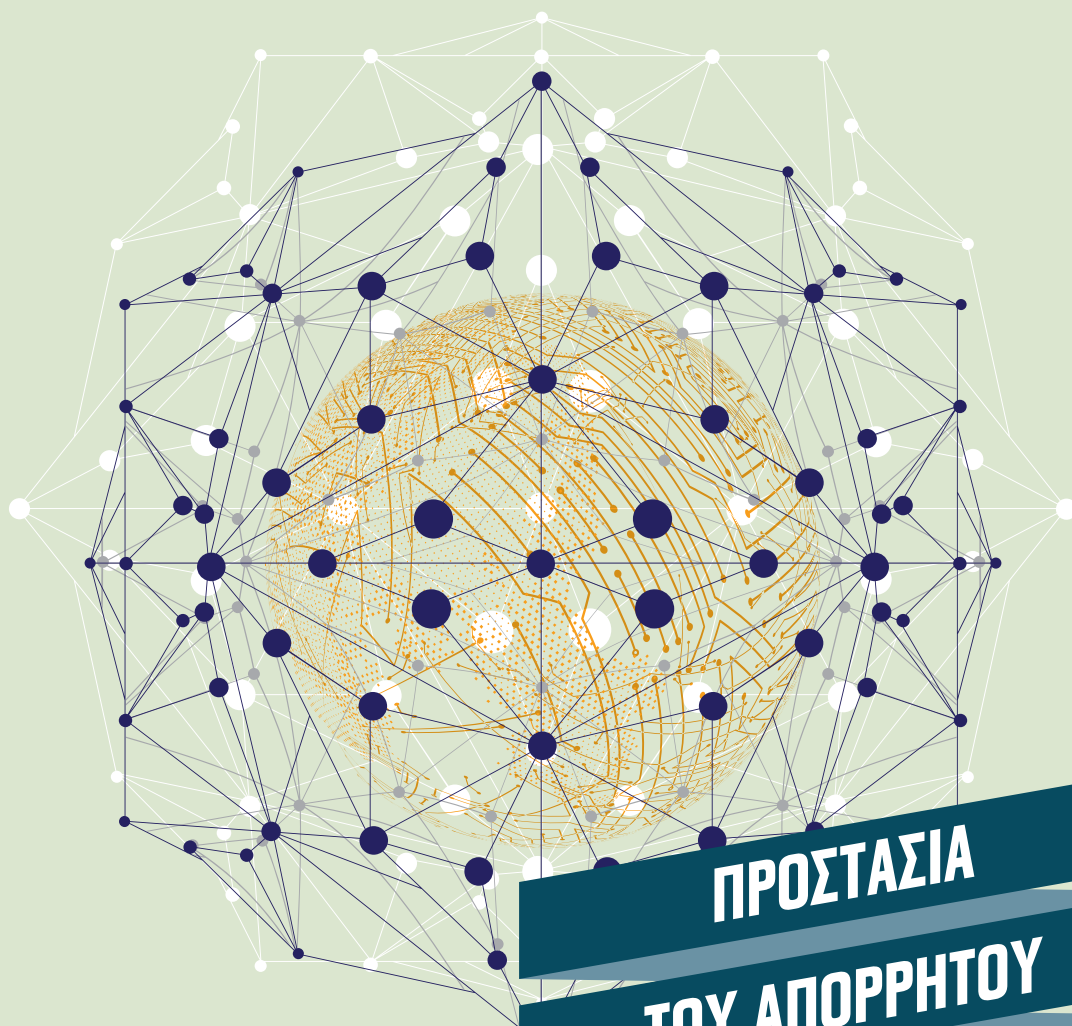
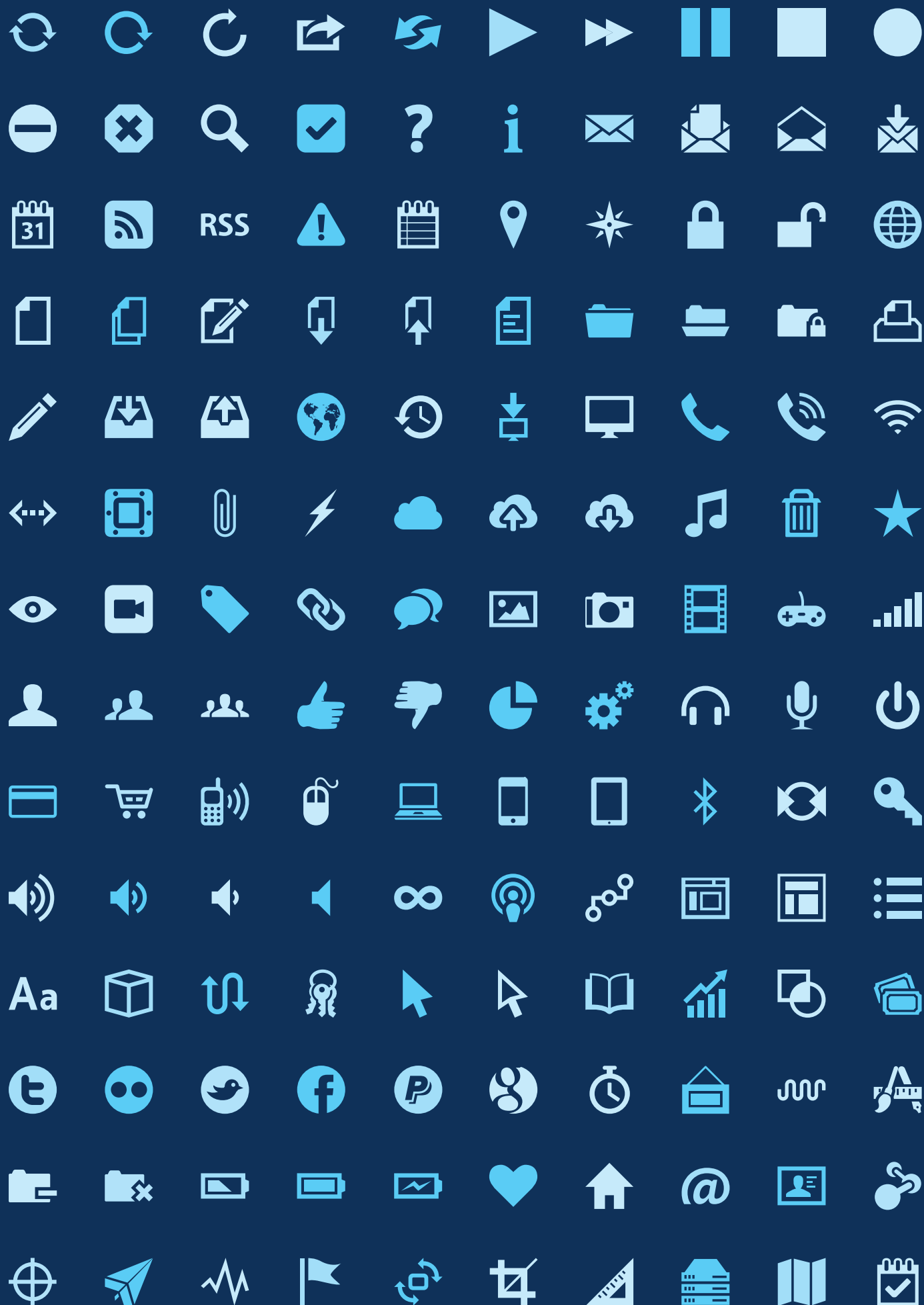




