Η Γενική Περιφερειακή Αστυνομική Διεύθυνση Θεσσαλίας υ-πενθυμίζει στους πολίτες τις πιο συχνές μεθόδους που χρη-σιμοποιούν οι επιτήδειοι για να τους εξαπατήσουν...

και να τους αποσπάσουν χρήματα και παραθέτει χρήσιμες συμβουλές για την αποφυγή τους.
Συχνές μορφές απατώ ν:
• Απάτες σε βάρος ιδιοκτητώ ν επιχειρήσεων, με το πρόσχημα της λανθασμένης τραπεζικής κατάθεσης
• οι δράστες τηλεφωνούν σε ιδιοκτήτες επιχειρήσεων, παρουσιαζόμενοι ως υπαρκτά – αναγνωρίσιμα πρόσωπα της περιοχής (μέλη τοπικής αυτοδιοίκησης, ιατροί, φαρμακοποιοί κ.α.) και προβαίνουν σε παραγγελίες προϊόντων, ζητώ ντας παράλληλα αριθμούς τραπεζικώ ν λογαριασμώ ν, προκειμένου να καταβάλλουν τα συμφωνηθέντα χρήματα για την αγορά αυτώ ν,
• για να γίνουν πιο πειστικοί, συνήθως αποστέλλουν μέσω ηλεκτρονικού ταχυδρομείου ή άλλων διαδικτυακώ ν εφαρμογώ ν επικοινωνίας, πλαστά αποδεικτικά μεταφοράς χρημάτων (εμβάσματα), στα οποία εμφαίνονται «μεταφορές» μεγαλύτερων χρηματικώ ν ποσώ ν από τα συμφωνηθέντα αντίτιμα των παραγγελιώ ν,
• ακολούθως, τηλεφωνούν εκ νέου στους ιδιοκτήτες των επιχειρήσεων και τους πείθουν ότι έχουν καταβάλει λανθασμένα μεγαλύτερα χρηματικά ποσά από την αξία των προϊόντων που αγόρασαν, ζητώ ντας να τους επιστραφεί η υποτιθέμενη χρηματική διαφορά (ισχυρίζονται, συνήθως, ότι κατά την πληκτρολόγηση του ποσού «πάτησαν κατά λάθος» ένα μηδενικό παραπάνω και αντί π.χ. για 100 ευρώ

κατέθεσαν 1.000 ευρώ ή αντί για 1.200 ευρώ κατέθεσαν 12.000 ευρώ).
• Απάτες με πιστωτικές κάρτες
Οι απάτες αυτής της μορφής πραγματοποιούνται με την αλίευση («phising») στο διαδίκτυο των ευαίσθητων προσωπικώ ν δεδομένων (κυρίως στοιχεία τραπεζικώ ν λογαριασμώ ν), προκειμένου να επιτύχουν την παράνομη μεταφορά χρημάτων σε λογαριασμούς μελώ ν τους ή να χρεώ σουν τις πιστωτικές κάρτες πολιτώ ν μέσω του διαδικτύου για αγορές διάφορων προϊόντων.
Αυτή η μέθοδος πραγματοποιείται κυρίως ως ακολούθως:
• είτε κάποιος κακόβουλος χρήστης του διαδικτύου δημιουργεί μια πλασματική ιστοσελίδα και με αυτόν τον τρόπο καταφέρνει να συγκεντρώ νει στοιχεία κι αριθμούς πιστωτικώ ν καρτώ ν χρηστώ ν του διαδικτύου, οι οποίοι «νομίζουν» ότι πρόκειται για κάποιο διαδικτυακό κατάστημα και κάνουν τις αγορές τους,
• είτε επιτήδειοι καταφέρνουν να αποκτούν φυσική πρόσβαση στα στοιχεία πιστωτικώ ν καρτώ ν πολιτώ ν, σημειώ νοντας αυτά και εν συνεχεία τα χρησιμοποιούν σε διαδικτυακές αγορές, καθώ ς για τις αγορές αυτές δεν είναι απαραίτητη η φυσική κατοχή της πιστωτικής κάρτας, παρά μόνο τα στοιχεία αυτής,
• είτε οι ίδιοι οι πολίτες ως χρήστες του διαδικτύου δίνουν άθελά τους τα στοιχεία σε κακόβουλους χρήστες του διαδικτύου. Ειδικότερα, ο ανυποψίαστος πολίτης λαμβάνει μήνυμα ηλεκτρονικού ταχυδρομείου από Πιστωτικό Ίδρυμα, στο οποίο τηρεί λογαριασμό, με το οποίο του ζητείται να συμπληρώ σει τα στοιχεία του (ονοματεπώ νυμο, αριθμός λογαριασμού και πιστωτικής κάρτας κλπ), για λόγους π.χ. ενημέρωσης των αρχείων της τράπεζας, ειδάλλως ο λογαριασμός του θα κλείσει. Το μήνυμα, μέσω υπερσυνδέσμου, τους οδηγεί σε μια πλασματική ιστοσελίδα της τράπεζας, με αποτέλεσμα ο πολίτης να πείθεται και να χορηγεί τα επίμαχα στοιχεία.
