Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

ΠΡΟΣΩΠΙΚΗ ΑΣΦΑΛΕΙΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ

ΠΡΩΤΑ ΒΗΜΑΤΑ

cyber.gov.au

Σειρά προσωπικής ασφάλειας στον κυβερνοχώρο

Προσωπική ασφάλεια στον κυβερνοχώρο: Πρώτα βήματα είναι ο πρώτος από μια σειρά τριών οδηγών που έχουν σχεδιαστεί για να βοηθήσουν τους καθημερινούς Αυστραλούς να κατανοήσουν τα βασικά στοιχεία της ασφάλειας στον κυβερνοχώρο. Μάθετε πώς μπορείτε να αναλάβετε δράση για να προστατεύσετε τον εαυτό σας από τις συνήθεις απειλές στον κυβερνοχώρο.

Πρώτα Βήματα

Επόμενα Βήματα

Προχωρημένα Βήματα

Πίνακας Περιεχομένων

Εισαγωγή

Τι είναι η προσωπική ασφάλεια στον κυβερνοχώρο;

Σε έναν ολοένα και περισσότερο τεχνολογικά καθοδηγούμενο κόσμο χρησιμοποιούμε καθημερινά συσκευές και λογαριασμούς που είναι ευάλωτοι σε κυβερνοαπειλές:

- Οι συσκευές σας μπορεί να περιλαμβάνουν υπολογιστές, κινητά τηλέφωνα, ταμπλέτες και άλλες συσκευές που συνδέονται στο διαδίκτυο.
- Μπορεί επίσης να χρησιμοποιείτε διαδικτυακούς λογαριασμούς για ηλεκτρονικό ταχυδρομείο, τραπεζικές συναλλαγές, αγορές, μέσα κοινωνικής δικτύωσης, παίγνια και άλλα.

Η προσωπική ασφάλεια στον κυβερνοχώρο είναι τα συνεχή μέτρα που μπορείτε να λάβετε για να προστατεύσετε τους λογαριασμούς και τις συσκευές σας από απειλές στον κυβερνοχώρο.

Τι είναι οι απειλές στον κυβερνοχώρο;

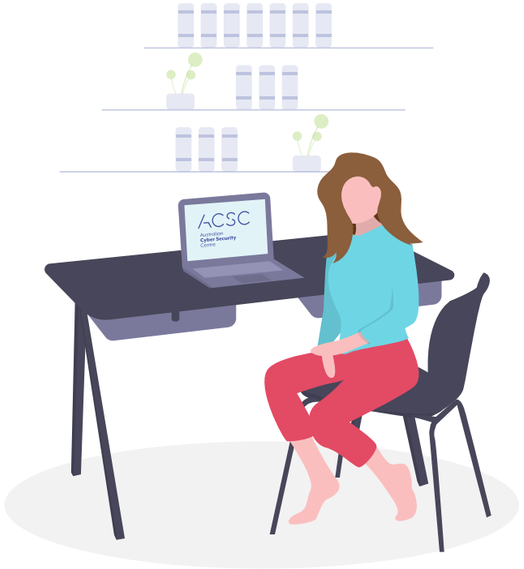
Οι κύριες απειλές στον κυβερνοχώρο που επηρεάζουν τους καθημερινούς Αυστραλούς είναι οι **απάτες και το επιβλαβές λογισμικό**.

- **Το επιβλαβές λογισμικό είναι ένας γενικός όρος που χρησιμοποιείται για να περιγράψει κακόβουλο λογισμικό** σχεδιασμένο να προκαλέσει βλάβη. Αυτό μπορεί να περιλαμβάνει ιούς, «σκουλήκια» (worms), λογισμικό υποκλοπής (spyware), «δούριους ίππους» trojans και λογισμικό λύτρων (ransomware). Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν κακόβουλο λογισμικό για να κλέψουν τις πληροφορίες και τα χρήματά σας και να ελέγξουν τις συσκευές και τους λογαριασμούς σας.
- **Οι απάτες είναι μηνύματα που αποστέλλονται από εγκληματίες του κυβερνοχώρου** με σκοπό να σας χειραγωγήσουν ώστε να δώσετε ευαίσθητες πληροφορίες ή να ενεργοποιήσουν κακόβουλο λογισμικό στη συσκευή σας.

Αυτές οι επιθέσεις μπορεί να έχουν σημαντικές προσωπικές και οικονομικές επιπτώσεις στα θύματα. Αυξάνονται επίσης σε πολυπλοκότητα και συχνότητα.

