Αυξημένα τα κρούσματα αποστολών spam και phishing email

Αύξηση στις αποστολές spam και phishing email, που ως στόχο έχουν την εξαπάτηση των χρηστών, καταγράφουν οι ερευνητές. Οι κακόβουλοι χρήστες του Διαδικτύου φαίνεται ότι αξιοποιούν όλο και περισσότερο φόρμες εγγραφής, συνδρομής και ανατροφοδότησης σε ιστότοπους, για να εισάγουν spam περιεχόμενο ή phishing links σε επιβεβαιωτικά μηνύματα από αξιόπιστες εταιρείες, που χαίρουν μεγάλης εκτίμησης σε παγκόσμια κλίμακα.

Οι κακόβουλοι χρήστες αναζητούν συνεχώς νέες μεθόδους για την παράδοση spam και phishing μηνυμάτων σε παραλήπτες, παρακάμπτοντας τα υπάρχοντα φίλτρα περιεχομένου. “Στην ιδανική περίπτωση, προσπαθούν να κάνουν τις επιστολές να φαίνεται ότι προέρχονται από νόμιμη πηγή με καλή φήμη, ώστε οι χρήστες να μην μπορούν να αγνοήσουν το ανεπιθύμητο email. Αυτό δημιουργεί επίσης μια πρόκληση για τις εταιρείες, καθώς αυτό το ανεπιθύμητο spam ή ακόμη και κακόβουλο περιεχόμενο, φαινομενικά αποστέλλεται εξ ονόματος τους και θα μπορούσε να θέσει σε κίνδυνο την εμπιστοσύνη των πελατών τους ή ακόμη και να οδηγήσει σε διαρροές προσωπικών δεδομένων”, αναφέρει σχετικά η Kaspersky.

Όπως εξηγούν οι ερευνητές της εταιρείας, η μέθοδος είναι αρκετά απλή και αποτελεσματική. Σήμερα, σχεδόν κάθε εταιρεία ενδιαφέρεται να λαμβάνει σχόλια από τους πελάτες της για τη βελτίωση της ποιότητας των υπηρεσιών, τη διατήρηση των πελατών και της φήμης της. Για να γίνει αυτό, οι εταιρείες ζητούν από τους πελάτες να δημιουργήσουν έναν προσωπικό λογαριασμό, να εγγραφούν σε newsletters ή να επικοινωνήσουν μέσα από φόρμες ανατροφοδότησης στην ιστοσελίδα, για παράδειγμα, με σκοπό να υποβάλουν ερωτήσεις ή να αφήσουν προτάσεις. Αυτοί είναι ακριβώς οι μηχανισμοί που οι επιτιθέμενοι εκμεταλλεύονται.

Τρόπος δράσης

Και οι τρεις μηχανισμοί απαιτούν το όνομα και το email των πελατών, ώστε να μπορούν να λάβουν ένα επιβεβαιωτικό email ή σχόλια. Σύμφωνα με τους ερευνητές της Kaspersky, οι απατεώνες προσθέτουν περιεχόμενο spam και phishing σε αυτό το μήνυμα. Απλώς προσθέτουν το email του θύματος στη φόρμα εγγραφής ή συνδρομής και πληκτρολογούν το μήνυμα τους αντί για το όνομα. Στη συνέχεια, ο ιστότοπος θα στείλει μια τροποποιημένη επιστολή επιβεβαίωσης στη διεύθυνση αυτή, η οποία θα περιέχει μια διαφήμιση ή phishing link στην αρχή του κειμένου αντί του ονόματος του παραλήπτη.

“Οι περισσότερες από αυτές τις τροποποιημένες επιστολές συνδέονται με online έρευνες που αποσκοπούν στην απόκτηση προσωπικών δεδομένων από τους επισκέπτες. Οι ειδοποιήσεις από μια αξιόπιστη πηγή συνήθως περνούν εύκολα μέσω φίλτρων περιεχομένου, καθώς είναι επίσημα μηνύματα από μια αξιόπιστη εταιρεία. Αυτός είναι ο λόγος για τον οποίο αυτή η νέα μέθοδος ανεπιθύμητων, αλλά φαινομενικά αθώων, spam emails είναι τόσο αποτελεσματική και ανησυχητική”, επισημαίνει η εταιρεία.

Πηγή: **sepe.gr**