Ερευνητική εργασία Β Λυκείου με θέμα: «Διαδικτυακές απάτες»

Υπεύθυνος καθηγητής: Δ. Πριόβολος

Περιγραφή: Σε αυτή την εργασία θα ερευνήσουμε το πρόβλημα των διαδικτυακών απατών και τους τρόπους αντιμετώπισής τους. Για αυτό το σκοπό μπορούμε να χρησιμοποιήσουμε ως ερευνητικά εργαλεία κυρίως το Διαδίκτυο.

Ομάδες: Για τη διεξαγωγή της έρευνάς μας χωριστήκαμε σε 4 ομάδες.

Ομάδα 1η: Αλέξανδρος Γαραντζιώτης, Γάννης Καραβέλλας, Θανάσης Αθανασίου και Κώστας Παπακώστας.

Ομάδα 2η: Όλγα Ψαρρά, Ελευθερία Κλίνη, Ισμήνη Σαμπάνη και Λορέλα Χότζα.

Ομάδα 3η: Ελένη Βλάικου, Καρατσόλη Χριστίνα, Στέλιος Αδαμαντίδης και Νίκος Αργύρης.

Ομάδα 4η: Αρτέμης Αρμακόλας, Γιώργος Λεβαντής, Φώτης Γαλάνης και Αλέξανδρος Νούσιας.

Βασικά ερευνητικά ερωτήματα:

- Να εντοπίσουμε και να καταγράψουμε γνωστές διαδικτυακές απάτες.
- Να εντοπίσουμε και να καταγράψουμε γνωστούς «αστικούς θρύλους».
- Να μάθουμε πώς να διασταυρώνουμε μια πληροφορία.
- Σε ποιες περιπτώσεις μπορούμε να πέσουμε θύματα απάτης μέσω διαδικτύου;
- Με ποιους τρόπους μπορούμε να προστατευτούμε;
- Τι πρέπει και τι δεν πρέπει να κάνουμε στο Διαδίκτυο σχετικά με τα προσωπικά μας στοιχεία, κωδικούς, τραπεζικές κάρτες κλπ;
- Πως μπορούμε να ενισχύσουμε και να βελτιώσουμε τη σκέψη μας ώστε να ελαχιστοποιηθεί η πιθανότητα εξαπάτησης;

Πως εργαστήκαμε: Οι ερευνητικές ομάδες ανέλαβαν να ερευνήσουν τα ερωτήματα:

Η 1η ομάδα ανέλαβε να ερευνήσει και να συγγράψει κείμενο σχετικό με τους τρόπους που διασταυρώνουμε και επαληθεύουμε ή απορρίπτουμε πληροφορίες. Μπορεί να υπάρχει αναφορά στο ζήτημα της αμφιβολίας και της αμφισβήτησης και στην κριτική στάση που μπορούμε να αναπτύξουμε μέσω αυτών.

Πιθανές λέξεις-κλειδιά για την αναζήτηση: Σκεπτικισμός, αμφιβολία, αμφισβήτηση…

Η 2η ομάδα ανέλαβε να ερευνήσει και να συγγράψει κείμενο σχετικό με τις πρακτικές που πρέπει να ακολουθούμε έτσι ώστε να ελαχιστοποιήσουμε την πιθανότητα να γίνουμε θύματα διαδικτυακής απάτης. Δόθηκε έμφαση στην προστασία των προσωπικών μας δεδομένων. Αναφορά στις πηγές.

Πιθανές λέξεις-κλειδιά για την αναζήτηση: Ασφάλεια δεδομένων, προστασία προσωπικών δεδομένων, χάκερς – κράκερς – διαδίκτυο…

Η 3η ομάδα ανέλαβε να ερευνήσει και να συγγράψει κείμενο στο οποίο να καταγράφονται γνωστές διαδικτυακές απάτες με αναφορά στις πηγές.

Πιθανές λέξεις-κλειδιά για την αναζήτηση: Διαδικτυακές απάτες - hoaxes…

Η 4η ομάδα ανέλαβε να ερευνήσει και να συγγράψει κείμενο στο οποίο να καταγράφονται γνωστοί αστικοί θρύλοι με αναφορά στις πηγές τους.

Πιθανές λέξεις-κλειδιά για την αναζήτηση: Αστικοί θρύλοι, urban legends…

ΑΣΤΙΚΟΙ ΘΡΥΛΟΙ

Αλέξανδρος Νούσιας

Οι αστικοί θρύλοι αποτελούν ιστορίες ή θρύλους συνήθως φανταστικών γεγονότων που διαδίδονται μαζικά. Εναλλακτικά θα μπορούσαν να χαρακτηριστούν ως ευρέως διαδεδομένες φήμες. Ωστόσο, δεν είναι απαραιτήτως δημιουργήματα της φαντασίας, καθώς αρκετοί θρύλοι στηρίζονται σε πραγματικά γεγονότα. Κάποιοι αστικοί θρύλοι έχουν καταφέρει να επιβιώσουν για αρκετά χρόνια με μικρές παραλλαγές. Για τη διάδοση τους είναι συνήθης η χρήση του ηλεκτρονικού ταχυδρομείου.

