

Προστασία των προσωπικών σας στοιχείων στο διαδίκτυο

Σχεδόν κάθε εφαρμογή, πλατφόρμα κοινωνικών μέσων δικτύωσης ή ιστοσελίδα σας ζητά τουλάχιστον κάποια προσωπικά στοιχεία. Τα προσωπικά σας στοιχεία περιλαμβάνουν οποιαδήποτε στοιχεία ή δεδομένα που μπορούν να χρησιμοποιηθούν για την ταυτοποίησή σας, όπως στοιχεία εντοπισμού του μέρους που βρίσκεστε ή πού ζείτε, και άλλα μοναδικά συγκεκριμένα στοιχεία. Είναι σημαντικό να είστε πάντα επιφυλακτικοί για την κοινοποίηση προσωπικών στοιχείων.



Η προστασία των προσωπικών σας στοιχείων έχει σημασία

Η προστασία των προσωπικών σας στοιχείων είναι πολύ σημαντική καθώς οι απατεώνες και οι κλέφτες ταυτότητας μπορούν να τα χρησιμοποιήσουν για να προσποιηθούν ότι είστε εσείς. Μπορούν να δημιουργήσουν ψεύτικους λογαριασμούς στο όνομά σας και να ενεργήσουν με τρόπους που θα μπορούσαν να σας επηρεάσουν τώρα ή στο μέλλον. Αυτό θα μπορούσε να περιλαμβάνει απάτη, όπως κλοπή χρημάτων από τον τραπεζικό λογαριασμό σας ή λήψη δανείου στο όνομά σας.

Οι απατεώνες μπορούν να χρησιμοποιήσουν τα στοιχεία σας από μόνα τους ή σε συνδυασμό με άλλες πληροφορίες. Αυτό μπορεί να περιλαμβάνει καθημερινά πράγματα που είναι συγκεκριμένα για εσάς, όπως:

Προσωπικά στοιχεία

- Ονοματεπώνυμο
- Διεύθυνση κατοικίας
- Αριθμό τηλεφώνου
- Ημερομηνία γέννησης
- Αριθμό άδειας οδήγησης
- Στοιχεία τραπεζικού λογαριασμού
- Διεύθυνση email
- Ονόματα χρήστη και κωδικούς πρόσβασης

Έγγραφα ταυτότητας

- Άδεια οδήγησης
- Διαβατήριο
- Πιστοποιητικό γέννησης
- Κάρτα Medicare
- Αυστραλιανή βίζα ή πιστοποιητικό ιθαγένειας
- Κάρτα ImmiCard



Να έχετε την επίγνωση του τι κοινοποιείτε

Μέσα κοινωνικής δικτύωσης

Είναι καλή ιδέα να αποφύγετε την κοινοποίηση προσωπικών στοιχείων στους λογαριασμούς σας στα μέσα κοινωνικής δικτύωσης. Οι απατεώνες μπορούν να μάθουν πολλά για εσάς από στοιχεία που μοιράζεστε στο διαδίκτυο. Μερικές φορές δημιουργούν κούιζ ή αναρτήσεις ερωτήσεων που έχουν σχεδιαστεί για να σας εξαπατήσουν να κοινοποιήσετε προσωπικά στοιχεία. Χρησιμοποιούν αυτά τα στοιχεία για να μαντέψουν τους κωδικούς πρόσβασης του λογαριασμού σας ή να σας στοχοποιήσουν για άλλες απάτες.

Να θυμάστε: Αποδεχτείτε αιτήματα φιλίας μόνο από άτομα που γνωρίζετε στην πραγματική ζωή, ρυθμίστε τους λογαριασμούς σας στα μέσα κοινωνικής δικτύωσης σε ιδιωτικούς και ελέγξτε ποιοι μπορούν να δουν τι κοινοποιείτε.