• Απάτες μέσω αγοραπωλησίας οχημάτων
Οι δράστες χρησιμοποιούν δύο διαφορετικές μεθοδολογίες (modus operandi), που περιγράφονται ως ακολούθως:
α) Οι δράστες εμφανίζονται ως πωλητές των οχημάτων
• καταχωρούν μέσω διαδικτύου ηλεκτρονικές αγγελίες πώ λησης εικονικώ ν οχημάτων, με σκοπό την εξαπάτηση υποψήφιων αγοραστώ ν. Σε πολλές περιπτώ σεις προσφέρουν τα προς πώ ληση οχήματα σε δελεαστικές τιμές,
• οι υποψήφιοι αγοραστές έρχονται σε επικοινωνία μαζί τους και χωρίς να έχουν δει στην πλειοψηφία των περιπτώ σεων το προς πώ ληση όχημα, πείθονται και συμφωνούν για την αγορά του,
• στη συνέχεια, καταβάλλουν σε λογαριασμό Πιστωτικού Ιδρύματος που τους υποδεικνύεται από τους δράστες το αντίτιμο που έχει συμφωνηθεί, ως προκαταβολή. Σε ορισμένες περιπτώ σεις, όταν το προς αγορά όχημα βρίσκεται σε απομακρυσμένη περιοχή, πείθονται και καταβάλλουν αντίτιμο και για τη μεταφορά του,
• οι δράστες, εφόσον τα χρήματα έχουν καταβληθεί στον υποδεικνυόμενο από αυτούς λογαριασμό, διακόπτουν κάθε επικοινωνία με τον υποψήφιο αγοραστή και εκταμιεύουν απευθείας το χρηματικό ποσό που κατατέθηκε στο Πιστωτικό Ίδρυμα.
β) Οι δράστες εμφανίζονται ως υποψήφιοι αγοραστές οχημάτων
• μέσω του διαδικτύου, αναζητούν και βρίσκουν ηλεκτρονικές αγγελίες πώ λησης οχημάτων, με σκοπό την εξαπάτηση των ιδιοκτητώ ν τους,

• αφού έρχονται σε επικοινωνία με τους κατόχους των οχημάτων, συμφωνούν για την αγορά και το αντίτιμο της συναλλαγής,
• στη συνέχεια, επιδεικνύουν στον πωλητή του οχήματος είτε ανύπαρκτο αριθμό λογαριασμού, στον οποίο φαίνεται ψευδής ηλεκτρονική μεταφορά του αντιτίμου της συναλλαγής στο λογαριασμό του, είτε πλαστές βεβαιώ σεις μεταφοράς εμβασμάτων στον προαναφερθέντα λογαριασμό,
• οι πωλητές των οχημάτων παραπλανούνται – πείθονται και χωρίς να έχουν διασταυρώ σει αν είναι πραγματική η μεταφορά χρημάτων, υποβάλλουν υπεύθυνες δηλώ σεις μεταβίβασης οχήματος, τις οποίες οι δράστες χρησιμοποιούν για τη μεταβίβαση του οχήματος στο όνομά τους,
• οι δράστες, έχοντας στην κατοχή τους το όχημα εξαφανίζονται, χωρίς να καταβάλλουν το αντίστοιχο τίμημα και συνήθως προβαίνουν στην άμεση μεταπώ ληση του οχήματος.
