#Απάτες μέσω Διαδικτύου

και οικονομικά εγκλήματα

Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

#Απάτες μέσω Διαδικτύου
και οικονομικά εγκλήματα

Βασική αρχή στις απάτες που διαπράττονται μέσω Διαδικτύου είναι να πείσουν το θύμα να καταβάλει ένα μικρό αρχικό ποσό με σκοπό να εξασφαλίσει ένα πολύ μεγαλύτερο στο μέλλον, όπως για παράδειγμα οι νιγηριανές απάτες, ή γενικότερα να πείσουν το θύμα για την ασφάλεια των διαδικτυακών συναλλαγών, με σκοπό στη συνέχεια να του αποσπάσουν μεγάλα χρηματικά ποσά (απάτες με πιστωτικές κάρτες, κ.τ.λ).

Spamming-Scamming

Η λέξη «spam» περιγράφει τη μαζική αποστολή μηνυμάτων ηλεκτρονικού υπολογιστή (e-mails), τα οποία έχουν συνήθως απρόκλητο και εμπορικό χαρακτήρα και αποστέλλονται αδιακρίτως. Όταν ο στόχος του αποστολέα των μηνυμάτων αυτών είναι να εξαπατήσει τον αποδέκτη και να χρησιμοποιήσει με κακόβουλο τρόπο τα δεδομένα που θα υποκλέψει, τότε κάνουμε λόγο για τη διαδικασία «scamming». Πρόκειται για τον πλέον διαδεδομένο τρόπο δράσης σε πολλά είδη ηλεκτρονικών οικονομικών εγκλημάτων (νιγηριανές απάτες, ισπανικό λόττο, phishing, απατηλές θέσεις εργασίας στο εξωτερικό, διαφημίσεις για χάσιμο βάρους κ.τ.λ.). Επιπλέον, η μαζική αποστολή κακόβουλων μηνυμάτων γίνεται και προς κινητά τηλέφωνα, σε μια εποχή που οι χρήστες των Smartphones αυξάνονται ραγδαία.

«Νιγηριανές» Απάτες

Πρόκειται για e-mail που μας ενημερώνουν ότι κάποιος (συνήθως πρώην υψηλόβαθμο στέλεχος της νιγηριανής κυβέρνησης) χρειάζεται τη βοήθειά μας για να μεταφέρει ένα υψηλό χρηματικό ποσό (π.χ. 30 εκατ. δολάρια), έναντι υψηλής υποσχόμενης αμοιβής (ποσοστό επί του κεφαλαίου), το οποίο δεν μπορεί να διοχετευτεί εκτός της χώρας με το όνομα του δικαιούχου-αποστολέα του e-mail. Ζητείται δηλαδή στον παραλήπτη να βοηθήσει λειτουργώντας ως αποδέκτης του εν λόγω ποσού, αφού παράλληλα ενημερωθεί ότι η επιλογή του δεν έγινε τυχαία αλλά βάσει πληροφόρησης για τη φερεγγυότητά του (συχνά αναφέρεται κάποιο επιμελητήριο ή επαγγελματική ένωση). Παράλληλα δίνεται ιδιαίτερη έμφαση στην εμπιστευτικότητα που θα πρέπει να τηρηθεί. Σε πρώτη φάση, ζητείται από το υποψήφιο θύμα η συγκατάθεσή του και η παροχή στοιχείων που αφορούν τους τραπεζικούς του λογαριασμούς, και οποιωνδήποτε πληροφοριών κρίνονται απαραίτητες για την πραγματοποίηση των συναλλαγών. Πολλές φορές και ύστερα από απαίτηση του θύματος, προσκομίζονται και έγγραφα τα οποία δείχνουν αυθεντικά και επίσημα, εξαλείφοντας έτσι κάθε αμφιβολία του θύματος. Από τη στιγμή, λοιπόν, που το θύμα θα ανταποκριθεί, αρχίζει μια ατελείωτη διαδικασία ανταλλαγής e-mail, τηλεφωνημάτων και επιστολών κάνοντάς το να πιστεύει ότι βρίσκεται πολύ κοντά στην απόκτηση του εν λόγω ποσού. Ακριβώς, όμως, πριν την τελική μεταβίβαση των χρημάτων εμφανίζεται από πλευράς του αξιωματούχου κάποιο προσωρινό πρόβλημα (έκτακτος φόρος, απρόβλεπτο τέλος, πληρωμή κάποιου ενδιάμεσου υπαλλήλου κ.τ.λ.). Ο αξιωματούχος, βέβαια, προφασίζεται αδυναμία πληρωμής του ποσού λόγω του ότι έχει ήδη προχωρήσει σε μεταβίβαση των χρημάτων, με αποτέλεσμα τη δέσμευση αυτών έως ότου λυθεί το πρόβλημα που προέκυψε. Στα πλαίσια συνεργασίας τους, ζητείται από το θύμα να καταβάλει το ποσό, το οποίο φυσικά θα του επιστραφεί με την ολοκλήρωση της συναλλαγής. Αυτή βέβαια είναι η αρχή μιας σειράς «προβλημάτων» που προφασίζεται ο δράστης, καταφέρνοντας να αποσπάσει χρηματικό ποσό που μπορεί να φτάσει μέχρι και τα 500.000€. Η εμπειρία έχει δείξει πως κάποια από τα θύματα πείθονται να ταξιδέψουν μέχρι τη Νιγηρία για την ολοκλήρωση της συναλλαγής και, ενώ τους έχουν διαβεβαιώσει ότι δεν απαιτείται visa, καταλήγουν να βρίσκονται παράνομα στη χώρα, γεγονός που χρησιμοποιείται εκβιαστικά από το κύκλωμα των δραστών.

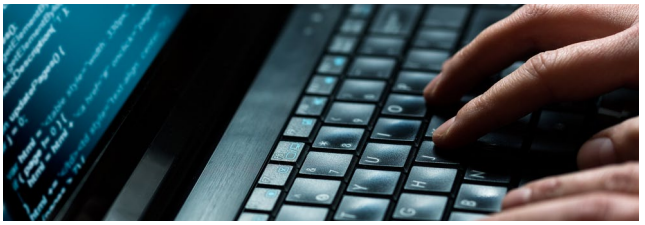
Δεν είναι λίγες οι περιπτώσεις συνανθρώπων μας που το κύκλωμα των δραστών πείθει να ταξιδέψουν στο εξωτερικό και οδηγεί σε θυρίδα τράπεζας δείχνοντάς τους τα λεφτά, ενώ εκείνοι έχουν ήδη καταβάλει κάποια χρηματικά ποσά για την αποδέσμευση του κεφαλαίου. Η παραμονή τους γίνεται σε ξενοδοχείο 5 αστέρων, με το κύκλωμα να τους παρακινεί να κάνουν για 4 ημέρες πολυτελή ζωή, την οποία και προφασίζονται ότι θα καλύψουν, χωρίς βεβαίως να το κάνουν.

