Ό,τι πρέπει να γνωρίζετε για την ασφαλή χρήση του Κινητού & του Διαδικτύου

WIND

ΚΙΝΗΤΗ • ΣΤΑΘΕΡΗ • INTERNET

Η επικοινωνία είναι ζήτημα... προσωπικό

Η κινητή τηλεφωνία και το Internet ως μέσα επικοινωνίας αποτελούν σήμερα αναπόσπαστο μέρος της καθημερινότητάς μας. Χάρη στις τεχνολογικές τους δυνατότητες απελευθέρωσαν και εμπλούτισαν την επικοινωνία μας, καταργώντας τα... σύνορα στη διακίνηση ιδεών και την ανταλλαγή πληροφοριών. Ωστόσο, η τεχνολογία εγκυμονεί κινδύνους αν δεν γνωρίζουμε πώς να τη χρησιμοποιούμε με ασφάλεια. Τα βήματα που μπορούμε να κάνουμε για να επικοινωνούμε... ασφαλώς είναι απλά και τα εργαλεία για να προστατευθούμε είναι στη διάθεσή μας.

Κινητή Τηλεφωνία: η υπεύθυνη χρήση της

Μέσω του κινητού μας τηλεφώνου επικοινωνούμε και οργανώνουμε την επικοινωνία μας αποθηκεύοντας στη συσκευή μας χρήσιμες πληροφορίες όπως τις επαφές του τηλεφωνικού καταλόγου, το πρόγραμμα των συναντήσεών μας, προσωπικά μηνύματα, φωτογραφίες κ.ά.

Διασφάλιση των προσωπικών μας δεδομένων

Όπως και οι ηλεκτρονικοί υπολογιστές, έτσι και τα κινητά τηλέφωνα ως ηλεκτρονικές συσκευές είναι ευάλωτα σε παράνομα λογισμικά/ιούς και για το λόγο αυτό, οφείλουμε εμείς ως χρήστες τους να είμαστε ιδιαίτερα προσεκτικοί καθώς η ασφαλής χρήση του κινητού μας τηλεφώνου είναι πρωτίστως δική μας ευθύνη.

Η εγκατάσταση ενός ιού είναι εφικτή μόνο εφόσον ο ίδιος ο χρήστης εγκαταστήσει μόνος του ή μέσω τρίτων μία άγνωστη εφαρμογή στο κινητό του.

Απλές προφυλάξεις για ασφαλή επικοινωνία

Η ασφαλής χρήση του κινητού τηλεφώνου δεν έχει καμία απολύτως σχέση με την ασφάλεια λειτουργίας του δικτύου κινητής τηλεφωνίας, η οποία αναλύεται παρακάτω. Ωστόσο, θεωρούμε σκόπιμο να σας προτείνουμε απλά προληπτικά μέτρα ώστε να προστατεύετε την τηλεφωνική σας συσκευή από εγκατάσταση παράνομων λογισμικών.

Ακολουθώντας τις παρακάτω «προφυλάξεις» θα είστε σίγουροι ότι η συσκευή σας λειτουργεί με ασφάλεια για την επικοινωνία σας:

- Κλείνετε το Bluetooth όταν δεν το χρησιμοποιείτε.
- Μην αποδέχεστε μηνύματα από άγνωστους χρήστες Bluetooth.
- Μην εγκαθιστάτε αρχεία sis στο κινητό σας ούτε και εν γένει άγνωστες εφαρμογές και αρχεία που σας αποστέλλονται μέσω Bluetooth, MMS ή e-mail. Επισημαίνεται ότι το δίκτυο της WIND δεν επιτρέπει μετάδοση αρχείων sis.
- Μην αποθηκεύετε αρχεία ή εφαρμογές στο κινητό τηλέφωνο από άγνωστες ιστοσελίδες WAP ή Internet. Το σύνολο του περιεχομένου και των υπηρεσιών του WIND Plus έχουν ελεγχθεί και είναι ασφαλή στη χρήση, ωστόσο πρέπει να γνωρίζετε ότι από το κινητό σας τηλέφωνο μπορείτε να πλοηγηθείτε ελεύθερα σε ολόκληρο το Internet, λαμβάνοντας όμως όλες τις προφυλάξεις που προβλέπονται για την πλοήγηση στο διαδίκτυο.
- Να θυμάστε ότι το κινητό τηλέφωνο είναι μια προσωπική συσκευή τον έλεγχο της οποίας πρέπει να έχετε αποκλειστικά εσείς. Συστήνουμε να μην τη «δανείζετε» σε τρίτα πρόσωπα και να μην επιτρέπετε τη χρήση της από τρίτους αν δεν είστε μπροστά.
- Θα πρέπει να σβήνουμε συζεύξεις με συσκευές τρίτων ή παλαιότερες που δεν χρησιμοποιούμε πια, εφόσον έχουν εξυπηρετήσει το σκοπό σύζευξής τους.

