Απειλές από δημόσια δίκτυα Wi-Fi, VPN και ασφαλής απομακρυσμένη εργασία

Ένας πρακτικός οδηγός για επαγγελματίες που εργάζονται εκτός γραφείου — και για τις επιχειρήσεις που θέλουν να τους προστατέψουν.

🎯 Στόχοι σεμιναρίου

Κατανόηση των κινδύνων και εφαρμογή πρακτικών μέτρων προστασίας

🏢 Γιατί μας αφορά

Η κυβερνοασφάλεια είναι υπόθεση κάθε επιχείρησης, ανεξαρτήτως μεγέθους

🌍 Νέα πραγματικότητα

Η απομακρυσμένη εργασία έχει καταστεί μόνιμο χαρακτηριστικό του σύγχρονου εργασιακού τοπίου

Επιμελητήριο Ηρακλείου
Heraklion Chamber of Commerce & Industry

safeLine.gr

ΙΤΕ
ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Τι είναι το δημόσιο Wi-Fi;

Το δημόσιο Wi-Fi είναι κάθε ασύρματο δίκτυο διαθέσιμο σε κοινόχρηστους χώρους — καφετέριες, ξενοδοχεία, αεροδρόμια, εμπορικά κέντρα και βιβλιοθήκες. Η πρόσβαση είναι συνήθως δωρεάν ή με απλή εγγραφή, χωρίς καμία εγγύηση για το επίπεδο ασφάλειας που παρέχεται.

📍 Πού το συναντάμε

Καφετέριες, ξενοδοχεία, αεροδρόμια, σταθμοί τρένων, εμπορικά κέντρα και δημόσιοι χώροι σε όλες τις πόλεις.

❓ Άγνωστο επίπεδο ασφάλειας

Δεν γνωρίζουμε ποιος διαχειρίζεται το δίκτυο, πόσο παλιός είναι ο εξοπλισμός ή αν εφαρμόζεται οποιαδήποτε κρυπτογράφηση.

👥 Κοινόχρηστο περιβάλλον

Εκατοντάδες χρήστες μοιράζονται την ίδια σύνδεση ταυτόχρονα — το κάθε πακέτο δεδομένων είναι θεωρητικά ορατό σε όλους.

Κίνδυνοι από τη χρήση δημόσιου Wi-Fi

Η σύνδεση σε ένα δημόσιο δίκτυο εκθέτει τη συσκευή και τα δεδομένα σας σε μια σειρά από σοβαρές κυβερνοαπειλές. Οι επιτιθέμενοι μπορούν να παρακολουθούν, να τροποποιούν ή να ανακατευθύνουν την κυκλοφορία σας χωρίς να το αντιληφθείτε.

Υποκλοπή δεδομένων

Κακόβουλοι χρήστες παρακολουθούν αθόρυβα την κυκλοφορία του δικτύου και συλλέγουν δεδομένα όπως emails, αρχεία και μηνύματα.

Evil Twin Attack

Ο επιτιθέμενος δημιουργεί ένα ψεύτικο σημείο πρόσβασης με πανομοιότυπο όνομα, παρασύροντας τους χρήστες να συνδεθούν σε αυτό.

DNS Spoofing

Χειραγώγηση των ρυθμίσεων DNS ώστε ο χρήστης να ανακατευθύνεται σε ψεύτικες ιστοσελίδες χωρίς να το γνωρίζει.

Man-in-the-Middle

Ο εισβολέας παρεμβάλλεται μεταξύ χρήστη και διακομιστή, υποκλέπτοντας ή τροποποιώντας την επικοινωνία σε πραγματικό χρόνο.

Κλοπή κωδικών

Καταγραφή διαπιστευτηρίων κατά τη σύνδεση σε υπηρεσίες email, εταιρικά συστήματα, ηλεκτρονικές τράπεζες και πλατφόρμες.

Επιπτώσεις για τις επιχειρήσεις

Μια μοναδική παραβίαση μέσω δημόσιου Wi-Fi μπορεί να έχει καταστροφικές συνέπειες για ολόκληρη την επιχείρηση — νομικές, οικονομικές και φήμης. Η αλυσιδωτή επίδραση ξεκινά από έναν υπολογιστή και φτάνει ως τα πιο ευαίσθητα εταιρικά στοιχεία.

📂 Διαρροή εταιρικών δεδομένων

Εμπιστευτικές πληροφορίες πελατών, οικονομικά στοιχεία και επιχειρηματικά σχέδια πέφτουν στα χέρια ανταγωνιστών ή εγκληματιών.