**ΠΡΟΣΤΑΣΙΑ
ΤΟΥ ΑΠΟΡΡΗΤΟΥ
ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ**



**ΕΝΗΜΕΡΩΣΗ
ΓΙΑ ΧΡΗΣΤΕΣ
ΚΑΙ ΣΥΝΔΡΟΜΗΤΕΣ
ΥΠΗΡΕΣΙΩΝ
ΗΛΕΚΤΡΟΝΙΚΩΝ
ΕΠΙΚΟΙΝΩΝΙΩΝ**



Με το έντυπο αυτό η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) απευθύνεται σε συνδρομητές και χρήστες υπηρεσιών ηλεκτρονικών επικοινωνιών με σκοπό να προσφέρει ενημέρωση σχετικά με βασικά μέτρα αυτοπροστασίας που θα πρέπει να εφαρμόζουν για την ασφάλεια του απορρήτου των επικοινωνιών τους.

Στις ηλεκτρονικές επικοινωνίες, σύμφωνα με τη νομοθεσία, απόρρητα θεωρούνται:

- Το περιεχόμενο της επικοινωνίας (*περιεχόμενο τηλεφωνικών κλήσεων, ηλεκτρονικού ταχυδρομείου και γενικά οποιασδήποτε επικοινωνίας φωνής, εικόνας, δεδομένων*).
- Η ταυτότητα του καλούντος και του καλουμένου.
- Η ταυτότητα του αποστολέα και του παραλήπτη ηλεκτρονικού ταχυδρομείου.
- Τα δεδομένα θέσης της τερματικής συσκευής (*γεωγραφικός εντοπισμός*).

Η προστασία του απορρήτου σε κάθε μορφής επικοινωνία αποτελεί συνταγματικά κατοχυρωμένο δικαίωμα και νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δεν δεσμεύεται από το απόρρητο για λόγους εθνικής ασφάλειας ή για τη διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων (*άρθρο 19 του Συντάγματος*). Η διαδικασία για τη νόμιμη άρση του απορρήτου καθορίζεται λεπτομερώς στην ισχύουσα νομοθεσία (**N.2225/1994, N.3115/2003, N.3674/2008, N.3917/2011, ΠΔ47/2005**).

Η παραβίαση του απορρήτου των επικοινωνιών είναι ποινικό αδίκημα. Στη νομοθεσία (**άρθρο 370Α του Ποινικού Κώδικα, N.3674/2008, N.3115/2003, όπως ισχύει**) προβλέπονται αυστηρές ποινικές κυρώσεις έναντι φυσικών προσώπων (*έως 10 ετής κάθειρξη*). Εξάλλου, η παραβίαση της νομοθεσίας περί απορρήτου των επικοινωνιών επισύρει την επιβολή διοικητικών κυρώσεων έναντι παρόχων ηλεκτρονικών επικοινωνιών (*σύσταση, χρηματικό πρόστιμο, ανάκληση του δικαιώματος παροχής υπηρεσιών*), από την ΑΔΑΕ και άλλες Δημόσιες Αρχές. Επομένως, κάθε χρήστης υπηρεσιών ηλεκτρονικών επικοινωνιών μπορεί, εάν παραβιάζεται το απόρρητο της επικοινωνίας του, να προσφεύγει στα δικαστήρια, πολιτικά ή/και ποινικά, για ικανοποίησή του.

Η ΑΔΑΕ εξετάζει καταγγελίες για παραβίαση του απορρήτου των επικοινωνιών και απαντά σε ερωτήματα σχετικά με το απόρρητο. Πληροφορίες για την υποβολή καταγγελίας, καθώς και για τη νομοθεσία που αφορά το απόρρητο υπάρχουν στον σύνδεσμο «**Συχνές ερωτήσεις και απαντήσεις για τον πολίτη**» της ΑΔΑΕ: www.adae.gr/online-ypiresies/erotiseis-gia-polites. Οι καταγγελίες και τα ερωτήματα υποβάλλονται ταχυδρομικώς ή αυτοπροσώπως (*στη διεύθυνση: Ιερού Λόχου 3, Μαρούσι 151 24, Αθήνα*), με τηλεομοιοτυπία (*fax*) στον αριθμό **+30 210 6387666**, καθώς και ηλεκτρονικά (www.adae.gr) ή μέσω ηλεκτρονικού ταχυδρομείου (info@adae.gr).

Καταγγελίες που σχετίζονται με ζητήματα προσωπικών δεδομένων υποβάλλονται στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (<http://www.dpa.gr>), ενώ για ζητήματα που αφορούν σε χρεώσεις λογαριασμού ηλεκτρονικών επικοινωνιών, αρμόδια είναι η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (<http://www.eett.gr>).

Η νομοθεσία επίσης καλύπτει την προστασία του απορρήτου των ηλεκτρονικών επικοινωνιών στους χώρους εργασίας, σε περίπτωση που οι εργαζόμενοι χρησιμοποιούν συνδέσεις εσωτερικών δικτύων επικοινωνιών. Η άρση του απορρήτου των τηλεφωνικών συνδιαλέξεων και της ηλεκτρονικής αλληλογραφίας των εργαζομένων μπορεί να γίνει μόνο υπό συγκεκριμένες προϋποθέσεις και υπό τις εγγυήσεις του Νόμου.



ΕΥΘΥΝΕΣ ΠΑΡΟΧΩΝ ΚΑΙ ΧΡΗΣΤΩΝ / ΣΥΝΔΡΟΜΗΤΩΝ

Η διασφάλιση του απορρήτου των ηλεκτρονικών επικοινωνιών πρέπει να αποτελεί μέλημα και ευθύνη τόσο των παρόχων των υπηρεσιών αυτών όσο και των χρηστών και συνδρομητών τους.

Οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών είναι υπεύθυνοι για τη διασφάλιση του απορρήτου των επικοινωνιών στο δημόσιο τηλεπικοινωνιακό δίκτυο (*δίκτυο κορμού και πρόσβασης*), καθώς και στους δρομολογητές (*routers*) και εξυπηρετητές (*servers*) μέσω των οποίων παρέχεται πρόσβαση στο Διαδίκτυο και στις διάφορες υπηρεσίες. Η ΑΔΑΕ είναι αρμόδια για την τήρηση της νομοθεσίας για τη διασφάλιση του απορρήτου των επικοινωνιών και για τον σκοπό αυτό έχει εκδώσει κανονισμούς και παρακολουθεί την εφαρμογή τους ελέγχοντας τακτικά και έκτακτα τους παρόχους.

