



Τι λένε αξιωματούχοι της ΕΛ.ΑΣ. για τους επιτήδειους που στήνουν επιχειρήσεις εξαπάτησης ανυποψίαστων πολιτών ▯ Phising, vishing, spamming, scamming. Λέξεις...

που έχουν κάνει την εμφάνισή τους τα τελευταία χρόνια και όλες έχουν κοινό παρονομαστή την επιχείρηση εξαπάτησης ανυποψίαστων πολιτών με στόχο την αφαίρεση προσωπικών στοιχείων και εν τέλει χρηματικών ποσών. Όπως σημειώνουν στα «ΝΕΑ» αξιωματούχοι της ΕΛ.ΑΣ., εκτός από τις συνήθεις μορφές τηλεφωνικής εξαπάτησης με το πρόσχημα ότι συγγενικό πρόσωπο είχε τροχαίο, χρειάζεται χρήματα για έκτακτο χειρουργείο ή για την εξυπηρέτηση χρέους, την εμφάνισή της και στη χώρα μας έχει κάνει μια νέα, διεθνής μορφή απάτης, η επονομαζόμενη Wangiri – μέθοδος του ενός μόνο κουδουνίσματος.

Σε αυτή την περίπτωση, όπως σημειώνουν έμπειρα στελέχη των Αρχών, οι απατεώνες επιδιώκουν οι πολίτες να καλέσουν αυτοί αριθμούς υψηλής χρέωσης. Συνήθως, δε, οι αριθμοί αυτοί ξεκινούν από κωδικούς χωρών του εξωτερικού, όπως 0035, 0040, 0044 και 0049. Οι επιτήδεις που στήνουν τη συγκεκριμένη παγίδα δημιουργούν ένα σύστημα μέσω του οποίου πραγματοποιούνται δεκάδες κλήσεις τυχαίων αριθμών.

Οι κλήσεις υψηλής χρέωσης

Όπως γράφουν τα «ΝΕΑ», κάθε κλήση ακούγεται μόνο μία φορά και στη συνέχεια εμφανίζεται ως αναπάντητη στο τηλέφωνο του παραλήπτη. Η κλήση συνήθως γίνεται σε εργάσιμες ώρες ή τη νύχτα για να μειωθεί η πιθανότητα ο ανυποψίαστος πολίτης να απαντήσει. Οι χρήστες βλέποντας τον αριθμό και θεωρώντας ότι είναι νόμιμη κλήση καλούν ξανά τον αριθμό με αποτέλεσμα να γίνεται υψηλή χρέωση στον λογαριασμό του, με τους δράστες να επωφελούνται οικονομικά. Όσο περισσότερο διαρκέσει η τηλεφωνική επικοινωνία τόσο

μεγαλύτερη θα είναι και η χρέωση.

Σε κάποιες περιπτώσεις, η φωνή στην άλλη άκρη της γραμμής ενημερώνει τον ανυποψίαστο πολίτη πως κέρδισε κάποιο έπαθλο, ωστόσο συχνότερα δεν ακούγεται το παραμικρό για αρκετά δευτερόλεπτα. Σε άλλες περιπτώσεις οι απατεώνες προσποιούνται τους τεχνικούς εταιρείας λογισμικού που, δήθεν θέλοντας να προστατέψουν τον υπολογιστή, το τάμπλετ ή το κινητό τηλέφωνο του υποψήφιου θύματος, ζητούν να τους επιτραπεί να εγκαταστήσουν ειδικό λογισμικό και έτσι αποκτούν πρόσβαση σε ευαίσθητα δεδομένα, όπως αριθμούς τραπεζικών λογαριασμών, ΑΦΜ κ.ο.κ. Επίσης, έχουν δυνατότητα να αποκτήσουν πρόσβαση σε προσωπικές φωτογραφίες ή βίντεο, εκβιάζοντας στη συνέχεια τους κατόχους τους προκειμένου να μη δημοσιεύσουν τα αρχεία.

