ΔΕΛΤΙΟ ΤΥΠΟΥ

Αθήνα 7-2-2017

Ενημέρωση για την προστασία του απορρήτου των επικοινωνιών στο διαδίκτυο

Με αφορμή την Παγκόσμια Ημέρα Ασφαλούς Διαδικτύου, η Συνταγματικά κατοχυρωμένη ανεξάρτητη Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών (ΑΔΑΕ) ενημερώνει τους ψηφιακούς χρήστες σχετικά με τα μέτρα που θα πρέπει να εφαρμόζουν για μια ασφαλή περιήγηση στο διαδίκτυο και για την προστασία του απορρήτου των επικοινωνιών τους. Ο ενημερωτικός κόμβος της Αρχής και το σχετικό έντυπο που διατίθεται στοχεύουν στην ευαισθητοποίηση των πολιτών και δίνουν πρακτικές οδηγίες για την αποφυγή των κινδύνων στον κυβερνοχώρο.

Στη διαδικτυακή πύλη της Αρχής, http://www.adae.gr/enimerosi-christon-kai-syndromiton/, οι ενδιαφερόμενοι μπορούν να βρουν συγκεντρωμένους τους συνδέσμους από πολλές πηγές πληροφόρησης, όπως Υπουργεία, οργανισμούς, ανεξάρτητες αρχές και παρόχους. Επίσης μπορούν να αξιολογήσουν τις γνώσεις τους σε θέματα ασφάλειας και απορρήτου των ηλεκτρονικών επικοινωνιών, συμπληρώνοντας το σχετικό **ερωτηματολόγιο,** και να κατεβάσουν το **ενημερωτικό έντυπο** της ΑΔΑΕ.

Παρακάτω δείτε κάποια από τα μέτρα που προάγουν την ασφάλεια στον κυβερνοχώρο

Μέτρα για την προστασία του απορρήτου κατά την πρόσβαση στο Διαδίκτυο

- Επιλέξτε και εγκαταστήστε στον υπολογιστή σας ένα πρόγραμμα προστασίας από κακόβουλο λογισμικό (antivirus) μιας γνωστής και αξιόπιστης εταιρείας.
- Ενεργοποιήστε τη δυνατότητα αυτόματης ενημέρωσης, ώστε να προστατεύεται ο υπολογιστής σας από τις πιο πρόσφατες περιπτώσεις κακόβουλου λογισμικού. Κάποια προγράμματα υποστηρίζουν και λειτουργίες anti-spyware.
- Εγκαταστήστε ένα τοίχος προστασίας στον υπολογιστή σας (firewall). Το firewall ελέγχει την επικοινωνία από και προς τον προσωπικό υπολογιστή σας, επιτρέποντας ή απαγορεύοντας συγκεκριμένα είδη κίνησης, ώστε να προλαμβάνει τη διάδοση ιών και ανεπιθύμητων εφαρμογών. Ορισμένες εκδόσεις λειτουργικών συστημάτων (π.χ. WindowsXP/SP2) έχουν ενσωματωμένο προσωπικό firewall.
- Πραγματοποιήστε τακτικές ενημερώσεις στα προγράμματα πλοήγησης (browser) στο Διαδίκτυο (Internet Explorer, Firefox, Chrome, Opera, Safari κλπ.). Συνιστάται η ενεργοποίηση της αυτόματης ενημέρωσης και η πραγματοποίηση ενημέρωσης όταν λαμβάνετε μια σχετική ειδοποίηση.

