# Τοπίο σύγχρονων κυβερνοαπειλών

Εισαγωγή στις βασικές απειλές κυβερνοασφάλειας για επιχειρήσεις και οργανισμούς. Μια ουσιαστική ενημέρωση για στελέχη και εργαζομένους που θέλουν να προστατευτούν στο σύγχρονο ψηφιακό περιβάλλον.

Επιμελητήριο Ηρακλείου
Heraklion Chamber of Commerce & Industry

safeLine.gr

ΙΤΕ
ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

# Γιατί είναι σημαντική η κυβερνοασφάλεια;

Κάθε ημέρα, επιχειρήσεις και οργανισμοί σε όλο τον κόσμο δέχονται εκατοντάδες χιλιάδες κυβερνοεπιθέσεις. Στόχοι δεν είναι μόνο οι μεγάλες εταιρείες — οποιοσδήποτε χρησιμοποιεί email, κινητό ή σύνδεση στο διαδίκτυο είναι δυνητικός στόχος.

### 🎯 Στόχοι

Κατανόηση των σύγχρονων απειλών και βασικής ορολογίας κυβερνοασφάλειας.

### 🛡️ Προετοιμασία

Εξοπλισμός των συμμετεχόντων με πρακτικές γνώσεις για ασφαλή ψηφιακή συμπεριφορά.

### 📚 Βάση

Εισαγωγή στις επόμενες θεματικές ενότητες του σεμιναρίου κυβερνοασφάλειας.

# Γιατί μας αφορά η κυβερνοασφάλεια;

Η σύγχρονη εργασία έχει μεταφερθεί στο ψηφιακό περιβάλλον. Κάθε εργαλείο που χρησιμοποιούμε καθημερινά αποτελεί ταυτόχρονα και μια πιθανή πύλη εισόδου για επιτιθέμενους.

## Cloud

Τα δεδομένα μας βρίσκονται πλέον στο διαδίκτυο, προσβάσιμα από παντού.

## Email

Το email παραμένει το No1 μέσο μετάδοσης κυβερνοεπιθέσεων παγκοσμίως.

## Κινητές συσκευές

Τα smartphones μας περιέχουν ευαίσθητα δεδομένα και συνδέονται σε δίκτυα συνεχώς.

## Τεχνητή Νοημοσύνη

Η ΤΝ δίνει νέες δυνατότητες τόσο στους χρήστες όσο και στους επιτιθέμενους.

## Απομακρυσμένη εργασία

Η εργασία εκτός γραφείου διευρύνει σημαντικά την επιφάνεια επίθεσης.

## Ψηφιακός μετασχηματισμός

Η ψηφιοποίηση επιταχύνεται — και μαζί της αυξάνονται οι κίνδυνοι.

# Οι βασικές κατηγορίες κυβερνοαπειλών

Οι σύγχρονες κυβερνοαπειλές χωρίζονται σε έξι μεγάλες κατηγορίες. Γνωρίζοντας τις κατηγορίες, μπορούμε να αναγνωρίσουμε ευκολότερα τον κίνδυνο όταν εμφανίζεται.

# Social Engineering — Χειραγώγηση ανθρώπων

Το social engineering αποτελεί την πιο διαδεδομένη μέθοδο επίθεσης. Ο επιτιθέμενος δεν χρειάζεται να παραβιάσει συστήματα — αρκεί να εξαπατήσει εσάς. Μάθετε να αναγνωρίζετε τις πιο συνηθισμένες μορφές.

### 🎣 Phishing

Μαζικά ψεύτικα email που υποδύονται νόμιμες υπηρεσίες για να κλέψουν κωδικούς ή στοιχεία.

### 🎯 Spear Phishing

Στοχευμένη επίθεση σε συγκεκριμένο άτομο ή οργανισμό με εξατομικευμένο περιεχόμενο.

### 📱 Smishing

Phishing μέσω SMS — ψεύτικα μηνύματα κειμένου με κακόβουλους συνδέσμους.

### 📞 Vishing

Τηλεφωνική απάτη — κλήσεις που υποδύονται τράπεζες, ΕΦΚΑ, ή τεχνική υποστήριξη.