Επενδύσεις μαϊμού

Παράλληλα υπάρχουν και περιπτώσεις αγνώστων που τηλεφωνούν προσπαθώντας να πείσουν τον αποδέκτη της κλήσης να επενδύσει χρήματα. Ενδεικτική της μεθόδου αυτής είναι η καταγγελία που πρόσφατα είδε το φως της δημοσιότητας, σύμφωνα με την οποία πολίτης λάμβανε κλήσεις από δήθεν εταιρείες που προσέφεραν υπηρεσίες επένδυσης σε κρυπτονομίσματα και ενώ τους ζητήθηκε να σταματήσουν την επικοινωνία εκείνοι επέμεναν, χρησιμοποιώντας διαφορετικούς αριθμούς, επωνυμίες και λογότυπα εταιρειών. Οι αριθμοί έδειχναν πως οι κλήσεις προέρχονταν κυρίως από τη Βρετανία, με τον «σύμβουλο επενδύσεων» να μιλάει ελληνικά (κάποιες φορές σπαστά), λέγοντας ότι εκπροσωπεί επενδυτική εταιρεία, ενώ πεισματικά απέκρυπτε πώς βρέθηκαν στην κατοχή του τα στοιχεία του υποψήφιου θύματος.

Σε ιστοσελίδα όπου γίνονται αναφορές για «ενοχλητικούς τηλεφωνικούς αριθμούς» που κρύβουν παγίδες εξαπάτησης, μάλιστα, άλλος πολίτης ανέφερε χαρακτηριστικά για τον ίδιο αριθμό ότι αυτοί που καλούν απειλούν πως εάν δεν τους καταθέσεις χρήματα θα συνεχίσουν την τηλεφωνική παρενόχληση.

Αυτή η πρακτική, γνωστή ως vishing –προέρχεται από τον συνδυασμό των λέξεων voice (φωνή) και phising («ψάρεμα») – αποτελεί μια μορφή εξαπάτησης που έχει επίσης ως «δούρειο ίππο» το τηλέφωνο, με τους εγκληματίες να αναζητούν τρόπο να υποκλέψουν προσωπικά και οικονομικά δεδομένα από τους πολίτες, χρησιμοποιώντας κατά κανόνα τηλεφωνικούς αριθμούς από το εξωτερικό (κυρίως ευρωπαϊκές χώρες). Όταν ο παραλήπτης της κλήσης απαντήσει, ακούει στην άλλη άκρη της γραμμής κάποιον που με διάφορα προσχήματα προσπαθεί να τον πείσει να του δώσει πληροφορίες με στόχο να αποκτήσει πρόσβαση στον τραπεζικό λογαριασμό του.

Μαζικά mails

Όπως αναφέρουν τα στελέχη της Δίωξης Ηλεκτρονικού Εγκλήματος, το «phishing» πραγματοποιείται συνήθως με την αποστολή μαζικών spam e-mails τα οποία δήθεν προέρχονται από κάποια υπαρκτή και νόμιμη εταιρεία, όπως τράπεζα, ηλεκτρονικό κατάστημα, υπηρεσία ηλεκτρονικών πληρωμών κ.ο.κ. Για να γίνουν πιστευτοί, δε, διαμορφώνουν τα μηνύματα κατά τέτοιο τρόπο ώστε να μοιάζουν με αυτά που στέλνουν οι τράπεζες, χρησιμοποιούν λογότυπα των τραπεζών και κάνουν χρήση ορολογίας που δίνει την αίσθηση του κατεπείγοντος.

Στελέχη της ΕΛ.ΑΣ., άλλωστε, τονίζουν ότι οι επιτήδριοι βασίζονται στο γεγονός πως οι πολίτες-στόχοι είναι απασχολημένοι και βιαστικοί και άρα μπορεί να

«πέσουν» πιο εύκολα στη διαδικτυακή παγίδα που τους έχουν στήσει. Σκοπός τους είναι να παραπλανήσουν τον παραλήπτη και να «ψαρέψουν» προσωπικά και οικονομικά δεδομένα. Για την επίτευξη του στόχου τους ζητούν από τον παραλήπτη να επισκεφθεί άμεσα ιστοσελίδα στην οποία οφείλει να καταχωρίσει τα προσωπικά του στοιχεία. Με τον τρόπο αυτόν αποκτούν άμεσα πρόσβαση στον τραπεζικό λογαριασμό του ανθρώπου που εξαπάτησαν.

Σε κάθε περίπτωση εξαπάτησης, στελέχη της ΕΛ.ΑΣ., μέσω των «ΝΕΩΝ», συστήνουν στους πολίτες να είναι ιδιαίτερα προσεκτικοί και εφόσον έχουν δεχθεί τηλεφωνικές παρενοχλήσεις από αριθμούς του εξωτερικού να ενημερώνουν την εταιρεία κινητής τηλεφωνίας αλλά και τις Αρχές. Οι πολίτες θα πρέπει να αποφεύγουν να δίνουν τα στοιχεία τους, ειδικά εάν πρόκειται για ευαίσθητα δεδομένα, όπως αριθμοί τραπεζικών λογαριασμών.

Τα ΝΕΑ