Όσον αφορά το περιεχόμενο των αστικών θρύλων, αυτό ποικίλει και περιλαμβάνει συχνά στοιχεία τρόμου ή καλλιέργειας κάποιου φόβου. Παραδείγματα αστικών θρύλων είναι η ύπαρξη κροκοδείλων στους υπονόμους της Νέας Υόρκης, το ότι το σώμα του Γουόλτ Ντίσνεϊ είναι παγωμένο σε θάλαμο κρυογονικής κλπ.

Κάποιοι από τους πιο γνωστούς Αστικούς Θρύλους :

- Η ιστορία της πορσελάνινης κούκλας.
- Στοιχειωμένη Μονοκατοικία της Άμφισσσας- Ποδηλάτης.
- Η μαυροφορεμένη του Έβρου.

Γιάννης Καραβέλλας

Οι αστικοί θρύλοι αποτελούν ιστορίες ή θρύλους —συνήθως φανταστικών— γεγονότων που διαδίδονται μαζικά. Εναλλακτικά θα μπορούσαν να χαρακτηριστούν ως ευρέως διαδεδομένες φήμες. Ωστόσο, δεν είναι απαραιτήτως δημιουργήματα της φαντασίας, καθώς αρκετοί θρύλοι στηρίζονται σε πραγματικά γεγονότα. Κάποιοι αστικοί θρύλοι έχουν καταφέρει να επιβιώσουν για αρκετά χρόνια με μικρές παραλλαγές. Παρά την ονομασία τους, οι θρύλοι αυτοί δεν συνδέονται απαραίτητα με ένα αστικό περιβάλλον μέσα στο οποίο διαδραματίζονται. Ο όρος αστικός χρησιμοποιείται προκειμένου να διαχωριστούν από άλλου είδους (λόγου χάρη, τους παραδοσιακούς μύθους που συνδέονται με την αγροτική ζωή) και εισήχθη από τον καθηγητή Jan Harold Brunvand στο βιβλίο του The Vanishing Hitchhiker: American Urban Legends & Their Meanings. Στο βιβλίο αυτό, ο Brunvand δημιούργησε μια συλλογή από αστικούς θρύλους και φανταστικές ιστορίες με κύριο σκοπό να αποδείξει πως η μυθοπλασία αποτελεί διαχρονική πρακτική του ανθρώπου αλλά και για να υποστηρίξει πως ακόμα και θρύλοι αυτού του είδους μπορούν να χρησιμοποιηθούν για την μελέτη της σύγχρονης κουλτούρας. Το περιεχόμενο των αστικών θρύλων ποικίλει και περιλαμβάνει συχνά στοιχεία τρόμου ή καλλιέργειας κάποιου φόβου. Παραδείγματα αστικών θρύλων είναι η ύπαρξη κροκοδείλων στους υπονόμους της Νέας Υόρκης, το ότι το σώμα του Γουόλτ Ντίσνεϊ είναι παγωμένο σε θάλαμο κρυογονικής.

Ο μύθος λέει ότι λυκάνθρωπος γίνεσαι μόνο άμα σε δαγκώσει άλλος λυκάνθρωπος. Πώς ξεκίνησε αυτός ο μύθος; Κάποτε υποτίθεται, στα βουνά της σημερινής Βαυαρίας, ένας κυνηγός με την παρέα του αποφάσισαν να πάνε για κυνήγι λύκων το βράδυ. Κατά την διάρκεια του κυνηγιού, χωρίστηκαν ο ένας από τον άλλο. Ο Γιάνς Χρέμεν, ο πρώτος λυκάνθρωπος, όπως καταγράφεται στους μύθους ανά τον κόσμο ήρθε σε επαφή με ένα πελώριο μαύρο λύκο με τον οποίο παλέψανε. Ο Γιάνς τον τραυμάτισε θανάσιμα και ο λύκος τον δάγκωσε στο χέρι. Ο λύκος αφού ξέφυγε από τον κυνηγό του, ανέβηκε στην κορυφή ενός βουνού και καταράστηκε τον κυνηγό που τον τραυμάτισε, έτσι ώστε κάθε φορά που θα έχει πανσέληνο, να μεταμορφώνεται σε λύκο. Έτσι δημιουργήθηκε ο πρώτος λυκάνθρωπος. Στους επόμενους αιώνες ακολούθησαν πολλά κρούσματα από λυκόμορφα πλάσματα αλλά μέχρι σήμερα δεν υπάρχει καμία απόδειξη.