Πώς μπορεί αυτός ο οδηγός να με βοηθήσει να προστατευτώ από απειλές στον κυβερνοχώρο;

Εάν μαθαίνετε για πρώτη φορά για την ασφάλεια στον κυβερνοχώρο ή εάν ενημερώνεστε για την ασφάλεια στον κυβερνοχώρο, ο παρών οδηγός είναι ένα εξαιρετικό μέρος για να ξεκινήσετε. Η προσωπική κυβερνοασφάλεια: Ο οδηγός πρώτων βημάτων είναι ο πρώτος από μια σειρά τριών οδηγών που έχουν σχεδιαστεί για να σας βοηθήσουν να κατανοήσετε τα βασικά στοιχεία της ασφάλειας στον κυβερνοχώρο.



Ενεργοποιήστε τις αυτόματες ενημερώσεις

Τι είναι οι ενημερώσεις;

Μια ενημέρωση είναι μια βελτιωμένη έκδοση λογισμικού (προγράμματα, εφαρμογές και λειτουργικά συστήματα) που έχετε εγκαταστήσει στον υπολογιστή και τις κινητές συσκευές σας.

- **Οι ενημερώσεις λογισμικού συμβάλλουν στην προστασία των συσκευών σας** με την εξάλειψη των «κοριών» (σφάλματα) του λογισμικού (σφάλματα κωδικοποίησης ή ευπάθειες). Οι εγκληματίες του κυβερνοχώρου και κακόβουλο λογισμικό μπορούν να χρησιμοποιήσουν αυτούς τους «κοριούς» για να αποκτήσουν πρόσβαση στη συσκευή σας και να κλέψουν τα προσωπικά σας δεδομένα, τους λογαριασμούς, τις οικονομικές πληροφορίες και την ταυτότητά σας.
- **Νέοι «κοριοί» λογισμικού ανακαλύπτονται συνεχώς** και αξιοποιούνται από τους εγκληματίες του κυβερνοχώρου. Η ενημέρωση του λογισμικού στις συσκευές σας βοηθά στην προστασία σας από κυβερνοεπιθέσεις.

Πώς μπορώ να ρυθμίσω τις αυτόματες ενημερώσεις;

Οι αυτόματες ενημερώσεις είναι μια προεπιλεγμένη ρύθμιση που εγκαθιστά τις νέες ενημερώσεις μόλις αυτές είναι διαθέσιμες.

- Ενεργοποιήστε και ρυθμίστε τις αυτόματες ενημερώσεις σε όλο το λογισμικό και τις συσκευές.
- Ο τρόπος ενεργοποίησης των αυτόματων ενημερώσεων μπορεί να διαφέρει ανάλογα με το λογισμικό και τη συσκευή.
- Ορίστε μια βολική ώρα για τις αυτόματες ενημερώσεις, αν είναι δυνατόν, όπως όταν κοιμάστε ή όταν δεν χρησιμοποιείτε συνήθως τη συσκευή σας.

Η συσκευή σας πρέπει να είναι ενεργοποιημένη, συνδεδεμένη με το ρεύμα και να έχει αχρησιμοποίητο χώρο αποθήκευσης.

Συμβουλή: Εάν σας ζητηθεί να ενημερώσετε το λογισμικό της συσκευής σας, θα πρέπει να το κάνετε το συντομότερο δυνατό.

Λεπτομερέστερες πληροφορίες για το πώς να ενεργοποιήσετε τις αυτόματες ενημερώσεις μπορείτε να βρείτε αναζητώντας «Ενημερώσεις» στο cyber.gov.au

Τι γίνεται αν η ρύθμιση αυτόματης ενημέρωσης δεν είναι διαθέσιμη;

Εάν η ρύθμιση αυτόματης ενημέρωσης δεν είναι διαθέσιμη, θα πρέπει να ελέγχετε τακτικά για νέες ενημερώσεις και να τις εγκαθιστάτε μέσω της μενού ρυθμίσεων του λογισμικού ή της συσκευής σας.

Τι γίνεται αν η παλαιότερη συσκευή και το λογισμικό μου δεν λαμβάνουν καμία ενημέρωση;

Εάν η συσκευή, το λειτουργικό σύστημα ή το λογισμικό σας είναι πολύ παλιά, ενδέχεται να μην υποστηρίζεται πλέον από τον κατασκευαστή ή τον προγραμματιστή.

Όταν τα προϊόντα φτάσουν σε αυτό το στάδιο «λήξη υποστήριξης», δεν θα λαμβάνουν πλέον ενημερώσεις. Αυτό μπορεί να σας αφήσει ευάλωτους σε κυβερνοεπιθέσεις. Παραδείγματα προϊόντων που βρίσκονται σε κατάσταση τέλους υποστήριξης περιλαμβάνουν το λειτουργικό σύστημα Windows 7 και το iPhone 7.

