Australian Government | Be Connected
Every Australian online.

Εισαγωγή στην ασφάλεια του διαδικτύου

Ας βοηθήσουμε ώστε να βεβαιωθούμε ότι χρησιμοποιούμε το διαδίκτυο με ασφάλεια.

Ασφάλεια του υπολογιστή και του ηλεκτρονικού ταχυδρομείου

Μερικοί από τους σημαντικότερους κινδύνους στο διαδίκτυο είναι:

- **Ιοί**, οι οποίοι εξαπλώνονται από υπολογιστή σε υπολογιστή μέσω του διαδικτύου. Ορισμένοι είναι απλώς ενοχλητικοί, άλλοι μπορούν επίσης να διαγράψουν τα δεδομένα σας.
- **Δούρειοι ίπποι,** οι οποίοι είναι φαινομενικά αθώα προγράμματα που προσπαθούν να σας παραπλανήσουν για να τα εγκαταστήσετε.
- **Κατασκοπευτικό λογισμικό (spyware),** που είναι προγράμματα που κλέβουν πληροφορίες όπως κωδικούς πρόσβασης ή στοιχεία τραπεζικού λογαριασμού.

Υπάρχουν βήματα που μπορείτε να ακολουθήσετε για να προστατεύσετε τον εαυτό σας και τον υπολογιστή σας από τις διαδικτυακές απειλές.

1. Χρησιμοποιήστε **λογισμικό προστασίας από ιούς**, το όποιο βοηθάει να βρείτε, σταματήσετε και αφαιρέσετε τους ιούς.
2. Χρησιμοποιήστε **λογισμικό anti-spyware**, το οποίο σας βοηθάει να σταματήσετε την κλοπή των δεδομένων σας.
3. Χρησιμοποιήστε ένα τείχος προστασίας (firewall), το οποίο προστατεύει τον υπολογιστή σας από μη εξουσιοδοτημένη πρόσβαση από το διαδίκτυο.
4. Να έχετε ενημερωμένο το λογισμικό ασφαλείας στο διαδίκτυο.
5. Εάν πήρατε λογισμικό προστασίας από ιούς με τον καινούργιο υπολογιστή σας, ανανεώστε το όταν τελειώσει η περίοδος δοκιμής ή πάρτε δωρεάν λογισμικό όπως το AVG. Σημείωση: τα Windows 10 συνοδεύονται από αποτελεσματικό λογισμικό προστασίας από ιούς που λέγεται Windows Defender. Τα Windows θα το ενημερώνουν για λογαριασμό σας.
6. Αν δεν είστε βέβαιοι, ζητήστε συμβουλές από **https://www.staysmartonline.gov.au/**.

Εισαγωγή στην ασφάλεια του διαδικτύου

Θα πρέπει να προσέχετε ιδιαίτερα να μην εκθέτετε τον υπολογιστή σας σε κακόβουλο λογισμικό.

1. Ξανασκεφτείτε το πριν ανοίξετε ηλεκτρονικές επιστολές (email) και ειδικά τα συνημμένα ηλεκτρονικού ταχυδρομείου από άτομα που δεν γνωρίζετε.
2. Να συναλλάσσεστε με επιχειρήσεις στο διαδίκτυο που γνωρίζετε και έχουν καλή φήμη. Να αναζητήσετε πληροφορίες για μια εταιρεία πριν αγοράσετε.
3. Κάντε τακτικά αντίγραφα ασφαλείας όλων των πληροφοριών στον υπολογιστή σας. Σε περίπτωση που μολυνθεί ο υπολογιστής σας, θα συνεχίσετε να έχετε πρόσβαση σε όλα τα σημαντικά δεδομένα σας.

Προστατεύστε τον εαυτό σας και τον υπολογιστή σας από τις διαδικτυακές απειλές

Χρήση προσωπικών στοιχείων στο διαδίκτυο

Μερικές φορές είναι αναγκαίο να δώσετε προσωπικά στοιχεία στο διαδίκτυο, αλλά υπάρχουν όρια για το πόσα στοιχεία θα πρέπει να ανταλλάξετε και να είστε ενήμεροι για τα δικαιώματά σας.