Η ΣΤΟΙΧΕΙΩΜΕΝΗ ΜΟΝΟΚΑΤΟΙΚΙΑ ΤΗΣ ΑΜΦΙΣΣΑΣ

Κώστας Παπακώστας

Κραυγές μέσα στη νύχτα, κοριτσάκια που βολτάρουν στα δωμάτια κι εξαφανίζονται, έπιπλα που κινούνται μόνα τους… Η ιστορία του εγκαταλελειμμένου σπιτιού της

οδού Γιδογιάννου στην Άμφισσα ξεκινάει από το 1940 και συνεχίζεται ακόμη και σήμερα. Όλοι στην περιοχή μιλούν για τη στοιχειωμένη μονοκατοικία. Της ΕΥΑΣ ΝΙΚΟΛΑΟΥ Είναι ίσως το πιο γνωστό στοιχειωμένο σπίτι της Στερεάς Ελλάδας.

Η ερειπωμένη μονοκατοικία της οδού Γιδογιάννου, αριθμός 13 (συμβολικός δεν νομίζετε;) είναι γεμάτη από μακάβριες ιστορίες που εδώ και δεκαετίες είναι γνωστές σε όλους τους κατοίκους της Άμφισσας. Το συγκεκριμένο σπίτι δεν βρίσκεται σε κάποιο απόμερο μέρος της πόλης, ίσα-ίσα που σε πολύ κοντινή απόσταση υπάρχουν πολυσύχναστα στέκια. Όμως οι θρύλοι που το ακολουθούν είναι τέτοιοι που οι κάτοικοι αλλά και οι επισκέπτες προσπαθούν να το αποφύγουν.

Ποια όμως είναι η ιστορία που κρύβεται πίσω από την ερειπωμένη μονοκατοικία; Γιατί το σπίτι της οδού Γιδογιάννου θεωρείται στοιχειωμένο; Σύμφωνα, λοιπόν, με όσα υποστηρίζονται, όλα ξεκίνησαν γύρω στο 1940. Ιδιοκτήτης του ήταν ένας άρχοντας της περιοχής, πάρα πολύ πλούσιος, ο οποίος είχε συνάψει παράνομο ερωτικό δεσμό με μια από τις υπηρέτριές του. Η υπηρέτρια έμεινε έγκυος από τον ιδιοκτήτη (οι φήμες έλεγαν ότι η εγκυμοσύνη προήλθε έπειτα από βιασμό) και στάθηκε η αιτία για ένα αποτρόπαιο έγκλημα που έμελλε να στιγματίσει για πάντα το σπίτι της οδού Γιδογιάννου.

Ο «άρχοντας» της περιοχής ζήτησε από τη νεαρή υπηρέτρια να κάνει έκτρωση και όταν η τελευταία αρνήθηκε, το πλήρωσε με την ίδια της τη ζωή. Σύμφωνα πάντα με το μύθο που ακολουθεί το οίκημα, ο πλούσιος ιδιοκτήτης φοβούμενος την κατακραυγή της μικρής κοινωνίας της Άμφισσας, οδήγησε τη νεαρή υπηρέτρια στο υπόγειο του σπιτιού όπου και την κρέμασε. Στη συνέχεια επιχείρησε να εξαφανίσει όλα τα ίχνη της στυγνής δολοφονίας της κοπέλας, αλλά δεν τα κατάφερε, αφού διάφορα περίεργα περιστατικά έκαναν την εμφάνισή τους, με αποτέλεσμα η μονοκατοικία να χαρακτηριστεί στοιχειωμένη.

Κάποιοι κάνουν λόγο για τρομακτικές κραυγές της κοπέλας που βγαίνουν από τα υπόγεια του σπιτιού καθ’ όλη τη διάρκεια της νύχτας. Κάποιοι υποστηρίζουν ότι ένα κοριτσάκι κόβει βόλτες στα δωμάτια προκαλώντας τρόμο, άλλοι είναι σίγουροι πως τα έπιπλα αλλάζουν θέση μόνα τους ενώ το τηλέφωνο του σπιτιού χτυπάει χωρίς να είναι στην πρίζα! Αλήθεια ή ψέματα, κανείς δεν γνωρίζει. Το μόνο σίγουρο είναι ότι το σπίτι της οδού Γιδογιάννου έχει πλέον εγκαταλειφθεί και κανείς δεν θέλει να μείνει εκεί. Και όσοι προσπάθησαν να πλησιάσουν την πόρτα του λέγεται ότι έφυγαν τρέχοντας…

ΔΙΑΔΙΚΤΥΑΚΕΣ ΑΠΑΤΕΣ

Ελευθερία Κλίνη

Οι συνηθέστερες μορφές διαδικτυακής απάτης είναι οι ακόλουθες:

α) Χρεώσεις της πιστωτικής κάρτας πολιτών μέσω του διαδικτύου για αγορές, οι οποίες δεν πραγματοποιήθηκαν από τους ίδιους.

