Ενημερωτικό έντυπο για χρήστες και συνδρομητές υπηρεσιών ηλεκτρονικών επικοινωνιών

Εισαγωγή

Στο έντυπο αυτό περιλαμβάνονται βασικά μέτρα προστασίας που θα πρέπει να εφαρμόζουν οι συνδρομητές και οι χρήστες υπηρεσιών ηλεκτρονικών επικοινωνιών για την διασφάλιση του απορρήτου των επικοινωνιών τους.

Οι συνδρομητές και οι χρήστες οφείλουν να μεριμνούν για το απόρρητο της επικοινωνίας στα ιδιωτικά δίκτυα τα οποία περιλαμβάνουν τις καλωδιώσεις στα κτίρια, τα εσωτερικά δίκτυα και τις τερματικές συσκευές (π.χ. σταθερά ενσύρματα και ασύρματα τηλέφωνα, κινητά τηλέφωνα, fax, προσωπικοί υπολογιστές).

Μέτρα για την προστασία του απορρήτου της επικοινωνίας στη σταθερή τηλεφωνία

Η προστασία των σταθερών τερματικών συσκευών (σταθερών τηλεφώνων) είναι πολύ σημαντική για την προστασία του απορρήτου της επικοινωνίας σας. Παρακάτω καταγράφονται μερικά από τα βασικά μέτρα ασφάλειας τα οποία μπορείτε να εφαρμόσετε άμεσα:

- Προστατέψτε την τηλεφωνική σας συσκευή ώστε να μην είναι δυνατή η πρόσβαση σε αυτή ή στο χώρο που βρίσκεται, από ανθρώπους που δεν γνωρίζετε.
- Αν χρησιμοποιείτε ασύρματη συσκευή αρχικά, θα πρέπει να ελέγχετε στο εγχειρίδιο του κατασκευαστή, εάν είναι πιστοποιημένη αναφορικά με τις χρησιμοποιούμενες συχνότητες για το σκοπό αυτό. Επιπλέον, δεν θα πρέπει να γίνεται χρήση της συσκευής σε πολύ απομακρυσμένα σημεία από το σταθμό βάσης διότι είναι πιθανό να υπάρχουν παρεμβολές από παρόμοιες ασύρματες συσκευές γειτονικών οικιών και να γίνεται συνακρόαση του περιεχομένου των συνομιλιών σας.
- Το κουτί διανομής στις κατοικίες και ο πίνακας διανομής στις πολυκατοικίες, στα οποία τερματίζει το δημόσιο τηλεπικοινωνιακό δίκτυο, θα πρέπει να είναι ασφαλισμένα και προσβάσιμα μόνο από εξουσιοδοτημένα άτομα. Επίσης, θα πρέπει να ελέγχετε τα εν λόγω σημεία σε τακτά χρονικά διαστήματα για πιθανή παραβίασή τους.
- Να ελέγχετε τα τμήματα της εσωτερικής καλωδίωσης από τον πίνακα διανομής μέχρι την τηλεφωνική συσκευή, τα οποία δεν είναι επαρκώς προστατευμένα, για πιθανή παραβίασή τους.
- Στην περίπτωση που δεχθείτε επίσκεψη ατόμου που υποστηρίζει ότι ανήκει στο προσωπικό τηλεπικοινωνιακού παρόχου και επιθυμεί να κάνει τεχνικές εργασίες στο σπίτι ή στην πολυκατοικία, απαιτήστε να σας δείξει διαπίστευση της εταιρίας. Εν ανάγκη επικοινωνήστε με τον πάροχο για να επιβεβαιώσετε την ταυτότητα του τεχνικού.

