Ενημέρωση/Προειδοποίηση
της Αρχής Καταπολέμησης της Νομιμοποίησης Εσόδων από Εγκληματικές Δραστηριότητες (Αρχή για το Ξέπλυμα Βρώμικου Χρήματος)

Η Αρχή Καταπολέμησης της Νομιμοποίησης Εσόδων από Εγκληματικές Δραστηριότητες (''Αρχή'') ενημερώνει και εφιστά την προσοχή των πολιτών για διάφορες πρακτικές εξαπάτησής τους, που λαμβάνουν χώρα το τελευταίο έτος στη χώρα μας και έχουν ως αποτέλεσμα την οικονομική ζημία τους.

Ειδικότερα, η Α' Μονάδα της ''Αρχής'' διεξήγαγε σημαντικό αριθμό ερευνών για νομιμοποίηση εσόδων από εγκληματικές δραστηριότητες, ως απόρροια επεξεργασίας αναφορών υπόπτων συναλλαγών. Οι έρευνες οδήγησαν στον εντοπισμό του βασικού αδικήματος της απάτης και στην αποσαφήνιση των μεθόδων διάπραξής του.

Παρακάτω παρουσιάζονται οι πρακτικές που ακολουθούν οι δράστες προκειμένου να πείσουν τα θύματά τους και να αποκομίσουν από αυτά παράνομο περιουσιακό όφελος. Όπως διαπιστώθηκε, αυτές οι πρακτικές παράστασης ψευδών γεγονότων ως αληθινών στα θύματα, διαφοροποιούνται, κυρίως, ανάλογα με τη συγκυρία (π.χ. περίοδος έκδοσης επιδόματος θέρμανσης, market pass, έκδοση οφειλών/προσδιορισμός φόρου από Δημόσια Αρχή, αύξηση των τιμών των κρυπτονομισμάτων κτλ.) και την εκάστοτε χρησιμοποιούμενη τεχνολογία (π.χ. χρήση e-mail, τηλεφωνικής επικοινωνίας κλπ).

Επιπλέον, όπως αποτυπώνεται στην τελευταία ενότητα, προκειμένου να ολοκληρωθεί η απάτη και να μεταφερθούν τα χρηματικά ποσά σε λογαριασμούς που ελέγχουν οι δράστες απαιτούνται αποκλειστικές ενέργειες του θύματος.

Τέλος, γίνεται ιδιαίτερη μνεία ότι ανάμεσα στις παρακάτω περιπτώσεις ιδιαίτερα δημοφιλείς για το έτος 2023 είναι αυτές του ''Λογιστή'' και του ''Εκπροσώπου Δημοσίου Φορέα''.

Περίπτωση 1η ''Λογιστής''

Ο δράστης προσποιείται ότι καλεί από το λογιστικό γραφείο, με το οποίο συνεργάζεται το θύμα, με πρόσχημα αφενός την ενημέρωση, αφετέρου την παροχή βοήθειας επί της διαδικασίας καταβολής διαφόρων ειδών επιδομάτων ή οφειλόμενων ποσών, που υποτίθεται ότι δικαιούται το θύμα. Ενδεικτικά, αναφέρονται τα επιδόματα **«Market Pass»**, **θέρμανσης**, **ηλεκτρικού ρεύματος** καθώς και οι **γεωργικές επιδοτήσεις**. Στη συνέχεια ο δράστης πείθει το θύμα να του αποδώσει χρηματικό ποσό για να προβεί στις εν λόγω διευθετήσεις και να ολοκληρωθεί η καταβολή των επιδομάτων/επιδοτήσεων.

Περίπτωση 2η ‘’Τεχνικός Microsoft’’

Ο δράστης προσποιείται τον τεχνικό της εταιρείας Microsoft, με πρόσχημα την επίλυση προβλήματος παραβίασης της ασφάλειας του ηλεκτρονικού υπολογιστή του θύματος. Με αυτόν τον τρόπο, το θύμα πείθεται να παραχωρήσει στον δράστη απομακρυσμένη πρόσβαση στον ηλεκτρονικό υπολογιστή του, με αποτέλεσμα να υποκλαπούν τα στοιχεία πρόσβασης του στην εφαρμογή ηλεκτρονικής τραπεζικής (e-banking) και να ακολουθήσει η υφαρπαγή χρηματικών ποσών.

Περίπτωση 3η ‘’Εκπρόσωπος Δημοσίου Φορέα’’

Ο δράστης προσποιείται τον εκπρόσωπο δημόσιου φορέα, επί παραδείγματι Δ.Ε.Δ.Δ.Η.Ε., Ε.Φ.Κ.Α., Υπουργείο Οικονομικών, Υπουργείο Μεταφορών, Περιφέρειες, Δήμοι, ΜΕΡ. ΥΠ. (Μεραρχία Υποστήριξης) Στρατού, με πρόφαση την ενημέρωση και παροχή βοήθειας επί της διαδικασίας καταβολής διαφόρων ειδών οφειλόμενων ποσών. Στη συνέχεια ο δράστης πείθει το θύμα να του αποδώσει χρηματικό ποσό για να προβεί στις εν λόγω διευθετήσεις.

Περίπτωση 4η ‘’Απατηλές Ηλεκτρονικές Αγγελίες’’

Ο δράστης αναρτά απατηλή αγγελία σε ιστοσελίδες αγοραπωλησιών ή στα μέσα κοινωνικής δικτύωσης, για την οποία το θύμα εκδηλώνει τηλεφωνικά ενδιαφέρον. Ενδεικτικά αναφέρονται οι ιστοσελίδες «www.car.gr» και «Marketplace» της εφαρμογής «Facebook». Εν συνεχεία, ο δράστης με διάφορες προφάσεις, όπως το αυξημένο ενδιαφέρον για το προς πώληση αγαθό ή την ορθή λογιστική τακτοποίηση της συναλλαγής, πείθει και καθοδηγεί το θύμα να προβεί στη μεταφορά μέρους ή ολόκληρου του αντίτιμου της πώλησης, χωρίς να υπάρχει προηγουμένως οποιαδήποτε εξασφάλιση.