Χρήση εφαρμογών

Κατεβάστε εφαρμογές μόνο από τα επίσημα καταστήματα εφαρμογών, και διαβάστε τις πολιτικές απορρήτου και τις κριτικές πριν κατεβάσετε οτιδήποτε. Μπορείτε επίσης να περιορίσετε τις πληροφορίες στις οποίες έχουν πρόσβαση οι εφαρμογές. Ορισμένες εφαρμογές ζητούν περιττή πρόσβαση στις λίστες επαφών σας, την κάμερα, την αποθήκευση, την τοποθεσία και το μικρόφωνο. Ελέγξτε και προσαρμόστε τα δικαιώματα εφαρμογής σας στο μενού ρυθμίσεων στην έξυπνη συσκευή σας.

Διατηρήστε τις πληροφορίες σας ασφαλείς

Χρησιμοποιήστε την ασφάλεια της συσκευής

Η χρήση λογισμικού ασφαλείας στον υπολογιστή σας είναι ένας από τους απλούστερους τρόπους για να προστατεύσετε τον εαυτό σας και το απόρρητό σας. Η καλή ασφάλεια του υπολογιστή περιλαμβάνει την εγκατάσταση αξιόπιστων σαρωτών προστασίας από κακόβουλο λογισμικό, ιούς και λογισμικού τείχους προστασίας. Θα πρέπει επίσης να διατηρείτε επικαιροποιημένα τα διαδικτυακά εργαλεία ασφαλείας και τις εφαρμογές σας ενεργοποιώντας τις αυτόματες ενημερώσεις. Χρησιμοποιήστε αυτόματες και χρονικά περιορισμένες κλειδαριές οθόνης ή προφυλάξεις οθόνης που προστατεύονται με κωδικό πρόσβασης και έχετε αυτόματο κλείδωμα για αποτυχία πολλαπλών προσπαθειών σύνδεσης.

Συμβουλή: Μια εφαρμογή διαχείρισης κωδικών πρόσβασης μπορεί επίσης να σας βοηθήσει να δημιουργήσετε και να αποθηκεύσετε σύνθετες φράσεις πρόσβασης που είναι δύσκολο για άλλους να μαντέψουν ή να παραβιάσουν. Μπορείτε να βρείτε πληροφορίες σχετικά με τους **διαχειριστές κωδικών πρόσβασης** και τον τρόπο ρύθμισής τους στην ιστοσελίδα Be Connected.

Φράσεις πρόσβασης

Διατηρήστε τους λογαριασμούς σας ασφαλείς με ισχυρές φράσεις πρόσβασης. Οι φράσεις πρόσβασης είναι η πιο ασφαλής έκδοση των κωδικών πρόσβασης και αποτελούνται από τέσσερις ή περισσότερες τυχαίες λέξεις.

Δοκιμάστε να σκεφτείτε μια διαφορετική φράση πρόσβασης για κάθε λογαριασμό σας και μην ανακυκλώνετε τμήματα παλαιών.

Όταν επιλέγετε τη φράση πρόσβασης, κάντε την:

- **Μεγάλη** - τουλάχιστον 14 χαρακτήρες
- **Απρόβλεπτη** - χρησιμοποιήστε τέσσερις ή περισσότερες τυχαίες λέξεις με αριθμούς, σύμβολα και κεφαλαία και πεζά γράμματα
- **Μοναδική** - μην επαναχρησιμοποιείτε τις φράσεις πρόσβασης

Π.χ. *Yellow So Hey Plant* > *Yell*w-S0heyPl@nt!*

Συμβουλή: Ελέγξτε την ισχύ ενός κωδικού πρόσβασης χρησιμοποιώντας τον ελεγκτή ισχύος κωδικού πρόσβασης της Κυβέρνησης της ΝΝΟ στη διεύθυνση nsw.gov.au/id-support-nsw/be-prepared/passwords

Έλεγχος ταυτότητας με πολλαπλούς παράγοντες

Είναι πάντα καλή ιδέα να ενεργοποιείτε τον έλεγχο ταυτότητας πολλαπλών παραγόντων για τους λογαριασμούς σας. Ο έλεγχος ταυτότητας πολλαπλών παραγόντων (γνωστός και ως έλεγχος ταυτότητας 2 βημάτων) προσθέτει ένα επιπλέον επίπεδο ασφάλειας. Αυτό σημαίνει ότι όταν συνδέεστε σε έναν λογαριασμό με τον κωδικό πρόσβασής σας, μπορεί να σας ζητηθεί να κάνετε ένα επιπλέον βήμα για να επιβεβαιώσετε ότι είστε εσείς - όπως να εισαγάγετε έναν κωδικό από ένα μήνυμα κειμένου ή να χρησιμοποιήσετε αναγνώριση προσώπου.