Σημειώ νεται ότι την ίδια μεθοδολογία εφαρμόζουν οι δράστες και κατά την αγοραπωλησία άλλων αντικειμένων, όπως κινητά τηλέφωνα, φορητοί ηλεκτρονικοί υπολογιστές κ.α.
Επιπλέον, σε άλλες περιπτώ σεις, οι δράστες:
• εισέρχονται σε οικίες ανυποψίαστων πολιτώ ν, προσποιούμενοι ότι είναι τεχνικοί, όπως υπάλληλοι Δ.Ε.Η., συντηρητές ανελκυστήρων κ.λπ. (ανάλογα με την επικαιρότητα μπορεί να επικαλεσθούν οτιδήποτε) ή πωλητές διαφόρων ειδώ ν ή γνωστοί συγγενικώ ν προσώ πων, με σκοπό την κλοπή ή ληστεία,
• προσεγγίζουν, κυρίως ηλικιωμένους, δήθεν ως απεσταλμένοι συγγενικώ ν τους προσώ πων και προφασιζόμενοι άμεση και επείγουσα οικονομική ανάγκη, επιδιώ κουν να τους αποσπάσουν χρήματα. Συνήθως τους προσεγγίζουν κατά την έξοδο ή λίγο πριν την είσοδο στην κατοικία τους, έξω από τράπεζες, εμπορικά καταστήματα, αγορές κ.λπ.
Για την αποφυγή εξαπάτησης, συμβουλεύουμε τους πολίτες:
• να ενημερώ νετε πάντα τις αστυνομικές Αρχές, ακόμη και σε περίπτωση απόπειρας απάτης σε βάρος σας,
• να αποφεύγετε τη γνωστοποίηση προσωπικώ ν οικονομικώ ν δεδομένων (αριθμούς τραπεζικώ ν λογαριασμώ ν, προσωπικούς κωδικούς (PIN), αριθμούς πιστωτικώ ν καρτώ ν, πληροφορίες καρτώ ν ΑΤΜ, κωδικούς επαλήθευσης πιστωτικώ ν καρτώ ν κτλ),
• να επαληθεύετε τις κινήσεις στους τραπεζικούς σας λογαριασμούς πριν την οποιαδήποτε συναλλαγή και να δηλώ νετε ότι δεν πρόκειται να επιστρέψετε χρήματα, χωρίς προηγούμενη διασταύρωση οικονομικώ ν στοιχείων,
• να είστε ιδιαίτερα επιφυλακτικοί όταν εντοπίζετε αγγελίες πώ λησης οχημάτων σε δελεαστικές τιμές, ως «ευκαιρία αγοράς»,
• σε περίπτωση ηλεκτρονικής μεταφοράς χρημάτων σε υποψήφιο πωλητή, να διασταυρώ νετε τα στοιχεία του, ως δικαιούχου του υποδεικνυόμενου λογαριασμού (Ονοματεπώ νυμο, Α.Φ.Μ.),
• να αποφεύγετε την προκαταβολή χρημάτων σε ιδιώ τες πωλητές, τους οποίους δε γνωρίζετε, ακόμη και εάν αυτοί αποκαλύπτουν τα προσωπικά τους στοιχεία ή τον αριθμό του τραπεζικού τους λογαριασμού,
• να αποφεύγετε, κατά προτίμηση, τις συναλλαγές με πρόσωπα τα οποία παρέχουν στοιχεία επικοινωνίας εκτός Ελλάδας,

• να είστε ιδιαίτερα επιφυλακτικοί με άγνωστα άτομα που επιχειρούν με διάφορα προσχήματα και τεχνάσματα να εισέλθουν στην οικία σας,
• να μην πείθεστε εύκολα από άτομα, τα οποία σας "πλησιάζουν" ως γνωστοί συγγενικώ ν – φιλικώ ν προσώ πων,
• να μην πείθεσθε εύκολα σε ευκαιριακές αγορές προϊόντων που σας προτείνουν άγνωστα άτομα, ιδιαίτερα δε δίχως να δείτε πρώ τα τα προϊόντα αυτά,