- Στις περιπτώσεις αυτές, κάποιος κακόβουλος χρήστης του διαδικτύου δημιουργεί μια πλασματική ιστοσελίδα και με αυτόν τον τρόπο καταφέρνει να συγκεντρώνει στοιχεία κι αριθμούς πιστωτικών καρτών χρηστών του διαδικτύου, οι οποίοι έχοντας εξαπατηθεί, νομίζουν ότι πρόκειται για κάποιο διαδικτυακό κατάστημα και κάνουν τις αγορές τους.

- Επιπλέον, αρκετές είναι οι περιπτώσεις όπου επιτήδειοι καταφέρνουν να αποκτούν φυσική πρόσβαση στα στοιχεία πιστωτικών καρτών πολιτών τα οποία εν συνεχεία χρησιμοποιούν σε διαδικτυακές αγορές, καθώς για τις αγορές αυτές δεν είναι απαραίτητη η φυσική κατοχή της πιστωτικής κάρτας, παρά μόνο τα στοιχεία αυτής.

- Επιπροσθέτως, σε αρκετές περιπτώσεις οι χρήστες του διαδικτύου δίνουν οι ίδιοι άθελά τους τα στοιχεία σε κακόβουλους χρήστες του διαδικτύου (phishing). Ειδικότερα, ο ανυποψίαστος πολίτης λαμβάνει μήνυμα ηλεκτρονικού ταχυδρομείου από Πιστωτικό Ίδρυμα, στο οποίο τηρεί λογαριασμό, με το οποίο του ζητείται να συμπληρώσει τα στοιχεία του (ονοματεπώνυμο, αριθμό λογαριασμού και πιστωτικής κάρτας κλπ.), για λόγους πχ. ενημέρωσης των αρχείων της τράπεζας. Το μήνυμα, μέσω υπερσυνδέσμου, τους οδηγεί σε μια πλασματική ιστοσελίδα της τράπεζας, με αποτέλεσμα ο πολίτης να πείθεται και να χορηγεί τα επίμαχα στοιχεία.

β) Διακίνηση μηνυμάτων με απατηλό περιεχόμενο, που επιδιώκουν την εξαπάτηση ανυποψίαστων πολιτών.

- Ειδικότερα, ο τρόπος δράσης των κακόβουλων δραστών στην εν λόγω μορφή απάτης, που περιγράφεται υπό τον όρο «Ισπανικό Λόττο», είναι η μαζική αποστολή μηνυμάτων ηλεκτρονικής αλληλογραφίας σε τυχαίους χρήστες του διαδικτύου, με τα οποία τους ενημερώνουν ότι έχουν κερδίσει ένα μεγάλο χρηματικό ποσό της τάξεως των εκατομμυρίων δολαρίων σε ηλεκτρονική κλήρωση του διαδικτύου.

- Οι δημιουργοί των μηνυμάτων αυτών, για να γίνουν πιστευτοί, χρησιμοποιούν παραπλήσια ονόματα μεγάλων εταιρειών (πχ. Microsoft , Yahoo κλπ) και συνοδεύουν τα μηνύματα που αποστέλλουν με πλαστά πιστοποιητικά όσον αφορά στην 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.

γ) «Απάτες 419» ή «Νιγηριανές Απάτες»

- Στις περιπτώσεις αυτές αποστέλλονται, μηνύματα σε τυχαίους χρήστες του διαδικτύου, με τα οποία τους πληροφορούν ότι κάποιος κάτοχος ιδιαίτερα μεγάλης περιουσίας έχει αποβιώσει και είτε δεν υφίσταται κανείς κληρονόμος και ο παραλήπτης του μηνύματος έχει επιλεγεί ούτως ώστε να κληρονομήσει αυτός την περιουσία, είτε για να καταστεί δυνατό να αποδεσμευτεί η περιουσία, χρειάζεται αυτή να μεταφερθεί σε τραπεζικό λογαριασμό του εξωτερικού και ο παραλήπτης του μηνύματος ενημερώνεται ότι εάν διαθέσει το λογαριασμό του, θα αποκτήσει κάποιο ποσοστό επί της περιουσίας αυτής.