### 📷 Quishing

Phishing μέσω κακόβουλων QR codes — σκανάρετε και μεταφέρεστε σε ψεύτικες σελίδες.

### 🚪 Tailgating

Φυσική διείσδυση σε ασφαλή χώρο με πρόσχημα την εξυπηρέτηση ή ακολουθώντας αυθεντικό προσωπικό.

# Απειλές μέσω email

Το email είναι το πιο συχνό εργαλείο κυβερνοεπίθεσης στον επαγγελματικό χώρο. Οι παρακάτω τεχνικές στοχεύουν στην εξαπάτηση υπαλλήλων και στελεχών για οικονομικό όφελος ή κλοπή πληροφοριών.

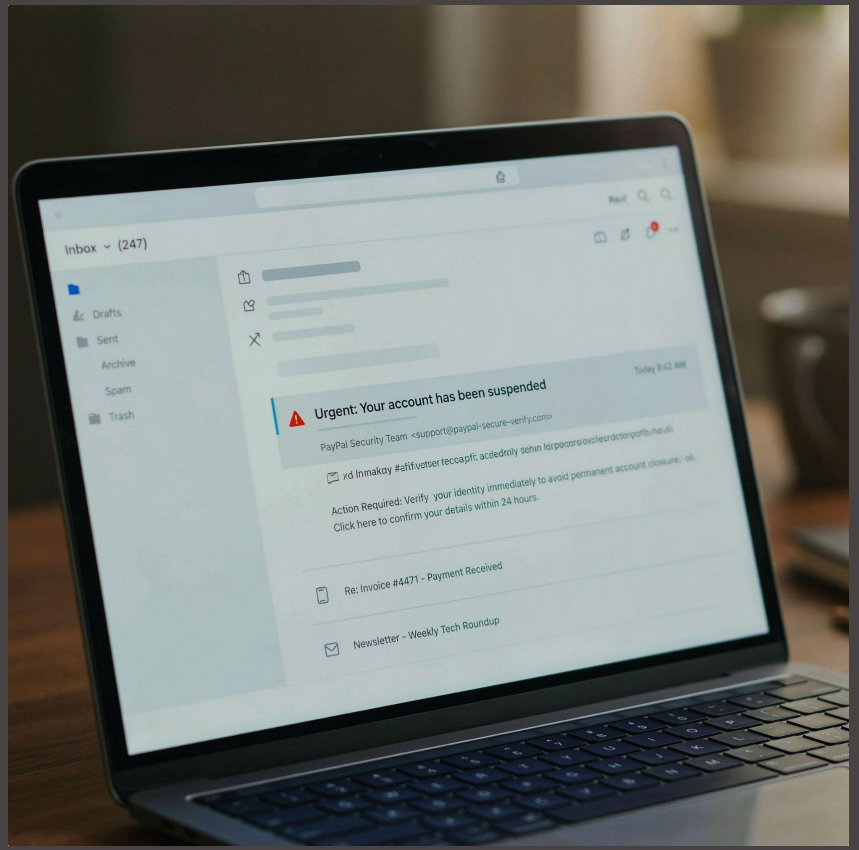
1. **Business Email Compromise:** Παραβίαση εταιρικού email για να εξαπατηθούν συνεργάτες ή η λογιστήρια.

2. **CEO fraud:** Email που υποδύεται ανώτερο στέλεχος ζητώντας άμεση μεταφορά κεφαλαίων.

3. **Email spoofing:** Πλαστογράφηση διεύθυνσης αποστολέα ώστε να μοιάζει με γνωστή πηγή.

4. **Credential theft:** Κλοπή κωδικών μέσω ψεύτικων σελίδων σύνδεσης που μιμούνται γνωστές πλατφόρμες.

5. **Invoice fraud:** Αποστολή ψεύτικων τιμολογίων για πληρωμή σε λογαριασμό επιτιθέμενου.



# Malware — Κακόβουλο λογισμικό

Ο όρος "Malware" (Malicious Software) περιγράφει κάθε είδους κακόβουλο λογισμικό που εγκαθίσταται στη συσκευή σας χωρίς να το γνωρίζετε. Ακολουθούν οι πιο συνηθισμένες μορφές που συναντώνται στο εταιρικό περιβάλλον.

