ΕΘΝΙΚΗ ΑΡΧΗ ΔΙΑΦΑΝΕΙΑΣ

Οδηγός ενημέρωσης και προστασίας από τεχνικές εξαπάτησης στην εποχή του κορωνοϊού - COVID 19

Η πανδημία της νόσου του **κορωνοϊού - COVID 19** επηρεάζει άμεσα την καθημερινότητά μας, την οικονομία, τη δημόσια υγεία, τις μεταφορές και τα δίκτυα επικοινωνίας. Δυστυχώς, όπως και στην περίπτωση άλλων φυσικών καταστροφών (πλημμύρες, τυφώνες, δασικές πυρκαγιές, σεισμοί κ.α.) ο κορωνοϊός έχει και μία ακόμα πολύ επικίνδυνη συνέπεια. Δημιουργεί πρόσφορο έδαφος και «ευκαιρίες» για απάτες και παράνομες ενέργειες, τις οποίες εκμεταλλεύονται οι επιτήδειοι.

Σε διεθνές επίπεδο έχουν ήδη καταγραφεί πολυάριθμα σχήματα και πρακτικές απάτης που εκμεταλλεύονται το φόβο και την ανασφάλεια των ανθρώπων για τον κορωνοϊό. Στη χώρα μας καταγράφονται ήδη κρούσματα και απόπειρες εξαπάτησης πολιτών, σε διάφορες περιοχές της χώρας.

Το παρόν φυλλάδιο αποσκοπεί στην ευαισθητοποίηση και την ενημέρωση των πολιτών σχετικά με τις συνηθέστερες πρακτικές εξαπάτησης και στην παροχή εύληπτων οδηγιών για την προστασία τους από τους επιτήδειους.

A. Η πρώτη κατηγορία περιστατικών απάτης αφορά σε επιτήδειους που προσεγγίζουν κυρίως άτομα τρίτης ηλικίας και με διάφορα τεχνάσματα και προσχήματα όπως, ιδίως, ότι εκπροσωπούν δημόσιους φορείς (για παράδειγμα το Υπουργείο Υγείας, τον Ε.Ο.Δ.Υ., Υγειονομικές Υπηρεσίες ΟΤΑ κ.α.), οι οποίοι ισχυρίζονται ότι γυρνούν πόρτα-πόρτα για να ενημερώσουν τους πολίτες, να διανείμουν σχετικά ενημερωτικά φυλλάδια, ή να απολυμάνουν δωρεάν την οικία τους ή να συγκεντρώσουν δωρεές για την ενίσχυση του συστήματος υγείας, τους αποσπούν χρηματικά ποσά ή αφαιρούν τιμαλφή και λοιπά αντικείμενα αξίας.

B. Η δεύτερη μεγάλη κατηγορία πρακτικών και τεχνασμάτων εξαπάτησης εκμεταλλεύεται την ανωνυμία και την απόσταση που εξασφαλίζουν οι νέες τεχνολογίες, όπως το διαδίκτυο, οι εφαρμογές για ηλεκτρονικές κινητές συσκευές, τα ηλεκτρονικά καταστήματα και οι ηλεκτρονικές τραπεζικές συναλλαγές. Τα περιστατικά απάτης διεθνώς υποδηλώνουν ότι οι απατεώνες θεωρούν πιο εύκολη τη χειραγώγηση και την εξαπάτηση ενός ανθρώπου μέσω διαδικτύου, προκειμένου να αποκτήσουν πρόσβαση στους προσωπικούς κωδικούς του (πρακτική που είναι γνωστή ως social engineering με τη χρήση Phishing emails και παρόμοιων μεθόδων) από την ανάπτυξη ειδικών προγραμμάτων και λογισμικού για την πραγματοποίηση κυβερνοεπιθέσεων.

<u>Ι. Βασική τυπολογία πρακτικών εξαπάτησης με πρόσχημα την κρίση του COVID-19:</u>

- **Θεραπεία (Treatment scams):** Οι απατεώνες προσφέρουν ψεύτικες θεραπείες, εμβόλια και ιατρικές συμβουλές σχετικά με μη δοκιμασμένες θεραπείες για τον COVID-19.
- **Προμήθεια (Supply scams):** Οι απατεώνες δημιουργούν ψεύτικα ηλεκτρονικά καταστήματα, ιστότοπους, λογαριασμούς μέσων κοινωνικής δικτύωσης και διευθύνσεις ηλεκτρονικού ταχυδρομείου, μέσω των οποίων ισχυρίζονται ότι πωλούν ιατρικά προϊόντα που στην παρούσα φάση βρίσκονται σε μεγάλη ζήτηση, όπως χειρουργικές μάσκες. Όταν οι καταναλωτές επιχειρούν να αγοράσουν προμήθειες μέσω αυτών των

καναλιών, οι απατεώνες εισπράττουν τα χρήματα και δεν παρέχουν ποτέ τις υποσχεθείσες προμήθειες ή παραδίδουν ελαττωματικά ή μη ανταποκρινόμενα στις διαφημιζόμενες ιδιότητες προϊόντα. Σε αυτές τις περιπτώσεις εκτός από την οικονομική ζημία ενδέχεται τα προϊόντα αυτά να είναι και επιβλαβή για την υγεία των καταναλωτών.

