ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Νοέμβριος 2024

dpo@eap.gr

Στην εποχή της Ψηφιακής Επανάστασης η προστασία των Δεδομένων Προσωπικού Χαρακτήρα (εφεξής ΔΠΧ ή προσωπικά δεδομένα) συνιστά μία από τις, πλέον, επιτακτικές και σύνθετες προκλήσεις για όλους μας. Καθώς η πλειονότητα των προσωπικών και επαγγελματικών δραστηριοτήτων λαμβάνει χώρα διαδικτυακά, η ανάγκη για τη θεμελιώδη προστασία της ιδιωτικότητας και της ασφάλειας των προσωπικών δεδομένων είναι, πλέον, αδιαμφισβήτητη και απολύτως κρίσιμη για την προστασία των δικαιωμάτων, ως υποκειμένων των δεδομένων, όπως προβλέπεται από τον Γενικό Κανονισμό για την Προστασία Δεδομένων (ΓΚΠΔ 2016/679).

Τα ΔΠΧ περιλαμβάνουν ευρύ φάσμα πληροφοριών που σχετίζονται με ταυτοποιήσιμα, φυσικά πρόσωπα, όπως το ονοματεπώνυμο, τον αριθμό ταυτότητας, τη διεύθυνση ηλεκτρονικού ταχυδρομείου και άλλες πληροφορίες που όταν συλλέγονται ή υποβάλλονται σε επεξεργασία, δύνανται να επηρεάσουν, άμεσα, την ιδιωτική ζωή των ατόμων. Η έννοια της προστασίας των προσωπικών δεδομένων δεν περιορίζεται, μόνο, στην ασφάλεια των δεδομένων έναντι μη εξουσιοδοτημένης πρόσβασης ή κακόβουλων ενεργειών αλλά καλύπτει την ορθή και νόμιμη διαχείριση των δεδομένων, σύμφωνα με τις αρχές της διαφάνειας, της αναλογικότητας και της λογοδοσίας, όπως ορίζονται στον ΓΚΠΔ και στην, εν γένει, κείμενη νομοθεσία.

Ο παρών οδηγός έχει ως σκοπό να ενισχύσει την κατανόησή σας, αναφορικά με τη σημασία της προστασίας των ΔΠΧ και να παρέχει πρακτικές συμβουλές και κατευθυντήριες οδηγίες για την ασφαλή διαχείρισή τους στην καθημερινή σας ζωή. Από την ασφαλή χρήση των ηλεκτρονικών σας συσκευών και τη θωράκιση των λογαριασμών σας σε κοινωνικά δίκτυα μέχρι την ασφαλή περιήγηση σε διαδικτυακές υπηρεσίες και τη χρήση κρυπτογραφημένων επικοινωνιών, ο οδηγός αυτός περιέχει καλές πρακτικές και αναγκαία μέτρα που θα συμβάλλουν στην προστασία των δικαιωμάτων σας, ως υποκειμένων των δεδομένων, καθιστώντας σας όχι μόνο συμμορφούμενους αλλά και ενεργούς φορείς προστασίας της ιδιωτικής σας ζωής.

Συμβουλές και καλές πρακτικές

Οι παρακάτω συμβουλές και καλές πρακτικές είναι ενδεικτικές για την προστασία των ΔΠΧ στον ψηφιακό κόσμο. Είναι σημαντικό να σημειώσουμε ότι οι ψηφιακοί κίνδυνοι εξελίσσονται συνεχώς, γι' αυτό και πρέπει να παρακολουθούμε τα γεγονότα και να εμπλουτίζουμε, συνεχώς, τις ψηφιακές μας γνώσεις. Ορισμένες από τις προτάσεις ενδέχεται να απαιτούν επιπρόσθετη, εξειδικευμένη γνώση, γι' αυτό συνίσταται να επικοινωνήσετε με κάποιον ειδικό. Καμία τεχνολογική λύση δε μπορεί να εγγυηθεί απόλυτη ασφάλεια, ανεξαρτήτως των μέτρων που λαμβάνονται καθώς πάντα θα υπάρχει ο ανθρώπινος παράγοντας.