Μέτρα για την προστασία του απορρήτου στην ηλεκτρονική αλληλογραφία

- Οι κωδικοί πρόσβασης είναι η πρώτη γραμμή άμυνας ενάντια στους εισβολείς λογαριασμών. Αν ο λογαριασμός σας παραβιάστηκε πρόσφατα ή τρίτοι απέκτησαν πρόσβαση, θα πρέπει να αλλάξετε άμεσα τον κωδικό πρόσβασής σας.
- Χρησιμοποιήστε ένα σύνθετο κωδικό πρόσβασης (με γράμματα και αριθμούς), διαφορετικό για κάθε 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. Τέλος, κράτησε τους κωδικούς σας μυστικούς.
- Αλλάξτε τους κωδικούς ηλεκτρονικού ταχυδρομείου σας σε τακτικά χρονικά διαστήματα (τουλάχιστον μια φορά ανά 6 μήνες).

- Μην ανοίγετε συνημμένα αρχεία που προέρχονται από άτομα που δεν γνωρίζετε ή από μη έμπιστες πηγές. Αυτά μπορεί να περιέχουν ιούς ή προγράμματα που μπορούν να σβήσουν τα αρχεία στον υπολογιστή σας ή να αποστείλουν ανεπιθύμητα μηνύματα στις επαφές σας.
- Προσέχετε όταν λαμβάνετε e-mail ακόμη και από φαινομενικά έμπιστες πηγές όπως τράπεζες. Υπάρχουν συχνές απάτες από παραπλανητικές πηγές που ζητούν να εισάγετε τον κωδικό πρόσβασης σας ώστε να τον κλέψουν και να αποκτήσουν τον έλεγχο (Phising) του email σας. Εξετάστε προσεχτικά πριν πατήσετε κάποιο σύνδεσμο στο e-mail γιατί μπορεί να σας οδηγήσει σε ιστοσελίδα που φαίνεται ίδια με τη νόμιμη αλλά είναι ψεύτικη και επικίνδυνη.
- Μην στέλνετε τον κωδικό πρόσβασής σας μέσω ηλεκτρονικού ταχυδρομείου. Οι νόμιμοι ιστότοποι και υπηρεσίες δεν θα σας ζητήσουν ποτέ να στείλετε τους κωδικούς πρόσβασής σας μέσω ηλεκτρονικού ταχυδρομείου.
- Παρακολουθήστε τη δραστηριότητα των λογαριασμών e-mail για να δείτε ενέργειες που αφορούν την ασφάλεια, όπως τις συνδέσεις στο λογαριασμό σας, τις αλλαγές στον κωδικό πρόσβασης ή την προσθήκη μιας εναλλακτικής διεύθυνσης ηλεκτρονικού ταχυδρομείου ή ενός αριθμού τηλεφώνου που χρησιμοποιούνται για την ανάκτηση των κωδικών σας. Εάν παρατηρήσετε οποιαδήποτε ύποπτη δραστηριότητα, θα πρέπει άμεσα να αλλάξετε τον κωδικό πρόσβασης.
- Παρακολουθήστε την αποστολή και τη λήψη e-mail. Εάν παρατηρήσετε ότι πολλά μηνύματα στο λογαριασμό σας δεν μπορείτε να τα βρείτε ή εάν παρατηρήσετε ότι από το λογαριασμό σας στέλνονται άγνωστα μηνύματα, προβείτε άμεσα σε αλλαγή του κωδικού πρόσβασης.
- Επιβεβαιώστε ότι η αλληλογραφία σας δεν προωθείται σε ανεπιθύμητη διεύθυνση. Αν υπάρχει ανεπιθύμητη διεύθυνση προώθησης, καταργήστε την άμεσα.
- Μην χρησιμοποιείτε τη διεύθυνση ηλεκτρονικού ταχυδρομείου της εργασίας σας για ηλεκτρονικές αγορές, συμμετοχή σε δωμάτια συζητήσεων (chat rooms), διαγωνισμούς, συμπλήρωση ερωτηματολογίων, κ.α. Για τέτοιες περιπτώσεις, μπορείτε να χρησιμοποιείτε κάποια ιδιωτική διεύθυνση που μπορεί να καταργηθεί χωρίς άλλο κόστος.
- Ενεργοποιήστε τη διαδικασία επαλήθευσης σε δύο βήματα για την πρόσβαση στο λογαριασμό σας στην περίπτωση που αυτό είναι εφικτό. (π.χ. με την αποστολή ειδικού κωδικού μιας χρήσης στο κινητό σας τηλέφωνο).
- Κατά την ανταλλαγή των μηνυμάτων ηλεκτρονικού ταχυδρομείου συνιστάται η ενεργοποίηση στην αντίστοιχη εφαρμογή πρωτοκόλλων κρυπτογράφησης (π.χ. SSL, TLS) που εξασφαλίζουν την κρυπτογράφηση των μηνυμάτων στη διαδρομή από τον Η/Υ μέχρι τους εξυπηρετητές Ηλεκτρονικού Ταχυδρομείου. Έτσι εξασφαλίζεται η εμπιστευτικότητα και η ακεραιότητα της επικοινωνίας και κανείς δεν μπορεί να υποκλέψει το μήνυμα στη διαδρομή αυτή.
- Η ενεργοποίηση της πιστοποίησης της ταυτότητας του χρήστη (SMTP authentication) προσθέτει ένα επιπλέον επίπεδο ασφάλειας.

