4

Ενημέρωση του καταναλωτή

για την προστασία από το
ηλεκτρονικό έγκλημα

* δική μας ευθύνη η δική σας
Ενημέρωση!

μια αρχή για όλους
ΣΥΝΗΓΟΡΟΣ ΤΟΥ ΚΑΤΑΝΑΛΩΤΗ
Ανεξάρτητη Αρχή

Τί πρέπει να γνωρίζουν οι καταναλωτές για την προστασία τους από το ηλεκτρονικό έγκλημα

ΣΥΝΗΓΟΡΟΣ ΤΟΥ ΚΑΤΑΝΑΛΩΤΗ
Ανεξάρτητη Αρχή

Πρόλογος

Η ψηφιακή επανάσταση που συντελείται στην εποχή μας χάρη στην σύγκλιση πληροφορικής, οπτικοακουστικών και τηλεπικοινωνιών ευνοεί την ολοένα αυξανόμενη διείσδυση των ηλεκτρονικών επικοινωνιών στην καθημερινότητα των πολιτών. Το νέο ψηφιακό περιβάλλον διευκολύνει την εξ αποστάσεως σύναψη συναλλαγών εκ μέρους των πολιτών - καταναλωτών με οικονομία χρόνου και χρήματος. Μεταξύ αυτών περιλαμβάνονται συναλλαγές με το Δημόσιο, υποβολή φορολογικών δηλώσεων και ΦΠΑ, ηλεκτρονικές κρατήσεις και αγορές εισιτηρίων μεταφοράς και θεαμάτων, ηλεκτρονικές πληρωμές, τηλε-αγορές, διαχείριση μέσω διαδικτύου τραπεζικών λογαριασμών (web banking), τηλε-ιατρική, πρόσβαση σε χρηστικές υπηρεσίες πληροφοριών ή σε υπηρεσίες διασκέδασης και ψυχαγωγίας.

Η πρόσβαση στον κυβερνοχώρο και η μετάβαση στην Κοινωνία της Πληροφορίας συνεπάγεται πολλαπλά οφέλη για κάθε πολίτη ατομικά και για την εθνική οικονομία συνολικά. Εκτός όμως από την εξοικονόμηση χρόνου και χρήματος που συνεπάγεται, η ανωνυμία του διαδικτύου καλλιεργεί συνθήκες ανάπτυξης νέων μορφών εγκληματικότητας. Σε αυτές ανήκει η διαδικτυακή απάτη, η εξύβριση ή δυσφήμηση τρίτων μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, η εκβίαση μέσω παρανόμως κτηθέντων φωτογραφιών ή προσωπικών δεδομένων, η διασπορά μέσω δικτύων κακόβουλου λογισμικού υπό μορφή «ιών», η κατοχή και διακίνηση απαγορευμένου υλικού παιδικής πορνογραφίας και η υποκλοπή στοιχείων πιστωτικών καρτών με συνέπεια την αθέμιτη χρέωση του κατόχου τους. Στην ίδια κατηγορία παραβατικής συμπεριφοράς εντάσσεται και η δημιουργία ηλεκτρονικών «προφίλ» καταναλωτών μέσω ανάλυσης των επισκέψεων αυτών σε ιστοσελίδες με συνέπεια την προς αυτούς μαζική αποστολή ανεπιθύμητης εμπορικής αλληλογραφίας, η προσβολή πνευματικών δικαιωμάτων, η πειρατεία λογισμικού και ονομάτων χώρου, η μεταφορά κεφαλαίων μέσω υποκλοπής κωδικών από τον τραπεζικό λογαριασμό του ανύποπτου καταναλωτή στους λογαριασμούς των εισβολέων.

Σε σοβαρές περιπτώσεις ηλεκτρονικού εγκλήματος, οι οποίες όμως βρίσκονται εκτός πλαισίου αναφοράς του παρόντος Οδηγού, εντάσσονται ακόμα τρομοκρατικές επιθέσεις με αθέμιτη διείσδυση τρίτων σε πληροφοριακά συστήματα κρατικών επιχειρήσεων και οργανισμών κοινής ωφελείας. Αυτές έχουν ως συνέπεια την υποκλοπή από τον εχθρό κρατικών ή στρατιωτικών απορρήτων, την παράλυση ζωτικών λειτουργιών στους τομείς της ενέργειας, των μεταφορών ή των επικοινωνιών, ή τη βιομηχανική κατασκοπεία.