Κάνετε αγορές με ασφάλεια στο διαδίκτυο

Όταν ψωνίζετε στο διαδίκτυο, βεβαιωθείτε ότι χρησιμοποιείτε αξιόπιστους πωλητές και αναζητάτε κριτικές πελατών. Πριν εισαγάγετε τα προσωπικά σας στοιχεία, βεβαιωθείτε ότι η ιστοσελίδα χρησιμοποιεί το «https» στην αρχή του ονόματος τομέα του ή έχει ένα εικονίδιο ασφαλείας, συνήθως ένα μικρό, κλειδωμένο λουκέτο, στο πρόγραμμα περιήγησής του για να δείξει ότι είναι μια πιο ασφαλής ιστοσελίδα. Κατά την πραγματοποίηση μιας αγοράς, χρησιμοποιήστε έναν ασφαλή τρόπο πληρωμής όπως PayPal, BPAY ή την πιστωτική σας κάρτα.

Χρησιμοποιήστε μια ασφαλή σύνδεση

Όταν χρειάζεται να αποκτήσετε πρόσβαση σε σημαντικούς λογαριασμούς, να στείλετε ευαίσθητες πληροφορίες ή να εισαγάγετε κωδικούς πρόσβασης, συνδεθείτε σε μια αξιόπιστη σύνδεση στο Διαδίκτυο, όπως στο σπίτι ή στην εργασία, ή χρησιμοποιώντας τα δικά σας δεδομένα κινητής τηλεφωνίας, αν είναι διαθέσιμα. Το δημόσιο Wi-Fi δεν είναι τόσο ασφαλές όσο το Wi-Fi στο σπίτι ή στην εργασία σας.

Απάτες και παραβιάσεις δεδομένων

Προστατεύστε τον εαυτό σας από απάτες

Η γνώση των απατών και του τρόπου λειτουργίας τους είναι ένα από τα σημαντικά βήματα για την αποφυγή τους. Οι απατεώνες προσποιούνται ότι προέρχονται από έναν οργανισμό ή ένα άτομο που γνωρίζετε για να προσπαθήσουν να σας εξαπατήσουν να παραδώσετε τα προσωπικά σας στοιχεία. Αυτές ονομάζονται απάτες πλαστοπροσωπίας.

Θυμηθείτε να:

Σταματήστε - μην δίνετε χρήματα ή προσωπικά στοιχεία σε κανέναν εάν δεν είστε σίγουροι
Οι απατεώνες συχνά σας ζητούν να επαληθεύσετε ποιοι είστε ή σας ζητούν να κάνετε μια πληρωμή.

Σκεφτείτε - αναρωτηθείτε θα μπορούσε το μήνυμα ή η κλήση να είναι ψεύτικη;

Προσοχή στις απροσδόκητες κλήσεις, μηνύματα και μηνύματα email. Εάν δεν είστε σίγουροι για ένα μήνυμα, καλέστε απευθείας τον οργανισμό, χρησιμοποιώντας τον αριθμό τηλεφώνου στην ιστοσελίδα του.

Προστατευτείτε - ενεργήστε γρήγορα αν κάτι φαίνεται λάθος

Επικοινωνήστε με την τράπεζά σας αν παρατηρήσετε κάποια ασυνήθιστη δραστηριότητα ή εάν ένας απατεώνας πάρει τα χρήματα ή τα στοιχεία σας.



