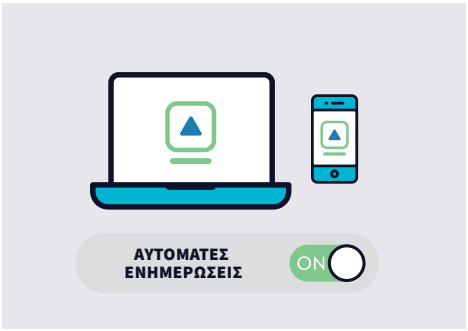
ΧΡΗΣΙΜΕΣ ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΤΗΝ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

ΠΡΑΚΤΙΚΟΙ ΤΡΟΠΟΙ ΓΙΑ ΝΑ ΠΡΟΣΤΑΤΕΥΕΣΤΕ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

cyber.gov.au/learn



Ενημερώνετε τις συσκευές σας

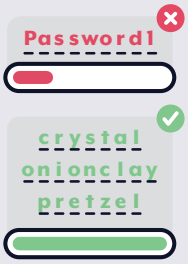
Οι ενημερώσεις των συσκευών σας μπορεί να διορθώσουν προβλήματα και να αντιμετωπίσουν νέες ανησυχίες ή αδυναμίες ασφαλείας που θα μπορούσαν να εκμεταλλευτούν οι χάκερ για να αποκτήσουν πρόσβαση στις συσκευές σας. Μπορούν επίσης να προσθέτουν νέες λειτουργίες στις εφαρμογές ή τη συσκευή σας.

Ενεργοποιήστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA)

MFA σημαίνει να έχετε πάνω από έναν τρόπο ελέγχου για να αποδείξετε την ταυτότητά σας σε ένα λογαριασμό. Για παράδειγμα, μπορεί να χρειαστείτε κωδικό από ένα μήνυμα κειμένου και τη φράση πρόσβασής σας. Αυτό καθιστά πολύ πιο δύσκολη την πρόσβαση των εγκληματιών του κυβερνοχώρου στους λογαριασμούς σας.

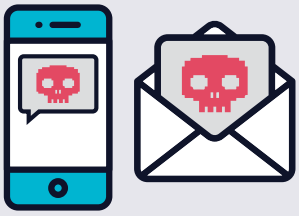
Οργανώνετε και δημιουργείτε τακτικά αντίγραφα ασφαλείας

Το αντίγραφο ασφαλείας είναι ένα ψηφιακό αντίγραφο των πιο σημαντικών δεδομένων σας είτε σε μια εξωτερική συσκευή αποθήκευσης είτε σε ένα διακομιστή στο διαδίκτυο, όπως στο cloud. Αυτό σημαίνει ότι μπορείτε να επαναφέρετε τα αρχεία σας εάν κάτι δεν πάει καλά.



Δημιουργείτε ασφαλείς φράσεις πρόσβασης

Όταν δεν είναι διαθέσιμο το MFA, χρησιμοποιήστε μια φράση πρόσβασης για να προστατεύσετε το λογαριασμό σας. Οι φράσεις πρόσβασης είναι η πιο ασφαλής εκδοχή κωδικών πρόσβασης, αφού χρησιμοποιούν τέσσερις ή περισσότερες τυχαίες λέξεις ως κωδικό πρόσβασής σας. Αυτό δυσκολεύει τους εγκληματίες του κυβερνοχώρου να τις μαντέψουν, αλλά διευκολύνει εσάς να τις θυμάστε.



Αναγνωρίζετε και καταγγέλλετε απάτες

Για να εξαπατήσουν το κοινό, οι εγκληματίες συχνά χρησιμοποιούν email, SMS, τηλεφωνικές κλήσεις και μέσα κοινωνικής δικτύωσης, που εμφανίζονται σκοπίμως σαν να έχουν σταλεί από άτομα ή οργανισμούς που νομίζετε ότι γνωρίζετε, ή νομίζετε ότι θα πρέπει να τους εμπιστευτείτε.

Να βρίσκεστε πάντα σε επιφυλακή όταν κάνετε κλικ σε συνημμένα ή συνδέσμους σε email.

Ενισχύετε το επίπεδο κυβερνοασφάλειάς σας με το να...

- Σκέφτεστε τι αναρτήσεις δημοσιεύετε στο διαδίκτυο.
- Λαμβάνετε προειδοποιήσεις για νέες απειλές. Εγγραφείτε για τις δωρεάν προειδοποιήσεις της υπηρεσίας μας.
- Μιλάτε για την κυβερνοασφάλεια με την οικογένεια και τους φίλους σας.
- Αποφεύγετε τα δημόσια Wi-Fi όταν κάνετε τραπεζικές συναλλαγές ή αγορές στο διαδίκτυο.
- Καταγγέλλετε επιθέσεις και περιστατικά στον κυβερνοχώρο για να διατηρείται ασφαλής η Αυστραλία.

Μάθετε περισσότερα στο **cyber.gov.au/learn**

Αναφέρετε περιστατικά που αφορούν την κυβερνοασφάλεια:
cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Έχετε κάποια σχόλια γι' αυτό το προϊόν; Πηγαίνετε στο **cyber.gov.au** και ενημερώστε μας.