Ο Συνήγορος του Καταναλωτή, ανταποκρινόμενος στο θεσμικό καθήκον του για την υπεύθυνη ενημέρωση των πολιτών και την προστασία τους από αθέμιτες και παράνομες προσβολές της προσωπικότητας και της οικονομικής τους ελευθερίας, προχώρησε στην σύνταξη του παρόντος Οδηγού Προστασίας

του Καταναλωτή από το Ηλεκτρονικό Έγκλημα. Ο οδηγός είχε εκπονηθεί με επιμέλεια του κ. Γιάννη Αδαμόπουλου και επικαιροποιήθηκε με φροντίδα του διαδόχου του κ. Ευάγγελου Ζερβέα. Στόχος της Αρχής μας είναι να συμβάλλει, ανεξάρτητα από τα πρόσωπα που εκάστοτε την στελεχώνουν, στην ευαισθητοποίηση του οικιακού καταναλωτή για τα οφέλη αλλά τους κινδύνους που απορρέουν από τη χρήση του διαδικτύου. Επιπλέον, με τον Οδηγό αυτό ο Συνήγορος του Καταναλωτή αποσκοπεί να ενημερώσει τους καταναλωτές, με απλό τρόπο, για τις δυνατότητες τεχνικής και νομικής προστασίας τους σε περίπτωση προσβολής των δικαιωμάτων τους, με στόχο την εξώδικη επίλυση των διαφορών τους με προμηθευτές και τρίτους και την ενίσχυση της ασφάλειας των συναλλαγών στην Κοινωνία της Πληροφορίας.

Σεπτέμβριος 2008
Ο Συνήγορος του Καταναλωτή
Ευάγγελος Ζερβέας

Τι είναι το Ηλεκτρονικό έγκλημα;

Πρόκειται για μια εγκληματική και παράνομη πράξη προσβολής περιουσιακών ή άλλων δικαιωμάτων φυσικών και νομικών προσώπων που γίνεται μέσω της χρήσης μιας οποιασδήποτε συσκευής ηλεκτρονικής επεξεργασίας δεδομένων. Μέσο τέλεσης της πράξης μπορεί να είναι ένας ηλεκτρονικός υπολογιστής συνδεδεμένος σε ένα δίκτυο επικοινωνιών όπως το διαδίκτυο (ίντερνετ) ή άλλη τερματική συσκευή, όπως ένα σταθερό ή κινητό τηλέφωνο.

Το ηλεκτρονικό έγκλημα, για το οποίο έχουν δοθεί διεθνώς πολλοί ορισμοί (computer crime, cyber-crime, hitech-crime) εκδηλώνεται τόσο στο συμβατικό περιβάλλον, όσο και σε χώρους που χρησιμοποιούνται δίκτυα υπολογιστών. Η τέλεση του εγκλήματος επιτυγχάνεται με την αθέμιτη παράκαμψη των μέτρων ασφαλείας και την εκ αποστάσεως διείσδυση τρίτων σε πληροφοριακά συστήματα επιχειρήσεων ή οργανισμών (hacking, cracking). Η πράξη αυτή έχει συνήθως ως στόχο την καταστροφή αρχείων ή την αποκομιδή αθέμιτου περιουσιακού οφέλους του προσβολέα σε βάρος του θιγομένου φυσικού ή νομικού προσώπου, επιχείρησης ή ιδιώτη, ενώ δεν αποκλείονται περαιτέρω κίνδυνοι για την υγεία, την ασφάλεια ακόμα και για την ίδια τη ζωή του θύματος, ιδιαίτερα δε των ανηλίκων.

Ποιες οι μορφές του ηλεκτρονικού εγκλήματος;

Οι μορφές του «ηλεκτρονικού εγκλήματος» ποικίλουν. Η αντικειμενική υπόστασή του πληρούται με διάφορους τρόπους, ανάλογα με το περιβάλλον στο οποίο εκδηλώνεται και τα τεχνικά μέσα που χρησιμοποιούνται για τη διάπραξή του. Μία συσκευή όπως ο υπολογιστής ή το κινητό τηλέφωνο μπορεί κατά περίπτωση να είναι μέσο διάπραξης ενός αδικήματος (π.χ. πρόσβαση σε παράνομο ρατσιστικό ή πορνογραφικό υλικό, μέσο εξύβρισης, δυσφήμησης, απειλής, εκβίασης, προσβολής απορρήτων, ή διασποράς ιών) ή να γίνεται η ίδια η συσκευή στόχος της εγκληματικής επίθεσης (αθέμιτη πρόσβαση, υποκλοπή και αλλοίωση δεδομένων, αθέμιτη χρέωση λόγω τηλεπικοινωνιακής απάτης, καταστροφή λειτουργικών προγραμμάτων, παγίδευση ζωτικών λειτουργιών συστημάτων ελεγχομένων από υπολογιστή κλπ). Το διαπραττόμενο αδίκημα μπορεί να συνίσταται νομικά σε απάτη, πλαστογραφία, παράνομη πρόσβαση, αθέμιτη παγίδευση, αθέμιτη επέμβαση σε σύστημα η δεδομένα, υποκλοπή στοιχείων, παραβίαση κρατικών ή ιδιωτικών απορρήτων. Μπορεί ακόμα να συνιστά αδικήματα σε σχέση με το διακινούμενο επιβλαβές και παράνομο περιεχόμενο (ρατσισμός, τρομοκρατία, παιδική πορνογραφία…), προσβολές πνευματικής ή βιομηχανικής ιδιοκτησίας επί έργων και προϊόντων της διανοίας τρίτων κλπ.