Εάν η συσκευή, το λειτουργικό σύστημα ή το λογισμικό σας έχει φτάσει στη λήξη της υποστήριξης, η ACSC συνιστά αναβάθμιση το συντομότερο δυνατό για να παραμείνετε ασφαλείς.

Για περισσότερες πληροφορίες, αναζητήστε «Λήξη υποστήριξης» στο cyber.gov.au

Ενεργοποιήστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA).

Τι είναι ο MFA;

Μπορείτε να χρησιμοποιήσετε τον έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA) για να βελτιώσετε την ασφάλεια των πιο σημαντικών λογαριασμών σας. Ο MFA απαιτεί από εσάς να παράγετε έναν συνδυασμό δύο ή περισσότερων τύπων ελέγχου ταυτότητας πριν από τη χορήγηση πρόσβασης σε έναν λογαριασμό.

- **Κάτι που γνωρίζετε** (π.χ. PIN, κωδικός πρόσβασης ή φράση πρόσβασης)
- **Κάτι που έχετε** (π.χ. έξυπνη κάρτα, φυσικό διακριτικό, εφαρμογή ελέγχου ταυτότητας, SMS ή ηλεκτρονικό ταχυδρομείο)
- **Κάτι που είστε** (π.χ. αποτύπωμα, αναγνώριση προσώπου ή σάρωση ίριδας).

Ο MFA δυσκολεύει τους εγκληματίες του κυβερνοχώρου να αποκτήσουν αρχική πρόσβαση στο λογαριασμό σας. Προσθέτει περισσότερα επίπεδα ελέγχου ταυτότητας, που απαιτούν επιπλέον χρόνο, προσπάθεια και πόρους για να παραβιαστούν.

Πώς μπορώ να ενεργοποιήσω το MFA για να προστατεύσω τα τους πιο σημαντικούς λογαριασμούς μου;

Τα βήματα για την ενεργοποίηση του MFA είναι διαφορετικά ανάλογα με τον λογαριασμό, τη συσκευή ή το λογισμικό της εφαρμογής. Θα πρέπει να ενεργοποιήσετε το MFA τώρα, ξεκινώντας με τους σημαντικούς σας λογαριασμούς:

- Όλοι οι λογαριασμοί ηλεκτρονικών τραπεζικών και χρηματοοικονομικών συναλλαγών (π.χ. η τράπεζά σας, το PayPal)
- Όλοι οι λογαριασμοί ηλεκτρονικού ταχυδρομείου (π.χ. Gmail, Outlook, Hotmail, Yahoo!)

Εάν έχετε πολλούς λογαριασμούς ηλεκτρονικού ταχυδρομείου, δώστε προτεραιότητα σε αυτούς που συνδέονται με τις ηλεκτρονικές σας τραπεζικές συναλλαγές ή άλλες σημαντικές υπηρεσίες.

Μπορείτε να διαβάσετε περισσότερα σχετικά με το πώς να ενεργοποιήσετε τον έλεγχο ταυτότητας πολλαπλών παραγόντων αναζητώντας «Multi-factor MFA' ή 'MFA' στο cyber.gov.au

Δημιουργείτε τακτικά αντίγραφα ασφαλείας των συσκευών σας

Τι είναι το εφεδρικό αντίγραφο ασφαλείας;

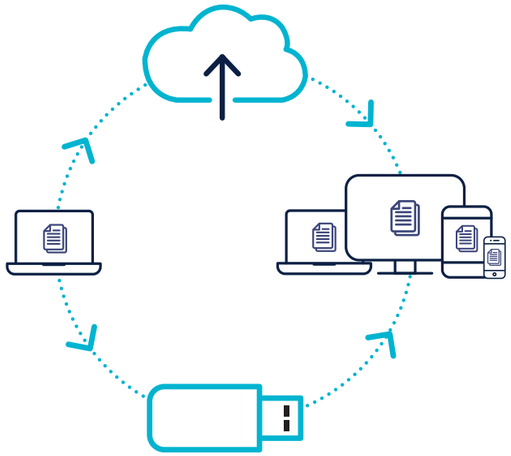
Ένα αντίγραφο ασφαλείας είναι ένα ψηφιακό αντίγραφο των πληροφοριών σας. Αυτό μπορεί να περιλαμβάνει πράγματα όπως φωτογραφίες, οικονομικές πληροφορίες ή αρχεία που έχετε αποθηκεύσει σε μια εξωτερική συσκευή αποθήκευσης ή στο cloud.

