Τμήμα Εκπαιδευτικής και Κοινωνικής Πολιτικής

Σημειώσεις μαθήματος: **Πληροφορική Ι: Εισαγωγή στους Η/Υ**

Ασφάλεια στο Διαδίκτυο

Πώς να Προστατεύσεις τα Δεδομένα και τα Χρήματά σου

Περιεχόμενα

Εισαγωγή: Η Πραγματική Απειλή στο Ψηφιακό Μέτωπο

Το Διαδίκτυο είναι σαν μια μεγάλη πόλη: σου προσφέρει ευκαιρίες, αλλά κρύβει και κινδύνους. Ως digital native, νομίζεις ότι αναγνωρίζεις τους κινδύνους, αλλά οι σημερινοί απατεώνες (cyber criminals) δεν ψάχνουν πια μόνο για ιούς. Χρησιμοποιούν **κοινωνική μηχανική (social engineering)**, εκμεταλλευόμενοι την εμπιστοσύνη ή την απροσεξία σου.
Στόχος: Να μετατρέψεις την τεχνολογική σου εξοικείωση σε **ψηφιακή αυτοάμυνα**.

Οι Τρεις Βασικοί Πυλώνες της Ασφάλειας

Η ασφάλεια στο Διαδίκτυο στηρίζεται σε τρεις βασικές έννοιες:

1. **Εμπιστευτικότητα (Confidentiality):** Μόνο οι εξουσιοδοτημένοι χρήστες (εσύ και η τράπεζά σου) μπορούν να δουν τα δεδομένα. **Παράδειγμα:** Κρυπτογράφηση email και προσωπικών μηνυμάτων.
2. **Ακεραιότητα (Integrity):** Τα δεδομένα είναι σωστά και δεν έχουν αλλοιωθεί από τρίτους (π.χ. ένας ιός δεν άλλαξε το αρχείο της εργασίας σου). **Παράδειγμα:** Το αρχείο της πτυχιακής σου εργασίας πρέπει να παραμείνει ακριβώς όπως το αποθήκευσες.
3. **Διαθεσιμότητα (Availability):** Τα δεδομένα και οι υπηρεσίες είναι διαθέσιμα όταν τα χρειάζεσαι (π.χ. το Webmail λειτουργεί). **Παράδειγμα:** Το να έχεις Backup (αντίγραφα ασφαλείας) εξασφαλίζει τη διαθεσιμότητα των αρχείων σου ακόμα και μετά από βλάβη.

Είδη Απειλών: Από το Phishing στην Κοινωνική Μηχανική

Οι κυριότεροι κίνδυνοι που αντιμετωπίζεις online χωρίζονται σε δύο μεγάλες κατηγορίες:

Α. Απειλές Λογισμικού (Malware)

Απειλή	Περιγραφή	Πώς μολύνεσαι συνήθως;
Malware (Κακόβουλο Λογισμικό)	Γενικός όρος για ιούς, trojans, και spyware που σκοπό έχουν να κλέψουν δεδομένα ή να καταστρέψουν το σύστημά σου.	Άνοιγμα συνημμένων αρχείων από άγνωστα email ή λήψη πειρατικού/δωρεάν λογισμικού (π.χ. παιχνίδια, ταινίες, free software).
Ransomware	Λογισμικό που **κλειδώνει** τα	Ανοίγοντας ψεύτικα,

	αρχεία σου και ζητά λύτρα (ransom) για να τα ξεκλειδώσει.	επείγοντα email ή κάνοντας κλικ σε κακόβουλους συνδέσμους.

Β. Απειλές Εξαπάτησης (Social Engineering)

Η κοινωνική μηχανική είναι η τέχνη της χειραγώγησης του χρήστη ώστε να αποκαλύψει οικειοθελώς εμπιστευτικά στοιχεία.