Ο παρών συνοπτικός ενημερωτικός Οδηγός αφορά αποκλειστικά τις μορφές εγκληματικότητας που θίγουν κατά

βάση τον απλό οικιακό καταναλωτή εξ αντιδιαστολής με τρομοκρατικές επιθέσεις που θίγουν κρίσιμες υποδομές κυβερνήσεων, κρατικών οργανισμών ή επιχειρήσεων. Για την αντιμετώπιση τέτοιων απειλών απαιτείται μια συνολική και συντονισμένη πολιτική ασφαλείας που η οριοθέτησή της βρίσκεται προδήλως εκτός πλαισίου αναφοράς του Οδηγού μας.

Όπως προαναφέρθηκε, πολλές εγκληματικές πράξεις βρίσκουν πρόσφορο έδαφος να εκδηλωθούν στο χώρο του διαδικτύου. Πράγματι, ο «δικτυωμένος» καταναλωτής που έχει πρόσβαση στον κυβερνοχώρο, αφήνει πίσω του «ηλεκτρονικά ίχνη», όπως διευθύνσεις ηλεκτρονικού ταχυδρομείου, αριθμούς μητρώων κοινωνικής ασφάλισης, στοιχεία αγορών, πιστωτικών καρτών κλπ.

Τα προσωπικά αυτά δεδομένα συλλέγονται επιμελώς μέσω διαφόρων μεθόδων και αξιοποιούνται κατάλληλα από τους προμηθευτές μέσω δημιουργίας «προφίλ» και ομάδων καταναλωτών ανάλογα με τις προτιμήσεις τους. Στη συνέχεια ο καταναλωτής βομβαρδίζεται κυριολεκτικά από δεκάδες ηλεκτρονικά μηνύματα με προσφορές κάθε είδους αγαθών ή υπηρεσιών. Μεταξύ αυτών περιλαμβάνονται προσφορές πλήθους καταναλωτικών ειδών, καλλυντικών, συμπληρωμάτων διατροφής, σεξουαλικών βοηθημάτων, χαπιών αδυνατίσματος και φαρμακευτικών σκευασμάτων άγνωστης προέλευσης, τα οποία συνήθως δεν διαθέτουν άδεια κυκλοφορίας στην Ελλάδα και έγκριση του ΕΟΦ.

Πολύ συχνά ο καταναλωτής λαμβάνει προσκλήσεις για συμμετοχή σε διαγωνισμούς, να στοιχηματίσει σε ηλεκτρονικά καζίνο, δέχεται δήθεν αναγγελίες κέρδους χρηματικών ποσών σε λοταρίες, όπου του ζητείται η καταβολή των εξόδων μεταφοράς των χρημάτων τα οποία φυσικά ουδέποτε του εμβάζονται. Συνηθισμένη μορφή απάτης, ιδιαίτερα κατά το πρόσφατο παρελθόν, ήταν τα γράμματα και μηνύματα ηλεκτρονικού ταχυδρομείου από τη Νιγηρία. Μέσω αυτών, εγκληματίες εμφανιζόμενοι ως κρατικοί αξιωματούχοι ζητούν τον τραπεζικό λογαριασμό του χρήστη με σκοπό δήθεν την εκ μέρους του διευκόλυνση παράνομης εξαγωγής χρημάτων από τη χώρα με αντάλλαγμα την καταβολή ποσοστού από αυτά. Εάν τυχόν ο χρήστης διαπράξει το λάθος να παράσχει τα στοιχεία, οι κακοποιοί του ζητούν στη συνέχεια να κάνει ο ίδιος κατάθεση ενός ποσού για την ενεργοποίηση του λογαριασμού ή να τους παράσχει εξουσιοδότηση πρόσβασης στον τραπεζικό λογαριασμό του, για να του κάνουν δήθεν την κατάθεση, τον οποίο όμως στην πραγματικότητα αδειάζουν με συνοπτικές διαδικασίες.

Συναφής με την προηγούμενη μορφή απάτης είναι το «ψάρεμα» κωδικών τραπεζικών λογαριασμών (γνωστό ως Phising, και με παραλλαγές ως Vishing και SMishing). Η απάτη αρχίζει μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου, ή σύντομων μηνυμάτων SMS στο κινητό τηλέφωνο του καταναλωτή. Με τα μηνύματα αυτά οι αποστολείς παραπέμπουν τον αποδέκτη σε μία ιστοσελίδα που μοιάζει με την επίσημη ιστοσελίδα της τράπεζας ή τον παρακινούν να καλέσει χωρίς χρέωση ένα τηλεφωνικό αριθμό. Αν το πράξει, ο χρήστης συνδέεται εν αγνοία του με τους εγκληματίες, οι οποίοι δήθεν χάριν ενημέρωσης των αρχείων της τράπεζας, καλούν τον ανύποπτο χρήστη να τους δώσει αριθμούς τηρουμένων λογαριασμών και κωδικούς πρόσβασης. Η συνέχεια είναι γνωστή, οι παράνομοι

εισβολείς αξιοποιούν άμεσα τα πολύτιμα αυτά στοιχεία που υπέκλεψαν για να μεταφέρουν τις καταθέσεις του ανύποπτου καταναλωτή σε λογαριασμούς τους σε εξωτικές χώρες από όπου είναι πρακτικά αδύνατο να ανακτηθούν.