Ισπανικό Λόττο

Η εν λόγω μορφή απάτης πραγματοποιείται με τη μαζική αποστολή μηνυμάτων ηλεκτρονικής αλληλογραφίας σε τυχαίους χρήστες του Διαδικτύου. Τα μηνύματα αυτά τους ενημερώνουν ότι έχουν κερδίσει ένα μεγάλο χρηματικό ποσό της τάξεως των εκατομμυρίων δολαρίων σε ηλεκτρονική κλήρωση του Διαδικτύου, στην οποία όμως ποτέ δεν δήλωσαν συμμετοχή! Οι δράστες, για να γίνουν πιστευτοί, χρησιμοποιούν παραπλήσια ονόματα μεγάλων εταιρειών (π.χ. Microsoft, Yahoo κ.λπ.) και συνοδεύουν τα μηνύματα που αποστέλλουν με πλαστά πιστοποιητικά όσον αφορά την υποτιθέμενη ηλεκτρονική κλήρωση. Η απάτη έγκειται στο γεγονός ότι ζητούν από τους υποτιθέμενους νικητές την προπληρωμή κάποιων φόρων ή/και εξόδων εκταμίευσης των χρημάτων, ποσό που συνήθως είναι της τάξης των μερικών χιλιάδων δολαρίων.

Phising προσωπικών στοιχείων

Το «phishing» πραγματοποιείται συνήθως με την αποστολή μαζικών spam e-mails, τα οποία υποτίθεται ότι αποστέλλονται από κάποια υπαρκτή και νόμιμη εταιρεία (τράπεζα, ηλεκτρονικό κατάστημα, υπηρεσία ηλεκτρονικών πληρωμών κ.λπ.). Σκοπός είναι να παραπλανηθεί ο παραλήπτης και να του εκμαιευθούν απόρρητα προσωπικά και οικονομικά δεδομένα. Στη συνέχεια, οι εγκέφαλοι της απάτης χρησιμοποιούν τα στοιχεία αυτά για την πραγματοποίηση αξιόποινων πράξεων. Συγκεκριμένα, ο αποστολέας ζητάει στον παραλήπτη να ενημερώσει ή να επαληθεύσει κάποια προσωπικά στοιχεία του για λόγους ασφαλείας και τον οδηγεί στο τέλος μέσω συνδέσμων σε κάλπικες ιστοσελίδες, οι οποίες και μιμούνται στο μέγιστο τις επίσημες. Τα κέρδη των δραστών παγκοσμίως υπερβαίνουν το 1 δις ευρώ σε ετήσια βάση.



Pharming

Η διαδικασία «pharming» αποτελεί μια παραλλαγή του «phishing». Περιγράφει την παρέμβαση τρίτων στον εξυπηρετητή DNS (DNS server) μιας ιστοσελίδας, που στόχο έχει την ανακατεύθυνση του προγράμματος περιήγησης σε άλλες ψεύτικες ιστοσελίδες. Το pharming μπορεί να πραγματοποιηθεί επιφέροντας αλλοίωση:

- Του «host» file ενός Η/Υ με αποτέλεσμα την ανακατεύθυνση ενός ονόματος χώρου σε ψευδή προορισμό.
- Του «router» ενός δικτύου LAN: Με την αλλοίωση των ρυθμίσεων ή ακόμη και του firmware ενός router ο δράστης μπορεί να πετύχει την ανακατεύθυνση ενός ονόματος χώρου για όλους τους Η/Υ του δικτύου.
- Ενός DNS server: Οι δράστες αποκτούν πρόσβαση σε έναν κεντρικό DNS server αλλοιώνοντας την κίνηση όλων των χρηστών του Διαδικτύου που εξυπηρετείται από αυτούς.

Με πιο απλά λόγια, όταν ο χρήστης του Διαδικτύου πληκτρολογεί την ιστοσελίδα κάποιου διαδικτυακού καταστήματος, εν αγνοία του μεταφέρεται σε έναν ψεύτικο ιστότοπο, ο οποίος προσομοιάζει την πραγματική ιστοσελίδα του εν λόγω καταστήματος, που έχει δημιουργηθεί για να παραπλανήσει το χρήστη. Στη συνέχεια, ο δράστης υφαρπάζει τα προσωπικά στοιχεία που ο ανυποψίαστος χρήστης θα καταχωρήσει κατά τη διαδικασία της συναλλαγής (ονοματεπώνυμο, κωδικοί πιστωτικών καρτών κ.τ.λ.), προκειμένου να τα χρησιμοποιήσει με κακόβουλο τρόπο.
Το φαινόμενο του «pharming» έχει παρουσιαστεί πρόσφατα σε δύο τραπεζικούς οργανισμούς. Με την ανακατεύθυνση των σελίδων του web banking, μέσω μόλυνσης του προσωπικού τους Η/Υ, οι χρήστες οδηγούνταν σε ψευδείς ιστοσελίδες όπου και υποκλέπτονταν τα προσωπικά τους δεδομένα.

Απάτες με πιστωτικές κάρτες

Τα περιστατικά απάτης με τη χρήση πιστωτικών καρτών σε online αγορές αυξάνονται με ραγδαίο ρυθμό. Υπολογίζεται ότι οι τράπεζες μετρούν απώλειες εκατομμυρίων ευρώ από ανθρώπους που κατασκευάζουν, παραχαράσσουν, υποκλέπτουν αριθμούς πιστωτικών καρτών, ή που κάνουν εικονικές αγορές μέσω Internet χρησιμοποιώντας αριθμούς καρτών που είναι σχετικά εύκολο να βρει ο απατεώνας ή να τους κατασκευάσει με τη βοήθεια κατάλληλων αλγοριθμικών προγραμμάτων με ηλεκτρονικούς υπολογιστές. Επιπλέον, η έλλειψη επαφής πρόσωπο με πρόσωπο στο Διαδίκτυο τείνει να κάνει τους απατεώνες πιο τολμηρούς. Online αγορές προϊόντων που ποτέ δεν παραδόθηκαν, υπέρογκες χρεώσεις πιστωτικών καρτών για υπηρεσίες που ποτέ δεν ζητήθηκαν ή είχαν αρχικά παρουσιαστεί ότι προσφέρονται δωρεάν, παραπλανητική πληροφόρηση για προϊόντα που αγοράζονται μέσω Διαδικτύου, είναι μόνο μερικές από τις καταγγελίες πολιτών που δέχονται καθημερινά οι διωκτικές αρχές της χώρας μας.

Χαρακτηριστικά αναφέρουμε περιπτώσεις ανθρώπων οι οποίοι ενδιαφερόμενοι να αγοράσουν κάποιο αυτοκίνητο, τρακτέρ, μηχανή κ.τ.λ. αναζητούν στο Διαδίκτυο την αγγελία που θα καλύψει τις ανάγκες τους. Στη συνέχεια και αφού έχουν αναπτύξει σχετική επικοινωνία με τον κάτοχο-δράστη, καταβάλλουν κάποια προκαταβολή, συνήθως μέσω εταιρείας πληρωμών (π.χ. Western Union). Εκεί ξεκινούν τα προβλήματα, καθώς ο δράστης προφασίζεται πλέον διάφορες δικαιολογίες για να εισπράξει επιπλέον χρήματα, να καθυστερήσει και τελικά να μην παραδώσει ποτέ το προϊόν.

Πυραμιδικά Συστήματα Εργασίας

Στις απάτες που διαπράττονται μέσω Διαδικτύου συμπεριλαμβάνονται και τα διαδικτυακά πυραμιδικά συστήματα εργασίας από το σπίτι. Πρόκειται για απάτες που υπόσχονται υψηλές αμοιβές και ασυνήθιστα υψηλά κέρδη από επενδύσεις που στην πραγματικότητα δεν υφίστανται. Τελικά, το σύστημα καταρρέει αφού οι επενδυτές δεν πληρώνονται ούτε τα υποσχόμενα μερίδια ούτε τις προσυμφωνημένες αποδόσεις, με αποτέλεσμα να χάνουν και την αρχική τους επένδυση.