Παραλλαγή της προαναφερόμενης μεθόδου, είναι αυτή κατά την οποία ο δράστης εκδηλώνει ο ίδιος ενδιαφέρον σε αγγελία του θύματος, οπότε κατά τη διαδικασία της πληρωμής καταφέρνει, με την παράσταση ψευδών γεγονότων ως αληθινών, να του αποσπάσει χρηματικό ποσό.

Περίπτωση 5η ''Εκπρόσωπος εταιρίας κρυπτονομισμάτων''

Ο δράστης προσποιείται τον υπάλληλο εταιρείας επενδύσεων κρυπτονομισμάτων, με πρόσχημα είτε την καταβολή της απόδοσης υποτιθέμενης προγενέστερης επένδυσης του παθόντος, είτε την τοποθέτηση κεφαλαίων σε νέα επένδυση. Λόγω της ταχύτατης ανάπτυξης του συγκεκριμένου είδους επενδύσεων, τα θύματα δελεάζονται και προβαίνουν στη μεταφορά χρημάτων, χωρίς να έχουν εξετάσει προηγουμένως την ταυτότητα του συνομιλητή τους.

Περίπτωση 6η ''Αποστολή απατηλού υπερσυνδέσμου (Hyperlink)''

Σε αυτή την περίπτωση το θύμα λαμβάνει είτε μέσω του e-mail του, είτε στην τηλεφωνική ηλεκτρονική εφαρμογή «Viber», απατηλό μήνυμα με πρόσχημα υποτιθέμενη παραβίαση ασφαλείας του τραπεζικού του λογαριασμού. Συνήθως στο κείμενο του μηνύματος υπάρχει απατηλός υπερσύνδεσμος, ο οποίος οδηγεί σε σελίδα η οποία προσομοιάζει με εκείνη της τράπεζας, με την οποία συνεργάζεται το θύμα. Ως αποτέλεσμα, το θύμα καταχωρεί τα στοιχεία πρόσβασής του, επιτρέποντας στον δράστη την πρόσβαση στον τραπεζικό του λογαριασμό.

Περίπτωση 7η ''Πελάτης''

Η περίπτωση αυτή αφορά απάτη εις βάρος είτε νομικών προσώπων, είτε φυσικών προσώπων στο πλαίσιο της επαγγελματικής τους δραστηριότητας. Ο δράστης παρουσιάζεται ως υπάρχων ή νέος πελάτης, με πρόσχημα τη διευθέτηση εκκρεμούσας συναλλαγής ή νέα συναλλαγή. Εν συνεχεία, με απατηλή καθοδήγηση καταφέρνει να αποσπάσει χρηματικό ποσό από εταιρικούς/επαγγελματικούς λογαριασμούς.

Σε ορισμένες περιπτώσεις έχει διαπιστωθεί ο δράστης να χρησιμοποιεί ελαφρά παραλλαγμένη διεύθυνση ηλεκτρονικού ταχυδρομείου υπάρχοντος πελάτη της εταιρίας προκειμένου να ξεκινήσει επικοινωνία και να παραπλανήσει την εταιρία.

Μεταφορά Χρηματικών Ποσών

Στο σύνολο των ανωτέρω περιπτώσεων απάτης, μετά την παράσταση των ψευδών γεγονότων ως αληθινών, η μεταφορά των χρηματικών ποσών, που συνιστούν το προϊόν του εγκλήματος, πραγματοποιείται από τους δράστες με έναν από τους παρακάτω τρόπους:

Α) Το θύμα με την απατηλή καθοδήγηση του δράστη πραγματοποιεί σταδιακά ο ίδιος τη μεταφορά των χρημάτων είτε μέσω ΑΤΜ, είτε με έμβασμα μέσω e-banking (περιπτώσεις: ‘’Λογιστή’’, ‘’Εκπρόσωπος Δημοσίου Φορέα’’, ‘’Εκπρόσωπος εταιρίας κρυπτονομισμάτων’’, ‘’Απατηλές ηλεκτρονικές αγγελίες’’ και ‘’Πελάτης’’).

Β) Το θύμα εκχωρεί στον δράστη απομακρυσμένη πρόσβαση στον ηλεκτρονικό του υπολογιστή, με αποτέλεσμα να υποκλαπούν τα στοιχεία πρόσβασής του στην εφαρμογή ηλεκτρονικής τραπεζικής (περίπτωση ‘’Τεχνικός Microsoft’’).

Γ) Το θύμα ακολουθεί απατηλό υπερσύνδεσμο που του έχει αποστείλει ο δράστης, με αποτέλεσμα να του εμφανίζεται εικονική ηλεκτρονική σελίδα που παρομοιάζει εκείνη της τράπεζας. Ως εκ τούτου, ο παθών καταχωρεί και εκχωρεί τα στοιχεία πρόσβασής του (περίπτωση ‘’Αποστολή απατηλού υπερσυνδέσμου’’) θεωρώντας ότι επικοινωνεί με την πραγματική τράπεζά του.

Σημειώνεται ότι η ‘’Αρχή’’ παρακολουθεί το θέμα και εάν κριθεί αναγκαίο θα επανέλθει άμεσα για την έγκαιρη ενημέρωση των πολιτών.

Γραφείο Προέδρου

Χαράλαμπος ΒΟΥΡΛΙΩΤΗΣ
Αντεισαγγελέας Αρείου Πάγου ε.τ.