Άλλες μορφές ηλεκτρονικής απάτης συνιστούν πράξεις όπως η διασπορά μέσω ίντερνετ, συνήθως μέσω ιστοσελίδων πορνογραφικού περιεχομένου, ιών, δηλαδή κακόβουλου λογισμικού και κατασκοπευτικών προγραμμάτων (spyware, adware, trojan horses). Αυτά τα δωρεάν παρεχόμενα προγράμματα περιέχουν κρυφές λειτουργίες από αυτές που επισήμως διαφημίζουν ότι κάνουν. Αφού εγκατασταθούν στον υπολογιστή του χρήστη, τον παρακολουθούν κρυφά κατά την πλοήγησή του στο διαδίκτυο, είτε για εμπορικούς σκοπούς (όπως τα λεγόμενα cookies που υπάρχουν σε συγκεκριμένες ιστοσελίδες που επισκέπτεται), είτε ανοίγουν ως «δούρειος ίππος» κερκόπορτα πρόσβασης του εισβολέα στα αρχεία του χρήστη του οποίου υποκλέπτουν συστηματικά τις επικοινωνίες. Τέτοια λειτουργία επιτελούν και οι λεγόμενοι dialers, που εγκαθίστανται στον υπολογιστή του χρήστη και διακόπτουν την κανονική (dial up) και με κόστος αστικής κλήσης επικοινωνία για να πραγματοποιήσουν μέσω του modem του διεθνείς κλήσεις σε αριθμούς υψηλής χρέωσης του εξωτερικού, τις οποίες ο ανύποπτος καταναλωτής διαπιστώνει εκ των υστέρων μόλις λάβει τον αναλυτικό τηλεφωνικό λογαριασμό. Η χρήση υπηρεσιών μόνιμης σύνδεσης τύπου DSL αποτρέπει αυτό το ενδεχόμενο.

Κίνδυνοι μπορούν ακόμα να ελλοχεύουν και σε ομάδες συζήτησης (chatrooms, newsgroups), όπου η ανωνυμία επιτρέπει σε εγκληματίες να εμφανίζονται υπό άλλη ιδιότητα, ηλικία ή φύλο, προσελκύοντας σε συνάντηση μέσω διαλόγου ανηλίκους για άνομους σκοπούς παιδικής πορνογραφίας, εμπορίας οργάνων, σατανισμού, διάδοσης ναζιστικού και εξτρεμιστικού πολιτικού υλικού και ούτω καθεξής.

Ποιες οι συνέπειες του ηλεκτρονικού εγκλήματος για τον καταναλωτή;

Οι δυσμενείς κοινωνικές και οικονομικές συνέπειες του ηλεκτρονικού εγκλήματος είναι πολλαπλές για τους πολίτες, ιδιαίτερα δε τους ανηλίκους. Καθημερινά σχεδόν γίνεται λόγος στα ελληνικά και διεθνή ΜΜΕ για περιπτώσεις σεξουαλικής εκμετάλλευσης παιδιών και εφήβων που προσελκύονται μέσω φόρουμ συζήτησης του διαδικτύου και καταλήγουν να υφίστανται σοβαρές προσβολές της προσωπικότητας, της τιμής, της γενετήσιας αξιοπρέπειας, ακόμα και της ζωής τους.

Η παρότρυνση των καταναλωτών, μέσω παραπλανητικών διαφημίσεων και απαγορευμένων εμπορικών πρακτικών, ήτοι αποστολής, χωρίς τη συναίνεση του χρήστη, ανεπιθύμητων μηνυμάτων (γνωστών ως spam) να αγοράσουν άγνωστης προέλευσης, διατροφικής αξίας και αμφίβολης ποιότητας προϊόντων και υπηρεσιών, μπορεί να βλάψει την υγεία, την ασφάλεια και την οικονομικά συμφέροντα των καταναλωτών.

Η αθέμιτη πρόσβαση τρίτων εισβολέων σε κωδικούς τραπεζικών λογαριασμών μέσω web banking συνεπάγεται την υπεξαίρεση των ποσών των καταθέσεων και τη

μεταφορά αποταμιευτικών κεφαλαίων του καταναλωτή τράπεζες του εξωτερικού και στη συνέχεια στις τσέπες των εγκληματιών.

Η υποκλοπή μέσω διαδικτύου στοιχείων πιστωτικών καρτών των γονέων παιδιών και εφήβων έχει ως συνέπεια την αθέμιτη χρέωση των γονέων, της οποία όμως οι γονείς ανακαλύπτουν πολύ αργότερα μαζί με το εκκαθαριστικό του λογαριασμού που λαμβάνουν από την τράπεζα.

Είναι γεγονός ότι ο κάτοχος της κάρτας, βάσει της νομοθεσίας, μπορεί να αρνηθεί τη χρέωση οποιασδήποτε συναλλαγής έχει πραγματοποιηθεί χωρίς την παρουσίαση του φυσικού σώματος της κάρτας. Συνεπώς, σε περίπτωση on line συναλλαγής με κλεμμένα στοιχεία καρτών, ο νόμιμος κάτοχος μπορεί να αρνηθεί την καταβολή του αντιτίμου, οπότε η τράπεζα κανονικά δεν θα καταβάλει το ποσό στον πωλητή αλλά κανονικά θα χρεώσει το κατάστημα με τα έξοδα ακύρωσης της συναλλαγής.

