Εισαγωγή στις επιθέσεις Phishing/Smishing

Επιμελητήριο Ηρακλείου
Heraklion Chamber of Commerce & Industry

safeLine.gr

ΙΝΣΤΙΤΟΥΤΟ ΠΛΗΡΟΦΟΡΙΚΗΣ

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Τι είναι το phishing;

Το phishing είναι μια μορφή ψηφιακής απάτης όπου οι επιτιθέμενοι υποδύονται αξιόπιστους οργανισμούς για να εξαπατήσουν χρήστες και να κλέψουν ευαίσθητα στοιχεία.

🎣 Ψεύτικο μήνυμα

Email, SMS ή μήνυμα που μιμείται νόμιμο αποστολέα — τράπεζα, δημόσια υπηρεσία ή γνωστή εταιρεία.

👤 Εξαπάτηση χρήστη

Ο παραλήπτης πείθεται να κάνει κλικ σε σύνδεσμο ή να ανοίξει συνημμένο αρχείο.

🔑 Υποκλοπή στοιχείων

Κωδικοί πρόσβασης, αριθμοί καρτών, προσωπικά ή εταιρικά δεδομένα παραδίδονται στον απατεώνα.

💰 Οικονομική απάτη

Το τελικό αποτέλεσμα είναι χρηματική ζημιά, παραβίαση λογαριασμών ή εταιρική κατασκοπεία.

Στατιστικά για το phishing

Τα νούμερα αποκαλύπτουν το πραγματικό μέγεθος της απειλής για επιχειρήσεις κάθε μεγέθους.

90% των κυβερνοεπιθέσεων παγκοσμίως ξεκινούν από ένα απλό email phishing.

3,4B Phishing emails αποστέλλονται καθημερινά παγκοσμίως, στοχεύοντας εκατομμύρια οργανισμούς.

#1 απειλή για τις μικρομεσαίες επιχειρήσεις καθώς συχνά υστερούν σε προστασία.

Γιατί πετυχαίνουν οι επιθέσεις;

Οι επιτιθέμενοι δεν εκμεταλλεύονται τεχνικά κενά — εκμεταλλεύονται ανθρώπινα συναισθήματα.
Αυτές είναι οι πέντε κύριες ψυχολογικές τεχνικές που χρησιμοποιούν:

Φόβος

«Ο λογαριασμός σας έχει παραβιαστεί!» — Η αίσθηση κινδύνου παρακάμπτει την κριτική σκέψη.

Βιασύνη

«Ενεργήστε εντός 24 ωρών!» — Η πίεση χρόνου εμποδίζει τον έλεγχο της αυθεντικότητας.

Εξουσία

«Εφορία / Τράπεζα / CEO» — Η υποδυόμενη εξουσία επιβάλλει υπακοή χωρίς αμφισβήτηση.

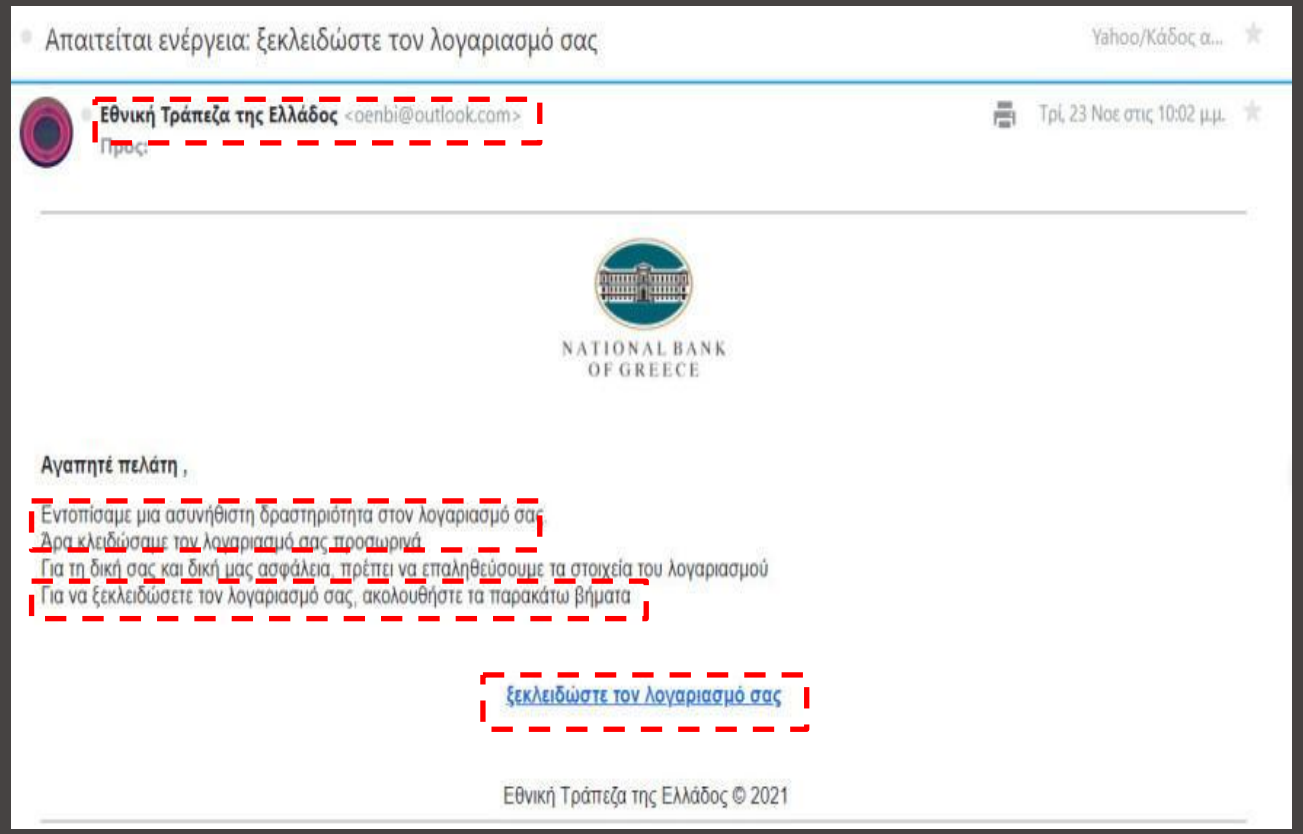
Δώρο

«Κερδίσατε βραβείο!» — Η υπόσχεση κέρδους μειώνει την επαγρύπνηση.

Εμπιστοσύνη

Το μήνυμα μοιάζει πανομοιότυπο με αυτά γνωστών εταιρειών ή συνεργατών.

Παράδειγμα phishing



Προειδοποιητικά σημάδια

Επείγουσα γλώσσα: Μηνύματα με λέξεις όπως «άμεσα», «κίνδυνος» ή «ο λογαριασμός σας κλειδώθηκε».

Ύποπτο email: Η διεύθυνση αποστολέα ή το domain δεν φαίνεται επίσημο ή αξιόπιστο.

Άγνωστος σύνδεσμος: Το link οδηγεί σε διαφορετική ή ύποπτη ιστοσελίδα.

Απαίτηση δράσης: Καμία τράπεζα ή υπηρεσία δεν ζητά κωδικούς μέσω email ή μηνυμάτων.

Παράδειγμα phishing

ΔΙΚΑΣΤΙΚΗ ΑΝΑΚΟΙΝΩΣΗ αριθ.887 - manoslak@gmail.com - Google Chrome

mail.google.com/mail/u/0/popout?ver=1kb54q60x21o5&msg=%23msg-f%3A1865327917933211260&attid=0.2

Θέμα: ΔΙΚΑΣΤΙΚΗ ΑΝΑΚΟΙΝΩΣΗ αριθ.887

Αρχηγός Αστυνομίας <std24514@phichai.ac.th>

προς

Γειά σου,

Διαβάστε το συνημμένο έγγραφο που ισχύει για εσάς.

Με σεβασμό.

Mike Wood

επικεφαλής της Ελλάδας

Αστυνομικό Τμήμα

Ένα συνημμένο • Σαρώθηκε από το Gmail ⓘ Προσθήκη στο Drive

ΥΠΟΥΡΓΕΙΟ ΔΙΚΑΙΟΣΥΝΗΣ ΚΑΙ ΔΗΜΟΣΙΑΣ ΤΑΞΕΩΣ

ΑΣΤΥΝΟΜΙΑ ΚΥΠΡΟΥ

INTERPOL

ΓΕΝΙΚΗ ΑΣΤΥΝΟΜΙΚΗ ΔΙΕΥΘΥΝΣΗ

ΔΙΚΑΣΤΙΚΗ ΚΛΗΣΗ

Για ερευνητικούς σκοπούς

(άρθρο 331-1-22 του Κώδικα Ποινικής Δικονομίας)

Είμαι ο Στυλιανός Παπαθεοδώρου, Γενικός Διευθυντής της Αστυνομίας Κύπρου και Επικεφαλής του Γραφείου Εγκληματολογικών Ερευνών. Σε συνεργασία με την Ευρωπαϊκή Αστυνομική Υπηρεσία (INTERPOL), επικοινωνώ μαζί σας αμέσως μετά την κατάσχεση διείσδυσης στον κυβερνοχώρο (επιτρέπεται, ιδίως σε παιδική πορνογραφία, πορνογραφικούς ιστότοπους, κυβερνοπορνογραφία) για να σας ενημερώσω ότι αντιμετωπίζετε διάφορες νομικές διαδικασίες:

* **ΚΥΒΕΡΝΟΠΟΡΝΟ**
* **ΠΟΡΝΟ ΙΣΤΟΣΕΛΙΔΕΣ**
* **ΠΑΙΔΙΚΗ ΠΟΡΝΟ**
* **ΝΟΜΙΜΟΣ ΒΙΑΣΜΟΣ**

Επικοινωνήστε μαζί μας μέσω e-mail γράφοντάς μας τις αιτιολογήσεις σας ώστε να ληφθούν υπόψη για την αξιολόγηση της κύρωσης.
Αυτό εντός αυστηρής προθεσμίας 48 ωρών. Μετά από αυτό το διάστημα, θα στείλουμε την αναφορά μας στον κ. Σάββα Αγγελίδη, εισαγγελέα, ώστε να εκδώσει ένταλμα σύλληψης εναντίον σας και να σας βάλει στη λίστα των σεξουαλικών παραβατών.
Το αρχείο σας θα δημοσιευτεί επίσης στα μέσα ενημέρωσης, ώστε το κοινό και η οικογένειά σας να γνωρίζουν τι κάνετε στον υπολογιστή σας.
Αναμένουμε την απάντησή σας για να ανοίξουμε μια αναφορά.

Είστε τώρα προειδοποιημένοι.

Η ΚΑΤΕΥΘΥΝΣΗ

Στυλιανός Παπαθεοδώρου

Γενικός Διευθυντής Κυπριακής Αστυνομίας
και επικεφαλής του Γραφείου Εγκληματολογικών Ερευνών

Το κινητό είναι πλέον ο βασικός στόχος

- Τα κινητά τηλέφωνα αποτελούν πλέον έναν από τους βασικότερους στόχους online απάτης.
- Σχεδόν το 98% των SMS ανοίγονται από τους χρήστες, ενώ οι περισσότεροι απαντούν μέσα σε λίγα μόνο λεπτά. Αυτό κάνει τα smishing attacks ιδιαίτερα αποτελεσματικά.
- Ένα μόνο link αρκεί ώστε ο χρήστης να οδηγηθεί σε κλοπή λογαριασμού, υποκλοπή προσωπικών στοιχείων ή οικονομική απάτη.

Smishing: Απάτες μέσω SMS & εφαρμογών μηνυμάτων

Το **smishing** είναι μια μορφή επίθεσης phishing που πραγματοποιείται μέσω SMS, Viber, WhatsApp, Messenger ή Telegram. Στόχος των επιτιθέμενων είναι η κλοπή κωδικών, στοιχείων καρτών ή η εγκατάσταση κακόβουλου λογισμικού — εκμεταλλευόμενοι την εμπιστοσύνη που έχουμε στα μηνύματα του κινητού μας.

Γιατί είναι τόσο επικίνδυνο;

- Το κινητό θεωρείται **προσωπική** και αξιόπιστη συσκευή
- Οι περισσότεροι ανοίγουν **άμεσα** τα εισερχόμενα μηνύματα
- Οι σύνδεσμοι είναι **δύσκολο να ελεγχθούν** σε μικρή οθόνη

Τυπικά παραδείγματα μηνυμάτων

📦 **«Το δέμα σας δεν παραδόθηκε. Επιβεβαιώστε τη διεύθυνσή σας.»**

💰 **«Κερδίσατε δωροεπιταγή €500. Διεκδικήστε τη.»**

Πώς να αναγνωρίσετε & να αντιδράσετε σε Smishing

Ενδείξεις απάτης

- **Επείγον ύφος** — «Απαντήστε άμεσα!», «Λήγει σήμερα!»
- **Συντομευμένοι σύνδεσμοι** — bit.ly, tinyurl και παρόμοια
- **Αίτημα για OTP**, κωδικούς ή στοιχεία κάρτας
- **Άγνωστος αποστολέας** ή μίμηση γνωστού οργανισμού
- **Ορθογραφικά λάθη** και αδέξια διατύπωση

✅ Τι κάνουμε αμέσως

ΔΕΝ πατάμε κανέναν σύνδεσμο

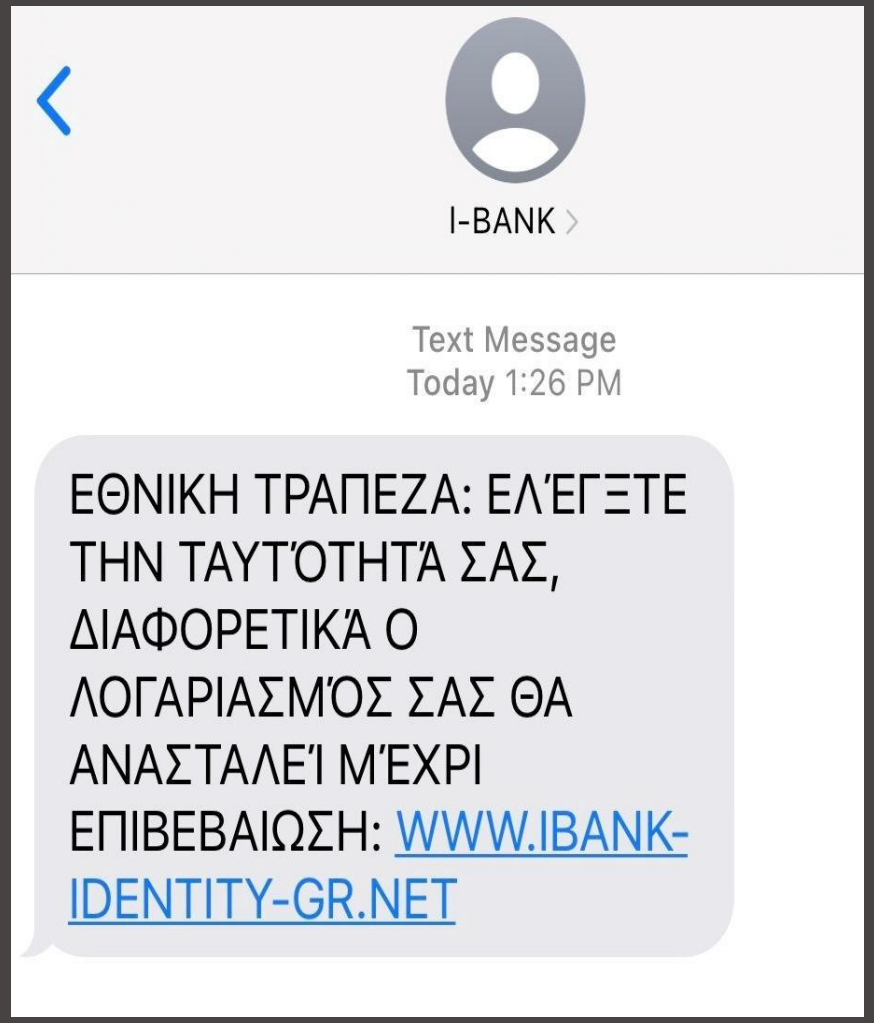
Επικοινωνούμε μέσω της **επίσημης ιστοσελίδας** ή γνωστού αριθμού

Αναφέρουμε το μήνυμα στο **τμήμα IT**

Διαγράφουμε το μήνυμα αμέσως

⚠ **Χρυσός Κανόνας:** Καμία τράπεζα ή δημόσια υπηρεσία **δεν ζητά ποτέ** κωδικούς ή στοιχεία κάρτας μέσω SMS ή εφαρμογών μηνυμάτων. Αν λάβετε τέτοιο αίτημα, είναι πάντα απάτη.

Smishing



Τι συμβαίνει πραγματικά;

- Ένα αθώο μήνυμα ή SMS δημιουργεί αίσθηση επείγοντος και οδηγεί τον χρήστη σε ψεύτικη σελίδα σύνδεσης.

- Μόλις εισαχθούν τα στοιχεία πρόσβασης, οι επιτιθέμενοι αποκτούν πρόσβαση στον λογαριασμό και στα προσωπικά δεδομένα του χρήστη.

QR Phishing — «Quishing»

Η νέα γενιά επιθέσεων παρακάμπτει τα φίλτρα email χρησιμοποιώντας QR codes αντί για συνδέσμους.

Το κινητό τηλέφωνο **δεν διαθέτει ειδική προστασία** — κάνει τον χρήστη πιο ευάλωτο. Ποτέ μη σκανάρετε QR code από email χωρίς να επαληθεύσετε την πηγή.

Αναγνωρίζοντας ύποπτα emails

Μάθετε να διαβάζετε τα **κρυφά σήματα** που προδίδουν ένα phishing email. Ο έλεγχος διαρκεί μόλις 10 δευτερόλεπτα.

🔍 Ύποπτο domain αποστολέα

Το email φαίνεται από «support@alphabank.com» αλλά το πραγματικό domain είναι «alphabank.support-login.net». Ελέγξτε ολόκληρη τη διεύθυνση.

✏️ Ορθογραφικά & γραμματικά Λάθη

Επίσημοι οργανισμοί στέλνουν επιμελημένα κείμενα. Λάθη στο κείμενο ή αδέξια μεταφρασμένο ελληνικό κείμενο είναι ισχυρό σήμα απάτης.

⏰ Πίεση & επείγον ύφος

Φράσεις όπως «αμέσως», «εντός 24 ωρών», «ο λογαριασμός σας κλείνει» είναι τακτικές χειραγώγησης για να δράσετε χωρίς σκέψη.

🔗 Ύποπτοι σύνδεσμοι

Πριν κάνετε κλικ, τοποθετήστε το ποντίκι πάνω στον σύνδεσμο (mouse over). Αν το URL δεν ταιριάζει με τον οργανισμό, μην το ακολουθήσετε.

Πώς προστατευόμαστε

Η προστασία από phishing δεν είναι μόνο τεχνολογικό ζήτημα — είναι **συνδυασμός εργαλείων και συνηθειών**.

MFA — Πολλαπλή Επαλήθευση

Ενεργοποιήστε two-factor authentication σε όλους τους εταιρικούς λογαριασμούς. Ακόμα και αν κλαπεί ο κωδικός, ο λογαριασμός παραμένει ασφαλής.

Τακτικά Backups

Δημιουργείτε αντίγραφα ασφαλείας σε offline αποθήκευση. Σε περίπτωση επίθεσης ransomware, τα δεδομένα σας παραμένουν διαθέσιμα.

Email Security Filters

Χρησιμοποιείτε εξειδικευμένα φίλτρα που αναλύουν εισερχόμενα μηνύματα και σημαίνουν ύποπτα email προτού φτάσουν στους εργαζόμενους.

Ενημερώσεις συστημάτων

Εγκαθιστάτε πάντα τις τελευταίες ενημερώσεις λογισμικού και antivirus. Οι περισσότερες επιθέσεις εκμεταλλεύονται γνωστές αδυναμίες σε παλιό λογισμικό.

Συμπεράσματα — ο κανόνας των 4 βημάτων

1

🛑 ΣΤΑΜΑΤΩ

Δεν δρω αυθόρμητα. Παίρνω ανάσα πριν κάνω οτιδήποτε.

2

🔎 ΕΛΕΓΧΩ

Εξετάζω αποστολέα, domain, σύνδεσμο και περιεχόμενο.

3

✅ ΕΠΙΒΕΒΑΙΩΝΩ

Επικοινωνώ με τον υποτιθέμενο αποστολέα μέσω επίσημου τηλεφώνου.

4

📣 ΑΝΑΦΕΡΩ

Ενημερώνω τον υπεύθυνο IT ή ασφάλειας της εταιρείας άμεσα.

Η ασφάλεια της επιχείρησης αρχίζει από **εσάς**. Το πιο ισχυρό «firewall» είναι ένας ενημερωμένος άνθρωπος.