- Σε άλλες περιπτώσεις, άτομα από τη Νιγηρία αναζητούν τη βοήθεια επιχειρηματιών ή ελεύθερων επαγγελματιών με σκοπό να μεταφέρουν τα κεφάλαιά τους, τα οποία προέρχονται από εγκληματικές πράξεις (λαθρεμπόριο, απάτες, δωροδοκία κλπ.), υποσχόμενοι για τη συνεργασία αυτή υψηλό ποσοστό αμοιβής. Για το σκοπό αυτό, κάνουν χρήση τίτλων επίσημων φορέων της χώρας τους (Υπουργεία, Κεντρική Τράπεζα, Εθνική Εταιρεία Πετρελαίων Νιγηρίας κλπ.), χρησιμοποιούν τίτλους κυβερνητικών ή στρατιωτικών παραγόντων με υπαρκτά και ψεύτικα ονόματα ή προφασίζονται σχέση τους με «διάσημα» ή «σημαντικά» πρόσωπα.

- Η απάτη έγκειται στο γεγονός ότι οι αποστολείς των μηνυμάτων ζητούν από τους παραλήπτες να τους αποστείλουν τα προσωπικά τους στοιχεία, τα στοιχεία των τραπεζικού λογαριασμού και πιστωτικής κάρτας κλπ. προκειμένου επιτευχθεί η συνεργασία τους και η αποκόμιση των χρηματικών ποσών.

Τι να κάνετε αν υποπτεύεστε ότι έχετε πέσει θύμα ηλεκτρονικής απάτης

Προωθήστε το ύποπτο μήνυμα στην ηλεκτρονική διεύθυνση e-crime@tnt.com προκειμένου να διακοπεί η λειτουργία του σχετικού δικτυακού τόπου ή της διεύθυνσης ηλεκτρονικού ταχυδρομείου. Σημειώστε ότι μετά την προώθηση δε θα λάβετε απαντητικό μήνυμα.

Επιπλέον, σας συνιστούμε να αναφέρετε την υπόθεση στην αστυνομία. Σε παρόμοια περιστατικά η αστυνομία προχώρησε σε συλλήψεις μετά από καταγγελίες και σχετικές αναφορές πολιτών.

Οι πληροφορίες που θα προωθήσετε στο e-crime θα διαβιβαστούν στο κεντρικό τμήμα ασφάλειας της εταιρείας. Στη συνέχεια, το τμήμα ασφάλειας θα επικοινωνήσει επισήμως με την εταιρεία-πάροχο του παραπλανητικού δικτυακού τόπου ή της διεύθυνσης ηλεκτρονικού ταχυδρομείου. Η TNT έχει αναπτύξει καλές σχέσεις με τους σημαντικότερους παρόχους υπηρεσιών διαδικτύου (ISP), όπως είναι οι Microsoft, Yahoo και AOL. Η TNT διαβιβάζει τα σχετικά έγγραφα στους παρόχους, οι οποίοι επεξεργάζονται το αίτημα και απαντούν συνήθως εντός 24-48 ωρών. Κατά το δεύτερο εξάμηνο του 2007, η TNT κατάφερε να διακόψει τη λειτουργία περισσότερων από 1.500 παραπλανητικών ιστοσελίδων και διευθύνσεων ηλεκτρονικού ταχυδρομείου.

Για περισσότερες συμβουλές και πληροφορίες, μπορείτε να ανατρέξετε στους ακόλουθους οργανισμούς:

Ηλεκτρονικές δημοπρασίες ή θέματα σχετικά με το Internet

Εάν έχετε πραγματοποιήσει ηλεκτρονικές αγορές μέσω του eBay, σας συνιστούμε να διαβάσετε τις πληροφορίες που περιέχονται στο Κέντρο Ασφαλείας και Αξιοπιστίας του eBay στην ηλεκτρονική διεύθυνση www.ebay.com. Σχετικά με τη χρήση υπηρεσιών πληρωμής μέσω Internet, η Western Union παρέχει οδηγίες με σκοπό την ενημέρωση των καταναλωτών για περιστατικά ηλεκτρονικού εγκλήματος, οι οποίες είναι διαθέσιμες στον παγκόσμιο δικτυακό τόπο της εταιρείας στην ηλεκτρονική διεύθυνση www.westernunion.com.

Περισσότερες πληροφορίες σχετικά με το ηλεκτρονικό έγκλημα παρέχονται από την αμερικανική επιτροπή εμπορίου (FTC) στη διεύθυνση: http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html

Θέματα σχετικά με κληρώσεις στο διαδίκτυο

Εάν χρειάζεστε καθοδήγηση σε περίπτωση που σας έχει ζητηθεί να προωθήσετε προκαταβολή για να λάβετε κέρδη από ψευδή κλήρωση ή κάτι παρόμοιο, επισκεφθείτε τη διεύθυνση: http://www.fraudwatchinternational.com/lottery/