- Χρησιμοποιήστε έναν ισχυρό κωδικό πρόσβασης με γράμματα, σύμβολα και αριθμούς, διαφορετικό για κάθε εφαρμογή στην οποία διατηρείτε λογαριασμό. Αποφύγετε τη χρήση κωδικών που είναι εύκολοι στην απομνημόνευση (όπως ημερομηνίες, γνωστούς όρους, ακολουθίες γραμμάτων ή κύρια ονόματα). Μια προτεινόμενη λύση για τη δημιουργία ενός κωδικού (password) είναι να επιλέξετε χρήση συνδυασμού πεζών – κεφαλαίων, γραμμάτων – αριθμών, με τουλάχιστον 8 ψηφία.
- Κρατήστε τους κωδικούς σας μυστικούς και αλλάζετέ τους σε τακτικά χρονικά διαστήματα (τουλάχιστον μια φορά ανά 6 μήνες).
- Ενεργοποιείτε πάντα τα ενσωματωμένα χαρακτηριστικά προστασίας των προγραμμάτων πλοήγησης όπως η φραγή των αναδυόμενων παραθύρων, διαχείριση των “Cookies” κλπ.
- Δώστε προσοχή σε ενδείξεις που μπορεί να σημαίνουν ότι ο υπολογιστής σας έχει προσβληθεί από κάποιον ιό, όπως οι παρακάτω:
    - το σύστημά σας γίνεται ξαφνικά αισθητά πιο αργό στην εκκίνησή του ή/και στη λειτουργία του
    - αργεί να ανοίξει τα αρχεία σας περισσότερο από το συνηθισμένο
    - κάποια αρχεία εμφανίζονται κατεστραμμένα ή δεν φορτώνουν
    - εμφανίζονται μηνύματα από το antivirus πρόγραμμά σας ή άλλα ασυνήθιστα μηνύματα
- Χρησιμοποιήστε προγράμματα μόνο από αξιόπιστες πηγές. Η χρήση προγραμμάτων που βρίσκετε στο Διαδίκτυο πρέπει να γίνεται μόνο όταν είστε βέβαιοι για την πηγή της προέλευσής τους.
- Αποφύγετε την προβολή άγνωστων αρχείων, μηνυμάτων ή συνδέσμων. Πριν ανοίξετε κάποιο αρχείο, ενεργοποιήστε το φίλτρο για ανίχνευση ιών (virus scanning).
- Βεβαιωθείτε ότι έχετε αποσυνδεθεί από τον λογαριασμό σας σε μια ιστοσελίδα ηλεκτρονικής υπηρεσίας (π.χ. ηλεκτρονικής τραπεζικής συναλλαγής) μέσω του προσφερόμενου συνδέσμου αποσύνδεσης (log out) πριν την εγκαταλείψετε.
- Αποφύγετε την ενεργοποίηση υπενθύμισης/απομνημόνευσης κωδικού κατά τη χρήση προγραμμάτων πλοήγησης, ειδικά όταν η πρόσβαση στο Διαδίκτυο γίνεται από κοινόχρηστους υπολογιστές.
- Επιβεβαιώστε ότι χρησιμοποιείτε μια ασφαλή σύνδεση όταν στέλνετε ευαίσθητες προσωπικές πληροφορίες μέσω του παγκόσμιου ιστού (Web). Αυτό φαίνεται από το εικονίδιο του κλειδωμένου λουκέτου, ενώ η διεύθυνση που συνδέεστε πρέπει να αρχίζει με https:// αντί του http.
- Αν συνδέεστε στο Διαδίκτυο από δίκτυο δημόσιας χρήσης (internet café, ξενοδοχεία κλπ.), μη χρησιμοποιείτε και μη μεταδίδετε προσωπικά σας στοιχεία. Αποφύγετε να επισκέπτεστε σελίδες που πρέπει να χρησιμοποιήσετε προσωπικούς σας μυστικούς κωδικούς (passwords), ιδιαίτερα αν η ανταλλαγή πληροφορίας δεν πραγματοποιείται κρυπτογραφημένα (π.χ. https). Είναι πιθανό τα δίκτυα αυτά να μην είναι ασφαλή και να υποκλαπούν προσωπικά σας δεδομένα.
- Φροντίστε να λαμβάνετε τακτικά αντίγραφα ασφάλειας (backups). Με τον τρόπο αυτό, σε περίπτωση που το σύστημα σας προσβληθεί από ιό, θα διασώσετε σημαντικά αρχεία σας και θα μπορείτε να το επαναφέρετε σε προηγούμενη κατάσταση.
- Οι υπηρεσίες Cloud (π.χ. Dropbox, Rapidshare, Google Drive) χρησιμοποιούνται κυρίως για την αποθήκευση αντιγράφων ασφαλείας και δεδομένων μεγάλου όγκου και προσφέρουν μεγαλύτερη ευελιξία στην κοινή χρήση της πληροφορίας (π.χ. άλμπουμ φωτογραφιών). Για τις υπηρεσίες Cloud συνιστάται να επιλέγετε με προσοχή τους κωδικούς πρόσβασης, να χρησιμοποιείτε μία ασφαλή σύνδεση (με αρχικό https:// αντί http) και να κρυπτογραφείτε τα δεδομένα που αποθηκεύετε.