Η συλλογή στοιχείων επικοινωνίας και προσωπικών δεδομένων των χρηστών, τα οποία χρησιμοποιούνται συχνά χωρίς τη συναίνεση των υποκειμένων, είτε από τους ίδιους τους προμηθευτές είτε διαβιβάζονται έναντι αντιτίμου σε τρίτους για προωθητικές ενέργειες μέσω αποστολής μαζικών SMS και MMS, έρευνες αγοράς, direct marketing, απαγορεύεται από τη νομοθεσία καθότι προσβάλλει την ιδιωτική ζωή του ατόμου.

Τι προβλέπει η νομοθεσία για την πάταξη της ηλεκτρονικής εγκληματικότητας;

Η αντιμετώπιση της ηλεκτρονικής εγκληματικότητας, ανάλογα με τη μορφή που αυτή λαμβάνει, μπορεί να γίνει από το Ελληνικό δίκαιο συνδυάζοντας διάσπαρτες διατάξεις της κείμενης νομοθεσίας. Σε αυτές ανήκουν οι διατάξεις του Ποινικού Κώδικα περί απάτης με τη χρήση υπολογιστή, περί αθέμιτης πρόσβασης σε συστήματα πληροφοριών, υποκλοπής και παραβίασης απορρήτων, η ειδική νομοθεσία περί προστασίας προσωπικών δεδομένων (ν. 2472/1997 όπως τροποποιήθηκε με το ν. 3625/2007, ν. 3471/2006), η νομοθεσία περί διασφάλισης του απορρήτου των επικοινωνιών (ν. 3674/2008), οι κανονιστικές αποφάσεις διοικητικών αρχών όπως η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ), η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ), η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) και ούτω καθεξής.

Ειδικότερα, το άρθρο 5 του ν. 1805/1988, προσέθεσε στο άρθρο 386 του Ποινικού Κώδικα περί απάτης το ειδικό άρθρο 386Α που αναφέρεται στην απάτη με υπολογιστή. Σύμφωνα με το άρθρο αυτό, όποιος, με σκοπό να προσπορίσει στον εαυτό του ή σε άλλον παράνομο περιουσιακό όφελος βλάπτει ξένη περιουσία, επηρεάζοντας τα αρχεία 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 φυλάκισης που προβλέπονται για την απάτη. Ανάλογα

με τη βαρύτητα του αδικήματος, οι ποινές αυτές μπορούν να ανέρχονται από φυλάκιση τουλάχιστον τριών μηνών έως φυλάκιση τουλάχιστον τριών ετών αν η ζημία που προκλήθηκε είναι ιδιαίτερα μεγάλη.

Υπό συγκεκριμένες προϋποθέσεις, η διαδικτυακή εγκληματικότητα, στο μέτρο που οδηγεί σε παραβίαση του απορρήτου των τηλεφωνημάτων και της προφορικής συνομιλίας, παραβίαση επαγγελματικών απορρήτων ή παράνομη αντιγραφή προγραμμάτων ηλεκτρονικού υπολογιστή, τιμωρείται και από τα άρθρα 370Α και 370Β του Ποινικού Κώδικα, που προβλέπουν αντίστοιχες ποινές φυλάκισης κατά των δραστών.

Πρόσφατα, ο νόμος 3674/2008 ψηφίστηκε για να ενισχύσει το θεσμικό πλαίσιο διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας, θεσπίζοντας ειδικές υποχρεώσεις του παρόχου υ-πηρεσιών για την ασφάλεια δικτύου και συγκεκριμένες διαδικασίες άρσης του απορρήτου υπό την εποπτεία της ΑΔΑΕ. Παράλληλα, ο νόμος αυτός προσέθεσε νέο άρθρο 292Α στον Ποινικό Κώδικα που τιμωρεί τα εγκλήματα κατά της ασφάλειας των τηλεφωνικών επικοινωνιών με φυλάκιση τουλάχιστον ενός έτους και χρηματικές ποινές που αρχίζουν από είκοσι χιλιάδες (20.000) Ευρώ και αυξάνονται ανάλογα με τη βαρύτητα του παραπτώματος και την ιδιότητα του δράστη. Ο ίδιος νόμος τροποποίησε ακόμα το άρθρο 370Α του Ποινικού Κώδικα θεσπίζοντας αυστηρές κυρώσεις, που μπορούν να φθάσουν ως κάθειρξη μέχρι δέκα ετών για όσους παραβιάζουν το απόρρητο της τηλεφωνικής επικοινωνίας και της προφορικής συνομιλίας. Τέλος, θέσπισε διοικητικές κυρώσεις (χρηματικά πρόστιμα, ανάκληση αδειών κλπ) κατά των εκπροσώπων εταιριών παροχής υπηρεσιών ηλεκτρονικών επικοινωνιών.

