

Πρέβεζα 06/12/2019

ΔΕΛΤΙΟ ΤΥΠΟΥ

Το Επιμελητήριο Πρέβεζας ενημερώνει τις επιχειρήσεις μέλη του ότι στην Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος το τελευταίο διάστημα καταγγέλλονται από πολίτες, νομικά πρόσωπα και επιχειρήσεις, πολλά κρούσματα για περιπτώσεις διαδικτυακών απατών.

Συγκεκριμένα, άγνωστοι δράστες επιχειρούν να εξαπατήσουν τα θύματά τους με τις ακόλουθες μεθοδολογίες – τρόπους δράσης:

Μέσω εταιρικού ηλεκτρονικού ταχυδρομείου (B.E.C.–Business Email Compromise, CEO Fraud & Man in the middle attacks):

Πρόκειται για περιπτώσεις στις οποίες οι δράστες αποκτούν μη εξουσιοδοτημένη πρόσβαση και παρεμβαίνουν σε τμήματα της ηλεκτρονικής αλληλογραφίας μεταξύ συναλλασσόμενων επαγγελματιών και εμπόρων με επιχειρήσεις (προμηθευτές ή πελάτες) στο εξωτερικό.

Μόλις εντοπίσουν μηνύματα που αφορούν επικείμενη πληρωμή σε τραπεζικό λογαριασμό του εξωτερικού, παρεμβαίνουν αποστέλλοντας απατηλά μηνύματα, από διευθύνσεις ηλεκτρονικού ταχυδρομείου που προσομοιάζουν με τις πραγματικές.

Στη συνέχεια υποδύονται υπαλλήλους της συνεργαζόμενης επιχείρησης και πείθουν τους συναλλασσόμενους να καταθέσουν χρήματα σε απατηλούς τραπεζικούς λογαριασμούς, διαφορετικούς από αυτούς που είχαν συμφωνηθεί.

Με την υπόσχεση παροχής επενδυτικών υπηρεσιών (Forex Scams, Ponzi & Pyramid Schemes):

Στην περίπτωση αυτή οι δράστες προσεγγίζουν τα θύματα, είτε μέσω τηλεφώνου είτε μέσω ηλεκτρονικού ταχυδρομείου, υποδύμενοι τους εργαζόμενους σε δήθεν μεγάλες επενδυτικές εταιρείες του εξωτερικού.

Υπόσχονται υψηλές αποδόσεις μέσω τοποθέτησής τους σε εικονικές διαδικτυακές επενδυτικές πλατφόρμες και τους αποσπούν μεγάλα χρηματικά ποσά.

Οι εικονικές αυτές πλατφόρμες παραπλανούν τους υποψήφιους επενδυτές, παρουσιάζοντάς τους αρχικά ιδιαίτερα υψηλές αποδόσεις, προκειμένου να τους ωθήσουν στην επένδυση μεγαλύτερων χρηματικών ποσών.

Ακολούθως, όταν τα θύματα αιτούνται την ανάληψη ποσού του αρχικού κεφαλαίου ή μέρους των κερδών τους, οι δράστες διακόπτουν κάθε επικοινωνία μαζί τους.

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

Όσον αφορά τις απάτες σε επιχειρήσεις μέσω εταιρικού ηλεκτρονικού ταχυδρομείου:

- Να αναβαθμίζετε και να ενημερώνετε το λογισμικό τεχνικής ασφαλείας.
- Να διασφαλίζετε ότι οι υπάλληλοί σας είναι ενημερωμένοι και προσεγγίζουν τα αιτήματα για τη διενέργεια πληρωμών με προσοχή.
- Εφαρμόστε διαδικασία για την επαλήθευση της νομιμότητας αιτημάτων διενέργειας πληρωμών που λαμβάνονται μέσω e-mail.
- Μην ανοίγετε ύποπτους ηλεκτρονικούς συνδέσμους (links) ή ύποπτα επισυναπτόμενα αρχεία που λαμβάνετε μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου.
- Αποφεύγετε την κοινοποίηση πληροφοριών σχετικά με την ιεραρχία, την ασφάλεια και τις ακολουθούμενες διαδικασίες της επιχείρησής σας.
- Περισσότερες πληροφορίες-συμβουλές μπορείτε να βρείτε στον ιστότοπο: <https://cyberalert.gr/apates-endiamesou-eraggelmaton/>

Όσον αφορά τις απάτες με την υπόσχεση παροχής επενδυτικών υπηρεσιών:

- Μην επενδύετε τα χρήματά σας σε υπηρεσίες χωρίς να είστε απολύτως βέβαιοι για την αξιοπιστία τους.
- Να είστε επιφυλακτικοί όταν σας προσεγγίζουν τηλεφωνικά ή μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου από επενδυτικές εταιρείες του εξωτερικού.
- Αναζητήστε πληροφορίες για την αξιοπιστία των επενδυτικών εταιρειών που σας προσεγγίζουν.
- Αιτηθείτε τους όρους και προϋποθέσεις, πριν πραγματοποιήσετε κάποια συναλλαγή.
- Αν η προσφορά φαίνεται υπερβολικά καλή για να είναι αληθινή, διατηρείστε επιφυλάξεις γιατί μάλλον δεν είναι πραγματική.
- Απευθυνθείτε στις αρμόδιες αστυνομικές αρχές όταν αντιληφθείτε ότι πέσατε θύμα απάτης.

Κατόπιν των ανωτέρω, υπενθυμίζεται στους πολίτες να είναι ιδιαίτερα προσεκτικοί, προκειμένου να μην εξαπατηθούν σε αντίστοιχες περιπτώσεις, ενώ μπορούν να επικοινωνούν, ανώνυμα ή επώνυμα, με τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος προκειμένου να παρέχουν πληροφορίες ή να καταγγέλλουν παράνομες ή επίμεμπτες πράξεις ή δραστηριότητες του τελούνται μέσω διαδικτύου, στα ακόλουθα στοιχεία επικοινωνίας:

- Τηλεφωνικά: 111 88
- Στέλνοντας μήνυμα ηλεκτρονικού ταχυδρομείου e-mail στο: ccu@cybercrimeunit.gov.gr
- Μέσω των εφαρμογών (applications) για έξυπνα τηλέφωνα (smart phones) με λειτουργικό σύστημα ios-android: CYBERKID και FEELSAFE
- Μέσω της διαδικτυακής πύλης (Portal) της Ελληνικής Αστυνομίας <https://portal.astynomia.gr>
- Μέσω twitter: @CyberAlertGR
- Επίσης σχετική ενημέρωση υπάρχει στο δικτυακό τόπο <https://cyberalert.gr/feelsafe>