## Virus

Αυτοαντιγράφεται και μολύνει άλλα αρχεία στο σύστημα.

## Worm

Εξαπλώνεται αυτόματα σε δίκτυα χωρίς ανθρώπινη παρέμβαση.

## Trojan

Μεταμφιέζεται ως χρήσιμο πρόγραμμα ενώ κρύβει κακόβουλο κώδικα.

## Spyware

Κατασκοπεύει τη δραστηριότητά σας και αποστέλλει δεδομένα σε τρίτους.

## Ransomware

Κρυπτογραφεί τα αρχεία σας και ζητά λύτρα για την αποκρυπτογράφησή τους.

## Keylogger

Καταγράφει κάθε πάτημα πλήκτρου — κλέβει κωδικούς και μηνύματα αθόρυβα.

## Cryptominer

Χρησιμοποιεί κρυφά τους πόρους της συσκευής σας για εξόρυξη κρυπτονομισμάτων.

# Απειλές Τεχνητής Νοημοσύνης

Η Τεχνητή Νοημοσύνη έχει δώσει στους κυβερνοεγκληματίες ισχυρά νέα εργαλεία. Πλέον μπορούν να δημιουργούν ψεύτικο περιεχόμενο τόσο πειστικό, που είναι δύσκολο να το ξεχωρίσουμε από αληθινό.

1. 🎭 Deepfakes
   Ρεαλιστικά βίντεο ή φωτογραφίες που δείχνουν πρόσωπα να λένε ή να κάνουν πράγματα που ποτέ δεν έγιναν.
2. 🎙️ Voice Cloning
   Κλωνοποίηση φωνής πραγματικού προσώπου με μόλις λίγα δευτερόλεπτα ηχητικού δείγματος.
3. ✉️ AI Phishing
   Αυτοματοποιημένη δημιουργία εξαιρετικά πειστικών phishing μηνυμάτων σε οποιαδήποτε γλώσσα.
4. 🤖 Fake Chatbots
   Κακόβουλα chatbots που υποδύονται εξυπηρέτηση πελατών και συλλέγουν προσωπικά δεδομένα.
5. 👤 Synthetic Identity
   Δημιουργία πλαστών ψηφιακών ταυτοτήτων με συνδυασμό πραγματικών και ψεύτικων στοιχείων.

# Απειλές Δικτύου και Διαδικτύου

Κάθε φορά που συνδεόμαστε στο διαδίκτυο — ιδιαίτερα εκτός γραφείου — εκτιθέμεθα σε δικτυακές απειλές. Το δημόσιο Wi-Fi, οι browser και οι QR codes μπορούν να αποτελέσουν πύλη εισόδου για επιτιθέμενους.

### 📶 Public Wi-Fi

Ανοιχτά δίκτυα σε καφετέριες ή αεροδρόμια — οι επικοινωνίες σας είναι εκτεθειμένες.

### 📡 Rogue Wi-Fi

Ψεύτικα σημεία πρόσβασης που μιμούνται γνωστά δίκτυα για να παγιδεύσουν χρήστες.

### ⬇️ Drive-by Downloads

Αυτόματη λήψη κακόβουλου λογισμικού απλώς επισκεπτόμενοι μολυσμένη ιστοσελίδα.

### 🌐 Browser Exploits

Εκμετάλλευση αδυναμιών του browser σας για εγκατάσταση κακόβουλου λογισμικού.

### 🔀 Man-in-the-Middle

Ο επιτιθέμενος «κάθεται» ανάμεσα σε εσάς και τον διακομιστή, υποκλέπτοντας δεδομένα.

### 📷 Κακόβουλα QR Codes

QR codes σε δημόσιους χώρους που ανακατευθύνουν σε επικίνδυνες ιστοσελίδες.

# Απειλές για δεδομένα

Τα δεδομένα είναι ο πολυτιμότερος πόρος κάθε οργανισμού. Πολλές φορές η διαρροή δεδομένων δεν προέρχεται από εξωτερική επίθεση, αλλά από λάθη, αμέλεια ή ακόμα και κακόβουλη εσωτερική συμπεριφορά.