Μέτρα για την προστασία του απορρήτου κατά την πρόσβαση στο Διαδίκτυο

Για να απολαμβάνετε τα οφέλη του κυβερνοχώρου αποφεύγοντας τους διαδικτυακούς κινδύνους χρειάζεται να εφαρμόζετε μέτρα ασφάλειας όπως τα παρακάτω:

- Επιλέξτε και εγκαταστήστε στον υπολογιστή σας ένα πρόγραμμα προστασίας από κακόβουλο λογισμικό από μια γνωστή και αξιόπιστη εταιρεία και εκτελέστε το όπως συνιστάται από τον προμηθευτή. Αν το πρόγραμμα διαθέτει δυνατότητα αυτόματου ελέγχου για κακόβουλο λογισμικό, ενεργοποιήστε την. Επίσης, αν προσφέρει δυνατότητα αυτόματης ενημέρωσης, θα πρέπει να τη χρησιμοποιήσετε ώστε να προστατεύεται ο υπολογιστής σας από τις πιο πρόσφατες περιπτώσεις κακόβουλου λογισμικού. Διαφορετικά, θα πρέπει να ενημερώνετε το πρόγραμμα με τις τελευταίες εκδόσεις. Κάποια προϊόντα anti-virus υποστηρίζουν και λειτουργίες anti-spyware. Τα προγράμματα ανίχνευσης ιών (antivirus, antispyware), μεγιστοποιούν την ασφάλεια του Η/Υ, καθώς ενημερώνονται συνεχώς και είναι σε θέση να αντιμετωπίσουν νέες απειλές.

- **Εγκατάσταση Προσωπικού Firewall:** Το firewall είναι ένα σύστημα, το οποίο ελέγχει την επικοινωνία από και προς τον προσωπικό υπολογιστή σας, επιτρέποντας ή απαγορεύοντας συγκεκριμένα είδη κίνησης, προλαμβάνοντας με τον τρόπο αυτό τη διάδοση των ιών και των ανεπιθύμητων εφαρμογών. Ορισμένες εκδόσεις λειτουργικού συστήματος (π.χ. WindowsXP SP2) έχουν ενσωματωμένο προσωπικό firewall.

- Ενημερώνετε τακτικά τα προγράμματα πλοήγησης (Explorer, Firefox, Chrome, κ.λ.π.).
- Ενεργοποιείτε πάντα τα ενσωματωμένα χαρακτηριστικά προστασίας των προγραμμάτων πλοήγησης (browser), όπως η φραγή των αναδυόμενων παραθύρων, διαχείριση των "Cookies" κ.λ.π.
- Επιβεβαιώνετε ότι οι ρυθμίσεις ασφάλειας του προγράμματος πλοήγησης στον Παγκόσμιο Ιστό (Web) είναι επαρκώς υψηλές
- 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 και με ιδιαίτερη σύνεση και προσοχή.
- Αποφύγετε την προβολή άγνωστων αρχείων, μηνυμάτων ή συνδέσμων.
  Στο διαδίκτυο κυκλοφορούν πολλά μηνύματα με "μολυσμένα" αρχεία, ιούς ή ακατάλληλο και παράνομο περιεχόμενο. Πριν ανοίξετε κάποιο αρχείο, ενεργοποιήστε το φίλτρο για το virus scanning.
- Πριν αναρτήσετε κάποια πληροφορία ή προσωπικό σας στοιχείο στο internet ή σε κοινωνικά δίκτυα, αναλογιστείτε αν τα δεδομένα αυτά είναι προς δημοσίευση.
- 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**://**