Υπόθεση μεταφορικής εταιρείας TNT

Την TNT γνωρίζουμε ότι γίνονται απόπειρες εξαπάτησης των χρηστών του διαδικτύου που πραγματοποιούν τις αγορές τους ηλεκτρονικά, μέσω ιστοσελίδων και μηνυμάτων του ηλεκτρονικού ταχυδρομείου, από άτομα που χρησιμοποιούν παράνομα την ταυτότητα της εταιρείας μας. Τα πλαστά μηνύματα αφορούν συνήθως κάποιο αίτημα προπληρωμής για παραγγελίες αγοράς αγαθών μέσω διαδικτύου, την αποστολή των οποίων φέρεται να έχει αναλάβει η TNT. Ενδέχεται

επίσης να τους ζητείται προπληρωμή των αγορών, ώστε να μπορούν να λάβουν συμμετοχή σε κληρώσεις με δώρα.

Συνιστούμε σε όλους τους πελάτες μας να είναι επιφυλακτικοί απέναντι σε τέτοιου είδους αιτήματα, ενώ θα πρέπει να γνωρίζουν ότι η ύπαρξη αριθμού αποστολής (ή αριθμού αναφοράς) δεν συνιστά απαραίτητα απόδειξη ότι πρόκειται για κάποια μεταφορά την οποία έχει αναλάβει η TNT.

Αν έχετε οποιαδήποτε αμφιβολία για την αυθεντικότητα κάποιας επικοινωνίας με την TNT ή αν θέλετε να επιβεβαιώσετε ότι η εταιρεία μας έχει πράγματι αναλάβει αποστολή που απευθύνεται σε εσάς, παρακαλούμε επικοινωνήστε με το τμήμα εξυπηρέτησης πελατών στη χώρα διαμονής σας. Για την Ελλάδα στο 801 11 868 868 και από κινητό στο 210 8905 868

Η TNT καταβάλλει κάθε δυνατή προσπάθεια για την αντιμετώπιση και αποτροπή περιστατικών ηλεκτρονικής απάτης. Το τμήμα εξυπηρέτησης πελατών, το τμήμα ασφάλειας καθώς και η νομική υπηρεσία της εταιρείας μας βρίσκονται σε στενή συνεργασία, με στόχο την ενημέρωσή σας σχετικά με τις απόπειρες εξαπάτησης μέσω διαδικτύου και την καταπολέμησή τους. Επιπλέον, η εταιρεία μας συνεργάζεται με κρατικούς και διεθνείς οργανισμούς (π.χ. εθνικές κυβερνήσεις, Western Union, eBay, Office of Fair Trading) για την καταπολέμηση του εν λόγω προβλήματος.

ΑΣΦΑΛΕΣ ΔΙΑΔΙΚΤΥΟ

Το διαδίκτυο αποτελεί ένα πολύτιμο εργαλείο μάθησης, δια βίου εκπαίδευσης, ενημέρωσης, ψυχαγωγίας και επικοινωνίας, τόσο για τα παιδιά όσο και για τους ενήλικες. Όμως, όπως κάθε εργαλείο, έτσι και το διαδίκτυο αποτελείται από κανόνες χρήσης τους οποίους πρέπει να τηρούμε όλοι για να μπορούμε να χρησιμοποιούμε το διαδίκτυο σωστά και με ασφάλεια.

Οι βασικοί κανόνες για την καλή χρήση του διαδικτύου είναι οι εξής:

-Δεν αποκαλύπτω ποτέ προσωπικές πληροφορίες στο Διαδίκτυο όπως το πραγματικό μου όνομα, τη διεύθυνση της κατοικίας μου κ.α. γιατί ποτέ δεν ξέρω που μπορούν να καταλήξουν. Αντίστοιχα, δε ζητώ από άλλους να αποκαλύψουν προσωπικές πληροφορίες, όσο είμαι ανήλικος.

-Δεν αποκαλύπτω σε κανέναν τον κωδικό πρόσβασης του λογαριασμού που έχω στο διαδίκτυο. Κάποιο άλλο άτομο θα μπορούσε να προσποιηθεί ότι είμαι εγώ στο διαδίκτυο και έτσι να διαβάσει το ηλεκτρονικό μου ταχυδρομείο, να αναρτήσει λανθασμένες ή κακές πληροφορίες κλπ.

-Πρέπει να συμπεριφέρομαι με κανόνες και με ηθική, όπως στον πραγματικό κόσμο.

-Ενημερώνω τους γονείς ή τους δασκάλους μου στην περίπτωση που διαβάσω στο Διαδίκτυο κάτι που με ενοχλεί ή που με κάνει να νοιώθω άβολα, δίχως να διστάσω.

-Ποτέ δεν συναντώ στο φυσικό κόσμο φίλους που γνώρισα στο Διαδίκτυο και που δεν γνωρίζω στον πραγματικό κόσμο. Τα άτομα αυτά δεν είναι πάντοτε αυτά που ισχυρίζονται ότι είναι.

