  - Έχει μείνει ο ίδιος κωδικός πολλά χρόνια σταθερός σε κρίσιμη υπηρεσία
- **Να ενεργοποιήσετε διπλή ταυτοποίηση (2FA)** σε email, cloud και τραπεζικές υπηρεσίες. Είναι ένας τρόπος σύνδεσης που απαιτεί περισσότερα από ένα στοιχεία ταυτοποίησης για να επιβεβαιώσει ότι είμαστε όντως εμείς που προσπαθούμε να μπούμε. Οι πιο συνήθεις τέτοιοι είναι:
  - **Εφαρμογή 2FA**: Π.χ. Google authenticator ή Microsoft authenticator, την οποία κατεβάζετε στο κινητό σας.
  - **Email**: Ο αριθμός που λειτουργεί ως δεύτερος παράγοντας ταυτοποίησης έρχεται στο email σας.
  - **SMS σε Κινητό**: Ο αριθμός που λειτουργεί ως δεύτερος παράγοντας ταυτοποίησης έρχεται στο κινητό σας.

Προσοχή: η πρόσβαση στον λογαριασμό σας είναι ιδιαίτερα δυσχερής εάν χάσετε την πρόσβαση στον δεύτερο παράγοντα ταυτοποίησης. Συνιστούμε να έχετε εναλλακτικές και να ορίσετε κάποιον άλλο εταίρο στην εταιρεία ως εναλλακτικό λήπτη επαναφοράς κωδικού.

II. Ενημέρωση και Ασφάλεια Λογισμικού

Τι να κάνετε:

- Βεβαιωθείτε ότι χρησιμοποιείτε **γνήσιο λογισμικό**. Αυτό κατά κανόνα μπορείτε να το ελέγξετε στα settings του υπολογιστή σας ή της σχετικής εφαρμογής.
- Ενεργοποιήστε τις **αυτόματες ενημερώσεις** σε όλα τα προγράμματα.
- Εγκαταστήστε και να διατηρείτε ενεργό **λογισμικό προστασίας (antivirus / antimalware)** σε όλες τις εταιρικές συσκευές. Κάποια από τα πιο γνωστά είναι τα Norton, Bitdefender και McAfee.

III. Αντίγραφα Ασφαλείας (Backups)

Τι να κάνετε:

- Διατηρείτε **τουλάχιστον ένα αντίγραφο ασφαλείας** σε ξεχωριστή συσκευή (offline), για παράδειγμα σε εξωτερικό σκληρό δίσκο, και ένα αντίγραφο στο cloud (off-site).Υπάρχουν εργαλεία backup που αυτοματοποιούν την διαδικασία και λαμβάνουν αντίγραφα ασφαλείας

σε καθορισμένες χρονικές περιόδους, χωρίς κάποια ενέργεια από τον χρήστη.

- Ελέγχετε ότι τα αντίγραφα **λειτουργούν** και μπορούν να αποκατασταθούν. Για παράδειγμα, σε τακτική βάση δοκιμάστε δειγματοληπτικά να ανοίξετε αρχεία στο αντίγραφο ασφαλείας.

IV. Χρήση Προσωπικών Συσκευών και Εφαρμογών

Τι να κάνετε:

- Να περιορίσετε ή να μην επιτρέπετε τη χρήση προσωπικών email για επαγγελματικούς σκοπούς.

V. Φυσική Ασφάλεια

Τι να κάνετε:

- Να εξασφαλίσετε ότι οι χώροι σας διαθέτουν πόρτες ασφαλείας, **κλειδαριές**, **συναγερμό και κλειστό κύκλωμα τηλεόρασης CCTV**.
- Να κλειδώνετε την οθόνη του υπολογιστή και τα γραφεία σας όταν φεύγετε.

VI. Ασφαλές Email

Τι να κάνετε:

- Να χρησιμοποιείτε email με domain της εταιρείας (π.χ. info@onomaetaireias.gr).
- Να χρησιμοποιείτε email με προδιαγραφές συμβατές με GDPR. Μόνο τα πληρωμένα πακέτα των μεγάλων παρόχων είναι συμβατά με αποθήκευση όλων των δεδομένων στην ΕΕ.

VII. Για περίπτωση κυβερνοεπίθεσης

Τι να κάνετε:

- Να ορίσετε ένα πρόσωπο που θα είναι υπεύθυνος σε περίπτωση κυβερνοεπίθεσης.
- Να τηρείτε βασικό σχέδιο: ποιος κάνει τι, ποιος ειδοποιείται, πώς περιορίζεται η ζημιά.
- Να διατηρείτε τις οδηγίες και τα στοιχεία επικοινωνίας εκτυπωμένα και προσβάσιμα.