Είδος Απάτης	**Τρόπος Λειτουργίας**	**Παράδειγμα Στόχευσης (Student Context)**
Phishing (Ηλεκτρονικό Ψάρεμα)	Ψεύτικα email ή ιστοσελίδες (π.χ. τράπεζας, Πανεπιστημίου) που ζητούν τους κωδικούς σου για "επαλήθευση" ή λόγω "ύποπτης δραστηριότητας".	*Ψεύτικο Πανεπιστήμιο:* Λαμβάνεις email που φαίνεται να είναι από το **uom.edu.gr** (αλλά το email είναι *uomsupport@gmail.com*), λέγοντας: *«Ο κωδικός σας στο e-class λήγει. Κάντε κλικ εδώ για ανανέωση.»*
Smishing	Απάτη μέσω **SMS** (κινητό) ή Viber/WhatsApp.	SMS από υποτιθέμενο **ΕΛΚΕ** (Ειδικός Λογαριασμός Κονδυλίων Έρευνας): *«Έχετε εκκρεμότητα σε επιστροφή διδάκτρων του μεταπτυχιακού. Πατήστε στο link και πληκτρολογήστε τον IBAN σας.»*
Vishing	Απάτη μέσω **Τηλεφωνικής Κλήσης** (Voice Phishing).	Σε καλεί κάποιος που παριστάνει υπάλληλο της Τράπεζας ή τεχνικό της Google και σου ζητά **κωδικούς OTP** για να "επαναφέρει την κάρτα σου".
Impersonation/Scam	Κάποιος παριστάνει γνωστό σου στα social media (π.χ. χακαρισμένος φίλος) και ζητά χρήματα με επείγουσα δικαιολογία.	Μήνυμα: *«Κάνε μου μια κατάθεση 100€ γρήγορα γιατί έχασα την κάρτα μου, θα στα δώσω αύριο.»*

Προστασία σε Δημόσια Δίκτυα Wi-Fi (The Public Threat)

Όταν συνδέεσαι σε δωρεάν Wi-Fi (π.χ. καφέ, πλατεία, αλλά όχι Eduroam), εκτίθεσαι σε κινδύνους:

1. **Man-in-the-Middle (MitM) Attack:** Ο hacker παρεμβάλλεται ανάμεσα σε εσένα και τον server. Μπορεί να υποκλέψει (διαβάσει) όλα τα δεδομένα που στέλνεις, συμπεριλαμβανομένων κωδικών πρόσβασης, αν η ιστοσελίδα δεν είναι **HTTPS**.
2. **Evil Twin Attack (Ψεύτικος Δίδυμος):** Ο hacker δημιουργεί ένα ψεύτικο δίκτυο Wi-Fi με το ίδιο όνομα με το νόμιμο (π.χ. *Free_Coffee_Shop_WiFi*). Αν συνδεθείς, όλη η κίνησή σου πηγαίνει απευθείας στον hacker.

Η Άμυνα	**Πρακτική Δράση**
Χρήση VPN	Το **VPN (Virtual Private Network)** κρυπτογραφεί την κίνησή σου, δημιουργώντας ένα ασφαλές «τούνελ». Ακόμα κι αν ο hacker υποκλέψει τα δεδομένα σου στο δημόσιο Wi-Fi, δεν μπορεί να τα διαβάσει.
Έλεγχος HTTPS	Μην κάνεις ποτέ Login σε λογαριασμό (email, e-class, τράπεζα) αν δεν βλέπεις το **λουκέτο** και το **HTTPS** στη διεύθυνση.
Απενεργοποίηση Sharing	Όταν είσαι σε δημόσιο δίκτυο, απενεργοποίησε την κοινή χρήση αρχείων και εκτυπωτών του υπολογιστή σου (Network Sharing).

Ασφάλεια σε Κοινόχρηστους Υπολογιστές (Εργαστήρια/Βιβλιοθήκες)

Η χρήση κοινόχρηστων υπολογιστών (όπως στα εργαστήρια του Πανεπιστημίου ή σε βιβλιοθήκες) απαιτεί **αυξημένη προσοχή**, καθώς πολλοί χρήστες έχουν πρόσβαση στο ίδιο μηχάνημα:

1. **Ποτέ Μην Αποθηκεύεις Κωδικούς:** Μην επιτρέπεις ποτέ στον browser να αποθηκεύσει τους κωδικούς σου («*Save Password*») στο εργαστήριο. Κάθε επόμενος χρήστης θα έχει πρόσβαση στους λογαριασμούς σου (e-class, webmail, κτλ.).
2. **Πάντα Αποσύνδεση (Log Out):** Ποτέ μην αφήνεις τον υπολογιστή ξεκλείδωτο ή το email σου ανοιχτό όταν φεύγεις από το εργαστήριο. Πρέπει να κάνεις **πλήρη αποσύνδεση (Log Out)** από κάθε υπηρεσία και να κλείσεις τον browser.
3. **USB Sticks & Ιοί:** Όταν συνδέεις το προσωπικό σου USB stick σε ένα κοινόχρηστο PC,

υπάρχει **αυξημένος κίνδυνος μόλυνσης** από ιούς (Malware) που μπορεί να έχουν αφήσει προηγούμενοι χρήστες. Πρέπει να έχεις ενημερωμένο antivirus στον προσωπικό σου υπολογιστή και να κάνεις σάρωση (scan) κάθε φορά που χρησιμοποιείς το USB stick σε εργαστήριο.

4. **Ιδιωτική Περιήγηση (Incognito/Private Mode):** Χρησιμοποίησε τη λειτουργία «Ιδιωτικής Περιήγησης» (Incognito Mode) στον browser του κοινόχρηστου PC. Αυτό διασφαλίζει ότι, μόλις κλείσεις το παράθυρο, ο browser **δεν θα κρατήσει κανένα ιστορικό** ή **προσωρινό κωδικό** που πληκτρολόγησες.

Προστασία σε Τραπεζικές Συναλλαγές (Banking Security)

Λόγω της αύξησης των ηλεκτρονικών απατών, η ασφάλεια στις τραπεζικές συναλλαγές είναι πλέον **ευθύνη του χρήστη**.

Πρακτική Άμυνα	Περιγραφή	Συνέπεια
Έλεγχος URL και HTTPS	**Πάντα** ελέγχεις ότι η διεύθυνση της τράπεζας ξεκινά με **HTTPS** και έχει το **λουκέτο** δίπλα στο URL.	Αν το λουκέτο λείπει ή το URL είναι διαφορετικό, "**φύγε αμέσως"**.
OTP (One-Time Password) & My Code	Οι κωδικοί μίας χρήσης (OTP) που λαμβάνεις στο κινητό σου μέσω SMS ή app.	**ΜΗΝ τους δίνεις ποτέ σε κανέναν** (ούτε σε υποτιθέμενο υπάλληλο της τράπεζας). Αυτοί οι κωδικοί είναι το κλειδί για την ολοκλήρωση της συναλλαγής **από εσένα**.
Απομακρυσμένη Πρόσβαση	**Ποτέ** μην επιτρέπεις σε κανέναν να αποκτήσει απομακρυσμένη πρόσβαση στον υπολογιστή ή το κινητό σου, ακόμα κι αν προσποιείται τεχνικός.	Μέσω της απομακρυσμένης πρόσβασης, οι απατεώνες αποκτούν πλήρη έλεγχο στους λογαριασμούς σου.

Γενικές Πρακτικές Ψηφιακής Προστασίας (Digital Hygiene)

Αυτοί είναι οι κανόνες που πρέπει να ακολουθείς καθημερινά:

Πρακτική	Δράση	Γιατί είναι σημαντικό;
Ισχυροί Κωδικοί	Χρησιμοποίησε κωδικούς με **τουλάχιστον 12 χαρακτήρες** (γράμματα, αριθμούς, σύμβολα) και **μην** χρησιμοποιείς τον ίδιο κωδικό παντού.	Αν χακαριστεί ένας λογαριασμός, δεν χάνονται όλοι.
Διπλή Ταυτοποίηση (2FA/MFA)	Ενεργοποίησε την **Ταυτοποίηση Δύο Παραγόντων** (2FA) σε όλους τους σημαντικούς λογαριασμούς (Πανεπιστήμιο, Email, Τράπεζες).	Ακόμα κι αν κλέψουν τον κωδικό σου, ο hacker δεν μπορεί να συνδεθεί χωρίς τον κωδικό που στέλνεται στο κινητό σου.
Ενημέρωση Λογισμικού	Ενημέρωνε τακτικά το **Λειτουργικό Σύστημα** (Windows/macOS), τον **Browser** (Chrome/Firefox) και τα **Antivirus** σου.	Οι ενημερώσεις περιέχουν **διορθώσεις ασφαλείας** που σε προστατεύουν από νέους ιούς και κενά ασφαλείας.
Ιδιωτικότητα Social Media	Ρύθμισε την **ιδιωτικότητα** (Privacy Settings) των λογαριασμών σου στα social media, ώστε να βλέπουν τα προσωπικά σου δεδομένα μόνο οι φίλοι σου.	Οι εγκληματίτες χρησιμοποιούν τα δημόσια στοιχεία σου (π.χ. κατοικία, σχέσεις) για εξαπάτηση.