Θέσεις εργασίας

Η παγκόσμια οικονομική κατάσταση έχει φέρει στο προσκήνιο ένα ακόμη είδος απάτης. Πρόκειται για απατηλές διαδικτυακές αγγελίες που αναρτώνται σε ιστοσελίδες εύρεσης εργασίας ή αποστέλλονται μέσω e-mail στο θύμα και περιγράφουν ιδιαίτερα ελκυστικές θέσεις εργασίας συνήθως στο εξωτερικό, ενώ οι δράστες δεν διστάζουν να δημιουργήσουν ιστοσελίδα της εταιρείας-εργοδότη, στην οποία αναρτούν πληροφορίες για την απατηλή αγγελία προκειμένου να γίνουν ακόμη πιο πειστικοί. Ζητείται από τους ανυποψίαστους υποψήφιους εργαζόμενους να γνωστοποιήσουν τα προσωπικά τους στοιχεία, ακόμη και να αποστείλουν αντίγραφα εγγράφων τους όπως το δίπλωμα οδήγησης, την ταυτότητά τους και όποιο άλλο θεωρηθεί «χρήσιμο» και «απαραίτητο» για τη διεκδίκηση της εν λόγω θέσης εργασίας. Στη συνέχεια, ο εργαζόμενος ενημερώνεται ότι μιας και η εργοδότρια εταιρεία δεν κατέχει τραπεζικό λογαριασμό στη δική του χώρα, ένας από τους πιστωτές της θα του χορηγήσει επιταγή για τα έξοδα και το μισθό του. Η επιταγή συνήθως υπερβαίνει κατά πολύ τα συμφωνηθέντα και ζητείται από τον υποψήφιο να αποστείλει με έμβασμα το επιπλέον ποσό στον εργοδότη. Αφού η διαδικασία ολοκληρωθεί, ο εργαζόμενος αντιλαμβάνεται ότι η επιταγή είναι πλαστή. Σε άλλες περιπτώσεις, το θύμα πείθεται να καταβάλει ένα ποσό για να κατοχυρώσει την εν λόγω «κάλπικη» θέση εργασίας.

Απάλειψη Χρέους (Debt Elimination)

Επιπλέον, η ισχύουσα οικονομική κατάσταση έχει οδηγήσει στην άνθηση ενός ακόμη είδους απάτης. Πρόκειται για ιστοσελίδες που υπόσχονται τη διαχείριση και εξάλειψη του χρέους των νοικοκυριών και επιχειρηματιών, διαφημίζοντας νόμιμους τρόπους για την αντιμετώπιση των στεγαστικών δανείων και του χρέους από πιστωτικές κάρτες. Συνήθως, το μόνο που ζητείται είναι η καταβολή ενός αρχικού ποσού, η αποστολή όλων των απαραίτητων πληροφοριών που αφορούν τα επίμαχα δάνεια ή τις πιστωτικές κάρτες και, βέβαια, μια εξουσιοδότηση προς το άτομο που θα φέρει εις πέρας τη διαδικασία. Ο διαμεσολαβητής τότε εκδίδει ομόλογα και γραμμάτια προς τους δανειστές που φιλοδοξούν να ικανοποιήσει νόμιμα όλα τα χρέη. Σε αντάλλαγμα, το θύμα είναι υποχρεωμένο να καταβάλει ένα ποσοστό της αξίας των χρεών που θα καλύψει ο διαμεσολαβητής. Η προαναφερθείσα διαδικασία είναι ιδιαίτερα συνδεδεμένη με τα εγκλήματα που σχετίζονται με την κλοπή ταυτότητας, καθώς οι συμμετέχοντες παρέχουν όλες τις προσωπικές πληροφορίες τους προς τους διαμεσολαβητές.

Botnets

Εκατομμύρια υπολογιστές έχουν μετατραπεί σε υποχείρια οργανωμένων hackers, εν αγνοία των χρηστών τους, απειλώντας τη συνολική λειτουργία του Διαδικτύου. Έως και το ένα τέταρτο των υπολογιστών που συνδέονται στο Διαδίκτυο είναι μολυσμένοι με κρυφό λογισμικό που τους επιστρατεύει σε κακόβουλα δίκτυα, γνωστά ως botnets, ανέφερε ο «πατέρας του Internet» Βιντ Σερφ (επινόησε το πρωτόκολλο TCP/IP). Το φαινόμενο φαίνεται να αποκτά επιδημικές διαστάσεις, καθώς περίπου ένας στους έξι υπολογιστές με σύνδεση στο Διαδίκτυο έχουν μετατραπεί σε «ζόμπι» των botnets.

Ένας ηλεκτρονικός υπολογιστής θεωρείται ότι είναι υπολογιστής-ζόμπι όταν είναι συνδεδεμένος στο Διαδίκτυο και ελέγχεται από κάποιον εξωτερικό χρήστη. Αυτός ο εξωτερικός χρήστης είναι συνήθως κάποιος hacker που, εξαπολύοντας επιτυχημένη επίθεση ενάντια στον υπολογιστή, καταφέρνει να τον μετατρέψει σε υπολογιστή-ζόμπι. Η επίθεση αυτή περιλαμβάνει μεταξύ άλλων τη μόλυνση του υπολογιστή-θύματος από κάποιον ιό ή δούρειο ίππο. Οι υπολογιστές-ζόμπι χρησιμοποιούνται κυρίως για την αποστολή άχρηστων ή κακόβουλων ηλεκτρονικών μηνυμάτων (spam-scam). Με τον τρόπο αυτό οι spammers μπορούν να αποφύγουν τον εντοπισμό τους και χρησιμοποιούν το εύρος ζώνης (bandwidth) των ιδιοκτητών των υπολογιστών-ζόμπι για τους δικούς τους σκοπούς. Τα botnets χρησιμοποιούνται και για την εκτέλεση DDoS Attacks και brute force attacks σε πληροφοριακά συστήματα και για τη χρήση κατά τη διάρκεια απάτης pharming με τη συνεχή δημιουργία απατηλών κλώνων σε διαφορετικά σημεία ανά τον κόσμο. Μέχρι στιγμής, τα μεγαλύτερα botnets που έχουν καταγραφεί αριθμούσαν έως και 30.000.000 Η/Υ!

Στην Ελλάδα, μεγάλος βιομηχανικός οργανισμός έπεσε θύμα επίθεσης botnet που εκδηλώθηκε με την υποκλοπή όλων των ηλεκτρονικών συνομιλιών κατόπιν επίθεσης στον mail server με τη χρήση botnet, ενώ τραπεζικός οργανισμός δέχθηκε ισχυρό πλήγμα, όταν οι χρήστες των υπηρεσιών διαδικτυακής εξυπηρέτησής του έπεσαν θύματα απάτης τη στιγμή που οι Η/Υ τους κατέστησαν «ζόμπι» με τη χρήση ειδικού προγράμματος «Trojan».