Βασικές Ρυθμίσεις Απορρήτου και Ενημέρωση

- **Διαβάστε τις Πολιτικές Απορρήτου**: Πριν χρησιμοποιήσετε κάποια εφαρμογή ή υπηρεσία, δείτε την πολιτική απορρήτου της. Βεβαιωθείτε ότι κατανοείτε ποιά δεδομένα συλλέγονται και χρησιμοποιούνται. Αν κάτι δεν είναι σαφές, προτιμήστε να μη χρησιμοποιήσετε την υπηρεσία.
- **Χρησιμοποιήστε Ρυθμίσεις Απορρήτου**: Πολλές πλατφόρμες και συσκευές (smartphone, H/Y, tablet, smart TV, camera) παρέχουν εργαλεία και ρυθμίσεις απορρήτου. Αξιοποιήστε αυτές τις ρυθμίσεις για να περιορίσετε τα δεδομένα που μοιράζεστε.
- **Ελέγξτε τις Συγκαταθέσεις σας**: Αν έχετε δώσει συγκατάθεση για την επεξεργασία των δεδομένων σας σε διάφορες εταιρείες, θυμηθείτε να ελέγχετε, περιοδικά, αν θέλετε ακόμα, να ισχύει η συγκατάθεση ή αν πρέπει να την ανακαλέσετε.
- **Περιορίστε τις Εφαρμογές που Καταγράφουν Δεδομένα Υγείας**: Αν χρησιμοποιείτε εφαρμογές υγείας ή φυσικής κατάστασης, διαβάστε, προσεκτικά, την πολιτική απορρήτου και χρησιμοποιήστε, μόνο, αξιόπιστες, ασφαλείς εφαρμογές.
- **Ελέγχετε την Πολιτική Απορρήτου των IoT Συσκευών σας**: Αν έχετε έξυπνες συσκευές (smart led, smart watch, smart ηχείο, smart κουδούνι, κλπ.) στο σπίτι, βεβαιωθείτε ότι οι πολιτικές απορρήτου τους είναι διαφανείς και ασφαλείς. Απενεργοποιήστε τη συλλογή δεδομένων εφόσον δε χρειάζεται.
- **Αξιολογήστε τις προτιμήσεις "Do Not Track" στα προγράμματα περιήγησης**: Η ενεργοποίηση της επιλογής "Do Not Track" βοηθά στον περιορισμό της καταγραφής της δραστηριότητάς σας από ιστότοπους.
- **Δώστε Προσοχή σε Ενημερώσεις Λογισμικού**: Ενημερώνετε, τακτικά το λογισμικό και τις εφαρμογές σας για να προστατευτείτε από νέες απειλές ασφάλειας που μπορεί να εντοπίζονται και να διορθώνονται με νέες εκδόσεις.
- **Ελέγξτε Τακτικά τα Δεδομένα σας με Αναζητήσεις**: Μία απλή αναζήτηση στο διαδίκτυο με το όνομά σας μπορεί να σας βοηθήσει να δείτε τί πληροφορίες είναι, δημόσια, διαθέσιμες για εσάς και να ζητήσετε τη διαγραφή ή απόκρυψή τους εάν δεν θέλετε να παραμένουν προσβάσιμες.
- **Ελέγξτε τα Δικαιώματα Στις Επαφές Σας**: Εξετάστε ποιοι έχουν πρόσβαση στις επαφές σας στο κινητό σας τηλέφωνο και περιορίστε την πρόσβαση, μόνο, στις εφαρμογές που τη χρειάζονται, πραγματικά.
- **Αναθεωρήστε τις Ρυθμίσεις για Φωτογραφίες με Γεωγραφική Τοποθεσία**: Ορισμένες κάμερες και smartphones ενσωματώνουν πληροφορίες τοποθεσίας στις φωτογραφίες σας. Συνίσταται να απενεργοποιήστε την καταγραφή γεωγραφικής θέσης στις ρυθμίσεις της κάμερας.
- **Απενεργοποιήστε τη Δυνατότητα Ανίχνευσης Συσκευής**: Σε εφαρμογές που παρέχουν τη δυνατότητα ανίχνευσης της συσκευής (smartphone) σας, όπως για βελτίωση τοποθεσίας, εξετάστε αν είναι απαραίτητη ή αν μπορεί να απενεργοποιηθεί.
- **Χρησιμοποιήστε φίλτρα προστασίας προσωπικών δεδομένων στα κοινωνικά δίκτυα**: Ρυθμίστε το προφίλ σας στα social media ώστε, μόνο, εγκεκριμένα άτομα να

βλέπουν τις αναρτήσεις σας και περιορίστε τις πληροφορίες που είναι, δημόσια, διαθέσιμες.

- **Περιορίστε τα Metadata των Αρχείων σας**: Πολλά αρχεία, όπως φωτογραφίες και έγγραφα, περιέχουν πληροφορίες, όπως τοποθεσία, ημερομηνία και τύπο συσκευής. Μπορείτε να αφαιρέσετε αυτά τα δεδομένα πριν από την κοινοποίηση αρχείων.
- **Ρυθμίστε τις συσκευές σας να "απενεργοποιούνται αυτόματα"**: Αυτό είναι χρήσιμο σε περιπτώσεις απομακρυσμένης εργασίας ή απουσίας για να διασφαλίσετε ότι οι συσκευές δεν παραμένουν ενεργές και προσβάσιμες.
- **Προσαρμόστε τις ειδοποιήσεις ασφαλείας στο email σας**: Ενεργοποιήστε ειδοποιήσεις για ύποπτη δραστηριότητα και συνδεθείτε, σε τακτά διαστήματα, για να ελέγχετε αν υπάρχουν άγνωστες συνδέσεις.