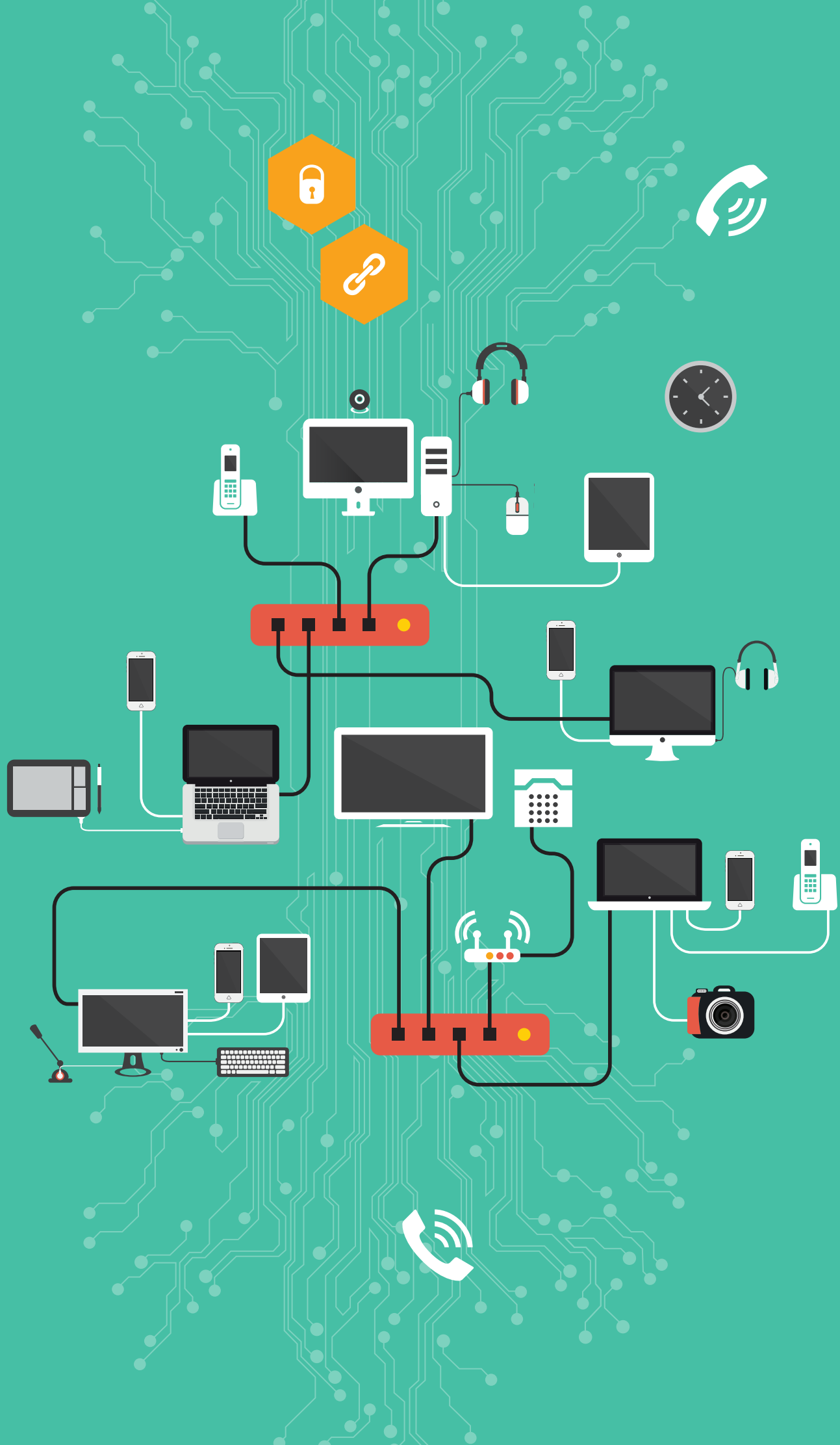
Οι συνδρομητές / χρήστες οφείλουν να μεριμνούν για τη διασφάλιση του απορρήτου της επικοινωνίας στα ιδιωτικά τους δίκτυα, τα οποία περιλαμβάνουν τις καλωδιώσεις στα κτήρια, τα τοπικά δίκτυα (*LANs*), τα ασύρματα τοπικά δίκτυα (*Wireless LANs - WLANs*), τα ιδιωτικά τηλεφωνικά κέντρα και τις τερματικές συσκευές (*π.χ. σταθερά ενσύρματα και ασύρματα τηλέφωνα, κινητά τηλέφωνα, συσκευές τηλεομοιοτυπίας (fax), κάθε είδους προσωπικοί υπολογιστές κλπ.*).

ΜΕΤΡΑ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ ΣΤΗ ΣΤΑΘΕΡΗ ΤΗΛΕΦΩΝΙΑ

Η προστασία των σταθερών τερματικών συσκευών (*σταθερών τηλεφώνων*) καθώς και του τμήματος του δικτύου που βρίσκεται μέσα στο σπίτι ή το γραφείο, είναι βασικός παράγοντας για την προστασία του απορρήτου της επικοινωνίας σας.

Τι μπορείτε να κάνετε:

- Προστατέψτε την τηλεφωνική σας συσκευή ώστε να μην είναι δυνατή η πρόσβαση σε αυτή ή στον χώρο που βρίσκεται, από ανθρώπους που δεν γνωρίζετε.
- Αν χρησιμοποιείτε ασύρματη συσκευή, να αποφεύγετε τη χρήση της σε πολύ απομακρυσμένα σημεία από τη βάση του της συσκευής, διότι είναι πιθανό να υπάρχουν παρεμβολές από παρόμοιες ασύρματες συσκευές γειτονικών σπιτιών.
- Οι κατανεμητές εσωτερικών δικτύων στις κατοικίες και στις πολυκατοικίες (*εσχαλίτ*), στους οποίους τερματίζει το δημόσιο τηλεπικοινωνιακό δίκτυο και διασυνδέεται με το εσωτερικό δίκτυο, θα πρέπει να είναι ασφαλισμένοι και προσβάσιμοι μόνο από άτομα που έχετε εξουσιοδοτήσει εσείς. Να ελέγχετε σε τακτά χρονικά διαστήματα τα παραπάνω σημεία για πιθανή παραβίασή τους, με τη βοήθεια τεχνικών της εμπιστοσύνης σας.
- 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 έχει οδηγίες να κάνει τεχνικές εργασίες στο σπίτι ή στην πολυκατοικία, απαιτήστε να σας δείξει τη διαπίστευση της εταιρείας στην οποία εργάζεται.