- **Πάροχοι υπηρεσιών υγείας (Health provider scams):** Οι απατεώνες επικοινωνούν με τηλεφωνικά και ηλεκτρονικά μηνύματα, προσποιούμενοι ότι είναι εκπρόσωποι δημόσιων φορέων (Υπουργείο Υγείας, Ε.Ο.Δ.Υ. κ.α.) ή / και επαγγελματίες της υγείας (γιατροί, νοσηλευτές, επόπτες υγείας κ.α.) που νοσηλεύουν έναν φίλο ή συγγενή για το COVID-19 και απαιτούν πληρωμή για την περίθαλψή του.
- **Έρανοι / Φιλανθρωπίες (Charity scams):** Οι απατεώνες ζητούν δωρεές για άτομα, ομάδες και περιοχές που έχουν πληγεί από τον COVID-19 ή για να χρηματοδοτήσουν την ιατρική έρευνα για το εμβόλιο, την αγορά ιατρικού εξοπλισμού κ.α.
- **Ηλεκτρονικό «ψάρεμα» (e-Phishing scams):** Οι απατεώνες εμφανίζονται ως δήθεν εκπρόσωποι εθνικών και παγκόσμιων υγειονομικών Αρχών, συμπεριλαμβανομένου του Παγκόσμιου Οργανισμού Υγείας (WHO) και των Κέντρων Ελέγχου και Πρόληψης Νοσημάτων (CDC), αποστέλλοντας ηλεκτρονικά μηνύματα ηλεκτρονικού «ψαρέματος» (phishing e-mails) που αποσκοπούν στο να παρασύρουν τους παραλήπτες στο «κατέβασμα» κακόβουλου λογισμικού, προκειμένου να υποκλέψουν προσωπικά στοιχεία ταυτοποίησης και τραπεζικές πληροφορίες.
- **Εφαρμογές Κινητών / Tablets (App scams):** Οι απατεώνες επίσης δημιουργούν και χειραγωγούν εφαρμογές για κινητά που έχουν σχεδιαστεί για την παρακολούθηση της εξάπλωσης του COVID-19 για να παρασύρουν τους χρήστες να κατεβάσουν κακόβουλο λογισμικό που θα θέτει σε κίνδυνο τις συσκευές και τις προσωπικές πληροφορίες τους.

II. Πρακτικές οδηγίες προστασίας από πρακτικές εξαπάτησης με πρόσχημα των COVID-19

1. Απάτη με άμεση προσωπική επαφή:

- Να είστε ιδιαίτερα επιφυλακτικοί με άτομα που επιχειρούν να εισέλθουν στην οικία σας δηλώνοντας ότι εκπροσωπούν δημόσιους φορείς που ασχολούνται με την αντιμετώπιση του κορωνοϊού.
- Μην πείθεστε εύκολα από άτομα, τα οποία σας «πλησιάζουν» ως γνωστοί συγγενικών - φιλικών προσώπων που δήθεν νοσούν από κορωνοϊό και ζητούν τη βοήθειά σας.
- Να είστε ιδιαίτερα επιφυλακτικοί όταν άγνωστοι προσπαθήσουν να σας πείσουν για την καταβολή χρηματικού ποσού, με το πρόσχημα επείγουσας εισαγωγής συγγενικού - φιλικού προσώπου για νοσηλεία λόγω κορωνοϊού. Το ίδιο μπορεί να προσπαθήσουν και τηλεφωνικά. Για τους ίδιους λόγους να μην ενδίδετε σε προτροπές για συνάντηση (ραντεβού κ.λπ.).
- Εφόσον άγνωστο άτομο εισέλθει στην οικία σας με οποιαδήποτε πρόφαση (π.χ. διεξαγωγή έρευνας για τον κορωνοϊό, πώληση σχετικού προϊόντος κ.α.), να μην

επιτρέπετε να μεταβαίνει σε άλλους χώρους του σπιτιού σας, πέραν αυτών που χρειάζεται και ποτέ να μην χάνετε την οπτική επαφή μαζί του.