Η δημιουργία αντιγράφων ασφαλείας των πληροφοριών σας είναι ένα προληπτικό μέτρο, ώστε να μπορούν να ανακτηθούν σε περίπτωση που ποτέ χαθούν, κλαπούν ή καταστραφούν.

Πώς μπορώ να δημιουργήσω αντίγραφα ασφαλείας των συσκευών και των σελίδων μου;

Θα πρέπει να δημιουργείτε τακτικά αντίγραφα ασφαλείας των αρχείων και των συσκευών σας. Το πώς φαίνεται αυτό, αν είναι καθημερινά, εβδομαδιαία ή μηνιαία, εξαρτάται από εσάς. Το πόσες φορές θα δημιουργήσετε αντίγραφα ασφαλείας μπορεί να εξαρτάται από το τον αριθμό των:

- νέων αρχείων που φορτώνετε στη συσκευή σας,
- των αλλαγών που κάνετε στα αρχεία.



Συμβουλή: Ελέγχετε τακτικά τα αντίγραφα ασφαλείας σας, ώστε να είστε εξοικειωμένοι με την διαδικασία ανάκτησης. Να βεβαιώνεστε πάντα ότι τα αντίγραφα ασφαλείας σας λειτουργούν σωστά.

Λεπτομερέστερες πληροφορίες σχετικά με τον τρόπο δημιουργίας αντιγράφων ασφαλείας των πληροφοριών σας μπορείτε να βρείτε αναζητώντας «Εφεδρικά αντίγραφα» στο cyber.gov.au

Χρησιμοποιήστε φράσεις πρόσβασης για να ασφαλίσετε τους σημαντικούς λογαριασμούς σας

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) είναι ένας από τους πιο αποτελεσματικούς τρόπους προστασίας των λογαριασμών σας από τους εγκληματίες του κυβερνοχώρου. Εάν ο MFA δεν είναι διαθέσιμος, μια μοναδική ισχυρή φράση πρόσβασης μπορεί να προστατεύσει καλύτερα τον λογαριασμό σας σε σύγκριση με έναν απλό κωδικό πρόσβασης.

Τι είναι η φράση πρόσβασης;

Μια φράση πρόσβασης χρησιμοποιεί τέσσερις ή περισσότερες τυχαίες λέξεις ως κωδικό πρόσβασης.

Για παράδειγμα: «κρυστάλλινο κρεμμύδι πρέτσελ».

- **Οι φράσεις πρόσβασης είναι πιο ασφαλείς** από τους απλούς κωδικούς πρόσβασης.
- Οι φράσεις πρόσβασης είναι δύσκολο να σπάσουν οι εγκληματίες του κυβερνοχώρου, αλλά **εύκολο να τις θυμάστε**.

Πώς μπορώ να δημιουργήσω μια φράση πρόσβασης;

Δημιουργήστε φράσεις πρόσβασης που είναι:

- **Μεγάλες:** τουλάχιστον 14 χαρακτήρες, χρησιμοποιώντας τέσσερις ή περισσότερες τυχαίες λέξεις. Όσο μεγαλύτερη είναι η φράση πρόσβασής σας τόσο πιο ασφαλής είναι.
- **Μη προβλέψιμες:** χρησιμοποιήστε ένα τυχαίο μείγμα τεσσάρων ή περισσότερων άσχετων λέξεων. Όχι διάσημες φράσεις, αποσπάσματα ή στίχους.
- **Μοναδικές:** που δεν επαναχρησιμοποιούνται σε πολλούς λογαριασμούς.

Εάν ένας ιστότοπος ή μια υπηρεσία απαιτεί σύνθετο κωδικό πρόσβασης που περιλαμβάνει σύμβολα, κεφαλαία γράμματα ή αριθμούς, μπορείτε να τα συμπεριλάβετε στη φράση πρόσβασής σας. Η φράση πρόσβασής σας θα πρέπει να εξακολουθεί να είναι μεγάλη, απρόβλεπτη και μοναδική για την καλύτερη δυνατή ασφάλεια..

Ποιους λογαριασμούς θα πρέπει να ασφαλίσω με μια φράση πρόσβασης;

Εάν οι πιο σημαντικοί λογαριασμοί σας δεν προστατεύονται με MFA, αλλάξτε τους κωδικούς πρόσβασης σε μοναδικές ισχυρές φράσεις πρόσβασης, ξεκινώντας με:

- Ηλεκτρονικές τραπεζικές συναλλαγές και χρηματοοικονομικούς λογαριασμούς.
- Λογαριασμούς ηλεκτρονικού ταχυδρομείου

Εάν έχετε πολλούς λογαριασμούς ηλεκτρονικού ταχυδρομείου, δώστε προτεραιότητα σε εκείνους που συνδέονται με τις ηλεκτρονικές τραπεζικές σας συναλλαγές ή άλλες σημαντικές υπηρεσίες.