ΜΕΤΡΑ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΗΣ ΕΠΙΚΟΙΝΩΝΙΑΣ ΣΕ ΙΔΙΩΤΙΚΑ ΤΗΛΕΦΩΝΙΚΑ ΔΙΚΤΥΑ

Εάν διαθέτετε ιδιωτικό τηλεφωνικό κέντρο (*PABX*) και το αντίστοιχο εσωτερικό δίκτυο (*LAN*), συνιστώνται τα παρακάτω μέτρα:

- Σε συνεργασία με τον προμηθευτή του τηλεφωνικού σας κέντρου, εξασφαλίστε την τακτική επικαιροποίηση των μηχανισμών ασφαλείας του εξοπλισμού *PABX* προς αποφυγή παραβίασής του.
- Απενεργοποιήστε τους προ-εγκατεστημένους κωδικούς πρόσβασης στις θύρες για εξ αποστάσεως συντήρηση (*maintenance port*) του εξοπλισμού σας (*PABX*) και αλλάζετε σε τακτά χρονικά διαστήματα τους κωδικούς πρόσβασης που έχετε ορίσει.
- Εξασφαλίστε ότι κάθε εσωτερική συσκευή έχει δικό της ανεξάρτητο κωδικό πρόσβασης (*password*), ο οποίος είναι διαφορετικός από τον κωδικό πρόσβασης άλλης συσκευής.
- Απενεργοποιήστε την πρόσβαση μέσω του εξοπλισμού (*PABX*) στο Διαδίκτυο στην περίπτωση που δεν χρειάζεται.
- Παραμετροποιήστε τον εξοπλισμό (*PABX*) με τέτοιο τρόπο ώστε να μην επιτρέπεται καμία σύνδεση προς τα εξωτερικά δίκτυα, *call forwarding* κλπ., εκτός από εκείνες που έχουν προσδιοριστεί ως αναγκαίες για τη λειτουργία των υπηρεσιών του εκάστοτε χρήστη.
- Ενεργοποιήστε τη δυνατότητα απομακρυσμένης πρόσβασης μόνο όταν κρίνεται απαραίτητο, διαφορετικά θα ήταν προτιμότερο να είναι απενεργοποιημένη.
- Περιορίστε τις *IP* διευθύνσεις που μπορούν να έχουν πρόσβαση στις ανοικτές πόρτες του κέντρου στις απόλυτα αναγκαίες περιπτώσεις.
- Εφαρμόστε τα κατάλληλα μέτρα φυσικής ασφάλειας κυρίως σε ό,τι αφορά στην πρόσβαση στο χώρο εγκατάστασης του *PABX* και του αντίστοιχου καταναεμητή, όπου συγκεντρώνονται οι καλωδιώσεις του δικτύου σας.
- Ελέγχετε συχνά όλα τα ευαίσθητα σημεία της εγκατάστασης, χρησιμοποιώντας εξειδικευμένους τεχνικούς της εμπιστοσύνης σας.

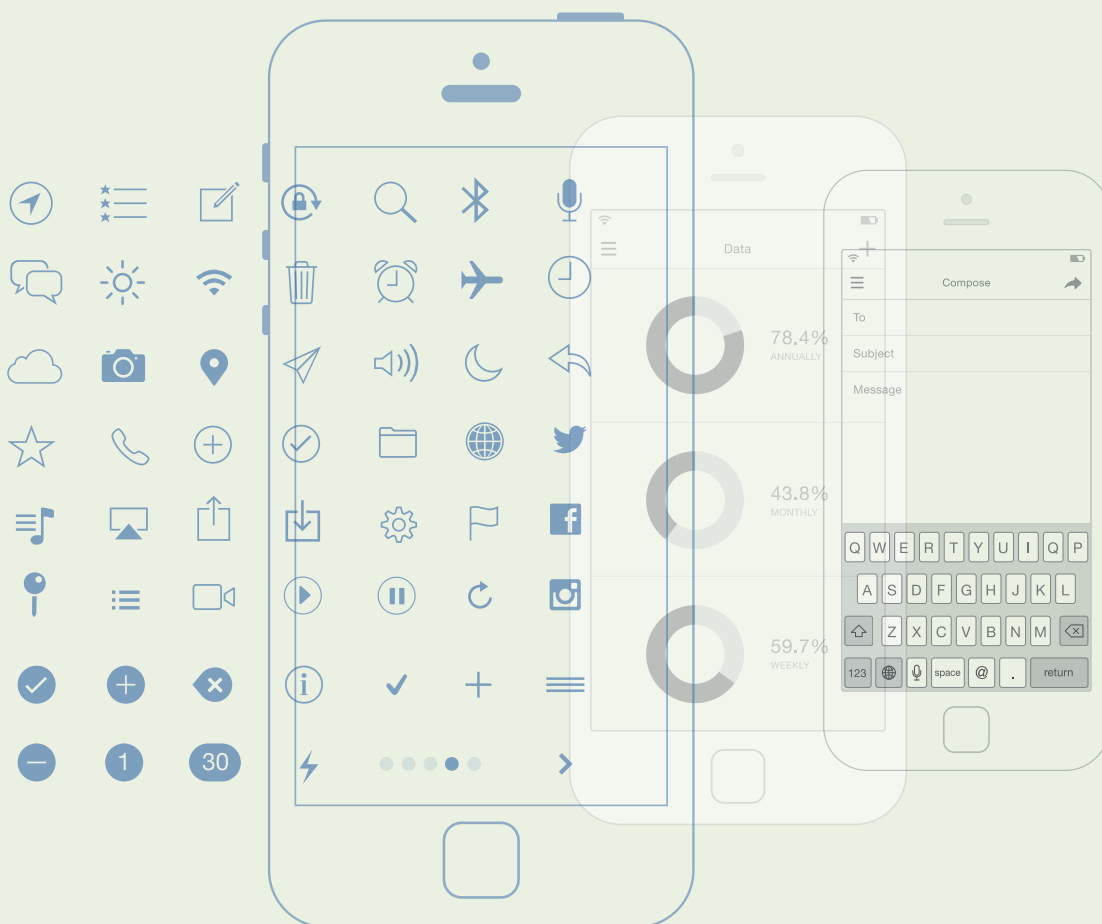


Ελεγχόμενη πρόσβαση στην τηλεφωνική συσκευή

- Εφαρμόστε κάποια μορφή ελεγχόμενης πρόσβασης στη συσκευή σας, όπως κλείδωμα της κάρτας SIM με τον 4-ψήφιο κωδικό PIN και ξεκλείδωμα της οθόνης του κινητού σας τηλεφώνου επιλέγοντας μεταξύ ενός απλού 4-ψήφιου κωδικού, ενός πιο σύνθετου κωδικού πρόσβασης (*password*) ή ενός μοτίβου ξεκλειδώματος συσκευής (*pattern lock*), το οποίο σχεδιάζεται στην οθόνη της συσκευής για να την ξεκλειδώνει.
- Ρυθμίστε τη συσκευή σας ώστε η οθόνη να κλειδώνει αυτόματα μετά από μερικά λεπτά.
- Επιλέξτε να μην εμφανίζονται οι κωδικοί πρόσβασης κατά την πληκτρολόγησή τους από τις σχετικές ρυθμίσεις της συσκευής σας.
- Μην αφήνετε το κινητό σας εκτεθειμένο και προστατεύστε το από το ενδεχόμενο κλοπής.
- Πριν από την αποστολή προς επισκευή αντικατάσταση ή ανακύκλωση της τηλεφωνικής σας συσκευής, βεβαιωθείτε ότι έχετε διαγράψει όλα τα προσωπικά ή άλλα εμπιστευτικά δεδομένα και έχετε αφαιρέσει την κάρτα SIM.