- Πραγματοποιείτε «επαναφορά στις εργοστασιακές ρυθμίσεις» της συσκευής (format) αν, παρ' όλα αυτά, έχετε βάσιμες υποψίες ότι κάποιος ιός έχει εγκατασταθεί.
- Μην απενεργοποιείτε το PIN και επιλέγετε PIN που να μην είναι «εύκολο» το οποίο να το αλλάζετε συχνά.

Η ασφάλεια του δικτύου κινητής τηλεφωνίας WIND

Όπως προαναφέραμε, η χρήση του κινητού τηλεφώνου με ασφάλεια είναι υπόθεση του καθενός μας εφόσον πρόκειται για μια προσωπική ηλεκτρονική συσκευή. Από την άλλη πλευρά, η ασφάλεια της επικοινωνίας μας μέσω του δικτύου κινητής τηλεφωνίας είναι υπόθεση του παρόχου με τον οποίο συνεργαζόμαστε.

Έτσι, η WIND Ελλάς σάς ενημερώνει ότι η υποδομή ασφάλειας στο δίκτυό της βασίζεται στο διεθνές πρότυπο ασφάλειας ISO 27001. Αναλυτικότερα, η αρχιτεκτονική ασφάλειας των πληροφοριακών και τηλεπικοινωνιακών συστημάτων και οι μηχανισμοί ελέγχου και καταγραφής προσβάσεων σε συνδυασμό με τη συνεχή αξιολόγηση των συστημάτων αυτών για αδυναμίες, έχουν ως αποτέλεσμα τη δημιουργία ενός περιβάλλοντος ολοκληρωμένης ασφάλειας για τα προσωπικά δεδομένα των πελατών της WIND Ελλάς.

Τη διασφάλιση του απορρήτου των επικοινωνιών και των προσωπικών δεδομένων των πελατών της WIND Ελλάς έχει στην ευθύνη της η Διεύθυνση Ασφαλείας Πληροφοριών της εταιρείας η οποία έχει στενή συνεργασία στον τομέα αυτό και με την αρμόδια ανεξάρτητη Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (ΑΔΑΕ).

Στο πλαίσιο αυτό, προστατεύουμε το απόρρητο των επικοινωνιών και των προσωπικών δεδομένων πελατών μας όχι μόνο σύμφωνα με το τι ορίζει η σχετική νομοθεσία του ελληνικού κράτους αλλά και με τη δική μας ηθική δέσμευση απέναντί σας.

Υπολογιστές & Διαδίκτυο: η ασφαλής χρήση τους

Όλοι μας χρησιμοποιούμε το Internet για ενημέρωση, ψυχαγωγία αλλά και εξυπηρέτηση. Απολαμβάνουμε τις δυνατότητες που μας προσφέρει αλλά ταυτόχρονα αναγνωρίζουμε ότι η ασφάλεια στη χρήση είναι ένα ζήτημα ιδιαίτερα σημαντικό. Αλλά και απλό. Αρκεί να ακολουθούμε κάποιες βασικές αρχές.

- **Χρησιμοποιήστε τις πιο ενημερωμένες εκδόσεις των προγραμμάτων**

Ενημερώνετε τακτικά τα προγράμματα πλοήγησης (Explorer, Firefox, Chrome κ.λπ.) αλλά και το λειτουργικό σύστημα του Η/Υ. Με αυτό τον τρόπο διατηρείται σε υψηλά επίπεδα η ασφάλεια του Η/Υ. Επίσης, είναι σημαντικό να ενεργοποιείτε πάντα τα ενσωματωμένα χαρακτηριστικά προστασίας των προγραμμάτων πλοήγησης (browser), όπως η φραγή των αναδυόμενων παραθύρων, διαχείριση των "Cookies" κ.λπ. Έτσι, μεγιστοποιούμε το επίπεδο ασφάλειας του Η/Υ.

- **Εγκαταστήστε προγράμματα ανίχνευσης ιών και πρόσθετο λογισμικό ασφαλείας**

Τα προγράμματα ανίχνευσης ιών (antivirus, antispyware), μεγιστοποιούν την ασφάλεια του Η/Υ, καθώς ενημερώνονται συνεχώς και είναι σε θέση να αντιμετωπίσουν νέες απειλές. Επίσης, τα προγράμματα τύπου firewall ελέγχουν όλες τις πληροφορίες του υπολογιστή μας και προλαμβάνουν τη διάδοση των ιών και των ανεπιθύμητων εφαρμογών.