Διαχείριση Κωδικών και Επαλήθευση Ταυτότητας

- **Ασφαλίστε τις Συσκευές και τους Λογαριασμούς σας**: Χρησιμοποιείτε ισχυρούς, μοναδικούς κωδικούς (τουλάχιστον 10 χαρακτήρων, με συνδυασμό κεφαλαίων γραμμάτων, πεζών γραμμάτων, αριθμών και συμβόλων) και ενεργοποιήστε την επαλήθευση δύο παραγόντων, όπου είναι διαθέσιμη. Αυτό μειώνει τον κίνδυνο μη εξουσιοδοτημένης πρόσβασης.
- **Χρησιμοποιήστε έλεγχο ταυτότητας πολλών παραγόντων (MFA)**: Οι μεγάλοι ή σύνθετοι κωδικοί πρόσβασης μπορούν να παραβιαστούν σε μία επίθεση ταυτότητας. Αποκτήστε περισσότερη προστασία με MFA. Χρησιμοποιήστε διάφορες μεθόδους MFA, όπως κείμενα, βιομετρικά στοιχεία και κωδικούς πρόσβασης μίας χρήσης για μεγαλύτερη ασφάλεια.
- **Μην Αποθηκεύετε Αυτόματα Κωδικούς Πρόσβασης σε Προγράμματα Περιήγησης**: Προτιμήστε τη χρήση εφαρμογών διαχείρισης κωδικών πρόσβασης (password managers) για να αποθηκεύετε τους κωδικούς σας με ασφάλεια.
- **Χρησιμοποιήστε Διαφορετικούς Κωδικούς Πρόσβασης για Κάθε Λογαριασμό**: Ένας ξεχωριστός κωδικός πρόσβασης για κάθε υπηρεσία ελαχιστοποιεί τον κίνδυνο παραβίασης όλων των λογαριασμών σας αν ένας από αυτούς «χακαριστεί».
- **Προστατέψτε τα Δεδομένα σας**: Αποφύγετε να δίνετε προσωπικές πληροφορίες, όπως αριθμό ταυτότητας ή διευθύνσεις, σε ιστότοπους ή εφαρμογές που δε διαφαίνονται αξιόπιστοι. Χρησιμοποιείτε ισχυρούς κωδικούς πρόσβασης και αλλάξτε τους συχνά (συνίσταται ανά εξάμηνο).
- **Μη Χρησιμοποιείτε Δεδομένα Εύκολα Αναγνωρίσιμα ως Απαντήσεις στις Ερωτήσεις Ασφαλείας**: Σε πολλές περιπτώσεις, οι ερωτήσεις ασφαλείας χρησιμοποιούν πληροφορίες που μπορεί να ανακαλύψει κάποιος, όπως το όνομα του κατοικίδιού σας ή το γυμνάσιο που πήγατε. Επιλέξτε μη προφανείς απαντήσεις, ιδανικά, κάτι που δε σχετίζεται με τα αληθινά σας δεδομένα.
- **Απενεργοποιήστε τις Ρυθμίσεις Αυτόματης Συμπλήρωσης σε Προγράμματα Περιήγησης**: Η αυτόματη συμπλήρωση μπορεί να καταχωρήσει ευαίσθητα δεδομένα (π.χ., κωδικούς και στοιχεία καρτών) σε μη ασφαλείς ιστοσελίδες. Απενεργοποιήστε την και εισάγετε τα δεδομένα, χειροκίνητα, σε περιβάλλοντα όπου εμπιστεύεστε, πλήρως, την ασφάλεια.
- **Μην Αποθηκεύετε Πληροφορίες Πιστωτικών Καρτών σε Ιστότοπους**: Όταν ψωνίζετε online, αποφύγετε την επιλογή «αποθήκευση κάρτας» στους λογαριασμούς σας για να περιορίσετε τον κίνδυνο διαρροής οικονομικών στοιχείων, σε περίπτωση παραβίασης.
- **Δημιούργηστε εικονικά προφίλ για ιστοσελίδες και κοινωνικά δίκτυα**: Χρησιμοποιήστε διαφορετικά στοιχεία για την κάθε πλατφόρμα ώστε να περιοριστεί η δυνατότητα σύνδεσης των πληροφοριών σας από διαφορετικούς ιστότοπους.

- **Χρησιμοποιήστε μοναδικά "patterns" για τις οθόνες ξεκλειδώματος των συσκευών**: Αντί για απλούς κωδικούς, τα μοτίβα ξεκλειδώματος που είναι πιο σύνθετα προσφέρουν μία παραπάνω βαθμίδα προστασίας.
- **Δημιουργήστε αντίγραφα ασφαλείας με κρυπτογραφημένες μεθόδους και όχι στο cloud**: Αντί να χρησιμοποιείτε cloud-based backups, προτιμήστε εξωτερικούς, κρυπτογραφημένους, σκληρούς δίσκους για αντίγραφα ασφαλείας.
- **Διατηρήστε offline αρχείο με τους κωδικούς για μεγαλύτερη ασφάλεια**: Αποθηκεύστε τους κωδικούς πρόσβασής σας σε offline αρχείο που φυλάσσεται με ασφάλεια, για αποφυγή διαρροών από διαρρήξεις σε λογαριασμούς cloud.
- **Αποφύγετε τη Χρήση Μοναδικών Προσωπικών Αριθμών ως ID**: Μη χρησιμοποιείτε το ΑΦΜ σας ή άλλους μοναδικούς αριθμούς (πχ. ΑΜΚΑ) ως ταυτότητα για λογαριασμούς και προφίλ.

