31 Ιουλίου 2021

Οδηγίες τις ΕΛ.ΑΣ για να μην σας χακάρουν τα social media

/ Επιστήμες, Τέχνες & Πολιτισμός

Την προσοχή των χρηστών του Διαδικτύου εφιστά η Δίωξη Ηλεκτρονικού Εγκλήματος για την παραβίαση λογαριασμών σε μέσα κοινωνικής δικτύωσης

Καταγγελίες για περιπτώσεις αλίευσης των στοιχείων εισόδου σε λογαριασμούς, σε μέσα κοινωνικής δικτύωσης (user name – password), με πρόσχημα την ολοκλήρωση της επίσημης πιστοποίησής τους (verify account – bluetick), δέχεται το τελευταίο διάστημα η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος (ΔΔΗΕ), σύμφωνα με όσα αναφέρει σε σχετική ανακοίνωσή της.

Οι δράστες, όπως αναφέρει η ΔΔΗΕ, αποστέλλουν άμεσο μήνυμα, κυρίως σε λογαριασμούς με μεγάλη ανταπόκριση στο κοινό, στο οποίο αναφέρουν ότι προκειμένου να ολοκληρωθεί η διαδικασία πιστοποίησης του λογαριασμού (verify account) πρέπει να ακολουθήσουν τον σύνδεσμο που τους υποδεικνύεται.

Οι επίμαχοι σύνδεσμοι οδηγούν σε ιστοσελίδες στις οποίες πρέπει να συμπληρωθούν τα στοιχεία εισόδου του χρήστη στο λογαριασμό (phishing pages),

το οποίο επιτρέπει στους δράστες να αποκτήσουν πρόσβαση στους λογαριασμούς που δεν είναι ασφαλισμένοι με έλεγχο ταυτότητας δύο παραγόντων.

Στη συνέχεια, οι δράστες αποστέλλουν εκβιαστικά μηνύματα στους χρήστες προκειμένου να ζητήσουν χρηματικό αντίτιμο για την επιστροφή του λογαριασμού στον κάτοχό του. Επισημαίνεται ότι τα άμεσα μηνύματα στα μέσα κοινωνικής δικτύωσης χρήζουν μεγάλης προσοχής, καθώς είναι εξαιρετικά αληθοφανή.

Η ΔΔΗΕ συμβουλεύει τους παραλήπτες των απατηλών αυτών μηνυμάτων εκβιαστικού περιεχομένου τα εξής:

– Να μην επιλέγουν τους προτεινόμενους συνδέσμους.
– Να μην απαντούν στα μηνύματα.
– Να μην καταχωρούν και να μην στέλνουν προσωπικά δεδομένα και στοιχεία λογαριασμών στα μέσα κοινωνικής δικτύωσης, καθώς σε καμία περίπτωση δεν είναι αληθινά.
Παράλληλα, η ΔΔΗΕ συστήνει:

– Οι εταιρείες που παρέχουν εφαρμογές και υπηρεσίες κοινωνικής δικτύωσης, δεν απαιτούν την επαλήθευση στοιχείων εισόδου σε λογαριασμούς με την αποστολή μηνυμάτων.
– Οι λογαριασμοί κοινωνικής δικτύωσης καθώς και οι λογαριασμοί ηλεκτρονικού ταχυδρομείου που συνδέονται με αυτούς, πρέπει απαραίτητα να ασφαλίζονται με έλεγχο ταυτότητας δύο παραγόντων, έτσι ώστε σε περίπτωση που οι χρήστες εισάγουν τα στοιχεία εισόδου των λογαριασμών τους σε παραπλανητικές ιστοσελίδες (phishing pages) να είναι αδύνατη η είσοδος σε αυτούς από τους δράστες.
– Χρησιμοποιήστε ένα νέο e-mail αποκλειστικά για να συνδέσετε τους λογαριασμούς σας στα μέσα κοινωνικής δικτύωσης.
– Ασφαλίστε τους λογαριασμούς σας με ισχυρούς κωδικούς πρόσβασης, διαφορετικούς για κάθε λογαριασμό, τους οποίους θα αλλάζετε ανά τακτά χρονικά διαστήματα.
– Μην ανοίγετε συνδέσμους ή ύποπτα επισυναπτόμενα αρχεία τα οποία αποστέλλονται μέσω εφαρμογών ανταλλαγής μηνυμάτων και μέσων κοινωνικής δικτύωσης χωρίς την προηγούμενη εξακρίβωση της αξιοπιστίας τους.
– Απευθυνθείτε στις αρμόδιες αστυνομικές Αρχές όταν αντιληφθείτε ότι πέσατε θύμα απάτης ή αλίευσης των προσωπικών σας δεδομένων.

Πηγή: gazzetta.gr