Μπορείτε συνήθως να αλλάξετε τον κωδικό πρόσβασής σας σε μια μοναδική ισχυρή φράση πρόσβασης μέσω του μενού ρυθμίσεων του λογαριασμού σας.

Συμβουλή: Αν δυσκολεύεστε να θυμάστε όλες τις φράσεις πρόσβασης, σκεφτείτε να χρησιμοποιήσετε έναν διαχειριστή κωδικών πρόσβασης. Με έναν διαχειριστή κωδικών πρόσβασης, χρειάζεται να θυμάστε μόνο έναν κωδικό πρόσβασης, ενώ ο διαχειριστής κωδικών πρόσβασης αναλαμβάνει τα υπόλοιπα. Για περισσότερες συμβουλές, αναζητήστε το «διαχειριστής κωδικών πρόσβασης» στο cyber.gov.au.

Λεπτομερέστερες πληροφορίες σχετικά με τον τρόπο δημιουργίας ασφαλών φράσεων πρόσβασης μπορείτε να βρείτε αναζητώντας «Φράσεις πρόσβασης» στον ιστότοπο cyber.gov.au

Ασφαλίστε την κινητή σας συσκευή

Σήμερα τα smartphones και τα tablets χρησιμοποιούνται στην καθημερινή ζωή. Τα χρησιμοποιούμε για να συνδεόμαστε, να ψωνίζουμε, να εργαζόμαστε, να κάνουμε τραπεζικές συναλλαγές, να παρακολουθούμε την υγεία μας και να ολοκληρώνουμε εκατοντάδες εργασίες ανά πάσα στιγμή και από οποιαδήποτε τοποθεσία.

Τι μπορεί να συμβεί αν η κινητή μου συσκευή παραβιαστεί, χαθεί ή κλαπεί;

- Μπορεί να χρησιμοποιηθεί από εγκληματίες του κυβερνοχώρου για να κλέψουν τα χρήματα ή την ταυτότητά σας. Αυτό το κάνουν χρησιμοποιώντας πληροφορίες που είναι αποθηκευμένες στη συσκευή σας, συμπεριλαμβανομένων των λογαριασμών κοινωνικής δικτύωσης και ηλεκτρονικού ταχυδρομείου.
- Μπορεί να χάσετε αναντικατάστατα δεδομένα, όπως φωτογραφίες, σημειώσεις ή μηνύματα (αν δεν έχει δημιουργηθεί αντίγραφο ασφαλείας).
- Ένας εγκληματίας του κυβερνοχώρου μπορεί να χρησιμοποιήσει τον αριθμό τηλεφώνου σας για να εξαπατήσει άλλους ανθρώπους.

Πώς μπορώ να ασφαλίσω την κινητή μου συσκευή;

Ασφάλεια συσκευής:

- **Κλειδώστε** τη συσκευή σας με μια φράση πρόσβασης, έναν κωδικό πρόσβασης, ένα PIN ή έναν κωδικό πρόσβασης. Κάντε το δύσκολο να το μαντέψει κάποιος - η ημερομηνία γέννησης και τα μοτίβα κλειδώματος είναι εύκολο να εξαχθούν από τους εγκληματίες του κυβερνοχώρου. Χρησιμοποιήστε μια φράση πρόσβασης για βέλτιστη ασφάλεια (βλ. σελίδα 6). Μπορείτε επίσης να εξετάσετε το ενδεχόμενο να χρησιμοποιήσετε αναγνώριση προσώπου ή ένα αποτύπωμα προσώπου για να ξεκλειδώνετε τη συσκευή σας.
- **Βεβαιωθείτε** ότι η συσκευή σας έχει ρυθμιστεί να κλειδώνει αυτόματα μετά από σύντομο χρονικό διάστημα αδράνειας.
- **Μην** φορτίζετε τη συσκευή σας σε δημόσιο σταθμό φόρτισης και αποφύγετε φορτιστές από τρίτους.
- **Αντιμετωπίστε** το τηλέφωνό σας όπως το πορτοφόλι σας. Διατηρήστε το ασφαλές και να το έχετε πάντα μαζί σας.