Ασφάλεια Συσκευών και Δικτύων

- **Αποφύγετε τις Δημόσιες Συνδέσεις Wi-Fi**: Οι ανοιχτές συνδέσεις Wi-Fi, όπως σε καφετέριες και αεροδρόμια, είναι λιγότερο ασφαλείς και ευάλωτες σε επιθέσεις. Χρησιμοποιείτε μόνο ασφαλείς, ιδιωτικές συνδέσεις ή VPN όταν χρειάζεται να μεταδώσετε προσωπικά δεδομένα.
- **Μην Ανοίγετε Ύποπτα Μηνύματα ή Συνδέσμους**: Τα emails ή μηνύματα με ύποπτες προσφορές ή συνδέσμους μπορούν να περιέχουν κακόβουλο λογισμικό που στοχεύει στην πρόσβαση στα δεδομένα σας.
- **Χρησιμοποιείτε Λογισμικά Ασφάλειας**: Εγκαταστήστε αξιόπιστο antivirus, antispyware και firewall σε όλες τις συσκευές σας. Έτσι, μπορείτε να αποτρέψετε κακόβουλα προγράμματα και επιθέσεις που μπορεί να θέσουν σε κίνδυνο τα δεδομένα σας.
- **Ελέγχετε Συχνά τις Συσκευές σας για Κακόβουλο Λογισμικό**: Κάνετε τακτικούς ελέγχους για ιούς και malware (κακόβουλο λογισμικό) ώστε να διασφαλίσετε ότι οι συσκευές σας είναι καθαρές και ασφαλείς.
- **Κρατήστε τα Δεδομένα σας σε Ασφαλείς Χώρους Αποθήκευσης**: Αν αποθηκεύετε προσωπικά δεδομένα σε εξωτερικούς δίσκους ή USB, κρυπτογραφήστε τα ώστε να είναι προστατευμένα ακόμα και αν χάσετε τη συσκευή.
- **Προτιμήστε Συσκευές με Ασφαλείς Ενημερώσεις**: Αγοράστε κινητές συσκευές ή υπολογιστές από κατασκευαστές που προσφέρουν τακτικές ενημερώσεις ασφαλείας καθώς οι αναβαθμίσεις αυτές διορθώνουν προβλήματα που μπορούν να θέσουν σε κίνδυνο τα δεδομένα σας.
- **Περιορίστε την Εγκατάσταση Εφαρμογών και Ενημερώσεων από Άγνωστες Πηγές**: Μην κατεβάζετε εφαρμογές ή ενημερώσεις από μη πιστοποιημένες πηγές, καθώς αυτές μπορεί να περιέχουν κακόβουλο λογισμικό.
- **Αποσυνδεθείτε από Λογαριασμούς Όταν Δε Χρησιμοποιούνται**: Μην αφήνετε τους λογαριασμούς σας ανοιχτούς, ιδιαίτερα, σε κοινόχρηστους ή δημόσιους υπολογιστές. Αποσυνδεθείτε, πάντα, αφού τελειώσετε τη χρήση.
- **Περιορίστε την Πρόσβαση των Συσκευών σας σε Bluetooth**: Διατηρήστε το Bluetooth απενεργοποιημένο όταν δεν το χρησιμοποιείτε, ειδικά, σε δημόσιους χώρους όπου μπορεί να χρησιμοποιηθεί για να αποκτήσει κάποιος πρόσβαση στα δεδομένα της συσκευής σας (smartphone και Η/Υ).
- **Κλείστε την Κάμερα και το Μικρόφωνο Όταν Δε Χρησιμοποιούνται**: Πολλές εφαρμογές ζητούν πρόσβαση στην κάμερα και το μικρόφωνό σας. Απενεργοποιήστε τα, ειδικά, σε ευαίσθητες εφαρμογές όταν δεν είναι απαραίτητα.
- **Χρησιμοποιήστε Εφαρμογές Προστασίας Απορρήτου για την Πλοήγησή σας στο Διαδίκτυο**: Προγράμματα περιήγησης που εστιάζουν στην προστασία της ιδιωτικότητας, όπως το Brave ή το Firefox Focus, προσφέρουν επιπλέον προστασία και περιορίζουν την παρακολούθηση των διαδικτυακών σας δραστηριοτήτων.

- **Περιορίστε εφαρμογές που χρησιμοποιούν δεδομένα τοποθεσίας στο παρασκήνιο**: Μπορείτε να επιλέξετε η τοποθεσία σας να χρησιμοποιείται, μόνο, όταν χρησιμοποιείτε, ενεργά, την εφαρμογή και όχι στο παρασκήνιο.
- **Διαχωρίστε τις επαγγελματικές και προσωπικές συσκευές**: Χρησιμοποιήστε διαφορετικές συσκευές ή τουλάχιστον διαφορετικά προφίλ για την εργασία και την προσωπική χρήση, για να αποφύγετε διαρροές δεδομένων από τη μία χρήση στην άλλη.
- **Ρυθμίστε χρονοδιακόπτες για αυτόματη αποσύνδεση**: Σε συσκευές και εφαρμογές που χρησιμοποιείτε, μπορείτε να ρυθμίσετε χρονοδιακόπτη αποσύνδεσης για περιόδους αδράνειας.
- **Ρυθμίστε συσκευές IoT (Internet of Things) με ισχυρά μέτρα ασφαλείας**: Οι έξυπνες συσκευές, όπως κάμερες και φώτα, είναι συχνά εκτεθειμένες σε κινδύνους παραβίασης. Χρησιμοποιήστε ισχυρούς κωδικούς και απενεργοποιήστε τις αν δεν τις χρειάζεστε.
- **Χρησιμοποιήστε ανεξάρτητους server για τα email σας**: Εξερευνήστε τη χρήση ανεξάρτητων email providers που προσφέρουν προστασία απορρήτου, όπως η διαχείριση email μέσω προσωπικού server για μεγαλύτερο έλεγχο.
- **Ρυθμίστε ανίχνευση πρόσβασης με βιομετρικά δεδομένα σε φυσικούς χώρους**: Εάν διαχειρίζεστε ευαίσθητα δεδομένα, μπορείτε να εξετάσετε βιομετρικές κλειδαριές, όπως αναγνώριση δακτυλικού αποτυπώματος, για να έχετε πρόσβαση με επιπρόσθετη ασφάλεια σε αυτούς του χώρους.
- **Χρησιμοποιήστε κρυπτογραφημένα "flash drives" για φορητή αποθήκευση**: Υπάρχουν USB drives που κρυπτογραφούνται αυτόματα και απαιτούν κωδικό πρόσβασης για να ανοίξουν.
- **Απομονώστε την επαγγελματική επικοινωνία από την προσωπική**: Δημιουργήστε ξεχωριστά προφίλ στον browser σας για εργασιακή και προσωπική χρήση, ώστε να περιορίσετε την αλληλοσύνδεση δεδομένων.
- **Χρησιμοποιήστε "shredders" για ψηφιακά αρχεία**: Για αρχεία που πρέπει να διαγραφούν μόνιμα, χρησιμοποιήστε λογισμικό "shredding" που διαγράφει τα δεδομένα πέρα από την απλή μετακίνηση στον κάδο ανακύκλωσης.