- Σε περίπτωση που χρησιμοποιείτε για πρόσβαση στο Διαδίκτυο συσκευή, στην οποία έχουν πρόσβαση και τρίτοι, συνιστάται να διαγράφετε το ιστορικό πλοήγησής σας (browsing history) και τα cookies. Έχετε επίσης τη δυνατότητα να απενεργοποιήσετε την αποθήκευση του ιστορικού πλοήγησης μέσω των ρυθμίσεων του προγράμματος πλοήγησης.

Μέτρα για την προστασία του απορρήτου στην ηλεκτρονική αλληλογραφία

Αν ο λογαριασμός ηλεκτρονικής αλληλογραφίας σας παραβιάστηκε πρόσφατα ή αν τρίτοι απέκτησαν πρόσβαση σε αυτόν, θα πρέπει να αλλάξετε άμεσα τον κωδικό πρόσβασής σας.

- Μη χρησιμοποιείτε ποτέ τον κωδικό πρόσβασης του λογαριασμού σας για την πρόσβαση σε άλλους ιστότοπους.
- Μην ανοίγετε συνημμένα αρχεία που προέρχονται από άγνωστους τρίτους ή από μη έμπιστες πηγές. Όταν λαμβάνετε ηλεκτρονικό μήνυμα, ακόμη και από φαινομενικά έμπιστες πηγές (όπως π.χ. τράπεζες), εξετάστε προσεχτικά την προέλευσή του πριν ανοίξετε ένα σύνδεσμο που περιέχεται σε αυτό, γιατί μπορεί να σας οδηγήσει σε ιστοσελίδα που, ενώ φαίνεται ίδια με τη νόμιμη, είναι πλαστή.
- Μην στέλνετε τους κωδικούς πρόσβασής σας μέσω ηλεκτρονικού ταχυδρομείου. Οι νόμιμοι ιστότοποι, που προσφέρουν ηλεκτρονικά υπηρεσίες, δεν θα σας ζητήσουν ποτέ να στείλετε τους κωδικούς πρόσβασής σας μέσω ηλεκτρονικού ταχυδρομείου.
- Παρακολουθήστε τη δραστηριότητα των λογαριασμών ηλεκτρονικού ταχυδρομείου, όπως τις συνδέσεις στον λογαριασμό σας, τυχόν αλλαγές στον κωδικό πρόσβασης ή στα στοιχεία που χρησιμοποιούνται για την ανάκτηση των κωδικών σας (προσθήκη μιας εναλλακτικής διεύθυνσης ηλεκτρονικού ταχυδρομείου ή ενός αριθμού τηλεφώνου). Εάν παρατηρήσετε οποιαδήποτε ύποπτη ένδειξη, θα πρέπει άμεσα να αλλάξετε τον κωδικό πρόσβασης.
- Παρακολουθήστε την αποστολή και τη λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου. Εάν παρατηρήσετε ότι πολλά μηνύματα στον λογαριασμό σας δεν μπορείτε να τα βρείτε ή εάν παρατηρήσετε ότι από τον λογαριασμό σας στέλνονται άγνωστα μηνύματα, αλλάξτε άμεσα τον κωδικό πρόσβασης.
- Επιβεβαιώστε ότι η αλληλογραφία σας δεν προωθείται σε κάποια διεύθυνση που δεν έχετε ορίσει εσείς. Σε περίπτωση που διαπιστώσετε ανεπιθύμητη προώθηση, καταργήστε την άμεσα.
- Στην περίπτωση που είναι εφικτό, ενεργοποιήστε τη διαδικασία επαλήθευσης σε δύο βήματα (two step verification) για την πρόσβαση στον λογαριασμό σας (π.χ. με την αποστολή ειδικού κωδικού μιας χρήσης στο κινητό σας τηλέφωνο).
- Μην παραλείπετε να αποσυνδεθείτε από τον λογαριασμό σας, ειδικά εάν έχετε συνδεθεί από έναν κοινόχρηστο υπολογιστή (π.χ. από μια βιβλιοθήκη ή ένα Internet cafe). Έχετε υπόψη σας ότι μπορεί να εξακολουθείτε να είστε συνδεδεμένοι, ακόμα και αφού κλείσετε το πρόγραμμα πλοήγησης.
- Κρυπτογραφήστε μηνύματα ή συνημμένα αρχεία που περιέχουν εμπιστευτικές πληροφορίες.