Ασφάλεια λογισμικού και εφαρμογών:

- **Χρησιμοποιήστε** τη λειτουργία αυτόματης ενημέρωσης της συσκευής σας για να εγκαταστήσετε νέες ενημερώσεις εφαρμογών και λειτουργικού συστήματος μόλις αυτές είναι διαθέσιμες.
- **Ρυθμίστε** τη συσκευή ώστε να απαιτεί μια φράση πρόσβασης/κλειδί πρόσβασης πριν από την εγκατάσταση εφαρμογών. Ο γονικός έλεγχος μπορεί επίσης να χρησιμοποιηθεί γι' αυτό το σκοπό.
- **Ελέγξτε** προσεκτικά τα δικαιώματα απορρήτου όταν εγκαθιστάτε νέες εφαρμογές στη συσκευή σας, ιδίως για τις δωρεάν εφαρμογές. Εγκαθιστάτε μόνο εφαρμογές από αξιόπιστους προμηθευτές.

Ασφάλεια δεδομένων:

- **Ενεργοποιήστε** το απομακρυσμένο κλείδωμα και καθάρισμα λειτουργιών, εάν η συσκευή σας τις υποστηρίζει.
- **Βεβαιωθείτε** ότι έχετε αφαιρέσει σχολαστικά τα προσωπικά Δεδομένα από τη συσκευή σας πριν το πουλήσετε ή το απορρίψετε.

Ασφάλεια συνδεσιμότητας:

- **Απενεργοποιήστε** το Bluetooth και το Wi-Fi όταν δεν τα χρησιμοποιείτε.
- **Βεβαιωθείτε** ότι η συσκευή σας δεν συνδέεται αυτόματα σε νέα δίκτυα Wi-Fi.

Λεπτομερέστερες πληροφορίες σχετικά με το πώς να ασφαλίσετε το κινητό σας μπορείτε να βρείτε αναζητώντας «Ασφαλίστε την κινητή σας συσκευή» στον ιστότοπο cyber.gov.au

Ανάπτυξη της ασφαλούς σκέψης σας στο κυβερνοχώρο

Η προσωπική ασφάλεια στον κυβερνοχώρο δεν έχει να κάνει μόνο με την αλλαγή των ρυθμίσεων, αλλά και με την αλλαγή της σκέψης και της συμπεριφοράς σας.

Προσοχή στις απάτες στον κυβερνοχώρο

Οι εγκληματίες του κυβερνοχώρου είναι γνωστό ότι χρησιμοποιούν ηλεκτρονικό ταχυδρομείο, μηνύματα, μέσα κοινωνικής δικτύωσης ή τηλεφωνήματα για να προσπαθήσουν να εξαπατήσουν τους Αυστραλούς. Μπορεί να προσποιηθούν ότι είναι κάποιο άτομο ή οργανισμός που νομίζετε ότι γνωρίζετε ή ότι πρέπει να εμπιστευτείτε.

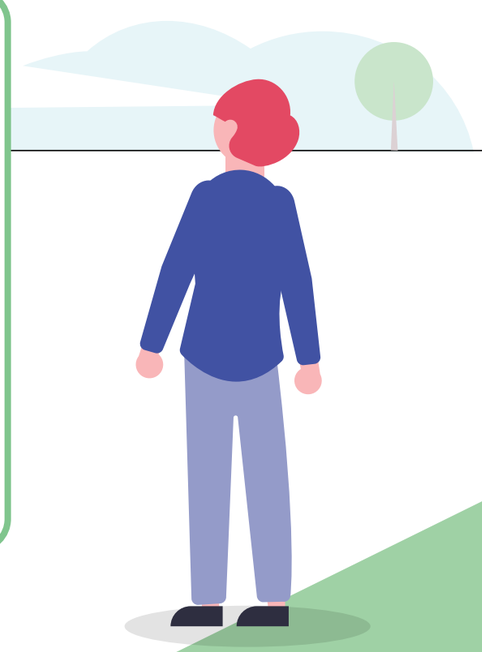
Τα μηνύματα και οι κλήσεις τους προσπαθούν να σας ξεγελάσουν για να εκτελέσετε συγκεκριμένες ενέργειες, όπως:

- Να αποκαλύψετε στοιχεία τραπεζικών λογαριασμών, κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών,
- Να δώσετε απομακρυσμένη πρόσβαση στον υπολογιστή σας,
- Να ανοίξετε ένα συνημμένο αρχείο, το οποίο μπορεί να περιέχει κακόβουλο λογισμικό,
- Να αποστείλετε χρήματα ή δωροκάρτες.