### 💧 Data leakage

Ακούσια ή εκούσια διαρροή ευαίσθητων δεδομένων εκτός οργανισμού.

### 🔓 Weak passwords

Απλοί ή προβλέψιμοι κωδικοί που παραβιάζονται εύκολα με αυτοματοποιημένα εργαλεία.

### 🔄 Password reuse

Χρήση ίδιου κωδικού σε πολλά συστήματα — μια παραβίαση αρκεί για να εκτεθούν όλα.

### 👤 Shadow IT

Χρήση μη εγκεκριμένων εφαρμογών ή υπηρεσιών cloud εκτός ελέγχου του IT τμήματος.

### 🏢 Insider threats

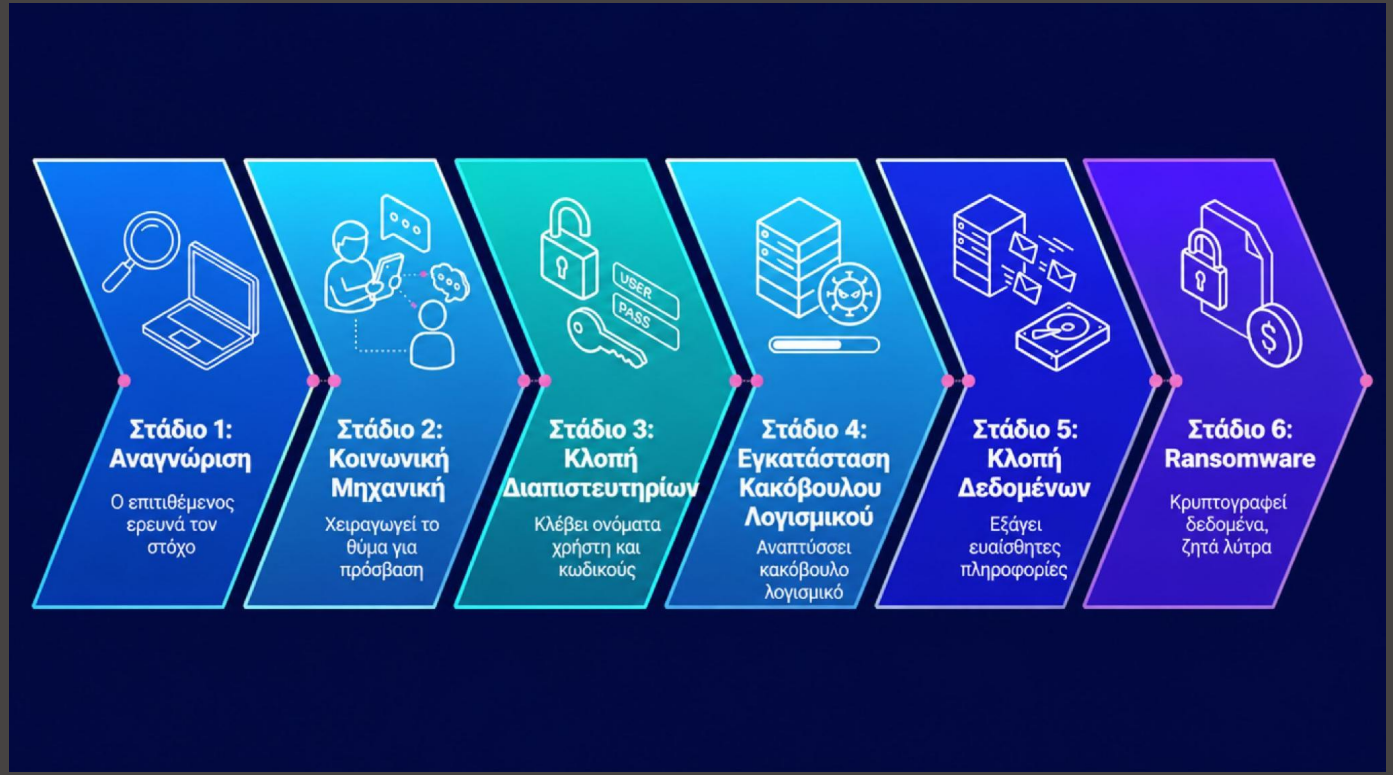
Εσκεμμένη ή τυχαία βλάβη από εργαζόμενους ή πρώην συνεργάτες με πρόσβαση σε συστήματα.