Ιός ransomware

Ένα ακόμη χαρακτηριστικό παράδειγμα της μεθόδου phishing αποτελεί και ο ιός ransomware ή, όπως είναι πλέον γνωστός, «ο ιός των 100€». Οι δράστες, εκμεταλλευόμενοι τις αδυναμίες του Η/Υ του θύματος, του μεταφέρουν κακόβουλο λογισμικό, καθώς εκείνο περιηγείται στο Διαδίκτυο. Το λογισμικό αυτό «κλειδώνει» όλες τις λειτουργίες του Η/Υ και εμφανίζει στην οθόνη του ένα μήνυμα που υποτίθεται ότι προέρχεται από τη Δίωξη Ηλεκτρονικού Εγκλήματος, ενημερώνοντας το χρήστη ότι του επιβάλλεται το πρόστιμο των 100€ για αδικήματα του Ποινικού Κώδικα που υποτίθεται ότι διέπραξε. Η καταβολή του προστίμου δύναται να πραγματοποιηθεί με τη χρήση προπληρωμένων καρτών paysafe ή ucash. Πρόκειται για έναν ιό με πανευρωπαϊκή παρουσία, που χρησιμοποιεί τα εμβλήματα της εκάστοτε αστυνομίας της χώρας από την οποία ο Η/Υ του θύματος έχει πρόσβαση στο Διαδίκτυο. Χιλιάδες χρήστες έχουν πέσει θύματα αυτού, ενώ δεν είναι λίγοι κι εκείνοι που έχουν τελικά καταβάλει το επίμαχο χρηματικό ποσό. Πρόκειται για ένα άριστα οργανωμένο κύκλωμα, το οποίο μέσα από μια πολύπλοκη διαδικασία και μέσα από μηχανισμούς ξεπλύματος μαύρου χρήματος, καταφέρνει να διασπά τις προπληρωμένες κάρτες των 100€ σε κάρτες αξίας 10€, τις οποίες και διανέμει σε όλο τον κόσμο.

Κινητά τηλέφωνα και διαδικτυακές παγίδες

Η χρήση των κινητών τηλεφώνων και δη των Smartphones αυξάνεται συνεχώς και όλο και περισσότεροι χρήστες τα θεωρούν ως απαραίτητα εργαλεία στην καθημερινότητά τους. Επιτήδειοι, εκμεταλλευόμενοι την τάση αυτή, προκαλούν απάτες αρκετών εκατομμυρίων ευρώ από την αγοραπωλησία εφαρμογών software για κινητά τηλέφωνα, όπως για παράδειγμα για τον εντοπισμό του κινητού τηλεφώνου κάποιου αγαπημένου προσώπου. Συνήθως ζητείται από τον ανυποψίαστο χρήστη να εισαγάγει το κινητό του τηλέφωνο, προκειμένου να αποκτήσει την εφαρμογή που έχει επιλέξει. Στη συνέχεια, ξεκινούν οι υπέρογκες χρεώσεις στον αριθμό του, τις οποίες ο ίδιος αποδέχτηκε καθώς αυτές περιγράφονται στα ψιλά γράμματα των όρων χρήσης που η πλειοψηφία των καταναλωτών δεν διαβάζει.

Ηλεκτρονικές Δημοπρασίες (Auctions)

Ένα είδος απάτης που είναι ιδιαίτερα διαδεδομένο σε χώρες του εξωτερικού αφορά τις διαδικτυακές δημοπρασίες. Αυτού του είδους οι απάτες εστιάζουν κυρίως στη διαστρεβλωμένη παρουσίαση ή στη μη παράδοση του δημοπρατούμενου προϊόντος. Οι καταναλωτές θα πρέπει να είναι ιδιαίτερα προσεκτικοί όταν οι πωλητές τούς ζητούν να καταβάλουν το συμφωνημένο χρηματικό ποσό σε λογαριασμό κάποιου τρίτου ή επικαλούνται έκτακτους λόγους που τους αναγκάζουν να εγκαταλείψουν τη χώρα τους, καθώς επίσης, όταν η καταβολή του ποσού ζητείται να πραγματοποιηθεί μέσω Western Union ή MoneyGram.

Οι Νόμοι στην Πράξη

Τα στελέχη της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος για την αντιμετώπιση των παραβατικών πράξεων που συντελούνται μέσα από το Διαδίκτυο και συνιστούν το αδίκημα της «Απάτης», καθοδηγούνται από δύο βασικά άρθρα του κοινού Ποινικού Κώδικα (Π.Κ.): α) άρθρο 386 «Απάτη», και β) άρθρο 386Α «Απάτη με υπολογιστή», τα οποία περιληπτικά περιγράφονται ως εξής:

Άρθρο 386 «Απάτη»

1. Όποιος, με σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία, πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με την εν γνώσει παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων, τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών και, αν η ζημιά που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον δύο ετών.

3. Επιβάλλεται κάθειρξη μέχρι δέκα ετών: α) αν ο υπαίτιος διαπράττει απάτες κατ' επάγγελμα ή κατά συνήθεια και το συνολικό όφελος ή η συνολική ζημιά υπερβαίνουν το ποσό των τριάντα χιλιάδων (30.000) ευρώ, ή β) εάν το περιουσιακό όφελος ή η προξενηθείσα ζημία υπερβαίνει συνολικά το ποσό των εκατό είκοσι χιλιάδων (120.000) ευρώ.

Άρθρο 386^{Α} «Απάτη με υπολογιστή»

Όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος, βλάπτει ξένη

περιουσία, επηρεάζοντας τα στοιχεία υπολογιστή είτε με μη ορθή διαμόρφωση του προγράμματος είτε με επέμβαση κατά την εφαρμογή του είτε με χρησιμοποίηση μη ορθών ή ελλιπών στοιχείων είτε με οποιονδήποτε άλλο τρόπο, τιμωρείται με τις ποινές του άρθρου 386. Περιουσιακή βλάβη υφίσταται και αν τα πρόσωπα που την υπέστησαν είναι άδηλα. Για την εκτίμηση του ύψους της ζημίας είναι αδιάφορο αν οι παθόντες είναι ένα ή περισσότερα πρόσωπα.

Πόσο άραγε κοστίζει το κυβερνοέγκλημα στις επιχειρήσεις;

Μια από τις μεγαλύτερες εταιρείες τεχνολογίας στον κόσμο παρουσίασε περί τα τέλη του 2012 μια νέα έρευνα, η οποία αναδεικνύει ότι το κόστος και η συχνότητα του κυβερνοεγκλήματος συνέχισαν να αυξάνονται για τρίτη συνεχόμενη χρονιά. Σύμφωνα με την τρίτη ετήσια έρευνα, που αφορούσε πολυεθνικές εταιρείες των Η.Π.Α., η συχνότητα των κυβερνοεπιθέσεων έχει σημειώσει ραγδαία αύξηση μέσα σε τρία χρόνια, ενώ οι οικονομικές τους επιπτώσεις αυξήθηκαν περίπου κατά 40%. Η έρευνα για το Κόστος του Κυβερνοεγκλήματος για το 2012 (Cost of Cyber Crime Study 2012), η οποία διενεργήθηκε από το «**Ponemon Institute**», κατέδειξε ότι το **μέσο ετήσιο κόστος του κυβερνοεγκλήματος** για ένα ενδεικτικό δείγμα επιχειρήσεων στις Η.Π.Α. ανήλθε στα **8,9 εκατ. δολάρια**. Το ποσό αυτό παρουσιάζει αύξηση 6% σε σχέση με το μέσο κόστος για το 2011 και 38% σε σχέση με το αντίστοιχο μέγεθος για το 2010. Επίσης, η φετινή έρευνα κατέγραψε μια αύξηση 42% στον αριθμό των κυβερνοεπιθέσεων, με τους οργανισμούς να αντιμετωπίζουν κατά μέσο όρο **102 ολοκληρωμένες επιθέσεις την εβδομάδα**, ενώ αντιμετώπιζαν 72 και 50 επιθέσεις την εβδομάδα το 2011 και το 2010 αντίστοιχα. Ανώτατο στέλεχος της εταιρείας που πραγματοποίησε την έρευνα δήλωσε:

Οι οργανισμοί ξοδεύουν συνεχώς περισσότερο χρόνο, χρήμα και ενέργεια για να ανταποκριθούν στις κυβερνοαπειλές, φτάνοντας σε επίπεδα που σύντομα θα καταστούν μη βιώσιμα. Υπάρχουν στοιχεία που ξεκάθαρα δείχνουν ότι η χρήση προηγμένων λύσεων "security intelligence" βοηθά στην ουσιαστική μείωση του κόστους, της συχνότητας και των επιπτώσεων αυτών των επιθέσεων.

