



Κυβερνοασφάλεια

Θέματα ασφάλειας Ηλεκτρονικών Υπηρεσιών

Παναγιώτης Βαβίλης
ΕΤΕΠ Τμ. Επιστήμης Υπολογιστών
ΥΑΣΠΕ Πανεπιστημίου Κρήτης



Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης



ΠΡΟΓΡΑΜΜΑ 2021 – 2027
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ

 **digiGOV**
innoHUB



ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
UNIVERSITY OF CRETE



Κωδικοί Πρόσβασης & Προστασία Προσωπικών Δεδομένων



Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης



ΠΡΟΓΡΑΜΜΑ 2021 – 2027
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ

digiGOV
innoHUB



ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
UNIVERSITY OF CRETE

Διαπιστευτήρια πρόσβασης (user credentials)

- **Τι είναι:** στοιχεία ταυτοποίησης χρήστη για πρόσβαση σε συστήματα/υπηρεσίες (π.χ. username + password, ή passkeys, ή MFA)
- **Συνιστώσες:**
 - **Κάτι που ξέρω:** κωδικός/ PIN.
 - **Κάτι που έχω:** κινητό για TOTP/Push, security key (FIDO2).
 - **Κάτι που είμαι:** βιομετρικά (δακτυλικό, Face ID).

Κίνδυνοι

- phishing
- credential stuffing (ίδιος κωδικός σε πολλά sites)
- διαρροές βάσεων
- brute-force
- keyloggers
- SIM-swap



Καλές πρακτικές χρήστη

- Καλός κωδικός = μακρύς, με λέξεις/φράση που μόνο εσύ θυμάσαι (όχι «123456», όχι ημερομηνίες).
- Μην χρησιμοποιείς τον ίδιο κωδικό παντού. Αν διαρρεύσει κάπου, δοκιμάζουν το ίδιο και αλλού
- Βάλε επαλήθευση 2 βημάτων (2FA) όπου γίνεται: εφαρμογή στο κινητό, sms κτλ
- Χρησιμοποίησε password manager για να κρατάει και να φτιάχνει δυνατούς κωδικούς για σένα
- Πρόσεχε τα μηνύματα-παγίδες (phishing): έλεγξε τη διεύθυνση του site πριν συνδεθείς, μην πατάς ύποπτους συνδέσμους
- Μην μοιράζεσαι κωδικούς με κανέναν. Καμία «τράπεζα/εταιρεία» δεν θα στον ζητήσει
- Χρήση ενιαίας σύνδεσης (SSO) πχ μέσω Google
- Νεότερος, πιο ασφαλής τρόπος: Passkeys (σύνδεση χωρίς κωδικό, με το κινητό/βιομετρικά)



Προσωπικών δεδομένα

Τα προσωπικά δεδομένα είναι **κάθε πληροφορία που αφορά ένα ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο** (δηλαδή έναν άνθρωπο). «Ταυτοποιήσιμο» σημαίνει ότι μπορεί να αναγνωρισθεί άμεσα ή έμμεσα, π.χ. από ένα όνομα, έναν αριθμό, ή από συνδυασμό στοιχείων.



Προστασία προσωπικών δεδομένων στον εργασιακό χώρο

Η προστασία δεδομένων ξεκινά από την καθημερινή μας συμπεριφορά. Ακόμα κι ένα εκτυπωμένο έγγραφο στο λάθος γραφείο μπορεί να είναι παραβίαση. Οφείλουμε να χειριζόμαστε τα δεδομένα των πολιτών με διακριτικότητα και ασφάλεια.

Διαβάζω την πολιτική ασφαλείας του οργανισμού και ακολουθώ κατά γράμμα τις οδηγίες του εκάστοτε Υπευθύνου προστασίας δεδομένων (DPO) και του Υπευθύνου ασφαλείας συστημάτων πληροφορικής και επικοινωνιών (ΥΑΣΠΕ).

Καλές πρακτικές

- Επεξεργασία μόνο των απολύτως απαραίτητων δεδομένων
- Όχι αποστολή προσωπικών δεδομένων χωρίς έλεγχο και επαλήθευση παραλήπτη
- Ασφαλής διαχείριση εγγράφων (ψηφιακών & φυσικών)
- Απόρριψη ευαίσθητων εγγράφων μέσω καταστροφέα
- Κλείδωμα οθόνης όταν φεύγουμε από το γραφείο



Με τη συγχρηματοδότηση
της Ευρωπαϊκής Ένωσης



ΠΡΟΓΡΑΜΜΑ 2021 – 2027
ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ



ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΡΗΤΗΣ
UNIVERSITY OF CRETE

Σας ευχαριστώ!