### ☁️ Cloud misconfiguration

Λανθασμένες ρυθμίσεις cloud υπηρεσιών που αφήνουν δεδομένα δημόσια προσβάσιμα.

# Πώς εξελίσσεται μια κυβερνοεπίθεση

Οι κυβερνοεπιθέσεις δεν συμβαίνουν τυχαία — ακολουθούν ένα συγκεκριμένο μοτίβο από την αρχή ως το τέλος. Κατανοώντας τα στάδια, μπορούμε να αναγνωρίσουμε και να διακόψουμε μια επίθεση νωρίτερα.




Κάθε στάδιο αποτελεί μια ευκαιρία για εμάς να αντιδράσουμε και να σταματήσουμε την επίθεση — ο πιο αποτελεσματικός τρόπος είναι η **πρόληψη στα πρώτα στάδια**.

# Πώς προστατευόμαστε

Η προστασία στον ψηφιακό χώρο δεν είναι θέμα μόνο της πληροφορικής — αφορά κάθε εργαζόμενο. Επτά βασικές συνήθειες μπορούν να αποτρέψουν την πλειονότητα των κυβερνοεπιθέσεων.

## MFA

Πολυπαραγοντικός έλεγχος ταυτότητας — ένα επιπλέον επίπεδο ασφάλειας πέρα από τον κωδικό.

## Εκπαίδευση

Η γνώση είναι η καλύτερη άμυνα — ενημερωμένοι εργαζόμενοι αναγνωρίζουν τις απειλές.

## Backup

Τακτικά αντίγραφα ασφαλείας — ο τελευταίος αμυντικός γραμμή ενάντια στο ransomware.

## Password Manager

Δημιουργία και αποθήκευση μοναδικών ισχυρών κωδικών για κάθε υπηρεσία.

## Antivirus

Ενεργοποιημένο και ενημερωμένο λογισμικό ασφάλειας σε όλες τις συσκευές.

## Updates

Τακτικές ενημερώσεις λειτουργικού και εφαρμογών κλείνουν γνωστές ευπάθειες.

# Οι θεματικές του σεμιναρίου

Αυτή η εισαγωγή θέτει τις βάσεις για τις επόμενες ενότητες. Κάθε θέμα θα αναλυθεί σε βάθος με πρακτικά παραδείγματα, οδηγίες αναγνώρισης απειλών και συγκεκριμένες συμβουλές προστασίας.

## 🎣 Phishing

Αναγνώριση απατηλών μηνυμάτων

## 📧 Email Security

Ασφαλής χρήση εταιρικού email

## 🔑 Password security

Δημιουργία ισχυρών κωδικών

## 🌐 Browser security

Ασφαλής πλοήγηση στο διαδίκτυο

## 📶 Public Wi-Fi

Προστασία σε δημόσια δίκτυα

## 📱 Mobile security

Ασφάλεια κινητών συσκευών

# Οι θεματικές του σεμιναρίου (συνέχεια)

Προχωρημένες θεματικές για ολοκληρωμένη κυβερνοπροστασία.

### 💾 Secure software
Ασφαλής εγκατάσταση λογισμικού

### ☁️ Cloud security
Ασφαλής χρήση cloud υπηρεσιών

### 🤖 AI security
Κίνδυνοι Τεχνητής Νοημοσύνης

### 🎭 Deepfakes
Αναγνώριση ψεύτικου περιεχομένου

### 💼 BEC
Business Email Compromise

### 🔒 Ransomware & Backup
Προστασία και ανάκτηση δεδομένων

Σε κάθε ενότητα θα μάθετε να αναγνωρίζετε την απειλή, να αντιδράτε σωστά και να αναφέρετε ύποπτα περιστατικά στην ομάδα σας.