Και φέτος, το **μεγαλύτερο κόστος** για τις επιχειρήσεις προήλθε από κυβερνοεγκλήματα όπως η χρήση κακόβουλων κωδικών, οι επιθέσεις άρνησης υπηρεσίας, η χρήση κλεμμένων ή παραβιασμένων συσκευών και η κακόβουλη δραστηριότητα προσώπων που βρίσκονται μέσα σε έναν οργανισμό. **Συνδυαστικά**, το **κόστος** που προέρχεται από αυτές τις απειλές αντιστοιχεί σε **περισσότερο από το 78% του ετήσιου κόστους του κυβερνοεγκλήματος ανά οργανισμό.** Επίσης, η έρευνα κατέληξε στα παρακάτω **βασικά ευρήματα:**

- Η κλοπή πληροφοριών και η διακοπή των εργασιών συνεχίζουν να αντιστοιχούν στο μεγαλύτερο εξωτερικό κόστος για τις επιχειρήσεις. Σε ετήσια βάση, **η υποκλοπή πληροφοριών ισοδυναμεί με το 44% του συνολικού εξωτερικού κόστους**, σημειώνοντας άνοδο 4% σε σχέση με το 2011. Η διακοπή των εργασιών ή η μείωση της παραγωγικότητας αντιστοιχεί στο 30% του εξωτερικού κόστους, σημειώνοντας άνοδο 1% από το 2011.
- Η χρήση **προηγμένων λύσεων ασφάλειας πληροφοριών και διαχείρισης περιστατικών (Security Information & Event Management –SIEM)** μπορεί να περιορίσει τις επιπτώσεις των κυβερνοαπειλών. Οι οργανισμοί που χρησιμοποίησαν τέτοιες λύσεις εξοικονόμησαν περίπου 1,6 εκατ. δολάρια το χρόνο. Γι' αυτούς τους οργανισμούς, το κόστος για την ανάκτηση των συστημάτων, τον εντοπισμό και τον περιορισμό των απειλών ήταν σημαντικά μικρότερο σε σχέση με το κόστος που αντιμετώπισαν όσοι δεν αξιοποίησαν λύσεις SIEM.
- Οι κυβερνοεπιθέσεις μπορεί να κοστίσουν ακριβά, αν δεν αντιμετωπιστούν γρήγορα. Ο **μέσος χρόνος αντιμετώπισης** μιας κυβερνοεπίθεσης είναι **24 μέρες**, αλλά μπορεί να φτάσει μέχρι και τις 50, σύμφωνα με τη φετινή μελέτη. Το μέσο κόστος που προέκυψε για την περίοδο των 24 ημερών ανερχόταν σε 591.780$, καταγράφοντας αύξηση 42% σε σχέση με το μέσο εκτιμώμενο κόστος των 415.748$ για την ίδια περίοδο πέρυσι.
- Η ανάκτηση δεδομένων και ο εντοπισμός των απειλών παραμένουν οι πιο δαπανηρές εσωτερικές δραστηριότητες σε σχέση με το κυβερνοέγκλημα. Σε ετήσια βάση, αυτές οι δραστηριότητες αντιστοιχούν στο **μισό σχεδόν του συνολικού εσωτερικού κόστους**, με τα

λειτουργικά έξοδα και το κόστος εργασίας να αντιστοιχούν στο μεγαλύτερο μέρος του.

Ο Πρόεδρος και ιδρυτής του Ponemon Institute, **Dr Larry Ponemon**, δήλωσε ότι σκοπός αυτής της έρευνας είναι να ποσοτικοποιήσει τις οικονομικές επιπτώσεις των κυβερνοεπιθέσεων και να καταγράψει τις διαχρονικές τάσεις που αφορούν το σχετικό κόστος, και ότι η καλύτερη κατανόηση του κόστους τού κυβερνοεγκλήματος θα βοηθήσει τους οργανισμούς να καθορίσουν τις κατάλληλες επενδύσεις και τους πόρους που χρειάζονται, ώστε να μετριάσουν τις καταστροφικές συνέπειες μιας επίθεσης.

Αντίστοιχες μελέτες για το κόστος του κυβερνοεγκλήματος έχουν πραγματοποιηθεί στην Αυστραλία, τη Γερμανία, την Ιαπωνία και το Ηνωμένο Βασίλειο με παρόμοια αποτελέσματα. Για παράδειγμα, η εταιρεία λύσεων τεχνολογίας ασφάλειας πληροφοριακών συστημάτων RSA δημοσίευσε για το 1ο εξάμηνο του 2012 έρευνα σχετικά με την αύξηση του κόστους που επέφερε το phishing σε εταιρείες του Η.Β., του Καναδά και των Η.Π.Α. Το phishing υφίσταται ως φαινόμενο για τα τελευταία 16 χρόνια και εξακολουθεί να αποτελεί έναν από τους μεγαλύτερους κινδύνους που κρύβει το Διαδίκτυο. Το κόστος του σημείωσε αύξηση κατά 19% σε σχέση με το αντίστοιχο του 1ου εξαμήνου του 2011 και προκάλεσε ζημιά ύψους 687 εκατ. δολαρίων για τις αμερικάνικες εταιρείες. Η έρευνα κατέδειξε ότι το Η.Β., οι Η.Π.Α., ο Καναδάς, η Βραζιλία και η Νότια Αφρική συγκαταλέγονται στις χώρες με τις περισσότερες επιθέσεις phishing διεθνώς. Συγκεκριμένα στον Καναδά τα φαινόμενα phishing σημείωσαν αύξηση κατά 400% κατά το 1ο εξάμηνο του 2012 σε σχέση με το αντίστοιχο περυσινό, γεγονός που ενδεχομένως οφείλεται στην οικονομική σταθερότητα της χώρας αλλά και στην ισοτιμία σχεδόν 1:1 σε σχέση με το αμερικάνικο δολάριο, καθώς οι «απατεώνες» αρέσκονται να ακολουθούν το χρήμα. Όπως και να έχει τελικά, παρά το γεγονός ότι το phishing ήδη μετρά 16 χρόνια ζωής και θεωρείται «παλαιό» φαινόμενο, κανείς δεν μπορεί να αγνοήσει ζημιά 687 εκατ. δολαρίων.