- **Χρησιμοποιήστε προγράμματα μόνο από αξιόπιστες πηγές**

Η χρήση προγραμμάτων που βρίσκουμε στο Διαδίκτυο πρέπει να γίνεται μόνο όταν είμαστε βέβαιοι για την πηγή της προέλευσής τους. Αποφεύγετε προγράμματα που μπορεί να περιέχουν κακόβουλο λογισμικό ή ιούς, τα οποία θα επιφέρουν δυσάρεστες συνέπειες για τον υπολογιστή σας.

- **Κάντε Backup**

Η διατήρηση αντιγράφων ασφαλείας (Backup) αποτελεί μια δικλίδα ασφαλείας του Η/Υ και των αρχείων μας. Αντίγραφα ασφαλείας μπορούν να δημιουργηθούν σε κινητές μονάδες σκληρών δίσκων, σε ψηφιακούς δίσκους CD ή DVD και σε φορητές μονάδες αποθήκευσης δεδομένων (USB stick).

- **Διαφυλάξτε τους κωδικούς σας**

Αποφεύγετε τη χρήση κωδικών στο διαδίκτυο που είναι εύκολοι στην απομνημόνευση ή αποτελούν εύκολη λεία υποκλοπής, (όπως σημαδιακές ημερομηνίες, γνωστοί όροι, ακολουθίες γραμμάτων ή κύρια ονόματα). Μία προτεινόμενη λύση για τη δημιουργία ενός κωδικού (password) είναι να επιλέξετε χρήση συνδυασμού πεζών – κεφαλαίων, γραμμάτων – αριθμών, με τουλάχιστον 8 ψηφία κ.λπ. Τέλος, θα πρέπει να προστατεύουμε τους κωδικούς μας κρατώντας τους μυστικούς.

- **Αποφεύγετε την προβολή άγνωστων αρχείων, μηνυμάτων ή συνδέσμων**

Στο διαδίκτυο κυκλοφορούν πολλά μηνύματα με μολυσμένα αρχεία, ιούς ή ακατάλληλο και παράνομο περιεχόμενο. Πριν ανοίξετε κάποιο μήνυμα άγνωστου, ενεργοποιήστε το φίλτρο για τα ανεπιθύμητα μηνύματα, στο υψηλότερο δυνατό επίπεδο.

- **Χρησιμοποιείτε πάντα νόμιμα αρχεία, μουσικής και βίντεο**

Είναι σημαντικό πριν χρησιμοποιήσετε οποιοδήποτε αρχείο να υπάρχει διαβεβαίωση ότι δεν είναι παράνομη η χρήση του ή το αρχείο δεν αποτελεί ένα πρόγραμμα "Trojan Horse".

- **Σεβαστείτε τα πνευματικά δικαιώματα**

Η εξασφάλιση των πνευματικών δικαιωμάτων των δημιουργών αποτελεί σημαντικό κανόνα για τη νόμιμη χρήση των αρχείων που βρίσκονται στο διαδίκτυο. Αποφεύγετε ιστοχώρους που διανέμουν περιεχόμενο χωρίς την άδεια των δημιουργών.

- **Ελέγξτε τη φερεγγυότητα των ηλεκτρονικών καταστημάτων**

Ελέγξτε τη φερεγγυότητα του ηλεκτρονικού καταστήματος από την «ταυτότητα» της ιστοσελίδας του, καθώς και αναζητώντας την κατάλληλη πληροφόρηση μέσα από τα μητρώα του Internet (όπως για παράδειγμα η διεθνής βάση δεδομένων www.whois.net ή η βάση ελληνικών καταχωρίσεων www.hostmaster.gr/cgibin/webwhois). Συνήθως το ηλεκτρονικό κατάστημα φιλοξενεί ένα ειδικό σήμα στην ιστοσελίδα που πιστοποιεί την ταυτότητά του και ενημερώνει το χρήστη για την ασφάλεια που χρησιμοποιεί το site.