- Στην περίπτωση αυτή, να προσέχετε τα προσωπικά σας αντικείμενα (τσάντες, πορτοφόλια, κινητά, φορητούς υπολογιστές, tablets κ.α.), προκειμένου να αποφευχθεί το ενδεχόμενο αφαίρεσής τους με τη μέθοδο της απασχόλησης.
- Στις περιπτώσεις που άγνωστοι επικαλούνται έκτακτη ανάγκη γνωστού - συγγενικού σας προσώπου, να επιδιώκετε πάντα οι ίδιοι να επικοινωνείτε τηλεφωνικά με το γνωστό - συγγενικό σας πρόσωπο ή κάποιον οικείο του / της, 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 δηλώνετε ότι δεν πρόκειται να παραδώσετε χρήματα, εάν δεν έρθετε σε επαφή με τους γνωστούς - συγγενείς σας και δεν επαληθεύσετε τι πραγματικά συμβαίνει.
- Να μην δέχεστε σε καμία περίπτωση άγνωστα άτομα να σας οδηγήσουν σε Πιστωτικό Κατάστημα (Τράπεζα) ή ΑΤΜ για ανάληψη χρηματικού ποσού.
- Να μην πείθεστε εύκολα σε ευκαιριακές αγορές προϊόντων που υπόσχονται να σας προστατεύσουν ή να σας θεραπεύσουν από τον κορωνοϊό που σας προτείνουν άγνωστα άτομα.
- Να έχετε πάντα διαθέσιμους τους τηλεφωνικούς αριθμούς, με τους οποίους πρέπει να επικοινωνήσετε σε περίπτωση ανάγκης και για να επαληθεύσετε τους ισχυρισμούς άγνωστων σε εσάς ατόμων (Ε.Ο.Δ.Υ., Αστυνομία, Πυροσβεστική, στενοί συγγενείς κ.α.).
- Προσπαθήστε να συγκρατήσετε τα χαρακτηριστικά των δραστών, καθώς και τα οχήματα με τα οποία κινούνται (αριθμό κυκλοφορίας, μάρκα οχήματος, χρώμα κ.λπ.), για να βοηθήσετε το έργο των διωκτικών Αρχών.
- Να ενημερώνετε πάντα τις αστυνομικές Αρχές, ακόμη και σε περίπτωση απόπειρας απάτης σε βάρος σας.

2. Απάτη μέσω νέων τεχνολογιών:

- Επαληθεύστε τα στοιχεία, την έδρα και τη φήμη της εταιρείας / προσώπου που προσφέρει τα αγαθά ή τις υπηρεσίες πριν από την πραγματοποίηση οποιωνδήποτε αγορών.
- Να είστε ιδιαίτερα επιφυλακτικοί με πολύ δελεαστικές προσφορές που υπόσχονται να σας αποστείλουν αγαθά, για τα οποία μάλισταδεν υπάρχει μεγάλη διαθεσιμότητα στην αγορά (χειρουργικές μάσκες, αντισηπτικά κ.α.), σε πολύ καλές τιμές ή διαφημίζουν φαρμακευτικά προϊόντα που θωρακίζουν ή / και θεραπεύουν τον οργανισμό από τον κορωνοϊό.
- Να είστε σε εγρήγορση για τον εντοπισμό ψεύτικων ιστότοπων δεδομένου ότι οι εγκληματίες συχνά χρησιμοποιούν μια διεύθυνση ιστού που μοιάζει σχεδόν με την νόμιμη διεύθυνση, π.χ. 'Abc.org' αντί για 'abc.com'.

