ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΕΠΙΜΕΛΗΤΗΡΙΟ ΠΡΕΒΕΖΑΣ

Πρέβεζα 14/09/2022

ΔΕΛΤΙΟ ΤΥΠΟΥ

Τι να προσέχετε για να μην πέσετε θύμα παραπλανητικών μηνυμάτων τύπου smishing (SMS phishing).

Το Επιμελητήριο Πρέβεζας ενημερώνει, ότι η Εθνική Αρχή Κυβερνοασφάλειας απευθύνει χρήσιμες οδηγίες για την ενίσχυση της ασφάλειας και της ιδιωτικότητας των πολιτών καθώς το τελευταίο διάστημα παρατηρούνται αυξημένες αναφορές για αποστολή παραπλανητικών μηνυμάτων τύπου smishing (SMS phishing).

Το Smishing (γνωστό και ως phishing μέσω SMS) συνιστά μια μορφή απόπειρας ηλεκτρονικής απάτης η οποία πραγματοποιείται μέσω σύντομων μηνυμάτων κειμένου (SMS) μέσω κινητού τηλεφώνου.

Μια επίθεση τύπου smishing εξελίσσεται ως εξής:

– Το θύμα λαμβάνει ένα μήνυμα SMS στο οποίο ο αποστολέας υποδύεται μία αξιόπιστη οντότητα, οργανισμό ή πρόσωπο.

– Το SMS είναι σύντομο, και περιέχει ένα σύνδεσμο (link).

– Κάνοντας κλικ ο ανυποψίαστος χρήστης κατεβάζει στη συσκευή του κακόβουλο λογισμικό (malware) ή ανακατευθύνεται σε παραπλανητική ιστοσελίδα (malicious website) όπου του ζητείται να παραχωρήσει δεδομένα του, όπως ευαίσθητα ιδιωτικά στοιχεία, κωδικούς, στοιχεία ταυτότητας ή διαβατηρίου, τραπεζικό λογαριασμό, τραπεζική κάρτα και άλλα.

Περιστατικά τύπου smishing αντιμετωπίζονται σε παγκόσμια κλίμακα. Ειδικά για την Ελληνική επικράτεια έχουν αναφερθεί κακόβουλα μηνύματα που φαίνεται να αφορούν δήθεν κάποια έκδοση εγγράφου από την Ενιαία Ψηφιακή Πύλη (Gov.gr), ή να έχουν περιεχόμενο φορολογικού ενδιαφέροντος (όπως επιστροφή φόρου), η να προέρχονται από τραπεζοπιστωτικά ιδρύματα, ή ακόμα και από εταιρείες εντοπισμού/παράδοσης δεμάτων.

Η Εθνική Αρχή Κυβερνοασφάλειας στην ανακοίνωσή της καλεί τους πολίτες να διαχειρίζονται με προσοχή και υπομονή τα SMS και γενικότερα τα μηνύματα που λαμβάνουν ακόμα και αν με μια πρώτη ματιά φαίνονται αληθή. Ειδικότερα συστήνονται τα ακόλουθα μέτρα πρόληψης και προστασίας:

– Δεν θα πρέπει να πατήσετε κανένα σύνδεσμο (link) που περιλαμβάνεται μέσα στο μήνυμα.

– Δε θα πρέπει να απαντάτε και να αντιδράτε βιαστικά σε τέτοια μηνύματα ακόμα και αν παρουσιάζονται ως επείγοντα. Αφιερώστε λίγο χρόνο αναζήτησης στο διαδίκτυο για να διερευνήσετε την γνησιότητα του μηνύματος. Αν είναι δυνατό επικοινωνήστε με τον φερόμενο ως αποστολέα για να επιβεβαιώσετε τη γνησιότητα του.

– Μην δίνετε προσωπικά στοιχεία όπως κωδικούς πρόσβασης, αριθμούς/PIN καρτών, όνομα χρήστη κλπ.

– Σε κάθε περίπτωση η πρόσβαση στον εκάστοτε φορέα δεν πρέπει να πραγματοποιείται μέσω συνδέσμων από κάποιο SMS μήνυμα ή email που λάβατε. Θα πρέπει να γίνεται μέσω της επίσημης ιστοσελίδας του φορέα, του οργανισμού ή της τράπεζας (ή μέσω της επίσημης εφαρμογής στο κινητό).

– Διατηρείτε τη συσκευή σας και τις εφαρμογές σας ενημερωμένες.