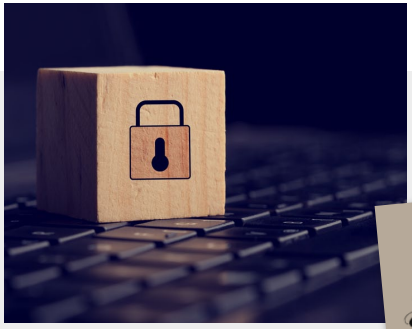
Online συναλλαγές και ασφάλεια

Με την πάροδο του χρόνου, όλο και περισσότερες επιχειρήσεις δραστηριοποιούνται μέσω του Διαδικτύου, αυξάνοντας τα έσοδά τους, μειώνοντας το κόστος τους και διευκολύνοντας τους χρήστες. Με τον τρόπο αυτό ο καθένας δύναται να έχει πρόσβαση όλο το 24ωρο στον κατάλογο μιας επιχείρησης και να αγοράσει ό,τι επιθυμεί. Οι περισσότερες ιστοσελίδες που πουλούν προϊόντα, χρησιμοποιούν συστήματα πληρωμών-συναλλαγών, όπως το Paypal, διατραπεζικά συστήματα, κ.λπ. Πώς μπορούμε να είμαστε βέβαιοι ότι δεν θα εξαπατηθούμε και πώς μπορούμε να υποψιαστούμε απάτες ώστε να τις αποφύγουμε;

Είναι όμως οι online συναλλαγές ασφαλείς;
Πώς μπορούμε να είμαστε βέβαιοι ότι δεν θα εξαπατηθούμε και πώς μπορούμε να υποψιαστούμε απάτες ώστε να τις αποφύγουμε;

Τι θα πρέπει να προσέχει κανείς όσον αφορά τις συναλλαγές του

1) Να μην κάνει τις συναλλαγές του χρησιμοποιώντας **δημόσιους υπολογιστές** (από net cafe, καφετέριες, βιβλιοθήκες, κ.λπ.). Μπορεί να έχουν keyloggers ή spywares, χωρίς να το γνωρίζει το προσωπικό του χώρου αυτού. Έτσι, κακόβουλοι χρήστες μπορούν εύκολα να υποκλέψουν τα ευαίσθητα προσωπικά στοιχεία κάποιου και να προβούν σε συναλλαγές αντ' αυτού.
2) Όταν πραγματοποιεί συναλλαγές από τον υπολογιστή του, θα πρέπει να είναι σίγουρος ότι έχει λάβει όλα τα **απαραίτητα μέτρα ασφαλείας πρόσφατα ενημερωμένα** (firewall, antivirus, anti-spyware, κ.λπ.).



3) Όταν συγκρίνει προϊόντα από διάφορες ιστοσελίδες, μπορεί να βρει σε κάποιες εξ αυτών **τα ίδια προϊόντα φθηνότερα σε σχέση με άλλες ιστοσελίδες**. Καλό θα ήταν, λοιπόν, να ψάξει μήπως οι ιστοσελίδες αυτές είναι φαντάσματα (μια αναζήτηση στο Google με την επωνυμία της ιστοσελίδας με τα πολύ φθηνά προϊόντα αρκεί).
4) Πάντα να κάνει τις συναλλαγές του **πληκτρολογώντας ο ίδιος τη διεύθυνση της ιστοσελίδας**. Να μην κλικάρει πάνω σε links από e-mail, καθώς μπορεί να είναι απατηλά.
5) Να πραγματοποιεί τις πληρωμές-συναλλαγές του μόνο μέσω ιστοσελίδων που έχουν το **εικονίδιο ασφαλείας** (μια κλειδαριά πάνω αριστερά στον browser). Το εικονίδιο αυτό μας ενδιαφέρει ουσιαστικά εκεί που πληκτρολογούμε π.χ. αριθμό κάρτας και τα υπόλοιπα ευαίσθητα προσωπικά στοιχεία και κλικάρουμε αποστολή.
6) Να επαληθεύει ότι εκεί που πληκτρολογεί τα ευαίσθητα στοιχεία του, στον browser δεν γράφει http αλλά **https**.
7) Προτού πραγματοποιήσει κάποια συναλλαγή μέσω μιας ιστοσελίδας, θα πρέπει να **καλέσει** στο ηλεκτρονικό κατάστημα, προκειμένου να επιβεβαιώσει εάν λειτουργεί η επιχείρηση. Εάν δεν απαντήσουν, το πιθανότερο είναι να μην αποστείλουν ούτε το αγορασθέν προϊόν, ακόμη κι αν έχει πληρωθεί.
8) Πάντα να τηρεί κάπου στον υπολογιστή του ή να εκτυπώνει τις **αποδείξεις** από τις αγορές του.
9) Να είναι ιδιαίτερα προσεκτικός όσον αφορά συναλλαγές μέσω **εταιρειών μεταφοράς χρημάτων και διεθνών πληρωμών** (Western Union, MoneyGram, BidPay κ.λπ.).
10) Να είναι βέβαιος ότι οι κωδικοί του, οι αριθμοί των καρτών του (χρεωστικών-πιστωτικών) και τα άλλα ευαίσθητα προσωπικά στοιχεία του είναι **φυλαγμένα επαρκώς**, ώστε να μην μπορεί κάποιος να τα υποκλέψει ή να τα απομνημονεύσει.
11) Να φροντίζει να **αλλάζει** τους **κωδικούς** του σε τακτά χρονικά διαστήματα και αυτοί να αποτελούνται από πεζά και κεφαλαία γράμματα, αριθμούς και σύμβολα.

Τι θα πρέπει να προσέχει κανείς όσον αφορά τις αγορές του

1) Ποτέ να μην πληρώνει προκαταβολικά σε πωλητή που δεν γνωρίζει, ακόμη κι αν αυτός αποκαλύπτει τα προσωπικά του στοιχεία ή τον αριθμό του τραπεζικού του λογαριασμού.
2) Να αναζητά πληροφορίες-αναρτήσεις σχετικά με το πώς το διαδικτυακό κατάστημα διαχειρίζεται τυχόν παράπονα πελατών του.
3) Να ζητά την αυθεντική απόδειξη ή γραπτή απόδειξη αγοράς.
4) Να προσέχει ιδιαιτέρως όταν η προσφορά φαίνεται πολύ καλή για να είναι αληθινή, και το άλλο μέρος ασκεί συνεχώς πίεση για την ολοκλήρωση της αγοραπωλησίας.
5) Να προσέχει όταν του ζητείται η πληρωμή μεγάλων ποσών σε ανθρώπους που δεν γνωρίζει: θα πρέπει να πραγματοποιείται συνάντηση σε κάποιο κατάστημα ή δημόσιο χώρο.
6) Να προσέχει εάν κατά την αγορά επώνυμων προϊόντων αυτά είναι όντως αυθεντικά.