-Εάν κάποιος μου στείλει ένα απρεπές μήνυμα ή μια απρεπή εικόνα ή με παρενοχλεί στο Διαδίκτυο, πρέπει να σταματήσω αμέσως την επικοινωνία μαζί του και να αναφέρω το γεγονός στους γονείς μου ή στους δασκάλους μου για να με βοηθήσουν.

-Εάν κάποιος μου προσφέρει κάτι στο Διαδίκτυο που μου φαίνεται υπερβολικό για να είναι αλήθεια, όπως π.χ. δώρα για συμμετοχή σε διαγωνισμό κ.α., τότε πιθανώς, όντως να μην είναι αληθινό και να πρόκειται για κάποιο τέχνασμα!

-Δεν ενδιαφέρομαι για υλικό που απευθύνεται σε ενηλίκους.

-Εάν βρω κάποια ιστοσελίδα που με τρομάζει, μου φαίνεται περίεργη ή περιέχει ρατσιστικό / εξτρεμιστικό ή άλλο ύποπτο περιεχόμενο, το αναφέρω στους γονείς μου ή στους δασκάλους μου.

-Διασταυρώνω πάντα το υλικό που βρίσκω στο Διαδίκτυο με άλλες πηγές, όπως βιβλία, εφημερίδες, περιοδικά, ρωτώ επίσης τους γονείς μου.

-Αντιμετωπίζω τους άλλους χρήστες του Διαδικτύου με τον ίδιο τρόπο που θα ήθελα να μου φέρονται αυτοί.

-Γνωρίζω ότι το κατέβασμα φωτογραφιών, μουσικής ή βίντεο μπορεί να είναι παράνομο. Γι' αυτό το λόγο ελέγχω εάν μπορώ να το κάνω αυτό στην ιστοσελίδα ή εάν πρέπει να πληρώσω.

Κατ' επέκταση όλοι ξέρουμε ότι το internet είναι ένα μέσο ψυχαγωγίας. Όμως, είναι και αρκετά επικίνδυνο, ειδικά, για τα μικρά παιδιά που το χρησιμοποιούν. Αρκετοί είναι οι κίνδυνοι, όπως ένα μήνυμα απειλητικό, ένα βίντεο ακατάλληλο, ένα παιχνίδι που ασκεί βία κ.α. Όμως για τα παιδιά αλλά και τους ενήλικες ανθρώπους που έχουν facebook και άλλα μέσα επικοινωνίας που συνδέονται άμεσα με το Internet οι κίνδυνοι είναι πολλοί περισσότεροι. Αρχίζουν να επικοινωνούν με αγνώστους και να ανταλλάσσουν στοιχεία που μπορεί να χρησιμοποιηθούν για διάφορους σκοπούς, να συναντηθούν και να ασκήσουν βία πάνω τους ή ακόμα και να τους παρενοχλούν μέσα από την επικοινωνία τους. Γι' αυτό την ώρα που σερφάρουν τα παιδιά καλό είναι να είναι μαζί τους και ένας γονιός και να μη δίνετε τα στοιχεία σας σε αγνώστους. Να προσέχετε και να θυμάστε ότι το internet μπορεί να είναι ψυχαγωγία και να μας ενημερώνει αλλά ποτέ δεν ξέρετε τι κινδύνους μπορεί να κρύβει!