Συμβουλή: Επισκεφθείτε την ιστοσελίδα Be Connected για τον δωρεάν [οδηγό παραπλανητικών μηνυμάτων](#) που αναπτύχθηκε με το Scamwatch.

Παραβιάσεις δεδομένων

Μια παραβίαση δεδομένων συμβαίνει όταν τα προσωπικά στοιχεία που έχει ένας οργανισμός γίνονται προσβάσιμα ή αποκαλύπτονται χωρίς εξουσιοδότηση ή χάνονται. Πολλοί οργανισμοί και κυβερνητικές υπηρεσίες έχουν νομική ευθύνη να σας ενημερώσουν αν τα προσωπικά σας στοιχεία περιέχονται σε παραβίαση δεδομένων που είναι πιθανό να σας προκαλέσει σοβαρή βλάβη.

Αν τα στοιχεία σας περιέχονται σε παραβίαση δεδομένων, βεβαιωθείτε ότι ενεργείτε γρήγορα και λαμβάνετε συμβουλές από το [Office of the Australian Information Commissioner \[Γραφείο του Επιτρόπου Πληροφοριών της Αυστραλίας\]](#). Η ενέργεια που κάνετε εξαρτάται από τα σχετικά στοιχεία. Κρατήστε ένα αρχείο για το τι κάνετε. Μπορείτε επίσης να λάβετε δωρεάν υποστήριξη και συμβουλές από το [IDCARE](#).

Για να μάθετε εάν μια ιστοσελίδα ή μια εφαρμογή που χρησιμοποιείτε έχει υποστεί παραβίαση δεδομένων, μπορείτε να ελέγξετε υπηρεσίες, όπως το [haveibeenpwned.com](#). Αν έχει συμβεί αυτό, αλλάξτε αμέσως τους κωδικούς πρόσβασής σας.

Κλοπή στοιχείων ταυτότητας

Εάν γνωρίζετε ή υποψιάζεστε ότι η ταυτότητά σας έχει κλαπεί:

- Υποβάλετε καταγγελία στο Australian Signals Directorate's Australian Cyber Security Centre [Αυστραλιανό Κέντρο Ασφάλειας στον Κυβερνοχώρο της Αυστραλιανής Διεύθυνσης Λήψης Σημάτων] στο [ReportCyber](#).
- Επικοινωνήστε με την αστυνομία στο 131 444. Ζητήστε μια αστυνομική αναφορά ή αριθμό αναφοράς ως απόδειξη ότι υποβάλλατε καταγγελία.
- Εάν γνωρίζετε ή υποπτεύεστε τον τύπο των προσωπικών στοιχείων που έχουν κλαπεί, επικοινωνήστε με τον αρμόδιο φορέα ή οργανισμό για να τους ενημερώσετε.
- Ενημερώστε το χρηματοπιστωτικό σας ίδρυμα το συντομότερο δυνατόν.
- Υποβάλετε καταγγελία στο National Anti-Scam Centre [Εθνικό Κέντρο Κατά της Απάτης] στο [Scamwatch](#) εάν ήταν μέρος απάτης.

Αφιερώστε χρόνο για να ανακαλύψετε τη Be Connected

Η Be Connected είναι μια ολοκληρωμένη ιστοσελίδα με δωρεάν ενημερωτικούς πόρους ειδικά σχεδιασμένους για να υποστηρίζουν τους ηλικιωμένους Αυστραλούς να συνδέονται με ασφάλεια στο διαδίκτυο και να περιηγούνται στον ψηφιακό κόσμο με αυτοπεποίθηση. Η ιστοσελίδα είναι επίσης χρήσιμη για οικογένειες και κοινοτικούς οργανισμούς που θέλουν να βοηθήσουν τα ηλικιωμένα μέλη της κοινότητας να έχουν πρόσβαση σε όλα τα οφέλη του Διαδικτύου.



Επισκεφθείτε τη διεύθυνση [beconnected.esafety.gov.au](#)



Αυτό το πρόγραμμα έχει αναπτυχθεί από την eSafety ως μέρος της πρωτοβουλίας Be Connected.