🔓 Παραβίαση λογαριασμών

Κλεμμένα διαπιστευτήρια εργαζομένων επιτρέπουν μη εξουσιοδοτημένη πρόσβαση σε εταιρικά συστήματα, email και cloud υπηρεσίες.

💰 Οικονομική απάτη

Εκτροπή τραπεζικών συναλλαγών, κλοπή εταιρικών κεφαλαίων ή εκβιαστικές απαιτήσεις λύτρων (ransomware).

⚖️ Παραβίαση GDPR

Η διαρροή προσωπικών δεδομένων πελατών ή εργαζομένων επισύρει βαριά πρόστιμα έως 4% του παγκόσμιου ετήσιου τζίρου.

📉 Πλήγμα στη φήμη

Η δημοσιοποίηση παραβίασης αλλάζει οριστικά την εικόνα της εταιρείας στα μάτια πελατών, συνεργατών και επενδυτών.

Παραδείγματα επιθέσεων στην πράξη

Οι παρακάτω σενάρια δεν είναι θεωρητικές υποθέσεις — αποτελούν πραγματικές τακτικές που χρησιμοποιούνται καθημερινά από κυβερνοεγκληματίες εναντίον ατόμων και επιχειρήσεων σε ολόκληρο τον κόσμο.

1

Ψεύτικο εταιρικό Wi-Fi

Επιτιθέμενος στήνει σημείο πρόσβασης με όνομα **"CorpNet_Guest"** σε lobby ξενοδοχείου όπου διεξάγεται εταιρικό συνέδριο. Δεκάδες στελέχη συνδέονται χωρίς να υποψιαστούν τίποτα.

2

Υποκλοπή σύνδεσης VoIP

Τηλεφωνική κλήση μέσω εφαρμογής (π.χ. Teams, Zoom) χωρίς VPN σε δημόσιο δίκτυο παρακολουθείται αθόρυβα, αποκαλύπτοντας εμπιστευτικές επιχειρηματικές συνομιλίες.

3

Κλοπή διαπιστευτηρίων

Εργαζόμενος συνδέεται στο εταιρικό email από αεροδρόμιο χωρίς VPN. Τα στοιχεία σύνδεσης υποκλέπτονται και χρησιμοποιούνται ώρες αργότερα για εταιρική κατασκοπεία.

4

Ανακατεύθυνση σε phishing

Μέσω DNS Spoofing, η διεύθυνση **bank.gr** ανακατευθύνεται σε πανομοιότυπο ψεύτικο site που κλέβει στοιχεία καρτών και κωδικούς.

Τι είναι το VPN;

Το **Virtual Private Network (VPN)** δημιουργεί μια κρυπτογραφημένη "σήραγγα" μεταξύ της συσκευής σας και του διακομιστή προορισμού. Όλα τα δεδομένα που διέρχονται από αυτή τη σήραγγα είναι αδύνατο να διαβαστούν από τρίτους, ακόμα κι αν υποκλαπούν.

> Το VPN είναι το πιο αποτελεσματικό εργαλείο για ασφαλή χρήση δημόσιου Wi-Fi — αλλά δεν είναι πανάκεια.

Πώς λειτουργεί

1 Κρυπτογράφηση δεδομένων

Όλη η κυκλοφορία κωδικοποιείται με ισχυρούς αλγόριθμους (AES-256) πριν φύγει από τη συσκευή σας.

2 Απόκρυψη IP διεύθυνσης

Η πραγματική σας τοποθεσία και ταυτότητα δικτύου αντικαθίστανται από αυτές του VPN server.

3 Προστασία σε δημόσια δίκτυα

Ακόμα και σε Evil Twin ή Man-in-the-Middle επίθεση, τα δεδομένα παραμένουν αδιάβαστα.

Ασφαλής απομακρυσμένη εργασία

Η ασφάλεια στην απομακρυσμένη εργασία δεν στηρίζεται σε ένα μόνο εργαλείο. Απαιτεί έναν συνδυασμό τεχνολογιών και καλών πρακτικών που αλληλοσυμπληρώνονται για να δημιουργήσουν μια ολοκληρωμένη ασπίδα προστασίας.

Εταιρικό VPN

Πάντοτε ενεργό κατά τη σύνδεση σε εταιρικά συστήματα από οποιοδήποτε εξωτερικό δίκτυο.

Πολυπαραγοντικός έλεγχος (MFA)

Ακόμα κι αν κλαπεί ο κωδικός σας, ο εισβολέας δεν μπορεί να συνδεθεί χωρίς τον δεύτερο παράγοντα επαλήθευσης.