Ηθική και Παιδαγωγική Διάσταση της Ασφάλειας

Ως μελλοντικοί εκπαιδευτικοί ή κοινωνικοί λειτουργοί, η ασφάλεια των δεδομένων δεν είναι μόνο προσωπικό ζήτημα, αλλά **επαγγελματική υποχρέωση**:

1. **Προστασία Ευαίσθητων Δεδομένων (GDPR):** Στο μέλλον, θα διαχειρίζεστε ευαίσθητα δεδομένα παιδιών, μαθητών ή κοινωνικών υποθέσεων. Η χρήση ισχυρών κωδικών και 2FA (**Ταυτοποίηση Δύο Παραγόντων**) **είναι ο φραγμός** που προστατεύει αυτούς τους ανθρώπους από την έκθεση.
2. **Ψηφιακός Γραμματισμός:** Η δική σου γνώση για την ασφάλεια θα γίνει το **μάθημα** που θα διδάξεις στους μαθητές σου, προστατεύοντάς τους από το Cyberbullying, το Phishing και τους διαδικτυακούς κινδύνους.

Περίληψη & Ερωτήσεις για Αυτοαξιολόγηση

Έννοια	Ορισμός-Κλειδί
Phishing	Απάτη μέσω ψεύτικων ιστοσελίδων/email για υποκλοπή κωδικών.
Vishing/Smishing	Απάτη μέσω **τηλεφώνου** (Vishing) ή **SMS** (Smishing).
2FA (Διπλή Ταυτοποίηση)	Ένα επιπλέον επίπεδο ασφαλείας (κωδικός + κινητό).
Man-in-the-Middle	Επίθεση υποκλοπής σε δημόσιο Wi-Fi.
OTP	Κωδικός μίας χρήσης (π.χ. για τραπεζική συναλλαγή). **Δεν δίνεται ποτέ.**

Σκέψου και Απάντησε:

1. Αν λάβεις ένα email που σου ζητά να κάνεις κλικ σε έναν σύνδεσμο επειδή "ο λογαριασμός σου έχει μπλοκαριστεί", ποιος τύπος απάτης είναι αυτός και τι πρέπει να κοιτάξεις **πριν** κάνεις κλικ;
2. Εξήγησε γιατί η **Ταυτοποίηση Δύο Παραγόντων (2FA)** θεωρείται η πιο σημαντική άμυνα έναντι της κλοπής κωδικών πρόσβασης.
3. Ποιος είναι ο κύριος κίνδυνος όταν χρησιμοποιείς το δημόσιο Wi-Fi σε μια καφετέρια και ποια είναι η πιο αποτελεσματική τεχνολογική λύση για να προστατευθείς;
4. Ένας άγνωστος σε καλεί και σου ζητά τον κωδικό **OTP** που μόλις έλαβες στο κινητό για να "ακυρώσει μια ύποπτη συναλλαγή". Ποιος είναι ο τύπος απάτης και γιατί δεν πρέπει να του δώσεις τον κωδικό;
5. **Κοινόχρηστος Υπολογιστής:** Εξηγήστε γιατί πρέπει πάντα να χρησιμοποιείτε τη λειτουργία **"Ιδιωτική Περιήγηση"** όταν εργάζεστε σε ένα εργαστήριο υπολογιστών του Πανεπιστημίου.