



Δεκάδες χρήστες του διαδικτύου και κυρίως χρήστες συγκεκριμένης ιστοσελίδας κοινωνικής Δικτύωσης, έ-χουν πέσει θύματα χάκερ το τελευταίο διάστημα, ...

οι οποίοι τους έχουν «μπλοκάρει» το προφίλ, στέλνοντας μηνύματα σ' όλες τους επαφές, ζητώντας χρήματα δήθεν για βοήθεια, με το πρόσχημα πως τους έκλεψαν το πορτοφόλι. Τις τελευταίες δυο εβδομάδες, η Δίωξη Ηλεκτρονικού Εγκλήματος δέχτηκε δεκάδες καταγγελίες πολιτών που έπесαν θύματα των χάκερς και ενημερώθηκαν από τους φίλους στην ιστοσελίδα κοινωνικής δικτύωσης πως τους ζητά χρήματα.

Ήδη η Δίωξη Ηλεκτρονικού εγκλήματος πραγματοποιεί έρευνες για τον εντοπισμό των απατεώνων, ενώ παράλληλα εξέδωσε ανακοίνωση με συμβουλές προς τους πολίτες και ενημέρωση για την νέα διαδικτυακή απάτη.

Συγκεκριμένα και σύμφωνα με την ανακοίνωση: «...άγνωστοι δράστες επιχειρούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε λογαριασμούς ιστοσελίδας κοινωνικής δικτύωσης και να εξαπατήσουν τα θύματά τους με την ακόλουθη μεθοδολογία – τρόπο δράσης:

Αρχικά αποστέλλουν μηνύματα στην εφαρμογή ανταλλαγής μηνυμάτων του μέσου κοινωνικής δικτύωσης, τα οποία :

Εμπεριέχουν συνδέσμους (links) που οδηγούν σε ιστοσελίδες στις οποίες πρέπει να συμπληρωθούν τα στοιχεία εισόδου του λογαριασμού κοινωνικής δικτύωσης (Phishing pages) ή αφορούν υποτιθέμενους διαγωνισμούς, με κακόβουλο περιεχόμενο που τους επιτρέπει να αποκτήσουν πρόσβαση τόσο στους λογαριασμούς που δεν είναι ασφαλισμένοι με έλεγχο ταυτότητας δύο παραγόντων, όσο και σε άλλες εφαρμογές της συσκευής που σχετίζονται με οικονομικές συναλλαγές.

Στη συνέχεια, εφόσον ο κάτοχος του λογαριασμού συμπληρώσει τα στοιχεία εισόδου, οι δράστες υποκλέπτουν τα στοιχεία ταυτοποίησης (username & password) και εισέρχονται στον λογαριασμό του.

Με τον τρόπο αυτό αποκτούν πρόσβαση στις επαφές του, στις οποίες αποστέλλουν μηνύματα μέσω της εφαρμογής ανταλλαγής μηνυμάτων του μέσου κοινωνικής δικτύωσης, ζητώντας χρηματική βοήθεια με το πρόσχημα της απώλειας πορτοφολιού, εγγράφων ή λόγω άμεσης ανάγκης που έχουν περιέλθει, υποσχόμενοι ότι θα τα επιστρέψουν το συντομότερο δυνατό.

Οι δράστες ζητούν από τα θύματά τους να τους αποσταλούν τα χρήματα είτε μέσω της υπηρεσίας άμεσης αποστολής χρημάτων και ανάληψης από ATM τραπεζικού ιδρύματος, όπου απαιτείται μόνο η αποστολή ενός κωδικού μέσω απλοποιημένης διαδικασίας, είτε με την γνωστοποίηση των στοιχείων πιστωτικής – χρεωστικής κάρτας ή των στοιχείων εισόδου ηλεκτρονικών πορτοφολιών.

Τι πρέπει να προσέξουν οι πολίτες

Στο πλαίσιο αυτό, η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος ενημερώνει τους πολίτες:

να μην ανοίγουν συνδέσμους ή ύποπτα επισυναπτόμενα αρχεία τα οποία αποστέλλονται μέσω εφαρμογών ανταλλαγής μηνυμάτων μέσω κοινωνικής δικτύωσης χωρίς την προηγούμενη εξακρίβωση του αποστολέα του μηνύματος, οι λογαριασμοί κοινωνικής δικτύωσης καθώς και οι λογαριασμοί ηλεκτρονικού ταχυδρομείου που συνδέονται με αυτούς, να ασφαρίζονται με έλεγχο ταυτότητας δυο (2) παραγόντων, έτσι ώστε και σε περίπτωση που εισάγουν τα στοιχεία εισόδου των λογαριασμών τους σε παραπλανητικές ιστοσελίδες (Phishing pages) να μην καταστεί δυνατή η είσοδος στους λογαριασμούς τους από τους δράστες, να αποσυνδέονται από τους λογαριασμούς κάθε φορά μετά τη περιήγηση και αν αυτό είναι δυνατό να μην απομνημονεύονται από τα λειτουργικά συστήματα τα διαπιστευτήρια εισόδου σε αυτούς, σε περίπτωση παραβίασης λογαριασμού και ανάκτησης αυτού, να ειδοποιούνται άμεσα οι επαφές του θύματος για το περιστατικό για την μη αποστολή των χρημάτων με οποιοδήποτε τρόπο, σε περίπτωση που λάβετε μήνυμα μέσω εφαρμογής ανταλλαγής μηνυμάτων μέσω κοινωνικής δικτύωσης από επαφή σας και σας ζητηθεί να αποστείλετε οικονομική βοήθεια, επικοινωνήστε πρώτα μαζί του με άλλο μέσο π.χ. τηλεφωνική κλήση για την επιβεβαίωση του περιστατικού, σε περίπτωση αποστολής χρημάτων, επικοινωνήστε άμεσα με το τραπεζικό ίδρυμα προκειμένου ακυρωθεί η εντολή της αποστολής των χρημάτων, σε περίπτωση αποστολής των στοιχείων πιστωτικής – χρεωστικής κάρτας επικοινωνήστε άμεσα με το τραπεζικό ίδρυμα προκειμένου να ακυρωθεί η κάρτα και να αμφισβητηθεί κάθε συναλλαγή με αυτήν, σε περίπτωση γνωστοποίησης στοιχείων εισόδου σε λογαριασμό ηλεκτρονικού πορτοφολιού, αλλάξτε άμεσα κωδικό πρόσβασης και βεβαιωθείτε αν έγινε συναλλαγή με αυτόν. Σε θετική περίπτωση ζητήστε από το τμήμα υποστήριξης της εκάστοτε εταιρείας την ακύρωση των συναλλαγών και απευθυνθείτε στις αρμόδιες αστυνομικές αρχές όταν αντιληφθείτε ότι πέσατε θύμα απάτης.»