Πώς να προστατεύσει κανείς τις συναλλαγές μέσω κινητού τηλεφώνου;

1) Διατηρήστε το λογισμικό προστασίας του κινητού τηλεφώνου σας επικαιροποιημένο και όλες τις συσκευές που συνδέονται με αυτό προφυλαγμένες από κακόβουλες επιθέσεις και ιούς.
2) Χρησιμοποιήστε έναν ισχυρό κωδικό προκειμένου να κλειδώνετε τη συσκευή του κινητού σας τηλεφώνου.
3) Μελετήστε προσεκτικά τις εφαρμογές που επιθυμείτε να εγκαταστήσετε πριν το κάνετε.
4) Δώστε τον αριθμό του κινητού σας τηλεφώνου μόνο σε άτομα της εμπιστοσύνης σας και μη δίνετε τον αριθμό του κινητού άλλων χωρίς την έγκρισή τους.
5) Ενεργοποιήστε την υπηρεσία γεωεντοπισμού του κινητού σας σε περίπτωση που το χάσετε.
6) Να είστε προσεκτικοί με τα δίκτυα Wi-Fi Hotspot στα οποία συνδέεστε με το κινητό σας τηλέφωνο.
7) Όταν γίνεστε αποδέκτης μηνυμάτων τον αποστολέα των οποίων δεν γνωρίζετε, μην ανταποκρίνεστε.
8) Μπλοκάρετε τους χρήστες των οποίων τον αριθμό και το e-mail δεν γνωρίζετε, χρησιμοποιώντας CALLER ID.
9) Επιβάλετε σε όσους προσπαθούν να σας τραβήξουν φωτογραφία ή βίντεο να λαμβάνουν πρώτα την άδειά σας.

Μπορούν οι επιχειρήσεις να αντιμετωπίσουν την κυβερνοαπάτη και με ποιον τρόπο;

Οι επιχειρήσεις θα πρέπει, εκτός από την εφαρμογή λογισμικών προστασίας και ασφάλειας των πληροφοριακών τους συστημάτων, να εκπαιδεύουν το προσωπικό τους, έτσι ώστε να αποκτήσει «Κουλτούρα Ασφάλειας» (Culture of Security). Είναι αρκετά συχνό το φαινόμενο, κατά την πρόσληψη των υπαλλήλων της, μια επιχείρηση να τους ζητά να υπογράψουν όρους και πολιτικές ασφαλείας που θα πρέπει να τηρούν, ώστε να προστατεύεται τόσο το πελατολόγιο της εταιρείας όσο και τα πληροφοριακά δεδομένα της. Στην προσπάθειά της αυτή μια επιχείρηση θα πρέπει να εφαρμόζει κάποια μέτρα, τα οποία συνοψίζονται στα εξής:

1) Να εντοπίσει ποια δεδομένα είναι εκτεθειμένα σε μεγαλύτερο κίνδυνο, εφόσον τα πληροφοριακά της συστήματα έχουν πρόσβαση στο Διαδίκτυο (π.χ. στοιχεία πελατών της ή λογιστικά δεδομένα και οικονομικά στοιχεία).
2) Να έχει εγκατεστημένα σε όλους τους Η/Υ ειδικά λογισμικά (π.χ. προγράμματα antivirus, προγράμματα anti-spyware, firewalls) και οι κωδικοί πρόσβασης και συναλλαγών να αλλάζουν κάθε 60 ή 70 μέρες.
3) Να εγκαθιστά πρόγραμμα που θα τηρεί backups (π.χ. σε εξωτερικό σκληρό δίσκο) όλων των σημαντικών δεδομένων, και να το αναβαθμίζει σε τακτά χρονικά διαστήματα, έτσι ώστε να μην υπάρχει απώλεια δεδομένων σε περίπτωση φυσικής καταστροφής ή κυβερνοεπίθεσης. Καλό θα ήταν να κρυπτογραφούνται όλα τα ευαίσθητα και υψίστης σημασίας δεδομένα.
4) Να έχει ήδη σχεδιασμένο πλάνο επείγουσας επέμβασης ή εναλλακτικών ενεργειών σε περίπτωση κυβερνοεπίθεσης, το οποίο θα πρέπει να ελέγχεται ετησίως.
5) Να εκπαιδεύει το προσωπικό της για την επίδραση που θα έχει σε όλους μια κυβερνοεπίθεση με τη μορφή της απάτης. Η εκπαίδευση μπορεί να γίνει με σεμινάρια πάνω σε πρακτικές του Διαδικτύου ή και τεχνολογικές λύσεις που θα πείθουν τους εργαζομένους ότι θα πρέπει να είναι ιδιαιτέρως προσεκτικοί απέναντι σε διαδικτυακές απάτες, καθώς μπορεί να εξαπατηθούν και να ζημιωθούν στην προσωπική τους ζωή μέσα από το Διαδίκτυο.
6) Να υπογράφει συμβόλαια με τους εργαζομένους της, τους οποίους θα δεσμεύει να αναφέρουν προς τις αρμόδιες αρχές τυχόν υποψία αλλά και πραγμάτωση διαδικτυακής απατηλής συναλλαγής.

Μερικές συμβουλές:

1) Συνεργαστείτε μόνο με εταιρείες που γνωρίζετε ή στα στοιχεία των οποίων μπορείτε να έχετε άμεση πρόσβαση από επίσημες βάσεις δεδομένων.
2) Κατανοήστε όλες τις λεπτομέρειες σχετικά με τις προσφερόμενες υπηρεσίες ή προϊόντα.
3) Ελέγξτε προσεκτικά όλα τα τιμολόγια και τους λογαριασμούς που καλείστε να πληρώσετε.
4) Διαφυλάξτε τα οικονομικά και τραπεζικά δεδομένα σας και μην τα αποκαλύπτετε σε άγνωστους τρίτους.
5) Καταστήστε το προσωπικό σας υπεύθυνο για τυχόν λανθασμένες ενέργειες, αφού πρώτα το εκπαιδεύσετε σχετικά.

Συμβουλές για Ηλεκτρονικές Δημοπρασίες (Auctions):

- Πριν δώσετε προσφορά, επικοινωνήστε με τον πωλητή και ξεκαθαρίστε αμφισβητούμενα σημεία σχετικά με το δημοπρατούμενο προϊόν.
- Να είστε ιδιαίτερα προσεκτικοί όσον αφορά αντισυμβαλλόμενους στο εξωτερικό.
- Επιβεβαιώστε τις πολιτικές επιστροφής και εγγύησης του προϊόντος, καθώς και τα μεταφορικά έξοδα.
- Ασφαλίστε τα δημοπρατηθέντα κατά τη μεταφορά τους.

Συμβουλές για Απάτες σχετικές με Πιστωτικές Κάρτες (credit card fraud):

- Επιβεβαιώστε ότι η ιστοσελίδα όπου δηλώνετε τα στοιχεία της πιστωτικής σας κάρτας είναι ασφαλής και γνωστή στο ευρύ κοινό.
- Επιβεβαιώστε και το κατάστημα που προβάλλεται μέσω της ιστοσελίδας.
- Ελέγχετε συχνά τις κινήσεις της πιστωτικής σας κάρτας μέσω της τράπεζάς σας ή μέσω web-banking.

Συμβουλές για εξάλειψη χρέους:

- Ελέγχετε εάν είναι υπαρκτά το όνομα, η διεύθυνση και ο τηλεφωνικός αριθμός της εταιρείας ή του φυσικού προσώπου που προβάλλεται ως «σωτήρας».
- Ελέγξτε τους όρους της συμφωνίας πριν υπογράψετε.

- Προσέξτε εταιρείες που δηλώνουν μόνο ταχυδρομικές θυρίδες για επικοινωνία.
- Προσέξτε μήπως αυτά που υπόσχονται είναι πολύ καλά για να είναι αληθινά.

Συμβουλές για θέσεις εργασίας:

- Προσέξτε μήπως υπόσχονται πολλά έσοδα ή κέρδη.
- Προσέξτε μήπως σας ζητήσουν να προκαταβάλετε χρήματα για διαδικαστικά θέματα.
- Προσέξτε αγγελίες εργασίας που δεν ζητούν προϋπηρεσία ως απαραίτητο προσόν.
- Επιβεβαιώστε ότι η εταιρεία-εργοδότης είναι υπαρκτή.