Προς την ίδια κατεύθυνση, το άρθρο 348 Α του Ποινικού κώδικα, που προστέθηκε με το άρθρο 6 του ν. 3064/2002 τιμωρεί με φυλάκιση και χρηματικές ποινές την πορνογραφία ανηλίκων, οποιοσδήποτε και αν είναι ο υλικός φορέας αποτύπωσης του πορνογραφικού υλικού.

Παρόμοιες κυρώσεις προβλέπονται από την ισχύουσα ειδική νομοθεσία περί προστασίας καταναλωτή, σε ότι αφορά ειδικότερα τις εξ αποστάσεως συμβάσεις πρόσβασης σε υπηρεσίες ηλεκτρονικού εμπορίου. Η νομοθεσία αυτή απαγορεύει τις παραπλανητικές εμπορικές πρακτικές (ν. 2251/1994 όπως ισχύει μετά την τροποποίηση του από το ν. 3587/2007), ενώ προβλέπει επίσης διοικητικές κυρώσεις κατά των παραβατών.

Αντίστοιχες διοικητικές, αστικές και ποινικές κυρώσεις προβλέπονται επίσης κατά των παραβατών, όπως προαναφέρθηκε, από τη νομοθεσία περί προστασίας προσωπικών δεδομένων (ν. 2472/1997 όπως ισχύει και 3471/2006). Τέτοιες πράξεις ηλεκτρονικής παραβατικότητας μπορούν ακόμα να συνιστούν πλαστογραφία, εξύβριση,

δυσφήμιση, προσβολή της νομοθεσίας περί απορρήτου, του ν. 2121/1993 περί πνευματικής ιδιοκτησίας ή του ν. 3431/2006 περί ηλεκτρονικών επικοινωνιών. Στην Ελλάδα το spam ρυθμίζεται από το αρ. 11 του ν. 3471/2006, ο οποίος ενσωμάτωσε στο εθνικό δίκαιο την Οδηγία 2002/58/ ΕΚ για την προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών. Σύμφωνα με το άρθρο αυτό η χρησιμοποίηση αυτόματων συστημάτων κλήσης, ιδίως με χρήση συσκευών τηλεομοιοτυπίας (φαξ) ή ηλεκτρονικού ταχυδρομείου, και γενικότερα η πραγματοποίηση μη ζητηθεισών επικοινωνιών με οποιοδήποτε μέσο ηλεκτρονικής επικοινωνίας, με ή χωρίς ανθρώπινη παρέμβαση, για σκοπούς απευθείας εμπορικής προώθησης προϊόντων ή υπηρεσιών και για κάθε είδους διαφημιστικούς σκοπούς, επιτρέπεται μόνο αν ο συνδρομητής συγκατατεθεί εκ των προτέρων ρητώς.

Εκτός από την ποινική προστασία και την ειδική νομοθεσία του τομέα που προβλέπει προσφυγή στις αρμόδιες αρχές, ο χρήστης που έπεσε θύμα ηλεκτρονικής απάτης μπορεί θεωρητικά να στραφεί δικαστικά κατά του προσβολέα ζητώντας αποζημίωση με βάση το άρθρο 914 του Αστικού Κώδικα περί αδικοπραξίας.

Πλην όμως, στις περισσότερες περιπτώσεις εγκλημάτων του κυβερνοχώρου, η ταυτότητα και η χώρα εγκατάστασης των προσβολέων είναι άγνωστη ενώ οι δράστες εξαφανίζονται μετά την εγκληματική πράξη τους. Επίσης ο τόπος διάπραξης του κυβερνο-εγκλήματος είναι συχνά αμφισβητούμενος, αν π.χ. η τεχνική υποδομή τέλεσης του εγκλήματος, ήτοι ο εξυπηρετητής (server) που φιλοξενεί την απατηλή ιστοσελίδα είναι εγκατεστημένος στην αλλοδαπή, οπότε είναι ενδεχόμενο να μην μπορούν να εφαρμοστούν οι προβλεπόμενοι Ελληνικοί νόμοι που τιμωρούν αποκλειστικά εγκλήματα τελούμενα στην Ελλάδα.

Η διεθνής διάσταση των εγκλημάτων του κυβερνοχώρου απαιτεί τη διεθνή συνεργασία. Η Διεθνής Σύμβαση του Συμβουλίου της Ευρώπης (Νοέμβριος 2001), που έχει υπογραφεί και από την Ελλάδα, εντάσσεται σε αυτήν την προοπτική. Εκτός όμως ότι δεν έχει ακόμα κυρωθεί από όλες τις χώρες η Σύμβαση αυτή έχει τύχει αρκετής διεθνούς κριτικής για ασάφεια των περιγραφομένων εγκλημάτων και προβλήματα εφαρμογής.