- **Ρώτα γιατί είναι απαραίτητα τα δεδομένα σου** – Σκέψου ποιος είναι αυτός που τα ζητάει. Είναι κάποιος που εμπιστεύεσαι; Πώς πρόκειται να τα χρησιμοποιήσει; Θα τα αποστείλει σε άλλους και, αν ναι, σε ποιους; Αν δεν είσαι σίγουρος για κάτι από όλα αυτά, ρώτα και μάθε πριν διαθέσεις πληροφορίες που σε αφορούν.
- **Σκέψου πριν αποκαλύψεις δεδομένα** – Αν λαμβάνεις γράμματα, e-mails, μηνύματα στο κινητό ή στο Facebook που σου ζητούν πληροφορίες, μην απαντήσεις αν δεν είσαι σίγουρος από ποιον προέρχονται.
- **Διάβαζε προσεκτικά τα «ψιλά γράμματα»** - Κάποιες εταιρείες μπορεί να γράφουν εκεί όρους για την χρησιμοποίηση των δεδομένων σου, π.χ. για διαφημιστικούς σκοπούς. Θυμήσου ότι πρέπει πάντα να δίνεις τη συγκατάθεσή σου γι' αυτό.
- **Διάβαζε την πολιτική ιδιωτικότητας στις ιστοσελίδες που επισκέπτεσαι** – μάθε πώς χρησιμοποιούν τα δεδομένα σου, π.χ. αν εγκαθιστούν αρχεία cookies και αν προωθούν τις πληροφορίες που σε αφορούν σε διαφημιστικές εταιρείες.
- **Εμπιστεύσου το ένστικτό σου** – Αν δεν είσαι σίγουρος για την ασφάλεια μιας ιστοσελίδας ή δεν νιώθεις άνετα με τον τρόπο που πρόκειται να χρησιμοποιηθούν τα προσωπικά σου δεδομένα, προτίμησε κάποια άλλη.
- **Δυσκόλεψε τους… «κακούς»** – Χρησιμοποίησε διαφορετικά συνθηματικά στουςλογαριασμούς σου (π.χ. e-mail, Facebook, Twitter). Διάλεξε συνθηματικά που είναι εύκολο για σένα να θυμάσαι, αλλά δύσκολο για τους άλλους να μαντέψουν.
- **Σκέψου ποιος μπορεί να βλέπει τα δεδομένα σου** – Μην επισκέπτεσαι ιστοσελίδες που δεν θα ήθελες οι άλλοι να γνωρίζουν όταν μοιράζεσαι τον υπολογιστή σου με άλλους.
- **Σκέψου πριν αγοράσεις στο διαδίκτυο** – Χρησιμοποίησε ασφαλείς ιστοσελίδες, στις οποίες φαίνονται καθαρά τα στοιχεία επικοινωνίας της εταιρείας και οι οποίες διαθέτουν πολιτική ιδιωτικότητας. Έλεγχε αν είναι ασφαλές το κανάλι επικοινωνίας π.χ. θα πρέπει η διεύθυνση της σελίδας να ξεκινάει με https και στο πρόγραμμα πλοήγησης στο διαδίκτυο να εμφανίζεται ένα λουκέτο ως εικονίδιο).
- **Θυμήσου να αποσυνδέεσαι από τις ιστοσελίδες**, στις οποίες έχεις εισέλθει/συνδεθεί με χρήση συνθηματικών (π.χ. όταν κάνεις αγορές από το διαδίκτυο ή την ιστοσελίδα κοινωνικής δικτύωσης).
- **Κράτα τον υπολογιστή σου ασφαλή** – Χρησιμοποίησε προγράμματα τείχους ασφαλείας (firewall) και προστασίας από ιούς (antivirus). Φρόντισε τα προγράμματα αυτά να είναι ενημερωμένα.

ΥΠΟΚΛΟΠΗ ΤΑΥΤΟΤΗΤΑΣ

Υποκλοπή ταυτότητας είναι όταν κάποιος παίρνει τα προσωπικά σας δεδομένα και παριστάνει ότι είναι εσείς για προσωπικό (συχνά οικονομικό) κέρδος.

Εγκληματίες κλέβουν την ταυτότητά σας για ν' ανοίξουν, παραδείγματος χάρη, τραπεζικούς λογαριασμούς ή για να πάρουν πιστωτικές κάρτες, διαβατήρια, συμβόλαια κινητής τηλεφωνίας και άλλα έγγραφα στο όνομά σας.

Εκτός από το να βρίσκουν προσωπικά δεδομένα στον πραγματικό κόσμο (παίρνοντας για παράδειγμα έγγραφα από τα σκουπίδια σας ή κλέβοντας την αλληλογραφία, το πορτοφόλι ή το τσαντάκι σας), εγκληματίες χρησιμοποιούν όλο και πιο πολύ την τεχνολογία για να κάνουν ευκολότερη την υποκλοπή ταυτότητας.

Στέλνουν email που ισχυρίζονται πως είναι από την τράπεζά σας και σας ζητούν να επιβεβαιώσετε τα στοιχεία του λογαριασμού σας και τον κωδικό πρόσβασής σας· στήνουν παραπλανητικούς ιστοτόπους και επιλέγουν, ως στόχο τους, χρήστες κινητού που έχουν Bluetooth στο τηλέφωνό τους.

Μια έρευνα το 2010 αποκάλυψε ότι η ραγδαία αύξηση των «έξυπνων» τηλεφώνων (smartphones) κάνει τους ανθρώπους ευάλωτους, με το 67% αυτών που έχουν πρόσβαση στο διαδίκτυο από το κινητό τους να μην χρησιμοποιεί κωδικό πρόσβασης ή αριθμό PIN. Τα «έξυπνα» τηλέφωνα (smartphones) θα πρέπει να αντιμετωπίζονται ως μίνι φορητός υπολογιστής. Αν σας κλέψουν το κινητό, ο κλέφτης ίσως έχει πρόσβαση στα email σας, το προφίλ σας κοινωνικής δικτύωσης ή ακόμα και το διαδικτυακό τραπεζικό λογαριασμό σας.