Μέτρα για την προστασία του απορρήτου κατά την ασύρματη πρόσβαση στο Διαδίκτυο

Ενεργοποιήστε την κρυπτογράφηση στον ασύρματο δρομολογητή σας. Προτιμήστε την κρυπτογράφηση WPA ή ακόμα καλύτερα WPA2. Να χρησιμοποιείτε ισχυρούς κωδικούς για το κλειδί κρυπτογράφησης, τους οποίους να αλλάζετε συχνά. Αλλάζετε το όνομα του δικτύου (αναγνωριστικό SSID), δίνοντας δική σας ονομασία, διαφορετική από αυτή που έχει θέσει ο κατασκευαστής.

- Ρυθμίστε το ασύρματο δίκτυο ώστε να δέχεται συνδέσεις μόνο από συγκεκριμένους υπολογιστές, tablet και κινητά τηλέφωνα (MAC address filtering).
- Αλλάζετε το όνομα χρήστη και τον κωδικό ασφαλείας για τη διαχείριση του ασύρματου δρομολογητή από την τιμή που έχει θέσει ο κατασκευαστής (username και password admin). Επιπλέον, αλλάζετε τον κωδικό, που έχετε θέσει, σε τακτά χρονικά διαστήματα.
- Απενεργοποιήστε την απομακρυσμένη σύνδεση (remote management access) με τον δρομολογητή σας σε περίπτωση που η πρόσβαση αυτή δεν είναι ήδη απενεργοποιημένη από τον κατασκευαστή.
- Αλλάξτε τη ρύθμιση ώστε να μην επιτρέπεται η διαχείριση του δρομολογητή σας μέσω ασύρματης (wireless) σύνδεσης.
- Μπορείτε να ελέγξετε τον ασύρματο δρομολογητή σας για το ποιες συσκευές έχουν συνδεθεί ή αιτούνται σύνδεσης με αυτόν. Σε περίπτωση που παρατηρήσετε συνδέσεις από άγνωστες συσκευές, αλλάξτε άμεσα τους κωδικούς σας.
- Απενεργοποιήστε το ασύρματο δίκτυο όταν δεν το χρησιμοποιείτε.

Για περισσότερες πληροφορίες:
Αναστασία Λύρα
Προϊσταμένη Τμ. Διεθνών Συνεργασιών & Δημοσίων Σχέσεων
Τ: 210 6387607
Κ: 6979 111938
E:alyra@adae.gr