Προς την ίδια κατεύθυνση εντάσσονται οι σχετικές πρωτοβουλίες της Ευρωπαϊκής Ένωσης για την καταπολέμηση διακίνησης επιβλαβούς και παράνομου περιεχομένου μέσω ίντερνετ, που στοχεύουν στη δημιουργία συνθηκών ασφαλούς χρήσης του Διαδικτύου μέσω αυτορρύθμισης και κωδίκων δεοντολογίας. Η πρόληψη υποστηρίζεται επίσης από τη λειτουργία ειδικών τηλεφωνικών γραμμών (hotlines), όπου οι χρήστες μπορούν να καταγγείλουν παραβατική συμπεριφορά προς τις αρμόδιες διωκτικές αρχές των κρατών- μελών. Ο Ευρωπαϊκός Οργανισμός για την ασφάλεια ENISA, έχει επίσης εκδώσει δύο εκθέσεις για την ασφάλεια και μέτρα καταπολέμησης της ανεπιθύμητης εμπορικής επικοινωνίας που εφαρμόζουν οι Πάροχοι Υπηρεσιών Διαδικτύου στην Ευρώπη.

Παρά τη διεθνή κινητοποίηση και συνεργασία, η δυσκολία εντοπισμού των δραστών, η πιθανή αρνητική δημοσιότητα για το θύμα που συνοδεύει τη δημοσιοποίηση

περιπτώσεων ηλεκτρονικής απάτης, σε συνδυασμό με την μικρή ταχύτητα ενεργοποίησης των διωκτικών μηχανισμών και απονομής δικαιοσύνης, καθώς και το κόστος της, είναι συνήθως αποτρεπτικοί παράγοντες διεκδίκησης της βλάβης από τον ζημιωθέντα καταναλωτή. Για το λόγο αυτό, η πρόληψη, η ευαισθητοποίηση και η λήψη μέτρων προστασίας κατά του ηλεκτρονικού εγκλήματος από τον συνειδητοποιημένο καταναλωτή είναι προτιμότερη από την καταστολή τέτοιων πράξεων σε βάρος των συμφερόντων του.

Ποια τα μέσα προστασίας του καταναλωτή από το ηλεκτρονικό έγκλημα ;

Με δεδομένη την δυσκολία εντοπισμού και τιμωρίας των δραστών από διάφορες κατά περίπτωση αρμόδιες αρχές, ο καταναλωτής μπορεί ο ίδιος να λάβει στοιχειώδη μέτρα τεχνικής προστασίας του και να ακολουθήσει κάποιους στοιχειώδεις κανόνες αυτοπροστασίας του κατά την πλοήγηση στο διαδίκτυο και τη διενέργεια ηλεκτρονικών συναλλαγών.

Εφόσον το επιθυμεί, ο καταναλωτής έχει δικαίωμα να χρησιμοποιεί υπηρεσίες ανωνυμοποιημένης πρόσβασης, ώστε τα ίχνη της δικτυακής του παρουσίας να μη μπορούν να χρησιμοποιηθούν για σκοπό που δεν έχει επιλέξει.

Σήμερα οι περισσότεροι δικτυακοί τόποι παρέχουν ενημέρωση σχετικά με τα προσωπικά δεδομένα που συλλέγουν και επεξεργάζονται. Η ενημέρωση αυτή είναι ταυτόχρονα υποχρέωση των υπευθύνων των δικτυακών τόπων αλλά και δικό μας δικαίωμα.

Επίσης, ο ενημερωμένος καταναλωτής οφείλει να προτιμά αναγνωρισμένα και επώνυμα ηλεκτρονικά καταστήματα αντί να συνδέεται με άγνωστες και ύποπτης προέλευσης ιστοσελίδες, ακόμα και αν προσφέρουν ελκυστικές τιμές.

Ακόμα, πριν από κάθε παραγγελία, οφείλει να λαμβάνει γνώση των ακριβών όρων χρήσης της κάθε υπηρεσίας και των ακριβών όρων συναλλαγής (τελικές χρεώσεις, χρόνοι παράδοσης, όροι υπαναχώρησης, πολιτική επιστροφών, πολιτική ασφαλείας, πληρωμών κλπ).

Συνιστάται επίσης στον καταναλωτή να εγκαθιστά στον προσωπικό υπολογιστή του λογισμικό προστασίας από ιούς (antivirus, firewalls), και να προτιμά ασφαλείς και κρυπτογραφημένες συνδέσεις πιστοποιημένων και γνωστών προμηθευτών, ιδιαίτερα όταν τους χορηγεί δεδομένα πληρωμών. Η χρήση μεθόδων κρυπτογραφίας, ψηφιακών πιστοποιητικών και διατάξεων προηγμένης ηλεκτρονικής υπογραφής παρέχει επιπρόσθετα εχέγγυα ασφαλείας.

Είναι συνετό ο καταναλωτής να χρησιμοποιεί ως μέσο πληρωμών χρεωστικές κάρτες αγορών μέσω διαδικτύου. Αυτές παρέχονται από τις τράπεζες ως ηλεκτρονικά πορτοφόλια και δίνουν τη δυνατότητα στον καταναλωτή να καταθέτει σε ένα ανεξάρτητο λογαριασμό ένα ποσό για αγορές μέσω διαδικτύου. Οι χρεωστικές κάρτες αγορών παρέχουν την ασφάλεια ενός ανωτάτου ορίου χρέωσης, αντί της θεωρητικά απεριόριστης χρέωσης που μπορεί να προκύψει για τον καταναλωτή σε περίπτωση υποκλοπής στοιχείων της πιστωτικής του κάρτας.