Ενημερώσεις λογισμικού

Τακτικές ενημερώσεις λειτουργικού συστήματος και εφαρμογών κλείνουν γνωστές ευπάθειες που εκμεταλλεύονται οι επιτιθέμενοι.

Antivirus και Firewall

Ενεργό antivirus και firewall σε κάθε εταιρική συσκευή αποτελούν το τελευταίο επίπεδο άμυνας απέναντι σε κακόβουλο λογισμικό.

Πρακτικές συμβουλές για τους εργαζομένους

Η τεχνολογία προσφέρει εργαλεία, αλλά η τελική γραμμή άμυνας είναι ο ίδιος ο εργαζόμενος. Με απλές καθημερινές συνήθειες μειώνεται δραματικά η πιθανότητα να πέσετε θύμα κυβερνοεπίθεσης.

Επιβεβαιώστε το σωστό δίκτυο

Ρωτήστε πάντα το προσωπικό για το επίσημο όνομα του Wi-Fi. Ένα λεπτό διαφορά στο SSID (π.χ. "Cafe_Free" vs "CaFe_Free") μπορεί να κρύβει Evil Twin επίθεση.

Χρησιμοποιείτε μόνο HTTPS

Ελέγξτε ότι κάθε ιστοσελίδα ξεκινά με **https://** και εμφανίζει το εικονίδιο κλειδαριάς. Αποφεύγετε κάθε σελίδα με HTTP μόνο.

Αποφύγετε ευαίσθητες συναλλαγές χωρίς VPN

Email, τραπεζικές συναλλαγές, εταιρικά συστήματα και αποστολή εμπιστευτικών αρχείων δεν πρέπει ποτέ να γίνονται χωρίς ενεργό VPN σε δημόσιο δίκτυο.

Κλειδώστε τις συσκευές σας

Ορίστε αυτόματο κλείδωμα σε 1-2 λεπτά αδράνειας. Μην αφήνετε ποτέ ξεκλείδωτη συσκευή χωρίς επιτήρηση σε δημόσιο χώρο.

Τι να κάνετε αν υποψιαστείτε επίθεση

Η γρήγορη αντίδραση μπορεί να περιορίσει σημαντικά τη ζημία. Αν παρατηρήσετε ασυνήθιστη συμπεριφορά, αργές συνδέσεις, ανακατευθύνσεις ή μη αναμενόμενες αιτήσεις σύνδεσης, ενεργήστε άμεσα.

⚠ Κάθε λεπτό καθυστέρησης αυξάνει την έκταση της πιθανής παραβίασης.

01

Άμεση αποσύνδεση

Αποσυνδεθείτε από το δίκτυο Wi-Fi αμέσως. Απενεργοποιήστε το Wi-Fi και τυχόν αυτόματη επανασύνδεση στη συσκευή.

02

Ενημέρωση τμήματος IT

Επικοινωνήστε αμέσως με τον υπεύθυνο ασφαλείας ή το τμήμα IT, περιγράφοντας τι παρατηρήσατε και πότε.

03

Αλλαγή κωδικών

Αλλάξτε άμεσα τους κωδικούς για κάθε λογαριασμό στον οποίο συνδεθήκατε ενόσω ήταν πιθανώς ενεργή η επίθεση.

04

Έλεγχος λογαριασμών

Ελέγξτε το ιστορικό δραστηριότητας email, τραπεζικών λογαριασμών και εταιρικών εφαρμογών για ύποπτες ενέργειες.

Συμπεράσματα & επόμενα βήματα

⚠️ Σημαντικοί κίνδυνοι

Το δημόσιο Wi-Fi ενέχει πολλαπλούς, σοβαρούς κινδύνους για δεδομένα, λογαριασμούς και εταιρικά συστήματα.

🛡️ Το VPN προστατεύει

Η χρήση εταιρικού VPN μειώνει δραματικά την έκθεση στους κινδύνους και πρέπει να είναι υποχρεωτική πολιτική.

🎓 Ενημέρωση = Άμυνα

Η εκπαίδευση και ευαισθητοποίηση των εργαζομένων είναι το πιο κρίσιμο επίπεδο κυβερνοασφάλειας κάθε οργανισμού.

> Η κυβερνοασφάλεια δεν είναι αποκλειστικά θέμα τεχνολογίας — είναι θέμα κουλτούρας, εκπαίδευσης και καθημερινής συνείδησης κάθε εργαζόμενου.

Ερωτήσεις; 🙋