



Καθώς το τελευταίο διάστημα παρατηρούνται αυξημέ-νες αναφορές για αποστολή παραπλανητικών μηνυμά-των τύπου phishing σε χρήστες ηλεκτρονικού...

ταχυδρομείου, κινητών τηλέφωνων αλλά και μέσω κοινωνικής δικτύωσης, η Εθνική Αρχή Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης υπενθυμίζει χρήσιμες οδηγίες για την ενίσχυση της ασφάλειας και της ιδιωτικότητας των πολιτών.

Το Phishing συνιστά ενέργεια εξαπάτησης των χρηστών του διαδικτύου, κατά την οποία ο αποστολέας υποδύεται μία αξιόπιστη οντότητα, οργανισμό ή πρόσωπο που καλεί τον αποδέκτη του μηνύματος να ακολουθήσει τις οδηγίες που του δίνονται. Αυτές οι οδηγίες μπορεί να ζητούν από τον αποδέκτη να ακολουθήσει κάποιο ηλεκτρονικό σύνδεσμο (link) ή και να παραχωρήσει δεδομένα του, όπως ευαίσθητα ιδιωτικά στοιχεία, κωδικούς, στοιχεία ταυτότητας ή διαβατηρίου, τραπεζικό λογαριασμό, τραπεζική κάρτα και άλλα. Περαιτέρω τις τελευταίες ημέρες παρατηρείται αυξημένος αριθμός μηνυμάτων σχετικά με επιστροφές φόρου ή χορήγηση επιδομάτων.

Καλούνται οι πολίτες να είναι ιδιαίτερα προσεκτικοί, όσο αληθοφανής φαίνεται ο αποστολέας ή και τα μηνύματα που λαμβάνουν, ώστε να μην πέσουν θύματα επιτήδειων που δρουν με αυτό τον τρόπο. Ακολουθούν κάποιες πρακτικές συμβουλές για την προστασία από τις επιθέσεις αυτού του τύπου (phishing attacks).

- Δεν θα πρέπει ποτέ να δίνετε τα προσωπικά στοιχεία (π.χ. κωδικούς e-Banking, αριθμούς/PIN καρτών, κωδικούς πρόσβασης, όνομα χρήστη) σε υποτιθέμενους διαμεσολαβητές, νομικά γραφεία, λογιστές, ή άλλους επιτήδειους για δήθεν εξυπηρέτηση (π.χ. σε θέματα κρατικής επιδότησης, Power/Fuel/Τουρισμός για όλους ή άλλες περιπτώσεις όπως ενοικίαση δωματίων κλπ).
- Θα πρέπει να πραγματοποιείτε πρόσβαση μέσω της επίσημης ιστοσελίδας του φορέα, του οργανισμού ή της τράπεζας ή μέσω της εφαρμογής στο κινητό σας (app) και όχι μέσω συνδέσμων από κάποιο μήνυμα ή email που λάβατε, μηχανές αναζήτησης ή άλλες ιστοσελίδες.

- Αν λάβατε κάποιο ύποπτο email, προτού ενεργήσετε θα πρέπει να επικοινωνήσετε με τους συνεργάτες σας ή με τον υποτιθέμενο αποστολέα για να ελέγξετε την αυθεντικότητα του.
- Θα πρέπει να ελέγχετε προσεκτικά τη διεύθυνση του αποστολέα. Τα μηνύματα τύπου phishing έχουν συχνά διευθύνσεις αποστολέα που δεν έχουν σχέση με αυτόν που υποτίθεται ότι τα στέλνει.
- Θα πρέπει να εξετάζετε το είδος των πληροφοριών που σας ζητούνται. Ακόμα και αν το μήνυμα που λάβατε φαίνεται αυθεντικό, είναι απίθανο κάποιος φορέας, τράπεζα ή εταιρία να επικοινωνήσει μέσω ηλεκτρονικού ταχυδρομείου για να σας ζητήσει προσωπικά στοιχεία, στοιχεία τραπεζικής ή πιστωτικής κάρτας, ή άλλα προσωπικά ή ευαίσθητα δεδομένα.
- Θα πρέπει να είστε επιφυλακτικοί εάν το μήνυμα δημιουργεί μια αίσθηση επείγοντος. Οι επιτιθέμενοι προσπαθούν συχνά να ασκήσουν πίεση χρησιμοποιώντας αυτήν την τακτική.
- Θα πρέπει επίσης να είστε επιφυλακτικοί με μηνύματα επιστροφής φόρου ή χορήγησης επιδομάτων.
- Είναι αποτελεσματικός ένας ενδεδειγμένος έλεγχος γραμματικής και ορθογραφίας καθώς τα τυπογραφικά λάθη και η κακή γραμματική είναι συχνά χαρακτηριστικά των μηνυμάτων τύπου phishing.
- Υπάρχουν αρκετές λύσεις ασφάλειας και αντιμετώπισης κακόβουλου λογισμικού (antispamming) που περιλαμβάνουν λειτουργίες αναγνώρισης και απόρριψης κακόβουλων μηνυμάτων.