Συμβουλές για νιγηριανές επιστολές:

- Προσέξτε μήπως αυτά που σας υπόσχονται είναι πολύ καλά για να είναι αληθινά.
- Μην απαντάτε σε e-mail που σας ζητούν στοιχεία τραπεζικού λογαριασμού.
- Μην εξαπατάστε από άτομα που παρουσιάζονται ως κυβερνητικοί υπάλληλοι μιας ξένης χώρας.
- Προσέξτε όταν σας ζητούν να βοηθήσετε στην τοποθέτηση χρημάτων σε υπεράκτιους λογαριασμούς.
- Μην εμπιστεύεστε όσους σας υπόσχονται μεγάλα χρηματικά ποσά σε περίπτωση συνεργασίας.

Συμβουλές για phishing:

- Να είστε καχύποπτοι όταν σας ζητούν μέσω απομονωμένων e-mail προσωπικές πληροφορίες.
- Μη συμπληρώνετε φόρμες με τα προσωπικά σας στοιχεία όταν σας αποστέλλονται από άγνωστες διευθύνσεις ηλεκτρονικών ταχυδρομείων.
- Πληκτρολογήστε στον browser τη διεύθυνση της ιστοσελίδας και μην μπαίνετε σε αυτή μέσω συνδέσμων.

Συμβουλές για spamming:

- Μην ανοίγετε τα μηνύματα spam.
- Μην απαντάτε στα μηνύματα spam, ώστε ο αποστολέας να μην αντιληφθεί ότι η διεύθυνσή σας είναι υπαρκτή και ενεργή.
- Διατηρείτε δύο e-mail διευθύνσεις, μία για τους οικείους σας και μία για κάθε άλλο σκοπό.
- Ποτέ μην αγοράζετε κάτι που σας αποστέλλεται μέσω ενός απομονωμένου e-mail.

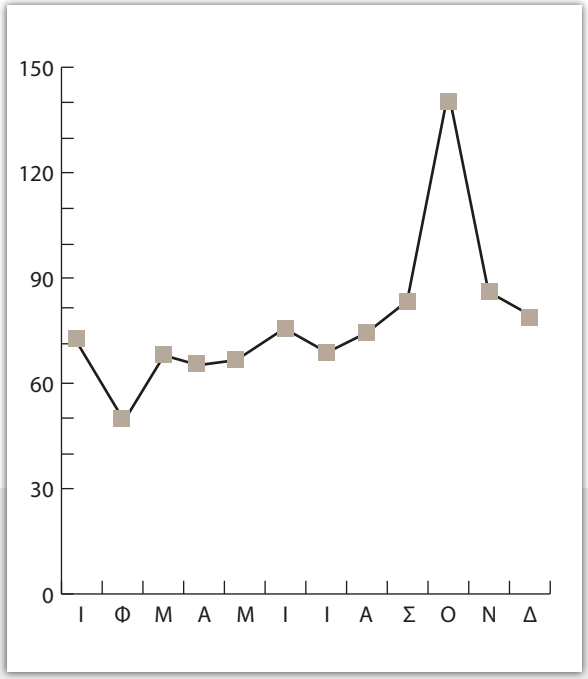
Συνοψίζοντας, δεν θα πρέπει να κυριεύεται κανείς από το αίσθημα του φόβου πριν προβεί σε online πληρωμές και συναλλαγές.
ΟΛΟΙ θα πρέπει να απολαμβάνουμε τα πλεονεκτήματα που μας παρέχουν αυτού του τύπου οι συναλλαγές και να πραγματοποιούμε τις αγορές μας πιο φθηνά, πιο ξεκούραστα, με μεγαλύτερη ποικιλία και τη δυνατότητα να επιλέξουμε και να αγοράσουμε όποτε και οτιδήποτε επιθυμούμε. Η Υπηρεσία μας αντιμετωπίζει θετικά τις online συναλλαγές, αρκεί να διαθέτει κανείς τα χρυσά εργαλεία για όλων των τύπων τις συναλλαγές και να μπορεί να τις ελέγχει πλήρως. Ποια είναι αυτά;

α) Μια **προπληρωμένη κάρτα** που θα έχει εκδότη ένα έγκριτο χρηματοπιστωτικό ίδρυμα.
β) Ένας λογαριασμός **Paypal** συνδεδεμένος με μια κάρτα ανάληψης.
γ) **E-banking** για την άμεση πρόσβαση στις κινήσεις των λογαριασμών και των καρτών, αλλά και για την άμεση πραγματοποίηση πληρωμών.

ΑΠΟΛΟΓΙΣΤΙΚΑ στατιστικά στοιχεία εξιχνίασης απατών από τη Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος για το 2015

Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος διαχειρίστηκε με επιτυχία εννιακόσιες είκοσι (920) περιπτώσεις διαδικτυακών απατών και παράνομης νομιμοποίησης εσόδων (money laundering), η μηνιαία εξέλιξη των οποίων περιγράφεται στο κατωτέρω διάγραμμα.

ΑΠΑΤΕΣ (ΜΗΝΙΑΙΑ ΕΞΕΛΙΞΗ)



ΒΙΒΛΙΟΓΡΑΦΙΑ

http://www.ic3.gov
http://www.fraud.org
http://www.staysafeonline.org
http://www.rsa.com
http://www.businessweek.com
http://www.acfe.gr
http://www.interpol.int

ΕΜΜΑΝΟΥΗΛ ΣΦΑΚΙΑΝΑΚΗΣ,
ΚΩΝΣΤΑΝΤΙΝΟΣ ΣΙΩΜΟΣ,
ΓΕΩΡΓΙΟΣ ΦΛΩΡΟΣ,
ΕΘΙΣΜΟΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ
ΚΑΙ ΑΛΛΕΣ ΔΙΑΔΙΚΤΥΑΚΕΣ
ΣΥΜΠΕΡΙΦΟΡΕΣ ΥΨΗΛΟΥ ΚΙΝΔΥΝΟΥ,
ΕΚΔΟΣΕΙΣ ΛΙΒΑΝΗ 2012.

ΑΝΑΣΤΑΣΙΑ Κ. ΜΑΛΛΕΡΟΥ,
ΤΟ ΔΙΚΑΙΟ ΤΟΥ ΗΛΕΚΤΡΟΝΙΚΟΥ ΧΡΗΜΑΤΟΣ,
ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ 2007.

ΘΕΟΔΩΡΟΣ Ν. ΚΡΙΘΑΡΑΣ,
ΠΟΙΝΙΚΟ ΔΙΚΑΙΟ ΚΑΙ ΔΙΑΔΙΚΤΥΟ,
ΝΟΜΙΚΗ ΒΙΒΛΙΟΘΗΚΗ 2009.

Bold Ogilvy & Mather

ΕΠΙΚΟΙΝΩΝΙΑ

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος - Cyber Crime Division
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Αθήνα, Τ.Κ. 11521
e-mail: ccu@cybercrimeunit.gov.gr, Τηλ.: 11188, Fax: 2106476462

Βρείτε μας στα:

www.cyberkid.gr

www.facebook.com/cyberkid.gov.gr

www.cyberalert.gr

www.facebook.com/CyberAlertGR

twitter.com/cyberalertgr