- **Προστασία προσωπικών δεδομένων**

Σύμφωνα με τις ρυθμίσεις που αφορούν την προστασία προσωπικών δεδομένων, η συλλογή και επεξεργασία τους επιτρέπεται μόνο υπό αυστηρές προϋποθέσεις. Όταν μας ζητείται να επικοινωνήσουμε προσωπικά στοιχεία θα πρέπει να έχει προηγηθεί η ρητή συγκατάθεσή μας για τη συλλογή και επεξεργασία τους. Ιδιαίτερα σε περιπτώσεις που το ηλεκτρονικό κατάστημα θέλει να διαβιβάσει τα στοιχεία μας σε τρίτη εταιρεία προς επεξεργασία, τότε η ρητή συγκατάθεσή μας είναι απαραίτητη, καθώς θεωρείται παράνομη οποιαδήποτε επεξεργασία.

- **Τι θα πρέπει να γνωρίζετε πριν προχωρήσετε σε μια ηλεκτρονική εμπορική συναλλαγή**

Σύμφωνα με τη νομοθεσία της Ευρωπαϊκής Ένωσης μπορούμε να ακυρώσουμε ή να επιστρέψουμε μια υπηρεσία/προϊόν, μέσα σε συγκεκριμένο χρονικό διάστημα, το οποίο συνήθως διαρκεί επτά ημέρες.

- Σε περίπτωση επιστροφής, τα έξοδα αποστολής επιβαρύνουν εμάς.
- Σε περίπτωση ελαττωματικού προϊόντος, μπορεί να γίνει καταγγελία σε αρμόδιες από τη χώρα αρχές και υπηρεσίες (βλ. παρακάτω).
- Σε περίπτωση μη εκτέλεσης μιας υπηρεσίας, δικαιούμαστε επιστροφή των χρημάτων μας.

- **Πού μπορούμε να απευθυνθούμε για συμβουλές ή επίλυση θεμάτων που αφορούν σε ηλεκτρονικές συναλλαγές**

- Στο ίδιο εμπορικό κατάστημα στο οποίο πραγματοποιήσαμε την ηλεκτρονική συναλλαγή.
- Στον επαγγελματικό σύλλογο ή/και το Επιμελητήριο που εκπροσωπεί τον κλάδο του συγκεκριμένου εμπόρου.
- Στην υπηρεσία προστασίας του καταναλωτή του Υπουργείου Ανάπτυξης.
- Στις επιτροπές «φιλικού διακανονισμού», στις Νομαρχίες όλης της Ελλάδας.
- Στην υπηρεσία πελατών ή την εκδίδουσα Διεύθυνση της Τράπεζας από την οποία έχει εκδοθεί η πιστωτική μας κάρτα που χρησιμοποιήθηκε κατά τη συναλλαγή.
- Στις Ενώσεις Καταναλωτών.
- Στο Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος στη Γενική Αστυνομική Διεύθυνση Αττικής.

- **Χρήση της πιστωτικής κάρτας σε εμπορικές συναλλαγές**

Η σύγχρονη κρυπτογράφηση των δεδομένων μειώνει σημαντικά τις περιπτώσεις ηλεκτρονικής απάτης. Ακόμη και σε περιπτώσεις που παρατηρηθούν περίεργες χρεώσεις έχουμε το δικαίωμα να ακυρώσουμε τη συναλλαγή και να ζητήσουμε την επιστροφή των χρημάτων μας.

- **Κανόνες για την ασφάλεια των συναλλαγών μας σε ηλεκτρονικά καταστήματα δημοπρασιών**

Σε περιπτώσεις που κάνουμε χρήση υπηρεσιών δημοπρασιών ή/και αγοραπωλησιών αγαθών, είναι σημαντικό να υπάρχει συνοχή και ακολουθία αναφορικά με τους κανόνες που διέπουν τη λειτουργία των συγκεκριμένων δικτυακών τόπων.

- **Προσέξτε κατά τη χρήση υπολογιστών στους οποίους έχουν πρόσβαση και άτομα που δεν γνωρίζουμε**

Για την ασφάλειά μας σε περιπτώσεις που γίνεται χρήση υπολογιστών από κοινό, απαιτείται η εφαρμογή κάποιων κανόνων προστασίας του χρήστη:

- καθαρισμός της προσωρινής μνήμης και
- καθαρισμός του ιστορικού ενεργειών.

TOP 10

10 χρήσιμες έννοιες σχετικά με την ασφάλεια στο Διαδίκτυο

1. Anti-Virus: Πρόκειται για προγράμματα τα οποία προστατεύουν τους χρήστες και τους Η/Υ τους από ιούς και άλλες μορφές κακόβουλου λογισμικού. Η χρήση προγραμμάτων Anti-Virus κρίνεται απαραίτητη, προκειμένου να εξασφαλιστεί η ασφαλής πλοήγηση στο διαδίκτυο. Προκειμένου να υπάρχει maximum αποτελεσματικότητα, τα προγράμματα Anti-Virus θα πρέπει να είναι ενημερωμένα με τα τελευταία update (ενημερώσεις ασφαλείας).