• να είστε ιδιαίτερα επιφυλακτικοί όταν άγνωστοι προσπαθήσουν να σας πείσουν για την καταβολή χρηματικού ποσού, με το πρόσχημα επείγουσας ανάγκης συγγενικού – φιλικού προσώ που (π.χ. νοσηλεία σε νοσοκομείο).Το ίδιο μπορεί να προσπαθήσουν και τηλεφωνικά. Για τους ίδιους λόγους να μην ενδίδετε σε προτροπές για συνάντηση (ραντεβού κ.λπ.),
• σε περιπτώ σεις που άγνωστοι επικαλούνται έκτακτη ανάγκη γνωστού -συγγενικού σας προσώ που, να επιδιώ κετε πάντα οι ίδιοι να επικοινωνείτε τηλεφωνικά με το γνωστό-συγγενικό σας πρόσωπο, προς επιβεβαίωση των όσων επικαλούνται. Η επικοινωνία να γίνεται με δικό σας τηλέφωνο και κατόπιν δικής σας πρωτοβουλίας και να μην δέχεστε να μιλάτε με άτομο, το οποίο κάλεσαν οι άγνωστοι,
• σε κάθε περίπτωση, να δηλώ νετε ότι δεν πρόκειται να παραδώ σετε χρήματα, εάν δεν εμφανιστούν οι γνωστοί-συγγενείς σας,
• να μην δέχεστε σε καμία περίπτωση άγνωστα άτομα να σας οδηγήσουν σε Πιστωτικό Κατάστημα ή ΑΤΜ για ανάληψη χρηματικού ποσού,
• να μην πείθεστε από άγνωστους, οι οποίοι εμφανίζονται ως υπάλληλοι δημόσιας Υπηρεσίας ή άλλου φορέα για την επιδιόρθωση κάποιου τεχνικού προβλήματος, εάν δεν τους έχετε εσείς προηγουμένως καλέσει,
• να μην πείθεστε όταν άγνωστοι σας ζητούν να καταβάλλετε χρήματα για οφειλές γνωστώ ν ή συγγενικώ ν προσώ πων σε δημόσιες υπηρεσίες ή σε καταστήματα-εταιρείες για αγορά αγαθώ ν-προσφορά υπηρεσιώ ν,
• επισημαίνεται ότι από νοσοκομεία ή από δημόσιες υπηρεσίες δεν χρησιμοποιείται η πρακτική υπάλληλοί τους να μεταβαίνουν σε οικίες ή σε δημόσιους χώ ρους και να ζητούν από πολίτες την καταβολή χρημάτων για υπηρεσίες που παρέχουν,
• να έχετε πάντα διαθέσιμους τους τηλεφωνικούς αριθμούς, με τους οποίους πρέπει να επικοινωνήσετε σε περίπτωση ανάγκης (Αστυνομία, Πυροσβεστική, Νοσοκομεία, στενοί συγγενείς κ.α.),
• προσπαθήστε να συγκρατήσετε τα χαρακτηριστικά των δραστώ ν, τα οχήματα με τα οποία κινούνται (αριθμό κυκλοφορίας, μάρκα οχήματος, χρώ μα κ.λπ.), τους τηλεφωνικούς αριθμούς από τους οποίους σας καλούν ή την ηλεκτρονική διεύθυνση της αγγελίας (URL) για να βοηθήσετε το έργο των διωκτικώ ν αρχώ ν.

Περισσότερες συμβουλές για την αποφυγή εξαπάτησης πολιτώ ν υπάρχουν αναρτημένες στην ιστοσελίδα της Ελληνικής Αστυνομίας (www.hellenicpolice.gr), στην ενότητα «Οδηγός του πολίτη/Χρήσιμες συμβουλές».
Επιπλέον, πληροφορίες και συμβουλές για περιστατικά ηλεκτρονικώ ν απατώ ν υπάρχουν στην ιστοσελίδα της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος www.cyberalert.gr.