Πώς μπορώ να αναγνωρίσω μηνύματα απάτης;

Μπορεί να είναι δύσκολο να αναγνωρίσετε μηνύματα απάτης. Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν συχνά ορισμένες μεθόδους για να σας ξεγελάσουν. Τα μηνύματά τους μπορεί να περιλαμβάνουν:

- **Επίσημο φορέα:** Ισχυρίζεται το μήνυμα ότι προέρχεται από κάποιον επίσημο φορέα, όπως η τράπεζά σας;
- **Επείγον:** σας λένε ότι υπάρχει κάποιο πρόβλημα ή ότι έχετε περιορισμένο χρόνο για να απαντήσετε ή να πληρώσετε;
- **Συναίσθημα:** το μήνυμα σας προκαλεί πανικό, ελπίδα ή περιέργεια;
- **Σπανιότητα:** το μήνυμα προσφέρει κάτι που βρίσκεται σε έλλειψη ή υπόσχεται μια καλή προσφορά;
- **Τρέχοντα γεγονότα:** το μήνυμα αφορά μια τρέχουσα είδηση ή ένα μεγάλο γεγονός;



Μάθετε πώς να εντοπίζετε μηνύματα "ψαρέματος" ή απάτης, επισκεπτόμενοι την ενότητα Μάθετε τα βασικά στον ιστότοπο cyber.gov.au

Τι μπορώ να κάνω αν λάβω ένα μήνυμα απάτης;

Εάν λάβετε ένα μήνυμα ή τηλεφώνημα απάτης, θα πρέπει να το αγνοήσετε, να το διαγράψετε ή να το αναφέρετε στο Scamwatch της ACCC στη διεύθυνση scamwatch.gov.au

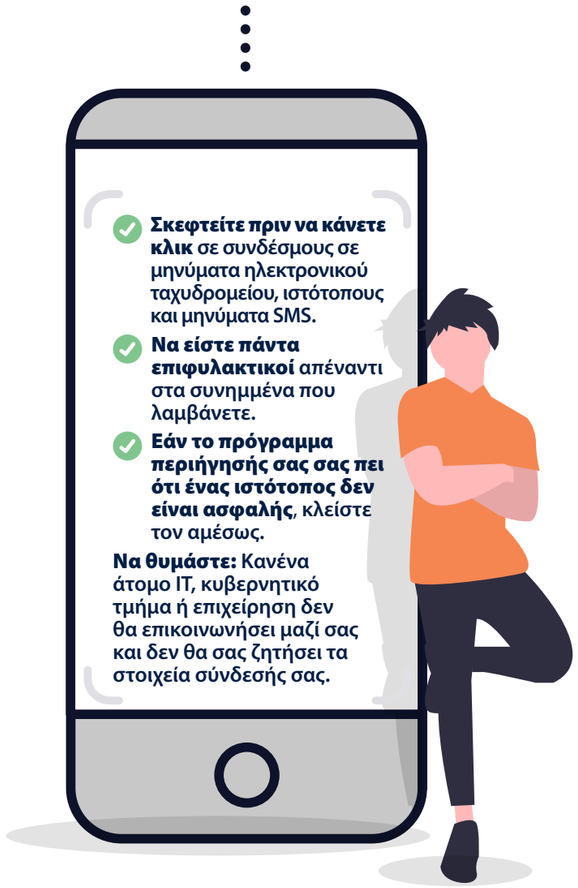
Μπορείτε επίσης να επικοινωνήσετε με τη Γραμμή για την ασφάλεια στον κυβερνοχώρο της ACSC στο **1300 CYBER1** (1300 292 371), εάν ανησυχείτε για την ασφάλεια στον κυβερνοχώρο.

Εάν έχετε εμπλακεί σε μια απάτη και πιστεύετε ότι οι τραπεζικοί σας λογαριασμοί, οι πιστωτικές ή χρεωστικές σας κάρτες μπορεί να κινδυνεύουν, επικοινωνήστε αμέσως με το χρηματοπιστωτικό σας ίδρυμα. Μπορεί να είναι σε θέση να κλείσουν το λογαριασμό σας ή να σταματήσουν μια συναλλαγή.

Τι γίνεται αν δεν είμαι σίγουρος/η εάν το μήνυμα είναι απάτη;

Αν πιστεύετε ότι ένα μήνυμα ή μια κλήση μπορεί πραγματικά να προέρχεται από έναν οργανισμό που εμπιστεύεστε (όπως η τράπεζά σας), βρείτε μια μέθοδο επικοινωνίας που μπορείτε να εμπιστευτείτε. Αναζητήστε τον ιστότοπο του οργανισμού, τηλεφωνήστε στον αριθμό τηλεφώνου που διαφημίζεται ή επισκεφθείτε ένα φυσικό κατάστημα ή υποκατάστημα. Μην χρησιμοποιείτε τους συνδέσμους ή τα στοιχεία επικοινωνίας στο μήνυμα που σας έχει σταλεί ή σας έχει δοθεί τηλεφωνικά, καθώς αυτά μπορεί να είναι δόλια.