2. Backup: Το Backup αποτελεί ένα από τα πιο σημαντικά μέτρα για την προστασία των δεδομένων ενός χρήστη ή μιας επιχείρησης από ενδεχόμενη σκόπιμη καταστροφή από ιούς και hacker, καθώς και από άλλα αίτια όπως φυσικές καταστροφές ή αστοχίες υλικού.

3. Cryptography: Μέσω της κρυπτογράφησης των ευαίσθητων δεδομένων αποτρέπεται ο κίνδυνος να περιέλθουν κρίσιμα προσωπικά ή εταιρικά στοιχεία σε χέρια επιτηδείων. Ως ευαίσθητα δεδομένα θεωρούνται τα στοιχεία που βρίσκονται αποθηκευμένα στους υπολογιστές μιας εταιρείας ή στο φορητό υπολογιστή ενός χρήστη.

4. Exploit: Το Exploit αποτελεί το μέσο, το οποίο εκμεταλλεύεται κάποιο κενό ασφάλειας, προκειμένου να επιτρέψει σε κάποιο hacker να αποκτήσει πρόσβαση σε κάποιο σύστημα. Ο μόνος τρόπος για να αποτραπεί το κενό ασφαλείας για το οποίο κυκλοφορεί κάποιο Exploit, είναι η άμεση ενημέρωση των συστημάτων με διορθωτικό κώδικα (update).

5. Hacker: Ως Hacker νοούνται οι υπερεξειδικευμένοι χρήστες που θέλουν να γνωρίζουν κάθε τεχνική λεπτομέρεια των συσκευών που χρησιμοποιούν, καθώς και οι κακόβουλες οντότητες με ειδικές γνώσεις σε θέματα ασφάλειας που επιθυμούν να παραβιάσουν υπολογιστικά συστήματα για προσωπικό όφελος.

6. Identity Theft: Η κλοπή ταυτότητας αφορά μια μορφή απάτης κατά την οποία κάποιος έχει αποκτήσει πρόσβαση σε προσωπικά στοιχεία ενός χρήστη, προκειμένου να οικειοποιηθεί πόρους ή υπηρεσίες που δεν του ανήκουν.

7. Password: Τα Password χρησιμοποιούνται σε όλες τις υπηρεσίες που απαιτούν εμπιστευτικότητα προκειμένου να πιστοποιήσουν την ταυτότητα του χρήστη. Μια χρήσιμη συμβουλή χρήσης Password αποτελεί η χρήση τουλάχιστον 8 χαρακτήρων, ανάμεσα στους οποίους θα περιλαμβάνονται χαρακτήρες, σύμβολα και αριθμοί.

8. Spam: Η μαζική αποστολή ηλεκτρονικών μηνυμάτων σε εκατομμύρια χρήστες (χωρίς οι χρήστες αυτοί να το επιθυμούν ή να το έχουν ζητήσει) καθημερινά με πληροφορίες για διάφορα προϊόντα. Στις περισσότερες περιπτώσεις τα προϊόντα αυτά είναι πλαστά, όπως για παράδειγμα το πειρατικό λογισμικό ή τα φτηνά σκευάσματα αντί για πραγματικά φάρμακα.

9. Trojan Horse: Αποτελεί μια μορφή κακόβουλου λογισμικού, η οποία συνήθως κρύβεται σε μια άλλη χρήσιμη εφαρμογή, που ο χρήστης εμπιστεύεται και χρησιμοποιεί. Μέσω του Trojan Horse δίνεται η πρόσβαση σε επιτήδειους να αποκτήσουν από απόσταση τον έλεγχο του μηχανήματος που έχει εγκατασταθεί.

10. Update: Η ενημερωμένη έκδοση ενός προγράμματος αποτελεί τον όρο Update και συνήθως χρησιμοποιείται όταν ένα πρόγραμμα εμφανίσει κάποιο πρόβλημα σχετικά με την ασφάλειά του ή τη λειτουργία του. Πολλές εφαρμογές ρυθμίζονται με τέτοιο τρόπο ώστε να μπορούν να ελέγχουν από μόνες τους για ενημερωμένες εκδόσεις.

Τμήμα Εταιρικών Σχέσεων WIND Ελλάς
Λεωφ. Κηφισίας 66, 151 25 Μαρούσι
Τηλ: 210 61 58 574, Fax: 210 61 05 022
E-mail: crpafr@wind.com.gr