Περιορισμός Πρόσβασης και Κοινοποίησης Δεδομένων

- **Αποφύγετε την Υπερβολική Κοινοποίηση Δεδομένων**: Πολλές εφαρμογές ζητούν πρόσβαση σε περισσότερα δεδομένα από όσα χρειάζονται, όπως τοποθεσία ή επαφές. Αν δεν είναι απαραίτητο, αρνηθείτε αυτήν την πρόσβαση ή απενεργοποιήστε την, αμέσως, μετά τη χρήση.
- **Αποφύγετε την Κοινοποίηση της Αληθινής Ημερομηνίας Γέννησης**: Σε ιστότοπους και εφαρμογές, μπορείτε να δίνετε παραλλαγές της ημερομηνίας γέννησής σας ώστε να μειώσετε τον κίνδυνο χρήσης αυτής της πληροφορίας για παραβιάσεις ή κλοπή ταυτότητας.
- **Περιορίστε τη Χρήση των Λογαριασμών σας, Μέσω Τρίτων**: Αποφύγετε να συνδέεστε σε εφαρμογές ή ιστότοπους, μέσω του Facebook, του Google ή άλλων πλατφορμών. Αν και είναι εύκολο, συνήθως, δίνει πρόσβαση σε δεδομένα σας.
- **Περιορίστε την Κοινοποίηση της Τοποθεσίας σας σε Εφαρμογές**: Απενεργοποιήστε την κοινή χρήση τοποθεσίας όταν δεν είναι απολύτως απαραίτητη, ιδιαίτερα, σε εφαρμογές κοινωνικής δικτύωσης.
- **Μη Δίνετε Δεδομένα Χωρίς Σκοπό**: Όταν κάποια υπηρεσία ζητά προσωπικά σας δεδομένα, σκεφτείτε αν τα χρειάζεται πραγματικά. Εάν τα δεδομένα σας δεν είναι απαραίτητα, μπορείτε να αρνηθείτε να τα παράσχετε.
- **Αποφύγετε τις Αυτόματες Κοινοποιήσεις στο Διαδίκτυο**: Ρυθμίστε τις εφαρμογές σας έτσι ώστε να μην κοινοποιούν αυτόματα τις δραστηριότητές σας (όπως η τοποθεσία ή η μουσική που ακούτε) στο διαδίκτυο ή στα κοινωνικά μέσα.

- **Διαγράψτε Συσκευές και Δεδομένα Πριν από την Ανακύκλωση**: Αν θέλετε να πετάξετε ή να ανακυκλώσετε παλιές συσκευές (smartphone, H/Y, tablet, smartTV, κλπ.), βεβαιωθείτε ότι έχετε διαγράψει όλα τα δεδομένα και έχετε επαναφέρει τη συσκευή στις εργοστασιακές ρυθμίσεις.
- **Αποφύγετε τις "Έξυπνες" Συσκευές που Συλλέγουν Δεδομένα**: Οι έξυπνες συσκευές όπως τα ηχεία, οι κάμερες ασφαλείας και τα "έξυπνα" ρολόγια συλλέγουν προσωπικά δεδομένα. Χρησιμοποιήστε τα με προσοχή και προτιμήστε αυτά που επιτρέπουν ρυθμίσεις απορρήτου.
- **Αποφύγετε την Κοινοποίηση Οικογενειακών Δεδομένων στο Διαδίκτυο**: Συνίσταται να μη δημοσιεύετε προσωπικές πληροφορίες παιδιών ή οικογενειακών δεδομένων σε δημόσιες πλατφόρμες καθώς μπορεί να χρησιμοποιηθούν για κακόβουλους σκοπούς.
- **Διατηρήστε Διαχωρισμένα τους Επαγγελματικούς και Προσωπικούς Λογαριασμούς**: Προσπαθήστε να διατηρείτε ξεχωριστούς λογαριασμούς και email για προσωπική και επαγγελματική χρήση ώστε να μειώσετε τον κίνδυνο διαρροής επαγγελματικών πληροφοριών, στο προσωπικό σας δίκτυο.
- **Ελέγχετε τη χρήση μικροφώνου και κάμερας στις εφαρμογές**: Επισκεφθείτε τις ρυθμίσεις ασφαλείας της συσκευής σας και βεβαιωθείτε, ότι μόνο, αξιόπιστες εφαρμογές έχουν άδεια πρόσβασης στο μικρόφωνο και την κάμερα.
- **Διαχειριστείτε τα δικαιώματα κοινής χρήσης αρχείων**: Αποκλείστε την πρόσβαση σε άτομα που δε χρειάζεται να δουν τα αρχεία σας και επανεξετάστε τις άδειες για παλαιότερες κοινοποιήσεις.
- **Μην ανακοινώνετε δημοσίως τις μελλοντικές τοποθεσίες σας ή τα σχέδια σας**: Η δημοσιοποίηση των σχεδίων σας μπορεί να σας κάνει ευάλωτους σε επιθέσεις ή παραβίαση απορρήτου.
- **Περιορίστε τις επαφές που έχουν πρόσβαση στις προσωπικές σας πληροφορίες σε συσκευές**: Αν χρησιμοποιείτε κοινόχρηστες συσκευές (Η/Υ), ελέγξτε αν οι επαφές σας είναι ιδιωτικές ή δημόσιες, και ρυθμίστε τις ανάλογα.
- **Χρησιμοποιήστε ψευδώνυμα για κάθε δημόσια πλατφόρμα**: Αν δεν είναι απαραίτητη η χρήση πραγματικού ονόματος, ψευδώνυμα ή κωδικές ονομασίες αποθαρρύνουν τη συγκέντρωση δεδομένων για συγκεκριμένα πρόσωπα.
- **Ελέγχετε για Φόρμες Ψεύτικων Ερωτηματολογίων**: Μη συμπληρώνετε ερωτηματολόγια ή φόρμες που δεν προέρχονται από έμπιστες πηγές καθώς μπορεί να συλλέγουν πληροφορίες για να σας στοχοποιήσουν με ανεπιθύμητα μηνύματα ή να εκμεταλλευτούν δεδομένα σας.
- **Απενεργοποιήστε τις ειδοποιήσεις στην οθόνη κλειδώματος για ευαίσθητες εφαρμογές**: Αν κάποιος αποκτήσει φυσική πρόσβαση στη συσκευή σας (smartphone), δεν θα δει τις ειδοποιήσεις ή μηνύματα από ευαίσθητες εφαρμογές χωρίς να ξεκλειδώσει τη συσκευή.
- **Απενεργοποιήστε τις Αυτόματες Συνδέσεις Συσκευών**: Εάν οι συσκευές σας είναι ρυθμισμένες να συνδέονται, αυτόματα, σε γνωστά δίκτυα Wi-Fi ή Bluetooth, απενεργοποιήστε αυτήν τη ρύθμιση για να αποτρέψετε τυχαίες συνδέσεις.

Ασφαλής Χρήση Διαδικτυακών Υπηρεσιών και Κοινωνικών Δικτύων

- **Επιλέξτε Ιστότοπους με Ασφαλή Σύνδεση (HTTPS)**: Όταν επισκέπτεστε ιστοσελίδες, προτιμήστε εκείνες με πιστοποιητικό ασφαλείας (HTTPS). Αυτές οι ιστοσελίδες προστατεύουν καλύτερα τα δεδομένα που εισάγετε.
- **Χρησιμοποιήστε τα Κοινωνικά Δίκτυα με σύνεση**: Προσέξτε τί κοινοποιείτε στα κοινωνικά δίκτυα. Πληροφορίες όπως η τοποθεσία σας, το επάγγελμά σας και οι επαφές σας μπορούν να χρησιμοποιηθούν από τρίτους για σκοπούς που ίσως, δε γνωρίζετε.

- **Ελέγχετε, τακτικά, το Ιστορικό Πλοήγησης και τα Cookies**: Περιορίστε τη χρήση cookies και διαγράφετε το ιστορικό πλοήγησης, ειδικά, αν χρησιμοποιείτε δημόσιους υπολογιστές ή κοινές συσκευές.
- **Χρησιμοποιήστε Πλατφόρμες Μηνυμάτων με Κρυπτογράφηση**: Προτιμήστε εφαρμογές επικοινωνίας που προσφέρουν κρυπτογράφηση από άκρο σε άκρο (end-to-end encryption), όπως το WhatsApp και το iMessage ώστε να διασφαλίζεται η ιδιωτικότητα των συνομιλιών σας.
- **Αποφύγετε την Κοινοποίηση Κωδικών Πρόσβασης με Μηνύματα ή Email**: Αποφύγετε να στέλνετε κωδικούς, μέσω μη ασφαλών καναλιών επικοινωνίας. Χρησιμοποιήστε, αντί αυτού, εφαρμογές που παρέχουν κρυπτογραφημένα μηνύματα. Σε περίπτωση που λάβετε κάποιον κωδικό με απλό μήνυμα ή email, συνίσταται η αλλαγή του αρχικού κωδικού.
- **Αξιολογήστε τις Εφαρμογές Πριν την Εγκατάσταση**: Πριν κατεβάσετε κάποια εφαρμογή, διαβάστε τις κριτικές και αξιολογήστε πόσο αξιόπιστη είναι. Αποφύγετε εφαρμογές με λίγες κριτικές ή αμφίβολες πολιτικές απορρήτου.
- **Ελέγχετε τις Άδειες Εφαρμογών, Περιοδικά**: Πολλές εφαρμογές μπορούν να αποκτήσουν πρόσβαση σε δεδομένα που δε χρειάζονται, πλέον. Αναθεωρείτε τις άδειες των εφαρμογών σας και περιορίστε τις, κατάλληλα.
- **Προσέξτε τα Διαδικτυακά Παιχνίδια και Κουίζ**: Αποφύγετε τα παιχνίδια και κουίζ που ζητούν προσωπικές πληροφορίες, όπως ημερομηνία γέννησης ή όνομα μητέρας. Αυτά μπορούν να χρησιμοποιηθούν για να κλέψουν τα στοιχεία σας ή να απαντήσουν σε ερωτήσεις ασφαλείας.
- **Δημιουργήστε την Ψηφιακή Παρουσία σας με Προσοχή**: Όταν δημιουργείτε προφίλ σε διάφορες πλατφόρμες, προσέξτε να μην περιέχουν υπερβολικές, προσωπικές πληροφορίες και σκεφτείτε πριν δημοσιεύσετε πληροφορίες που μπορεί να μείνουν δημόσιες.
- **Αξιολογήστε τη Χρήση Εναλλακτικών Μηχανών Αναζήτησης**: Οι μηχανές αναζήτησης, όπως το DuckDuckGo, έχουν πολιτικές προστασίας απορρήτου που δε συλλέγουν πληροφορίες για τις αναζητήσεις σας, σε αντίθεση με τις πιο δημοφιλείς.
- **Χρησιμοποιήστε κρυπτογραφημένο email για σημαντικές επικοινωνίες**: Υπάρχουν υπηρεσίες όπως το ProtonMail που παρέχουν κρυπτογραφημένη, ηλεκτρονική αλληλογραφία για αυξημένη προστασία.
- **Χρησιμοποιήστε ένα ξεχωριστό email για κοινωνικά δίκτυα**: Εγγραφείτε σε κοινωνικά δίκτυα με ένα διαφορετικό email από το επαγγελματικό ή το προσωπικό σας ώστε να αποφεύγετε την υπερβολική προβολή ή spam.
- **Περιορίστε τη Χρήση Ηλεκτρονικών Βοηθών**: Οι ηλεκτρονικοί βοηθοί συλλέγουν δεδομένα φωνής για να βελτιώσουν τις υπηρεσίες τους. Εξετάστε τις ρυθμίσεις απορρήτου και περιορίστε την αποθήκευση φωνητικών δεδομένων.
- **Διαγράψτε παλιές, αχρησιμοποίητες εφαρμογές**: Οι παλιές εφαρμογές μπορεί να έχουν πρόσβαση σε προσωπικά δεδομένα χωρίς λόγο. Διαγράψτε εφαρμογές που δε χρειάζεστε, πλέον, για να βελτιώσετε την ασφάλειά σας.
- **Απενεργοποιήστε την αυτόματη αναπαραγωγή στα κοινωνικά δίκτυα**: Βίντεο που αναπαράγονται, αυτόματα, μπορεί να καταγράφουν δεδομένα παρακολούθησης. Η απενεργοποίηση μειώνει την έκθεσή σας σε ανιχνεύσεις.
- **Διαγράψτε, Τακτικά, τα Κοινωνικά σας Προφίλ από Αχρησιμοποίητες Πλατφόρμες**: Ελέγχετε σε ποια κοινωνικά δίκτυα ή πλατφόρμες είστε εγγεγραμμένοι και διαγράψτε παλιά προφίλ που δε χρησιμοποιείτε, πλέον, για να μειώσετε την ψηφιακή σας έκθεση.
- **Χρησιμοποιήστε τη Λειτουργία "Guest" σε Κοινές Συσκευές**: Όταν άλλοι χρήστες χρειάζονται πρόσβαση στις συσκευές (Η/Υ, tablet, κλπ.) σας, ενεργοποιήστε τη λειτουργία «Επισκέπτης» για να προστατεύσετε τα δεδομένα σας από την κοινή χρήση.
- **Χρησιμοποιήστε Ειδικά Διαμορφωμένες Συσκευές για Παιδιά**: Αν τα παιδιά σας χρησιμοποιούν συσκευές (smartphone, Η/Υ, tablet, κλπ.), δημιουργήστε παιδικούς

λογαριασμούς, με αυξημένη προστασία και γονικό έλεγχο για την ασφάλεια των δεδομένων τους.

- **Διαγράψτε "εκτός σύνδεσης" τα ιστορικά περιήγησης συσκευών**: Στις κινητές συσκευές (smartphone, H/Y, κλπ.), καθαρίστε τα προσωρινά δεδομένα (cache) και το ιστορικό όταν δεν είστε συνδεδεμένοι, στο διαδίκτυο, για να περιορίσετε την αποστολή δεδομένων.

Επιπλέον Μέτρα Ασφαλείας

- **Εκπαιδεύστε τον εαυτό σας στον εντοπισμό "phishing traps"**: Αναγνωρίστε και αποφύγετε email ή ιστοσελίδες που μιμούνται την εμφάνιση επίσημων ιστοσελίδων. Ένας τρόπος είναι να ψάχνετε για λεπτομέρειες στα URL ή στους αποστολείς.
- **Εκπαιδεύστε τους Κοντινούς σας**: Η ενημέρωση για τις απειλές της διαδικτυακής ασφάλειας και των προσωπικών δεδομένων είναι απαραίτητη. Εκπαιδεύστε και τα υπόλοιπα μέλη της οικογένειας για να είναι όλοι πιο προσεκτικοί.
- **Προσέξτε στις Συνομιλίες, μέσω Email**: Το ηλεκτρονικό ταχυδρομείο ενδέχεται να παραβιαστεί ή να υποκλαπεί. Αποφύγετε, όπου είναι εφικτό, την αποστολή ευαίσθητων πληροφοριών, μέσω email εκτός αν χρησιμοποιείτε κρυπτογράφηση.
- **Διαγράψτε Αχρησιμοποίητους Λογαριασμούς**: Κάθε online λογαριασμός που δε χρησιμοποιείται πλέον αποτελεί ένα επιπλέον ρίσκο. Διαγράψτε παλιούς λογαριασμούς σε ιστότοπους και εφαρμογές που δε χρειάζεστε, πλέον.
- **Αναθεωρήστε το ιστορικό πρόσβασης στους λογαριασμούς σας**: Ορισμένες υπηρεσίες, όπως η Google ή το Facebook, παρέχουν λίστα με τις τελευταίες συσκευές ή τοποθεσίες που χρησιμοποίησαν το λογαριασμό σας, κάτι που μπορεί να βοηθήσει στον εντοπισμό ύποπτης δραστηριότητας.
- **Ενεργοποιήστε τις Ειδοποιήσεις Ασφάλειας**: Τράπεζες και διαδικτυακές υπηρεσίες παρέχουν ειδοποιήσεις για ύποπτες δραστηριότητες. Ενεργοποιήστε αυτές τις ειδοποιήσεις για να ενημερώνεστε, άμεσα, σε περίπτωση ύποπτων συνδέσεων ή συναλλαγών.
- **Αναπτύξτε τη δική σας "ψηφιακή συμπεριφορά"**: Ελαχιστοποιήστε τις αλληλεπιδράσεις με εφαρμογές και ιστότοπους που συγκεντρώνουν δεδομένα από τα likes ή τις προτιμήσεις σας.
- **Αποφεύγετε τις Δημόσιες Οθόνες για Ευαίσθητες Εργασίες**: Εάν εργάζεστε σε δημόσιο χώρο, χρησιμοποιήστε ένα φίλτρο προστασίας οθόνης για να αποτρέψετε την παρακολούθηση της δραστηριότητάς σας. Υπάρχουν ειδικά φίλτρα για την οθόνη που περιορίζουν τη γωνία θέασης ώστε μόνο εσείς να βλέπετε, καθαρά, την οθόνη σας. Αυτά βοηθούν να μη μπορεί κανείς δίπλα σας να δει τί κάνετε, ειδικά, σε δημόσιους χώρους.
- **Χρησιμοποιήστε Διαφορετικά Email για Εγγραφές και Φόρουμ**: Δημιουργήστε ένα ξεχωριστό email για εγγραφές σε φόρουμ, ειδήσεις ή άλλες υπηρεσίες που δε χρησιμοποιείτε, συχνά, για να διαχωρίζετε την προσωπική σας αλληλογραφία από εκείνη που μπορεί να εκτεθεί.
- **Χρησιμοποιήστε "Burner" Emails για Πρόχειρες Εγγραφές**: Για εγγραφές σε ιστότοπους ή δοκιμαστικές υπηρεσίες, χρησιμοποιήστε προσωρινά email (burner emails) ώστε να μην εκτίθεται το κύριο email σας.
- **Ρυθμίστε ειδοποιήσεις για ύποπτη δραστηριότητα**: Στους τραπεζικούς λογαριασμούς και τις πιστωτικές κάρτες, ενεργοποιήστε ειδοποιήσεις για συναλλαγές, έτσι ώστε να ενημερώνεστε, άμεσα, για οποιαδήποτε ύποπτη δραστηριότητα.
- **Διαγράψτε ιστορικό τοποθεσίας από Google και άλλες υπηρεσίες**: Μπορείτε να ρυθμίσετε τις επιλογές για να μην αποθηκεύεται το ιστορικό τοποθεσίας σας ή να το διαγράψετε από τον λογαριασμό σας.
- **Εξετάστε, Προσεκτικά, τις Κάμερες και τα Μικρόφωνα Σας**: Απενεργοποιήστε ή καλύψτε τις κάμερες και τα μικρόφωνα όταν δε χρησιμοποιούνται.

- **Διατηρήστε Ιδιωτικές τις Σημαντικές Πληροφορίες από Δυνατότητες Backup του Cloud**: Εάν δε χρειάζεται, πραγματικά, να έχετε ένα αρχείο στο cloud, επιλέξτε να το κρατήσετε σε τοπική αποθήκευση ή να απενεργοποιήσετε το αντίγραφο ασφαλείας για συγκεκριμένα, ευαίσθητα αρχεία.
- **Χρησιμοποιήστε Ασφαλή Εργαλεία Κοινής Χρήσης Αρχείων**: Αν πρέπει να στείλετε αρχεία, επιλέξτε υπηρεσίες που προσφέρουν ασφάλεια και κρυπτογράφηση (όπως το WeTransfer Pro ή το Google Drive με ελεγχόμενη πρόσβαση).
- **Κρυπτογραφήστε Ευαίσθητα Email**: Για αλληλογραφία που περιέχει ευαίσθητα δεδομένα, χρησιμοποιήστε ένα εργαλείο κρυπτογράφησης, όπως το PGP, που προστατεύει το περιεχόμενο των μηνυμάτων σας από μη εξουσιοδοτημένη πρόσβαση.
- **Προστατέψτε τα Βίντεο και τις Φωτογραφίες σας**: Εάν αποθηκεύετε προσωπικές φωτογραφίες ή βίντεο σε ηλεκτρονικές συσκευές ή cloud, εξετάστε το ενδεχόμενο να τα κρυπτογραφήσετε για επιπλέον προστασία.
- **Χρησιμοποιήστε κρυπτογραφημένα αποθηκευτικά μέσα**: Αν έχετε εξωτερικούς, σκληρούς δίσκους ή USB που περιέχουν ευαίσθητα δεδομένα, εξετάστε το ενδεχόμενο να τους κρυπτογραφήσετε για επιπλέον προστασία.
- **Αποφύγετε τη Χρήση Δημόσιων USB για Φόρτιση**: Μη συνδέετε τις συσκευές (smartphone, laptop, tablet) σας σε δημόσιους σταθμούς φόρτισης καθώς υπάρχει κίνδυνος να διαρρεύσουν δεδομένα, μέσω αυτών των συνδέσεων.
- **Απενεργοποιήστε τις δυνατότητες "βελτίωσης προϊόντος" που συλλέγουν δεδομένα**: Ορισμένες συσκευές και προγράμματα σας ζητούν την άδεια να συλλέγουν δεδομένα χρήσης για να βελτιώσουν τις υπηρεσίες τους. Μπορείτε να αρνηθείτε.
- **Απενεργοποιήστε τα "cookies" τρίτων σε προγράμματα περιήγησης**: Αυτά τα cookies επιτρέπουν την παρακολούθηση των online δραστηριοτήτων σας. Η απενεργοποίηση των cookies τρίτων, ενισχύει το απόρρητο της περιήγησής σας.
- **Χρησιμοποιήστε λογισμικά καθαρισμού δεδομένων (data cleaning)**: Ορισμένα εργαλεία σας επιτρέπουν να διαγράφετε, ασφαλώς, παλιά ή ευαίσθητα αρχεία από τον υπολογιστή ή το κινητό σας για να μην ανακτώνται, εύκολα.