Οδηγίες Δημιουργίας Κωδικών Πρόσβασης
Οι κωδικοί πρόσβασης είναι οι λέξεις ή φράσεις-κλειδιά που χρησιμοποιούνται για να αποκτήσετε πρόσβαση στους διαφόρους λογαριασμούς που διατηρείτε είτε στον προσωπικό υπολογιστή σας είτε στο διαδίκτυο.

Σε περίπτωση που ένας εισβολέας καταφέρει και υποκλέψει ή ανακαλύψει τον κωδικό πρόσβασης, θα μπορέσει να αποκτήσει πρόσβαση σε προσωπικά δεδομένα, να πραγματοποιήσει παράνομες αγορές, να δημιουργήσει νέους λογαριασμούς στο όνομα του θύματος ή να προκαλέσει καταστροφές. Είναι πολύ σημαντικό επομένως οι κωδικοί πρόσβασης να δημιουργούνται με τέτοιο τρόπο ώστε να είναι δύσκολο να τους μαντέψει κανείς και να προστατεύονται συνεχώς ώστε να μην είναι δυνατή η υποκλοπή τους. Ακολουθώντας μερικές εύκολες και βασικές οδηγίες αυτό μπορεί να επιτευχθεί χωρίς ιδιαίτερο κόπο.

Ο κωδικός πρόσβασης πρέπει να είναι μακρύς. Όσο περισσότεροι είναι οι χαρακτήρες σε ένα κωδικό τόσο δυσκολότερο γίνεται για κάποιον επιτιθέμενο να τον ανακαλύψει. Όμως αυτό δεν είναι αρκετό, σημαντικό ρόλο παίζει και η τυχαιότητα των χαρακτήρων αυτών. Ο καλύτερος τρόπος για να δημιουργήσει κάποιος ένα μακρύ κωδικό είναι να χρησιμοποιήσει μια φράση που μόνο αυτός θα ξέρει και την οποία θα μπορεί να θυμάται. Ο αριθμός των χαρακτήρων θα πρέπει οπωσδήποτε να ξεπερνάει τους 8, ενώ ο συνιστώμενος αριθμός είναι 14 και άνω. Γενικά, όσο περισσότεροι χαρακτήρες χρησιμοποιούνται τόσο το καλύτερο.
Πρέπει να χρησιμοποιούνται γράμματα, σύμβολα και αριθμοί. Όταν δημιουργείτε ένα κωδικό πρόσβασης θα πρέπει να συμπεριλάβετε και αριθμούς και σύμβολα (!@#$%"!@#$%^&*()_+=) πέραν των γραμμάτων. Με αυτό τον τρόπο θα αυξήσετε την περιπλοκότητα του κωδικού και θα είναι πολύ δύσκολο για κάποιον να τον ανακαλύψει.
Χρησιμοποιήστε σημεία στίξης και κεφαλαία. Η εναλλαγή μεταξύ κεφαλαίων και πεζών γραμμάτων καθώς και τα σημεία στίξης θα κάνουν τον κωδικό σας πολύ πιο ασφαλή.
Μην χρησιμοποιείτε επαναλαμβανόμενους χαρακτήρες ή αριθμούς.
Μην αποκαλύπτετε τον κωδικό σας σε κανένα.
Όταν εισάγετε τον κωδικό σας να είστε σε επιφυλακή μην σας παρακολουθούν.
Να αλλάζετε τακτικά τον κωδικό πρόσβασης.
Να μην χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης για όλους τους λογαριασμούς που διατηρείτε.
Αποφύγετε να καταγράφετε τους κωδικούς πρόσβασης σε χαρτί ή οποιοδήποτε άλλο μέσο.