Νόμοι ρυθμίζουν τη χρήση προσωπικών στοιχείων από ιδιωτικές εταιρείες

- Να δίνετε στοιχεία μόνο σε νόμιμες εταιρείες εάν χρειάζονται για να επαληθεύσουν την ταυτότητά σας.
- Αποφεύγετε να δημοσιοποιείτε προσωπικά σας στοιχεία (ημερομηνία γέννησης, διεύθυνση κατοικίας κλπ.) σε μέσα κοινωνικής δικτύωσης όπως το Facebook. Τα προσωπικά στοιχεία μπορούν να χρησιμοποιηθούν από εγκληματίες για κλοπή ταυτότητας.
- Νόμοι ρυθμίζουν τη χρήση προσωπικών στοιχείων από ιδιωτικές εταιρείες. Στην Αυστραλία, αυτός είναι ο Νόμος Προστασίας Προσωπικού Απορρήτου 1988.
- Ο Νόμος Ελευθερίας στην Πληροφόρηση μπορεί να ισχύει για στοιχεία που παρέχετε σε κρατικούς φορείς.
- Οι αξιόπιστες εταιρείες έχουν κανονισμούς για το πώς φυλάσσουν τα προσωπικά στοιχεία. Διαβάστε τους κανονισμούς τους για το προσωπικό απόρρητο στις ιστοσελίδες τους.
- Για περισσότερες πληροφορίες για τα δικαιώματα των καταναλωτών ή για ενημερωμένες πληροφορίες για το πώς να προστατευθείτε από απάτες, μπορείτε να επισκεφθείτε το ACCC: https://www.accc.gov.au/consumers.

Εισαγωγή στην ασφάλεια του διαδικτύου

Πληρωμές στο διαδίκτυο και ασφαλείς χώροι

Προσέχετε τα στοιχεία που ανταλλάσσετε στο διαδίκτυο

Η αγορά πραγμάτων στο διαδίκτυο μπορεί να είναι βολική και υπάρχουν μερικοί γρήγοροι έλεγχοι για να διασφαλίσετε ότι πληρώνετε με ασφάλεια.

1. Έχει καλή φήμη η εταιρεία που συναλλάσσεστε; Ελέγξτε τον κανονισμό προσωπικού απορρήτου της εταιρείας και τις πολιτικές επιστροφής προϊόντων στην ιστοσελίδα της. Χρησιμοποιήστε μια μηχανή αναζήτησης για να μάθετε περισσότερα πράγματα για την εταιρεία.
2. Αγοράστε με πιστωτική κάρτα ή PayPal. Και τα δύο προσφέρουν κάποιου είδους προστασίας του αγοραστή.
3. Μόλις πριν πληκτρολογήσετε τα στοιχεία της πιστωτικής σας κάρτας, ελέγξτε τη **Γραμμή Διεύθυνσης (Address bar)** του προγράμματος περιήγησης. Μια ασφαλής ιστοσελίδα θα πρέπει να είναι σημειωμένη με ένα λουκέτο και η ιστοσελίδα θα πρέπει να ξεκινάει με **https:** (όχι μόνο **http:**).

Ασφάλεια των παιδιών στο διαδίκτυο

Τα παιδιά είναι λιγότερο έμπειρα στη ζωή και έτσι διατρέχουν μεγαλύτερο κίνδυνο από:

- Να δουν υλικό σεξουαλικού περιεχομένου.
- Να αποκαλύψουν προσωπικά στοιχεία.
- Να πέσουν θύματα εκφοβισμού και παρενόχλησης.

Οι αίθουσες συζήτησης στο διαδίκτυο και τα μέσα κοινωνικής δικτύωσης είναι χώροι όπου μπορούν να γίνουν προσεγγίσεις. Ποτέ μην αφήσετε το παιδί σας να συναντηθεί με οποιοδήποτε άτομο που ‘συνάντησε’ στο διαδίκτυο εκτός εάν συνοδεύεται από ενήλικα.

Υπάρχουν προστατευτικά μέτρα που μπορείτε να πάρετε για να βοηθήσετε τα παιδιά να παραμείνουν ασφαλή στο διαδίκτυο.

1. Δημιουργήστε για το παιδί το δικό του λογαριασμό χρήστη για τον υπολογιστή.
2. Ενεργοποιήστε τους ελέγχους γονέα γι’ αυτόν τον λογαριασμό χρήστη.
3. Για το Google, ενεργοποιήστε την **Ασφαλή Αναζήτηση** και για το Bing ή Yahoo, ρυθμίστε την Ασφαλή Αναζήτηση στο ‘**αυστηρό**’.
4. Ρυθμίστε το πρόγραμμα YouTube στη θέση «απαγορευμένο» μαζί με οποιεσδήποτε άλλες ιστοσελίδες με βίντεο.
5. Μιλήστε στο παιδί σας για τους κινδύνους που θα μπορούσε να αντιμετωπίσει στο διαδίκτυο.

Εάν ένα παιδί καταλήξει τυχαία σε μια επικίνδυνη κατάσταση στο διαδίκτυο, καταγγείλετέ το στο Office of the eSafety Commissioner (Γραφείο του Επιτρόπου Ηλεκτρονικής Ασφάλειας) στο https://www.esafety.gov.au/complaints-and-reporting.