Συμβουλή: Σκεφτείτε πριν να κάνετε κλικ



Αν νομίζετε ότι είστε θύμα ηλεκτρονικού εγκλήματος, αναφέρετε το μέσω του ReportCyber της ACSC στη διεύθυνση cyber.gov.au/report ή καλέστε τη Γραμμή για την ασφάλεια στον κυβερνοχώρο στο 1300 CYBER1 (1300 292 371).

Μπορείτε επίσης να ενημερώνεστε για τις πιο πρόσφατες απειλές με την εγγραφή σας στη δωρεάν υπηρεσία ειδοποίησης της ACSC. Αναζήτηση "Εγγραφείτε στην υπηρεσία ειδοποίησης ACSC" στο cyber.gov.au
Θα σας στέλνουμε ειδοποίηση όταν εντοπίζουμε μια νέα απειλή στον κυβερνοχώρο.

Προσωπική Ασφάλεια στον Κυβερνοχώρο: Πρώτα Βήματα

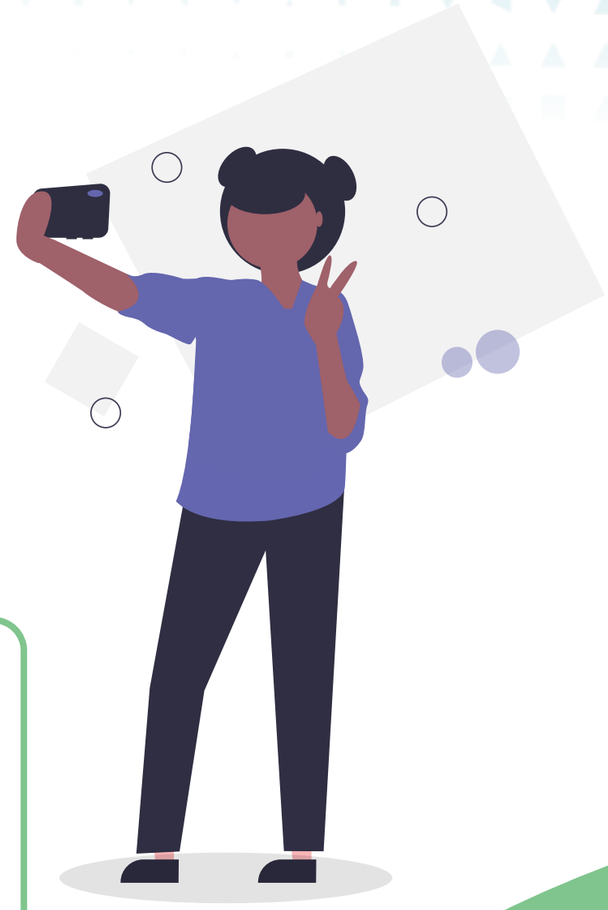
Σταματήστε και σκεφτείτε πριν μοιραστείτε κάτι στα μέσα κοινωνικής δικτύωσης

Οι εγκληματίες του κυβερνοχώρου μπορούν να χρησιμοποιήσουν τις πληροφορίες που έχετε δημοσιεύσει δημοσίως στον/στους λογαριασμό/ους σας στα μέσα κοινωνικής δικτύωσης στις απάτες και τις κυβερνοεπιθέσεις τους.

Να θυμάστε ότι οι πληροφορίες στο διαδίκτυο είναι μόνιμες και δεν μπορείτε ποτέ να αφαιρέσετε πλήρως ό,τι έχει αναρτηθεί.

Πώς μπορώ να σταματήσω και να σκεφτώ πριν κάνω μια ανάρτηση;

- **Σκεφτείτε:** Πώς θα μπορούσε ένας εγκληματίας του κυβερνοχώρου να χρησιμοποιήσει αυτές τις πληροφορίες για να στοχεύσει εμένα ή τους λογαριασμούς μου;
- **Σκεφτείτε:** Θα αισθανόμουν άνετα να δείξω αυτές τις πληροφορίες ή την εικόνα σε έναν εντελώς άγνωστο εκτός του διαδικτύου;



Ποιες πληροφορίες θα πρέπει να αποφεύγω να μοιράζομαι;

Αποφύγετε να μοιράζεστε πληροφορίες (συμπεριλαμβανομένων φωτογραφιών) στο διαδίκτυο, τις οποίες οι εγκληματίες του κυβερνοχώρου μπορούν να χρησιμοποιήσουν για να σας αναγνωρίσουν, να σας χειραγωγήσουν μέσω απάτης ή να μαντέψουν τις ερωτήσεις ανάκτησης του λογαριασμού σας. