ΤΙ ΕΙΝΑΙ ΤΟ PHISHING

ΕΝΗΜΕΡΩΣΗ ΣΧΕΤΙΚΑ ΜΕ ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ (Phishing)

ΟΚΤ 2023

Το ηλεκτρονικό “ψάρεμα” (Phishing) είναι μια μορφή επίθεσης κοινωνικής μηχανικής (social engineering), στην οποία ο δράστης μιμείται μια αξιόπιστη οντότητα, ζητώντας από το θύμα να αποκαλύψει ευαίσθητες πληροφορίες ή στέλνοντας αρχεία με κακόβουλο λογισμικό ή συνδέσμους, με σκοπό να υποκλέψει την ταυτότητά του ή τα διαπιστευτήριά του (log-in information) για να προβεί σε κλοπή ή να εξαπατήσει το θύμα. Τα τελευταία χρόνια τέτοιες επιθέσεις είναι πολύ συχνές και έχουν ως συνέπεια την απώλεια μεγάλων χρηματικών ποσών επ’ ωφελεία εγκληματικών οργανώσεων που δρουν συστηματικά με σκοπό την εξαπάτηση των χρηστών του Διαδικτύου.

ΙΩΑΝΝΗΣ ΙΓΓΛΕΖΑΚΗΣ
ΚΑΘΗΓΗΤΗΣ ΑΠΘ

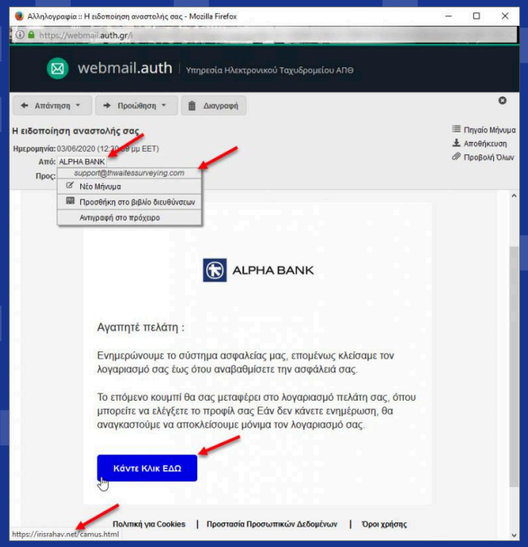
ΠΕΡΙΣΣΟΤΕΡΕΣ ΠΛΗΡΟΦΟΡΙΕΣ:

www.iglezakis.gr

I. ΕΙΣΑΓΩΓΗ
ΤΟ ΥΠΟΒΑΘΡΟ ΤΟΥ PHISHING

Η διείσδυση των ηλεκτρονικών υπολογιστών και των φορητών συσκευών, όπως είναι τα έξυπνα τηλέφωνα και τα tablets, με τις εφαρμογές (Apps) και το διαδίκτυο των πραγμάτων, έχουν δημιουργήσει ένα περιβάλλον διαρκούς δικτυακής συνδεσιμότητας. Η ηλεκτρονική επικοινωνία μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, μηνυμάτων SMS, εφαρμογών OTT (Viber, WhatsApp, Telegram κλπ.) και άμεσων μηνυμάτων μέσω υπηρεσιών κοινωνικής δικτύωσης, όπως είναι, λ.χ., το Facebook και το Instagram, έχει γίνει καθημερινή συνήθεια στην εργασία και την κοινωνική ζωή μας, ενώ και η τηλεργασία συνεπάγεται νέους κινδύνους, καθώς οι εργαζόμενοι με τη μέθοδο αυτή στοχοποιούνται από τους δράστες επιθέσεων κυβερνοεγκλημάτων.

Η αρνητική όψη της κοινωνίας της πληροφορίας είναι ότι οι δράστες αδικημάτων απάτης εκμεταλλεύονται τις αυξημένες δυνατότητες δικτύωσης και επικοινωνίας για να επιχειρήσουν επιθέσεις τύπου ηλεκτρονικού ψαρέματος. Θύματα τέτοιων επιθέσεων μπορεί να πέσουν χρήστες του διαδικτύου και των νέων τεχνολογιών από όλα τα κοινωνικά στρώματα και τις γεωγραφικές περιοχές, αστικές ή μη, ανεξαρτήτως ηλικίας και μορφώσεως.

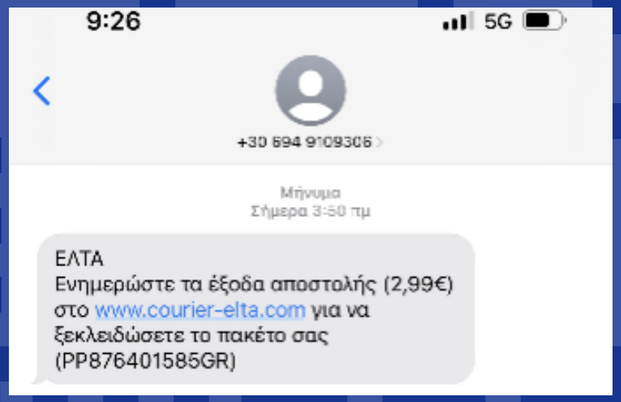


ΤΙ ΕΙΝΑΙ ΤΟ PHISHING?

Το ηλεκτρονικό “ψάρεμα” (ή Phishing) είναι μια μορφή επίθεσης κοινωνικής μηχανικής (social engineering), με χρήση της ηλεκτρονικής τεχνολογίας, στην οποία ο δράστης μιμείται μια αξιόπιστη οντότητα, μια γνωστή και αξιόπιστη εταιρεία ή μια δημόσια αρχή (την Αστυνομία ή το gov.gr), ζητώντας από το θύμα να αποκαλύψει ευαίσθητες πληροφορίες ή στέλνοντας αρχεία με κακόβουλο λογισμικό ή συνδέσμους, προκειμένου είτε να μολύνει τον υπολογιστή του είτε να ζητήσει τη συμπλήρωση των στοιχείων λογαριασμού και άλλα προσωπικά δεδομένα σε μια φόρμα ενσωματωμένη στο μήνυμα ή σε ένα επισυναπτόμενο αρχείο. Τέτοια στοιχεία περιλαμβάνουν, λ.χ., όνομα χρήστη και κωδικό πρόσβασης σε τραπεζικούς λογαριασμούς, ΑΦΜ ή ΑΜΚΑ, κωδικούς PIN, αριθμούς πιστωτικών καρτών και κωδικό ασφαλείας κλπ.

Εναλλακτικά, μπορεί ένα τέτοιο μήνυμα να κατευθύνει τον χρήστη προς μια πλαστή ιστοσελίδα. Στην περίπτωση αυτή, έχουμε το φαινόμενο Pharming, όπου ο χρήστης ανακατευθύνεται σε μία ψεύτικη ιστοσελίδα την οποία ο εισβολέας έχει προηγουμένως σχεδιάσει να μοιάζει με την ιστοσελίδα μιας Τράπεζας ή του PayPal ή άλλης γνωστής εταιρίας. Στη συνέχεια, ο δράστης προτρέπει το θύμα να χρησιμοποιήσει τα διαπιστευτήριά σύνδεσής του στον λογαριασμό e-banking ή σε άλλο λογαριασμό. Πιστεύοντας ότι βρίσκεται στην πραγματική σελίδα της Τράπεζας στην οποία έχει λογαριασμό ή άλλης γνωστής ιστοσελίδας, ο χρήστης εισάγει τα στοιχεία σύνδεσής του και την ίδια στιγμή παραδίδει τις πληροφορίες εισόδου στον λογαριασμό του στους δράστες (βλ. το παρακάτω παράδειγμα). Αξίζει να σημειωθεί ότι για να γίνει πειστική η επίθεση, οι δράστες χρησιμοποιούν τακτικές εκφοβισμού/παραπλάνησης στα μηνύματα που αποστέλλουν, όπως ότι «ο λογαριασμός θα τεθεί σε αναστολή» ή ότι «απαιτούνται πρόσθετες ενέργειες από τον χρήστη» και για το λόγο αυτό του ζητείται να

πατήσει επάνω σε έναν κακόβουλο σύνδεσμο μέσα στο μήνυμα ηλεκτρονικού ταχυδρομείου ή το μήνυμα SMS. Στη συνέχεια, ο δράστης χρησιμοποιεί τα στοιχεία αυτά για να κάνει μεταφορές χρηματικών ποσών από τον λογαριασμό του θύματος ή για να προβεί σε άλλες κακόβουλες πράξεις.



Η ιστορία των επιθέσεων ηλεκτρονικού ψαρέματος ξεκινά από τότε που δημιουργήθηκε το διαδίκτυο και πλέον οι εν λόγω επιθέσεις εμφανίζονται με πιο εξελιγμένες μορφές, όπως, λ.χ., με την αποστολή μηνυμάτων SMS σε κινητά τηλέφωνα μέσω τετραψήφιων ή πενταψήφιων αριθμών που αποστέλλονται μαζικά και παραπλανούν τους συνδρομητές, στους οποίους δημιουργείται η εντύπωση ότι προέρχονται από έναν αξιόπιστο φορέα (π.χ., αποστολή δέματος από τα ΕΛΤΑ), το αναφερόμενο ως SMShing.

Οι ζημίες από τις επιθέσεις αυτές έχουν πολλαπλασιαστεί το τελευταίο διάστημα. Διεθνώς, υπολογίζεται το κόστος τους για τις εταιρίες το έτος 2023 σε 4,45 εκατομμύρια δολάρια, σύμφωνα με έκθεση της IBM (Data Breach Report 2023). Για αυτό το λόγο, οι εταιρίες και οι οργανισμοί πρέπει να λαμβάνουν μέτρα για την αντιμετώπιση του φαινομένου του phishing. Ομοίως και οι χρήστες/συνδρομητές πρέπει να είναι ενημερωμένοι για τους κινδύνους και τις μορφές εμφάνισης του ηλεκτρονικού ψαρέματος, διότι αποτελούν στόχους των δραστών επιθέσεων αυτού του τύπου.

Η προστασία από τέτοιες επιθέσεις περιλαμβάνει, κατά κύριο λόγο, το φιλτράρισμα των μηνυμάτων ηλεκτρονικής αλληλογραφίας και την αναγνώρισή τους ως ανεπιθύμητων. Ορισμένα, όμως, μηνύματα ξεφεύγουν από τα φίλτρα, ενώ τέτοια δυνατότητα δεν υπάρχει όσον αφορά τα μηνύματα SMS, τα οποία δεν φιλτράρονται, με συνέπεια να είναι δυσχερής η αναγνώριση κακόβουλων μηνυμάτων SMS από τους χρήστες.

II. ΤΥΠΟΙ ΕΠΙΘΕΣΕΩΝ PHISING

Μαζική επίθεση:
Περιλαμβάνει μηνύματα ηλεκτρονικού ταχυδρομείου ή SMS που στοχοποιούν μια ομάδα ή ένα μεγάλο τμήμα του πληθυσμού με ένα γενικό μήνυμα, π.χ., «Η χρεωστική σας κάρτα έχει τεθεί προσωρινά σε αναστολή!». Ο δράστης αποστέλλει μαζικά (χιλιάδες ή εκατομμύρια) τέτοια μηνύματα, τα οποία είναι πανομοιότυπα, με σκοπό να πετύχει τη διάδοση σε μεγάλο αριθμό προσώπων, ώστε να έχει αυξημένες πιθανότητες να επιτύχει η επίθεση.

Στοχευμένη επίθεση (spear phishing):
Στην επίθεση αυτή αποστέλλεται ένα ατομικό μήνυμα που είναι προσαρμοσμένο σε ένα πρόσωπο (στον ενικό), ώστε να φαίνεται πιο αληθοφανές και πειστικό. Ο επιτιθέμενος χρησιμοποιεί πληροφορίες που συλλέγει από προφίλ σε κοινωνικά δίκτυα, σε δημόσια αρχεία ή άλλες πηγές, για να στείλει ένα προσωποποιημένο μήνυμα. Στην πιο απλή μορφή του τύπου αυτού ηλεκτρονικού ψαρέματος, αποστέλλεται ένα τυποποιημένο μήνυμα με το Ονομ/μο του παραλήπτη.

Επιπλέον, οι επιθέσεις phishing μπορεί να προέρχονται από διάφορα κανάλια, όπως είναι, π.χ., μολυσμένες ιστοσελίδες, κοινωνικά δίκτυα, ψεύτικες διαφημίσεις και μηνύματα SMS που παραπέμπουν σε πλαστές ιστοσελίδες («pharming»), στις οποίες ζητείται από τον χρήστη να καταχωρίσει τους κωδικούς του πρόσβασης. Ορισμένα μηνύματα phishing περιλαμβάνουν κωδικούς QR-code που αποστέλλονται σε ένα μήνυμα ηλεκτρονικού ταχυδρομείου που αναφέρει ότι δεν έγινε δεκτή η πληρωμή για μια υπηρεσία (λ.χ, ταχυδρομική) και προτρέπουν τον χρήση να σκανάρει τον κωδικό και να μεταφερθεί σε μια πλαστή ιστοσελίδα, όπως αναφέρθηκε παραπάνω.

Man-in-the-middle attack:
Σε αυτόν τον τύπο επίθεσης, ο εισβολέας παρεμποδίζει την επικοινωνία μεταξύ δύο μερών για να κρυφακούσει, να τροποποιήσει ή να εισαγάγει κακόβουλο κώδικα στην επικοινωνία. Για παράδειγμα, ο εισβολέας μπορεί να υποκλέψει την επικοινωνία μεταξύ του θύματος και ενός αξιόπιστου οργανισμού, όπως μιας τράπεζας ή ενός προμηθευτή, και στη συνέχεια να χρησιμοποιήσει αυτές τις πληροφορίες για να μιμηθεί την εν λόγω εταιρία και να εξαπατήσει το θύμα ώστε να του κλέψει χρήματα, μέσω τραπεζικής μεταφοράς για την αγορά εμπορευμάτων που, όμως, ποτέ δεν αποστέλλονται από τον δράστη της απάτης.

Συνήθως, οι απατεώνες χρησιμοποιούν μια παραποιημένη διεύθυνση ηλεκτρονικού ταχυδρομείου που μοιάζει με πραγματική, για παράδειγμα info-bank-usa@gmail.com και ξεγελούν το θύμα και ζητούν να γίνουν πληρωμές σε έναν ψεύτικο λογαριασμό ή να επισκεφτεί έναν ψεύτικο ιστότοπο (pharming).

SIM Swapping:

Η επίθεση αντικατάστασης SIM είναι μια επίθεση phishing κατά την οποία ο δράστης έχει ως στόχο να πάρει τον έλεγχο του αριθμού τηλεφώνου του θύματος. Ο δράστης επικοινωνεί με έναν πάροχο τηλεπικοινωνιών και παρουσιάζει πλαστά έγγραφα (πλαστό αναγνωριστικό και εξουσιοδότηση) για να πείσει τον πάροχο ότι είναι εξουσιοδοτημένος από το θύμα να αντικαταστήσει την κάρτα SIM. Οι δράστες ισχυρίζονται ψευδώς ότι η κάρτα SIM χάθηκε ή καταστράφηκε.

Μόλις πάρουν τη νέα κάρτα SIM, την τοποθετούν στο δικό τους τηλέφωνο. Μόλις ενεργοποιηθεί η νέα κάρτα SIM, η παλιά απενεργοποιείται αυτόματα και οι κλήσεις, τα SMS, η πρόσβαση στο διαδίκτυο κ.λπ. γίνονται από τη συσκευή του δράστη που λειτουργεί με τον ίδιο αριθμό. Με αυτόν τον τρόπο μπορούν να λαμβάνουν SMS 2FA ή OTP που τους επιτρέπει να συνδέονται σε τραπεζικούς λογαριασμούς, ηλεκτρονικά πορτοφόλια ή αριθμούς πιστωτικών καρτών και αριθμούς pin που ενδέχεται να είναι αποθηκευμένοι στο ιστορικό περιήγησης του κινητού τηλεφώνου. Έτσι, μπαίνουν χωρίς εξουσιοδότηση στον λογαριασμό e-banking του θύματος και μεταφέρουν χρήματα σε δικό τους λογαριασμό ή σε λογαριασμό τρίτου.

Vishing:

Μια άλλη πρακτική ηλεκτρονικού ψαρέματος είναι το vishing, η πρακτική όπου αποστέλλεται ένα μήνυμα ηλ. ταχυδρομείου που αναφέρει ως υποτιθέμενο αποστολέα

έναν γνωστό φορέα (π.χ., την υπηρεσία πληρωμών PayPal) που προτρέπει τους παραλήπτες να καλέσουν ένα τηλέφωνο και, αν αυτοί το κάνουν, τους ζητείται να αποκαλύψουν τηλεφωνικά τα προσωπικά τους στοιχεία και στοιχεία τραπεζικών λογαριασμών.

Customer support scam:

Η επίθεση τύπου τεχνικής υποστήριξης πελατών συνίσταται στην τηλεφωνική κλήση όπου ο δράστης προσποιείται ότι είναι εκπρόσωπος εταιρίας πληροφορικής, όπως είναι, λ.χ., η Microsoft και ισχυρίζεται ότι υπάρχει ένα πρόβλημα στον υπολογιστή του θύματος και είτε ζητάει χρήματα για να αποκαταστήσει στο πρόβλημα ή το προτρέπει να εγκαταστήσει ένα πρόγραμμα απομακρυσμένης διαχείρισης υπολογιστή, όπως είναι το TeamViewer και, εφόσον πεισθεί ο χρήστης και το εγκαταστήσει, υποκλέπτει κωδικούς πρόσβασης e-banking και προβαίνει σε τραπεζική μεταφορά χρημάτων από το λογαριασμό του θύματος σε δικό του ή σε λογαριασμό τρίτων.

IIII.ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΕΠΙΘΕΣΕΙΣ PHISHING

Οι επιθέσεις ηλεκτρονικού ψαρέματος μπορούν να στοιχίσουν ακριβά στις επιχειρήσεις σε χρήματα, όπως και σε φήμη, εφόσον αποκαλυφθεί ότι έπεσαν θύματα των hackers. Τέτοιες επιθέσεις μπορούν να στοιχειοθετήσουν και παραβίαση προσωπικών δεδομένων, εάν στόχος των δραστών είναι η απόκτηση πρόσβασης στις βάσεις δεδομένων των εταιριών, στις οποίες περιλαμβάνονται δεδομένα προσωπικού χαρακτήρα. Στην περίπτωση αυτή θα πρέπει να σταλεί ειδοποίηση στην Αρχή Προστασίας Δεδομένων εντός 72 ωρών και να καταγραφεί το συμβάν, αλλά και να ληφθούν επανορθωτικά μέτρα.

Το πρόβλημα δημιουργείται, όταν τα κακόβουλα μηνύματα δεν αναγνωρίζονται ως ανεπιθύμητα από το πρόγραμμα ηλεκτρονικού ταχυδρομείου της επιχείρησης ή όταν αποστέλλονται μέσω άλλων καναλιών (π.χ., μέσω SMS) και μπορεί να παραπλανηθεί ένας υπάλληλος ή στέλεχός της.

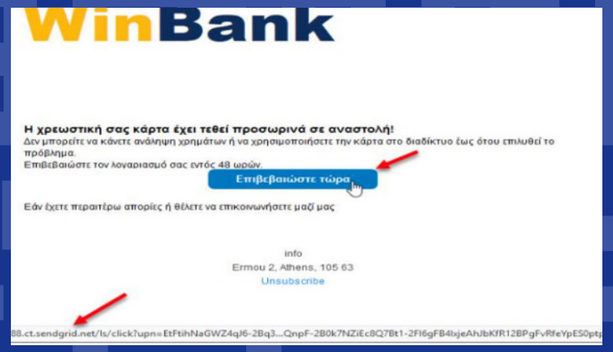
Οι επιχειρήσεις και οργανισμοί συχνά αμελούν να παρέχουν εξειδικευμένη εκπαίδευση στα στελέχη και τους υπαλλήλους τους, με συνέπεια να υφίσταται κίνδυνος παραπλάνησής τους από μηνύματα ηλεκτρονικού ψαρέματος. Για το σκοπό αυτό:

- Οι υπάλληλοι θα πρέπει να εκπαιδεύονται, ώστε να αναγνωρίζουν τα κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου και αυτό σημαίνει ότι θα πρέπει να παρέχεται εκπαίδευση για τις σύγχρονες απειλές.
- Επιπλέον, οι υπάλληλοι θα πρέπει να ενθαρρύνονται να αναφέρουν τις επιθέσεις ηλεκτρονικού ψαρέματος στον υπεύθυνο ασφαλείας, καθώς και κακόβουλο λογισμικό που κυκλοφορεί και άλλα συμβάντα ασφαλείας που έτυχαν της προσοχής τους.
- Ο υπεύθυνος ασφάλειας θα πρέπει να ενημερώνεται για τις νέες απειλές που εμφανίζονται, καθώς οι δράστες τέτοιων εγκλημάτων ανακαλύπτουν συνεχώς νέες τεχνικές εξαπάτησης.

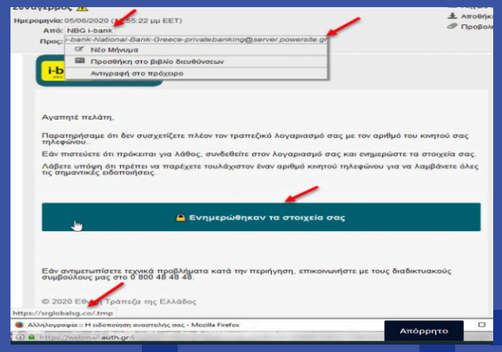
- Εάν λάβει χώρα κάποιο συμβάν ή μια απόπειρα εξαπάτησης μέσω ηλεκτρονικού ψαρέματος, πρέπει να ενημερώνεται η Δίωξη Ηλεκτρονικού Εγκλήματος και να κατατίθεται, ενδεχομένως, έγκληση κατά των αγνώστων δραστών.
- Θα πρέπει να διενεργείται τακτικά έλεγχος των συστημάτων ασφάλειας της επιχείρησης, ώστε να διαπιστώνονται τυχόν κενά ασφαλείας που εκμεταλλεύονται οι δράστες επιθέσεων.
- Οι εφαρμογές της εταιρίας θα πρέπει να κάνουν χρήση της ασφάλειας τύπου 2FA (Ο έλεγχος ταυτότητας δύο παραγόντων) για τους χρήστες και ασφάλεια endpoint
- Εάν λάβει χώρα κυβερνοεπίθεση, θα πρέπει να απομονωθεί το μολυσμένο σύστημα και να αποσυνδεθεί από το δίκτυο, όπως και οι μολυσμένες συσκευές.
- Τα αντίγραφα ασφαλείας θα πρέπει να διατηρούνται off-line και να σκανάρονται με λογισμικό anti-virus.
- Για την αποφυγή επιθέσεων spear-phishing πρέπει να προστατεύονται οι ηλεκτρονικές διευθύνσεις των υπαλλήλων και στελεχών, δηλ. α) να μη δημοσιεύονται σε καταλόγους διευθύνσεων της εταιρίας στο διαδίκτυο και β) να μην ακολουθούν τη λογική της απόδοσης του Ονομ/μου σε διεύθυνση email (π.χ., Ioannis.Papadopoulos@etairia.gr ή I.Papadopoulos@etairia.gr), αλλά να αποδίδεται μια τυχαία διεύθυνση.