Απαγορεύεται ρητά στον χρήστη να παρέχει προσωπικές πληροφορίες και τραπεζικούς

κωδικούς σε τρίτους μέσω ηλεκτρονικού ταχυδρομείου, που εξ ορισμού δεν αποτελεί ασφαλή επικοινωνία.

Συνιστάται ακόμα στον χρήστη να μην απαντά σε μηνύματα άγνωστης προέλευσης, τα οποία του ανακοινώνουν κάποιο κέρδος ή κάποια εξαιρετική προσφορά, αφού το πιθανότερο είναι αυτά να στοχεύουν στην εξαπάτησή του. Ομοίως, ο χρήστης πρέπει να αποφεύγει να ανοίγει συνημμένα αρχεία σε μηνύματα ηλεκτρονικού ταχυδρομείου προερχόμενα από άγνωστο αποστολέα, διότι είναι πιθανό να περιέχουν ιούς.

Οι γονείς των ανήλικων καταναλωτών έχουν επίσης την υποχρέωση εποπτείας και επιμέλειας των τέκνων τους, τα οποία δεν πρέπει να κάνουν ανεξέλεγκτη χρήση του υπολογιστή, που πρέπει να είναι εγκατεστημένος σε ελεγχόμενο χώρο. Χρήσιμη είναι επίσης η εγκατάσταση ειδικού λογισμικού, ως φίλτρου ελεγχόμενης πρόσβασης των παιδιών σε ιστοσελίδες που ενδεχομένως περιέχουν χυδαίες λέξεις και επιβλαβές και παράνομο περιεχόμενο για τους ανηλίκους (όπως ρατσισμός, τρομοκρατία, πορνογραφία) και συμμετοχής σε ομάδες συζήτησης (chatrooms) με άγνωστα άτομα καλυπτόμενα υπό ψευδώνυμο.

Αν παρά τα προληπτικά μέτρα γνώσης και ευαισθητοποίησης, καταναλωτής, γονέας ή ένωση καταναλωτών τυχόν διαπιστώσουν ότι δεν τηρείται από κάποιον πάροχο υπηρεσιών οποιαδήποτε από τις παραπάνω αρχές ως προς το περιεχόμενο, τη διαφήμιση, τη χρέωση, την πρόσβαση στην υπηρεσία, την προστασία προσωπικών δεδομένων κ.ο.κ., μπορούν να πράξουν τα εξής :
Να επικοινωνήσουν με τον πάροχο υπηρεσιών διαδικτύου καταγγέλλοντας το περιστατικό και ζητώντας τις διευθύνσεις αποστολής των μηνυμάτων.

Να αναστείλουν την πρόσβαση στον υπολογιστή και να ειδοποιήσουν αμέσως την αστυνομία και τις αρμόδιες διωκτικές αρχές.

Να ειδοποιήσουν την Ομάδα Ψηφιακής Ασφάλειας με το ακρωνύμιο D.A.R.T (Digital Awareness & Response to Threats), στην ηλεκτρονική διεύθυνση http://www.dart.gov.gr. Πρόκειται για μια κοινή προσπάθεια των συναρμόδιων φορέων, όπως η Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ), η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) και το Σώμα Δίωξης Ηλεκτρονικού Εγκλήματος της Ασφάλειας, με στόχο την αντιμετώπιση κινδύνων από χρήση τεχνολογίας ηλεκτρονικών επικοινωνιών.

Να καταθέσουν αναφορά-καταγγελία στον Συνήγορο του Καταναλωτή, ο οποίος είτε θα την εξετάσει ο ίδιος, αν εμπίπτει στην αρμοδιότητά του, καλώντας σε ακρόαση τα εμπλεκόμενα μέρη, όταν αυτό είναι εφικτό, είτε θα τη διαβιβάσει στα αρμόδια διωκτικά όργανα και ανεξάρτητες διοικητικές αρχές.

Ο τρόπος υποβολής καταγγελίας στον Συνήγορο του Καταναλωτή είναι ο ακόλουθος :
α) Τηλεφωνικά στους αριθμούς:
210 6460814, 210 6460284 και
210 6460 276
β) Μέσω συμπλήρωσης και υποβολής, με αυτοπρόσωπη παρουσία, με συστημένη επιστολή, τηλεομοιοτυπία ή μήνυμα ηλεκτρονικού ταχυδρομείου, της έντυπης φόρμας υποβολής παραπόνων που διατίθεται από τον διαδικτυακό τόπο του Συνηγόρου του Καταναλωτή http://www.synigoroskatanaloti.gr/

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΣΥΝΗΓΟΡΟΣ ΤΟΥ ΚΑΤΑΝΑΛΩΤΗ

Ανεξάρτητη Αρχή

ΛΕΩΦ. ΑΛΕΞΑΝΔΡΑΣ 144, 114 71 - ΑΘΗΝΑ

ΤΗΛ: 210 6460814, 210 6460284, 210 6460458, 210 6460612

FAX: 2106460414

E-mail: grammateia@synigoroskatanaloti.gr - www.synigoroskatanaloti.gr