- Επαληθεύστε προσωπικά ότι ο ιστότοπος ή η διεύθυνση ηλεκτρονικού ταχυδρομείου προέρχεται πραγματικά από τον Οργανισμό που φαίνεται με την πρώτη ματιά. Για παράδειγμα, ο Παγκόσμιος Οργανισμός Υγείας λέει ότι μπορείτε να επαληθεύσετε τον αποστολέα ελέγχοντας τη διεύθυνση ηλεκτρονικού ταχυδρομείου - ένα επίσημο μήνυμα ηλεκτρονικού ταχυδρομείου του Π.Ο.Υ. θα αποσταλεί μόνο από μια διεύθυνση που τελειώνει στο @who.int
- Ελέγξτε τις on-line αξιολογήσεις (reviews) των καταναλωτών για την πωλήτρια εταιρεία πριν πραγματοποιήσετε μια αγορά - για παράδειγμα, έχουν υπάρξει παράπονα άλλων πελατών που δεν λαμβάνουν τα υποσχεθέντα αγαθά / υπηρεσίες;
- Να είστε ιδιαίτερα επιφυλακτικοί, εάν σας ζητείται να κάνετε μια πληρωμή σε τραπεζικό λογαριασμό που βρίσκεται σε διαφορετική χώρα από εκεί που βρίσκεται η πωλήτρια εταιρεία και σε κάθε περίπτωση να παρακολουθείτε σε καθημερινή βάση την κίνηση των τραπεζικών λογαριασμών σας.
- Ειδοποιήστε αμέσως την Τράπεζά σας για να σταματήσετε την πληρωμή, εάν πιστεύετε ότι έχετε πέσει θύμα διαδικτυακής απάτης.
- Χρησιμοποιήστε προπληρωμένες πιστωτικές κάρτες ή τη μέθοδο της αντικαταβολής όταν κάνετε μια αγορά μέσω διαδικτύου για μεγαλύτερη προστασία και μην στέλνετε προκαταβολικά χρήματα σε άτομα που δεν γνωρίζετε.
- Να μην κάνετε κλικ σε ηλεκτρονικούς συνδέσμους (links) και μην ανοίγετε συνημμένα αρχεία που δεν περιμένατε να λάβετε, ή προέρχονται από άγνωστο αποστολέα.
- Μην μοιράζεστε διαδικτυακά ειδήσεις που δεν προέρχονται από επίσημες πηγές και δεν μπορείτε να τις επαληθεύσετε.
- Μην κάνετε δωρεές μέσω ηλεκτρονικών πλατφόρμων / συνδέσμων σε φιλανθρωπικές οργανώσεις χωρίς να ελέγχετε εάν όντως πρόκειται για νόμιμες οργανώσεις / φορείς.
- Μην αποκαλύπτετε προσωπικά, τραπεζικά ή οικονομικά στοιχεία (ΑΔΤ, κωδικούς e-banking, κωδικούς τραπεζικών καρτών, passwords και login κωδικούς ηλεκτρονικού ταχυδρομείου κ.α.) σε απάντηση ηλεκτρονικών μηνυμάτων, καθώς και σε εφαρμογές ή links που αποστέλλονται με την ένδειξη κάποιας επιβράβευσης ή προσφοράς.
- Να είστε προσεκτικοί σε μηνύματα ηλεκτρονικού ταχυδρομείου που σας ζητούν τα προσωπικά σας στοιχεία για να προγραμματίσουν ιατρικούς ελέγχους ή έρευνες. Οι δημόσιες υγειονομικές Αρχές κανονικά δεν έρχονται σε επαφή με το ευρύ κοινό κατ' αυτόν τον τρόπο.
- Μην ενδίδετε σε πιέσεις για να αποκαλύψετε οποιαδήποτε προσωπική πληροφορία. Οι κυβερνοεγκληματίες χρησιμοποιούν καταστάσεις έκτακτης ανάγκης, όπως ο κορωνοϊός, για να τρομάξουν τους ανθρώπους και να τους ωθήσουν σε επιπόλαιες αποφάσεις.
- Οι χρήστες του διαδικτύου καλούνται να ασφαλίζουν το wifi του σπιτιού τους, να ασφαλίζουν όλες τις συσκευές τους με κωδικούς, PIN ή με βιομετρικά στοιχεία (αποτύπωμα ή αναγνώριση προσώπου), να εγκαθιστούν λογισμικό προστασίας από ιούς, να ενημερώνουν το λογισμικό που χρησιμοποιούν, να βάζουν ισχυρούς και

διαφορετικούς ανά εφαρμογή κωδικούς πρόσβασης (passwords), να τηρούν αντίγραφα ασφαλείας σε εξωτερικά αποθηκευτικά μέσα, μη συνδεδεμένα με τις συσκευές, να ελέγχουν τις ρυθμίσεις απορρήτου των λογαριασμών των μέσων κοινωνικής δικτύωσης και να ελέγχουν τα δικαιώματα των εφαρμογών που είναι εγκατεστημένες στις συσκευές τους διαγράφοντας όποιες δεν χρησιμοποιούνται.

Πηγές: Παγκόσμιος Οργανισμός Υγείας, cybersecurity scams, *Μάρτιος 2020*, INTERPOL warns of financial fraud linked to COVID-19, *Μάρτιος 2020,* Κομισιόν: Προσοχή σε διαδικτυακές απάτες με προϊόντα που δήθεν θεραπεύουν τον κορωνοϊό, *Μάρτιος 2020*, Απάτη και κορονωϊός – Πώς να προστατευτείτε από τους επιτήδειους *Μάρτιος 2020*, Don't fall prey to these 5 cruel coronavirus scams, *Φεβρουάριος 2020,* Συμβουλές από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος της ΕΛ.ΑΣ, *Μάρτιος 2020*, Ανακοίνωση ΕΛΑΣ: Προσοχή σε απάτη με επιτήδειους που παριστάνουν τα στελέχη του ΕΟΔΥ, *Μάρτιος 2020*, ACFE, Coronavirus fraudsters add to the anxiety and misery, *Μάρτιος 2020*