IV. ΣΥΜΒΟΥΛΕΣ ΑΣΦΑΛΕΙΑΣ

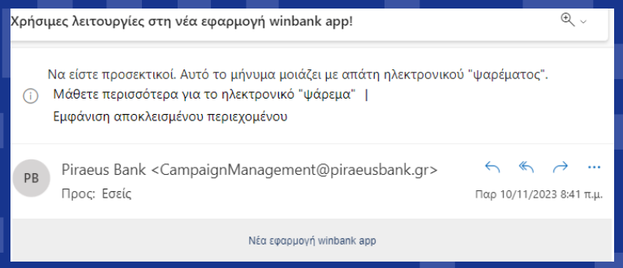
- Να επιδεικνύετε προσοχή όταν ο αποστολέας είναι άγνωστος. Να κάνετε πάντα έλεγχο των ονομάτων και διευθύνσεων ηλ. ταχυδρομείου που σας αποστέλλονται πριν απαντήσετε.
- Μην ανοίγετε συνημμένα αρχεία ή συνδέσμους (links) σε μη ζητηθέντα μηνύματα ηλ. ταχυδρομείου ή SMS.
- Προσοχή σε μηνύματα που αναφέρουν ότι κάτι είναι «επείγον».
- Μην δίνετε σημασία και μην απαντάτε σε μηνύματα που χρησιμοποιούν τακτικές εκφοβισμού, όπως την απειλή ότι ο λογαριασμός σας θα ανασταλεί, αν δεν αναλάβετε δράση.



- Όταν ένα μήνυμα ηλ. ταχυδρομείου αναφέρει ότι προέρχεται από έναν αξιόπιστο φορέα (π.χ. Τράπεζα) και σας ζητά να πληκτρολογήσετε στοιχεία λογαριασμού, για να ανανεώσετε την πρόσβασή σας ή κάτι παρόμοιο, μην απαντάτε, καθώς πότε μια Τράπεζα ή μια εταιρία δεν θα ζητούσε τέτοια στοιχεία από τους πελάτες της. Εάν το κρίνετε απαραίτητο, επαληθεύστε το μήνυμα επικοινωνώντας με τον αποστολέα ή τον οργανισμό που φαινομενικά αντιπροσωπεύει, καλώντας στα στοιχεία επικοινωνίας που δίνει στην επίσημη ιστοσελίδα του (και όχι στο μήνυμα email).

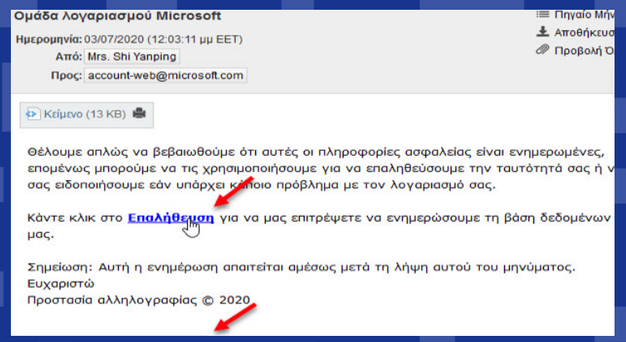


- Προσοχή σε μηνύματα που έχουν συντακτικά ή ορθογραφικά σφάλματα. Αρκετά από τα κακόβουλα μηνύματα έχουν τέτοια λάθη καθώς είτε δημιουργούνται αυτόματα από κάποιο πρόγραμμα είτε γίνεται μετάφραση μέσω προγράμματος μετάφρασης, όπως είναι, π.χ., το google translate.
- Διαβάστε προσεκτικά τις ειδοποιήσεις του προγράμματος ηλ. αλληλογραφίας που χρησιμοποιείτε, π.χ.:



- Μην δίνετε βάση σε μηνύματα που αναφέρονται σε «προσφορές» ή «επικερδείς συμφωνίες».
- Αν λαμβάνετε ανεπιθύμητα μηνύματα που δεν αναγνωρίζονται ως τέτοια από το πρόγραμμα email που χρησιμοποιείτε, αλλάξτε πάροχο ηλ.αλληλογραφίας. Γενικώς, θα πρέπει για επαγγελματικούς σκοπούς να χρησιμοποιείται ένας πάροχος με τον οποίο υπάρχει συνεργασία και όχι δωρεάν υπηρεσίες, όπως τα gmail, outlook κλπ.

• Μην απαντάτε σε μηνύματα που ζητούν οικονομικές ή άλλες συμβουλές ή είναι προσωπικά και μπορούν να οδηγήσουν σε εξαπάτηση (romance scam).
• Εάν λάβετε μήνυμα από κρατικούς φορείς (π.χ., gov.gr) ή Τράπεζες, μην ανοίγετε το μήνυμα, αλλά μεταβείτε απευθείας σε αυτούς, για να ενημερωθείτε.
• Ένδειξη ότι ένα μήνυμα είναι phishing είναι όταν απευθύνει έναν γενικό χαρακτηρισμό, π.χ., Αγαπητέ κύριε, κυρία ή αγαπητέ πελάτη. Το ίδιο ισχύει και όταν ένα μήνυμα περιέχει ψευδοατομικευμένα στοιχεία, με τυχαίους ή ψευδείς αριθμούς (π.χ., Αγαπητέ πελάτη user2020) ή το όνομά σας στα αγγλικά (π.χ. Αγαπητέ Ioannis Papadopoulos).
• Ελέγξτε αν συμφωνεί η ονομασία του αποστολέα με την πραγματική διεύθυνση email. Περάστε με το ποντίκι πάνω από τη διεύθυνση του αποστολέα, ώστε να εμφανιστεί η πραγματική διεύθυνση email.



• Μελετήστε την πολιτική για την αντιμετώπιση του ηλεκτρονικού ψαρέματος του παρόχου υπηρεσιών ηλεκτρονικής αλληλογραφίας που χρησιμοποιείτε.
• Μην παρέχετε πρόσβαση σε τρίτους, στον ηλεκτρονικό σας υπολογιστή ή τις συσκευές σας.
• Εάν λάβετε ένα μήνυμα που σας προτρέπει να εγκαταστήσετε ένα λογισμικό, να είστε ιδιαίτερα προσεκτικοί και να ρωτήσετε σχετικά στο Τμήμα πληροφορικής της εταιρίας,

• Εάν κάποιο άτομο σας τηλεφωνήσει και ισχυρισθεί ότι είναι από μια εταιρία πληροφορικής, όπως π.χ, τη Microsoft και ζητήσει πρόσβαση στον υπολογιστή σας (π.χ., μέσω TeamViewer), κλείστε το τηλέφωνο και μην επικοινωνείτε άλλο μαζί του.
• Μια ακόμη τακτική που χρησιμοποιείται είναι η αποστολή των μηνυμάτων ως εικόνες. Ο αποστολέας προσθέτει στο κύριο μέρος του μηνύματος μια εικόνα από ένα αληθοφανές μήνυμα με σκοπό να παραπλανήσει τους χρήστες και τους μηχανισμούς ελέγχου που χρησιμοποιούνται από τους διακομιστές αλληλογραφίας και από τις εφαρμογές ηλεκτρονικού ταχυδρομείου.