Ασφαλής χρήση Bluetooth

- Χρησιμοποιήστε το Bluetooth με τέτοιο τρόπο, ώστε η συσκευή σας να μην είναι «ορατή» από άλλες και μην επιτρέπετε την πρόσβαση σε μη έμπιστες συσκευές τις οποίες δεν αναγνωρίζετε.
- Θα πρέπει να είστε προσεκτικοί στην εγκατάσταση προγραμμάτων ή αρχείων που λαμβάνονται μέσω Bluetooth. Αν σας ζητηθεί μέσω του λογισμικού της συσκευής σας να εγκαταστήσετε κάποιο άγνωστο πρόγραμμα, συνιστάται να το αποφύγετε.

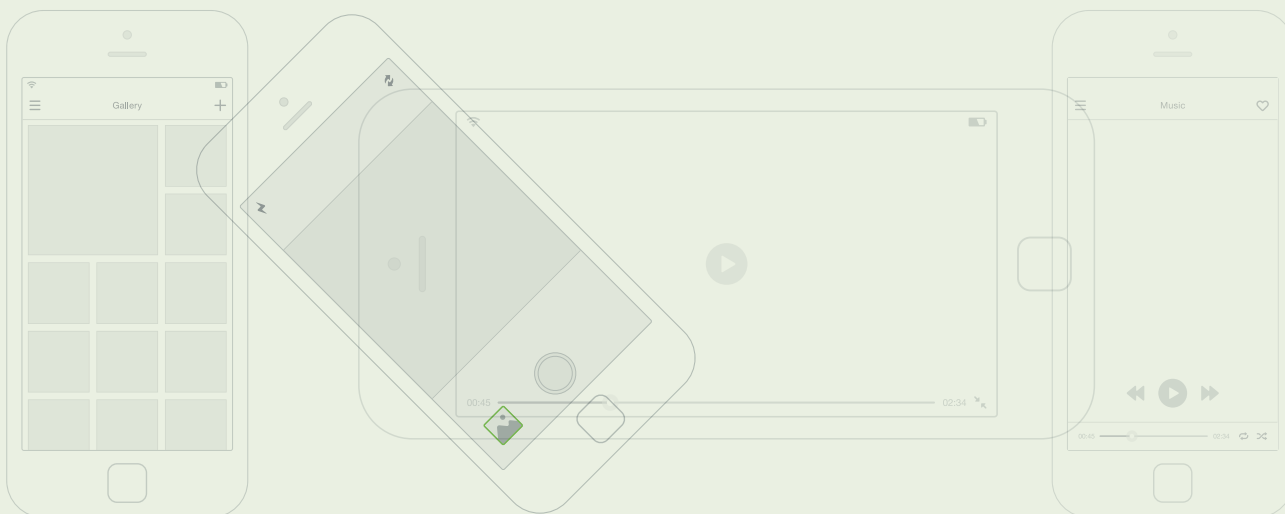


Δυνατότητα απόκρυψης του τηλεφωνικού σας αριθμού

• Οι συσκευές κινητής τηλεφωνίας δίνουν τη δυνατότητα απόκρυψης του τηλεφωνικού σας αριθμού από τον παραλήπτη της κλήσης σας. Εντούτοις, η απόκρυψη δεν ισχύει στην περίπτωση αποστολής μηνυμάτων κειμένου ή πολυμέσων (SMS, MMS).

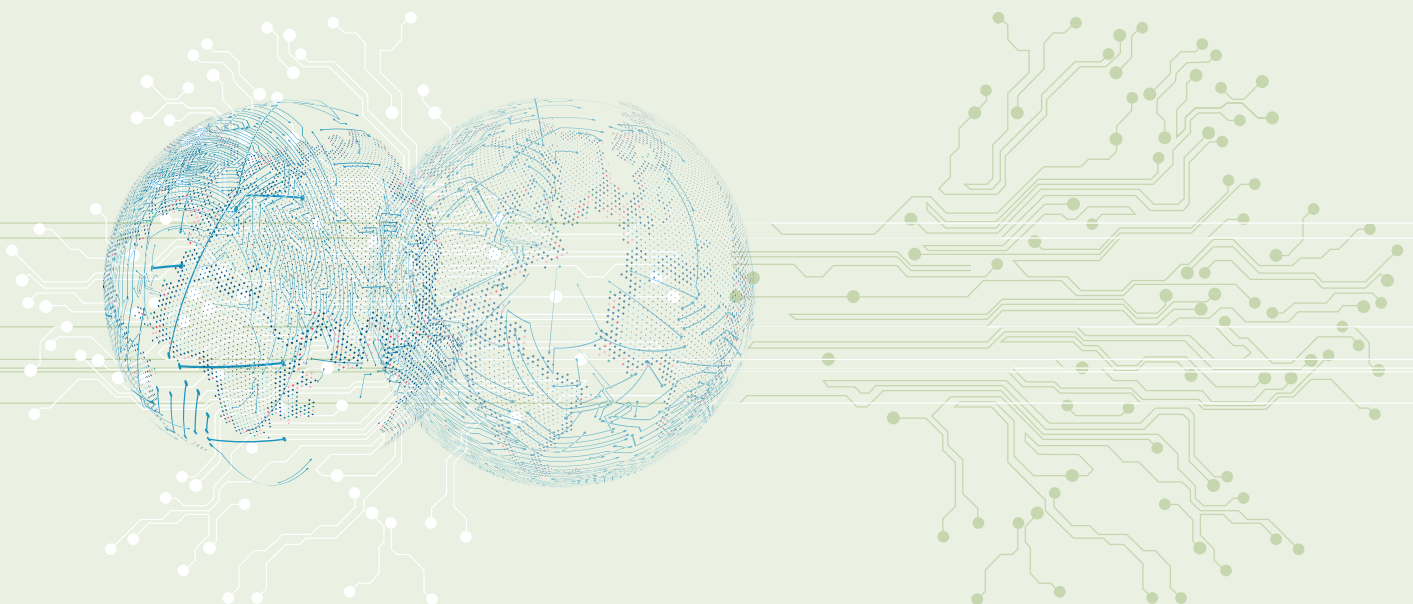
Προστασία συσκευών Smartphone

- Για προστασία από εγκατάσταση κακόβουλου λογισμικού, ελέγχετε περιοδικά τις εγκατεστημένες εφαρμογές, τον διαθέσιμο αποθηκευτικό χώρο, καθώς και τη χρήση της συσκευής σας (π.χ. αριθμός απεσταλμένων μηνυμάτων, διάρκεια κλήσεων), προσέχοντας για τυχόν ασυνήθιστη χρήση. Πραγματοποιήστε “επαναφορά στις εργοστασιακές ρυθμίσεις” της συσκευής, αν έχετε βάσιμες υποψίες ότι κάποιος ιός έχει εγκατασταθεί.
- Οι περισσότερες συσκευές κινητής τηλεφωνίας υποστηρίζουν ειδικές εφαρμογές που μπορούν να εντοπίσουν μια συσκευή που έχει χαθεί. Πιθανώς χρειάζεται να εγκαταστήσετε ή να ενεργοποιήσετε τέτοιες εφαρμογές, ώστε, σε περίπτωση κλοπής, να μπορείτε να διαγράψετε τα δεδομένα στη συσκευή σας μέσω απομακρυσμένης πρόσβασης.
- Η κρυπτογράφηση προστατεύει τα δεδομένα σας από προηγμένες επιθέσεις. Ορισμένες συσκευές χρησιμοποιούν προεπιλεγμένα την κρυπτογράφηση, ενώ σε άλλες χρειάζεται να ενεργοποιηθεί από τον χρήστη ή να εγκατασταθεί λογισμικό κρυπτογράφησης.
- Τα ηλεκτρονικά μηνύματα (e-mail, MMS), που λαμβάνετε σε συσκευές κινητής τηλεφωνίας, θα πρέπει να τα αντιμετωπίζετε με τον ίδιο τρόπο, όπως αυτά που λαμβάνετε στον προσωπικό σας υπολογιστή. Αν κάποιο μήνυμα φαίνεται ύποπτο ή δεν γνωρίζετε τον αποστολέα, αποφύγετε να το ανοίξετε.
- Αποφύγετε να κατεβάσετε περιεχόμενο στη συσκευή σας από το Διαδίκτυο από μία άγνωστη ή μη αξιόπιστη πηγή.
- Εγκαταστήστε στη συσκευή σας κάποιο πρόγραμμα προστασίας από κακόβουλο λογισμικό (antivirus) έξυπνων τηλεφώνων (smartphones).
- Για να αποφύγετε την κοινοποίηση της τοποθεσίας που βρίσκεστε (location information) μέσω εφαρμογών που χρησιμοποιείτε (π.χ. κοινωνικά δίκτυα, εφαρμογές instant messaging) μπορείτε να επιλέξετε στη συσκευή σας τη δυνατότητα μη αυτόματης κοινοποίησης της πληροφορίας αυτής.
- Στην περίπτωση χρήσης υπηρεσιών εντοπισμού θέσης και πλοήγησης (GPS navigation), μπορείτε να εγκαταστήσετε τους χάρτες στη συσκευή σας, ώστε να μην απαιτείται η πρόσβαση στο Διαδίκτυο για την πλοήγησή σας και έτσι να αποφύγετε την κοινοποίηση της τοποθεσίας που βρίσκεστε.
- Φροντίστε να λαμβάνετε σε τακτά διαστήματα αντίγραφα ασφαλείας των δεδομένων της συσκευής σας, τοπικά στον υπολογιστή σας ή σε έμπιστη υπηρεσία χώρου αποθήκευσης στο Διαδίκτυο (Cloud). Συνιστάται να κρυπτογραφείτε τα αντίγραφα ασφαλείας, ιδιαίτερα στην περίπτωση που μεταφέρονται ή αποθηκεύονται στο Διαδίκτυο.



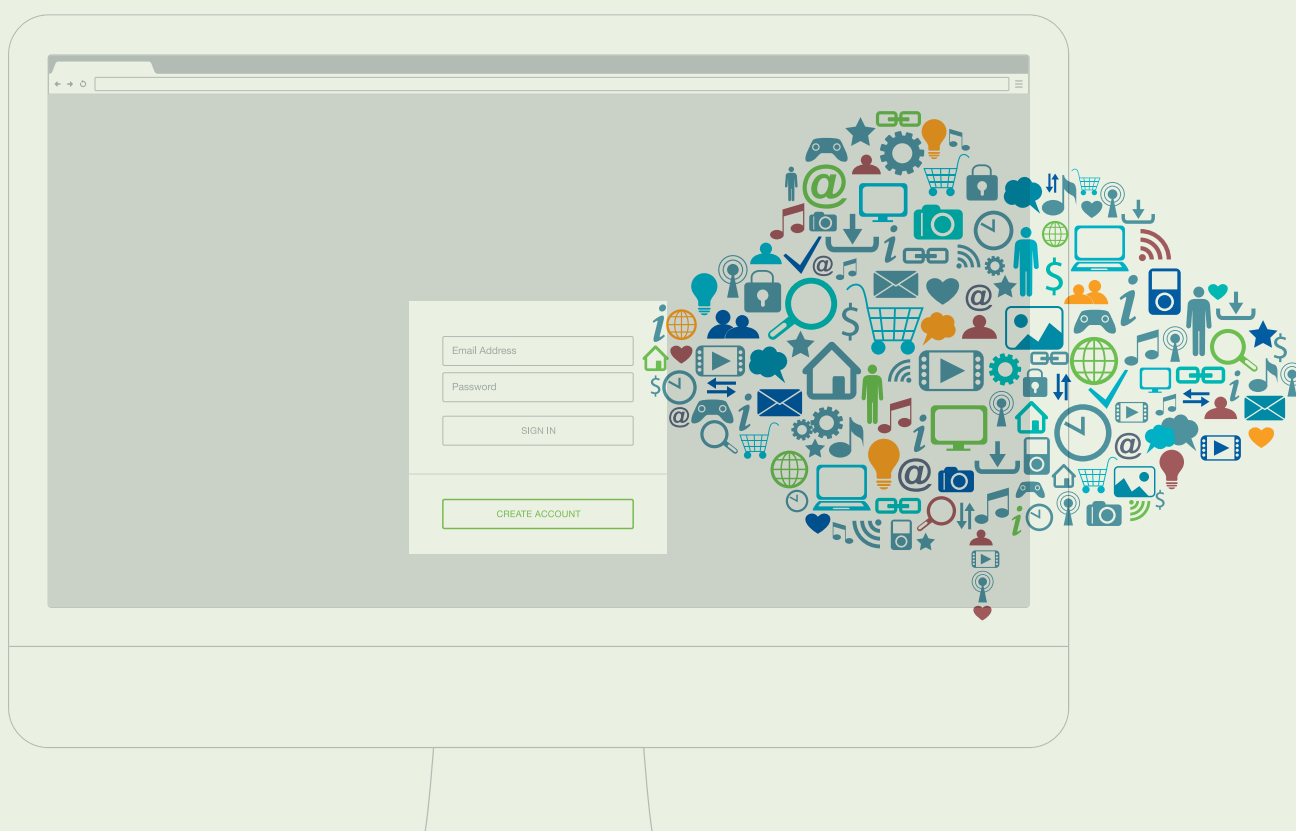
ΜΕΤΡΑ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΚΑΤΑ ΤΗΝ ΠΡΟΣΒΑΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

- 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 αλλάζετε τους σε τακτικά χρονικά διαστήματα (τουλάχιστον *μία 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.



ΜΕΤΡΑ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΚΑΤΑ ΤΗΝ ΠΡΟΣΒΑΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

- 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 διαγράψετε 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.



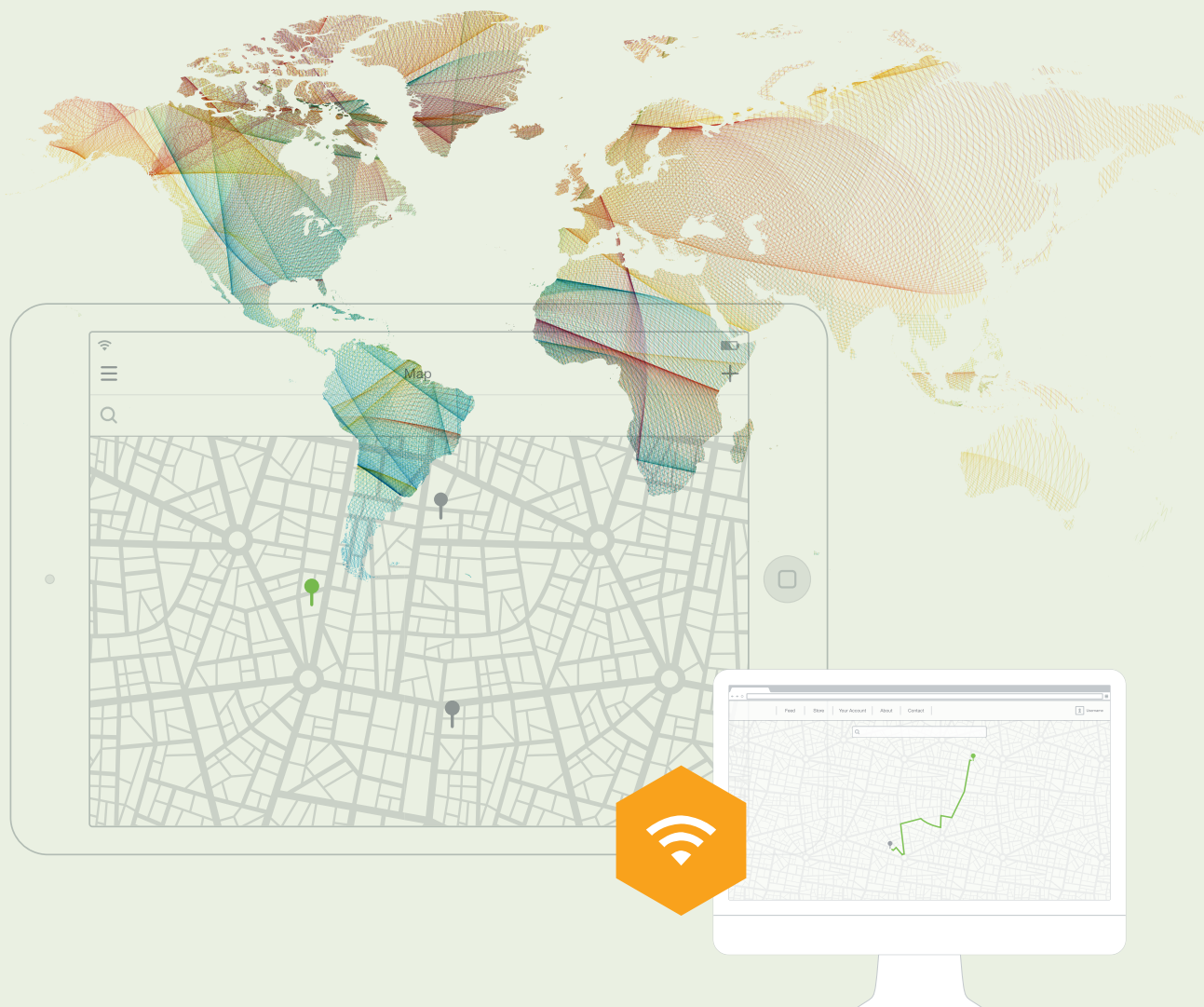
ΜΕΤΡΑ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΣΤΗΝ ΗΛΕΚΤΡΟΝΙΚΗ ΑΛΛΗΛΟΓΡΑΦΙΑ

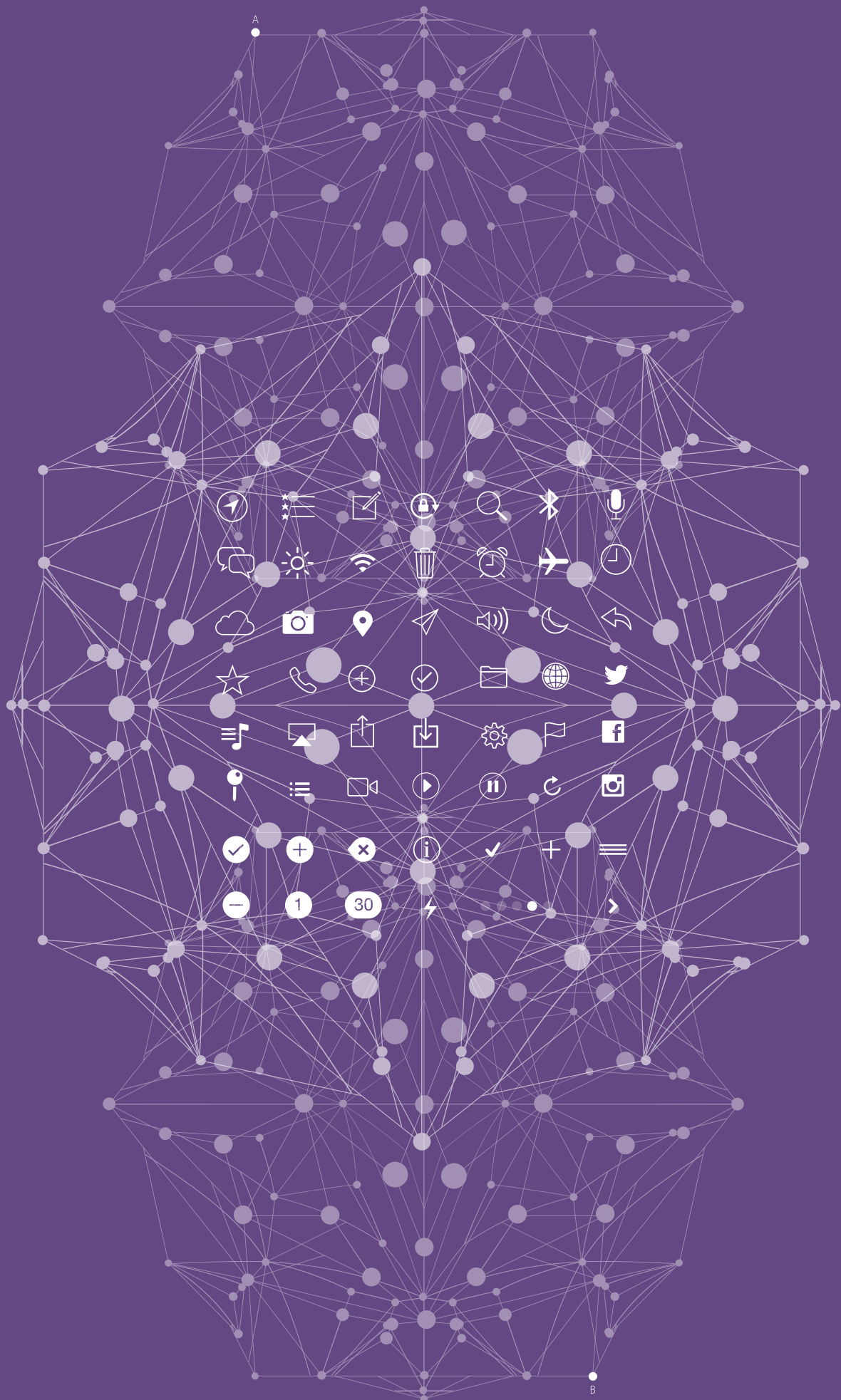
- Αν ο λογαριασμός ηλεκτρονικής αλληλογραφίας σας παραβιάστηκε πρόσφατα ή αν τρίτοι απέκτησαν πρόσβαση σε αυτόν, θα πρέπει να αλλάξετε άμεσα τον κωδικό πρόσβασής σας.
- Μη χρησιμοποιείτε ποτέ τον κωδικό πρόσβασης του λογαριασμού σας για την πρόσβαση σε άλλους ιστότοπους.
- Μην ανοίγετε συνημμένα αρχεία 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 προσεκτικά 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.



ΜΕΤΡΑ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΚΑΤΑ ΤΗΝ ΑΣΥΡΜΑΤΗ ΠΡΟΣΒΑΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

- 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 ελέγχετε 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.





ΚΑΚΟΒΟΥΛΕΣ ΚΑΙ ΕΝΟΧΛΗΤΙΚΕΣ ΚΛΗΣΕΙΣ

Εάν δέχεστε κακόβουλες ή ενοχλητικές κλήσεις με απόκρυψη, έχετε το δικαίωμα να ζητήσετε από τον πάροχο της σύνδεσής σας, για συγκεκριμένο χρονικό διάστημα που δεν μπορεί να υπερβαίνει τις δεκαπέντε ημέρες, να προχωρήσει στην εξουδετέρωση της δυνατότητας μη αναγραφής της καλούσας γραμμής για τις εισερχόμενες κλήσεις και να σας γνωστοποιήσει εγγράφως κατάλογο με τους αριθμούς που σας κάλεσαν στο διάστημα αυτό.

Στην περίπτωση που επιθυμείτε να ενημερωθείτε και για την ταυτότητα του συνδρομητή ή χρήστη που σας καλεί κακόβουλα, αυτό θα πρέπει να διαταχθεί από τον αρμόδιο κατά περίπτωση τακτικό ανακριτή ή εισαγγελέα με ειδική παραγγελία προς τους παρόχους, στο πλαίσιο τακτικής ανάκρισης ή προανάκρισης ή προκαταρκτικής εξέτασης κατόπιν σχετικής εγκλήσεως.

Περισσότερες πληροφορίες για τη διαδικασία αυτή μπορείτε να βρείτε στην ιστοσελίδα της ΑΔΑΕ, στην ενότητα «**Νομοθετικό Πλαίσιο**», (<http://www.adae.gr/nomothetiko-plaisio/elliniki-nomothesia/praxeis-tis-adae/>).

ΓΕΝΙΚΗ ΕΠΙΣΗΜΑΝΣΗ

Στην ιστοσελίδα της ΑΔΑΕ θα βρείτε μια πιο αναλυτική παρουσίαση των παραπάνω μέτρων.

Αν έχετε ενδείξεις παραβίασης του απορρήτου των επικοινωνιών σας - και αναλόγως του προβλήματος που εμφανίζεται - συνιστάται να εφαρμόσετε τα μέτρα που προτείνονται παραπάνω, στην αντίστοιχη κατηγορία ηλεκτρονικής επικοινωνίας (π.χ. για τις ηλεκτρονικές υπηρεσίες αλλαγή του κωδικού πρόσβασης ή για κινητό τηλέφωνο απενεργοποίηση της πρόσβασης στο Διαδίκτυο κ.ά.).

Στη συνέχεια, μεταξύ άλλων, μπορείτε να:

- Ζητήσετε από τον πάροκό σας να πραγματοποιήσει έλεγχο στη σύνδεσή σας και να σας ενημερώσει εγγράφως.
- Υποβάλετε καταγγελία στην ΑΔΑΕ για παραβίαση του απορρήτου των επικοινωνιών σας (δείτε παραπάνω στην ενότητα «Εισαγωγή»).
- Απευθυνθείτε στις δικαστικές αρχές με υποβολή μήνυσης ή αγωγής για αποζημίωση, αν έχετε δεδομένα που στοιχειοθετούν παραβίαση του απορρήτου σας.





Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) είναι μια από τις συνταγματικά καθιερωμένες Ανεξάρτητες Αρχές με διοικητική αυτοτέλεια, οι οποίες υπόκεινται σε κοινοβουλευτικό έλεγχο. Συστάθηκε το 2003 με τον νόμο 3115 και ανέλαβε αρμοδιότητες για την προστασία του απορρήτου της επικοινωνίας. Για τον σκοπό αυτό εκδίδει κανονισμούς με τους οποίους προβλέπει πολιτικές ασφάλειας που θα πρέπει να εφαρμόζουν οι εταιρείες παροχής δικτύων ή / και υπηρεσιών ηλεκτρονικών επικοινωνιών καθώς και οι πάροχοι ταχυδρομικών υπηρεσιών. Επίσης παρακολουθεί με ελέγχους την εφαρμογή των πολιτικών ασφάλειας για την προστασία του απορρήτου των επικοινωνιών, εξετάζει καταγγελίες και επιβάλλει κυρώσεις. Στις αρμοδιότητές της περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου που προβλέπονται από τον νόμο. Η ΑΔΑΕ παρακολουθεί τις συνεχείς εξελίξεις στον δυναμικό κλάδο των ηλεκτρονικών επικοινωνιών και συνεργάζεται με άλλες αρχές της χώρας και με ευρωπαϊκούς ή διεθνείς οργανισμούς για να αντιμετωπίσει τις νέες προκλήσεις που θέτουν σε θέματα ασφάλειας και προστασίας του απορρήτου των επικοινωνιών.

ΑΔΑΕ

› ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ <

Ιερού Λόχου 3 _ 151 24 Μαρούσι

Τηλ.: 210 6387600 _ Fax: 210 6387666

E-mail: info@adae.gr

URL: www.adae.gr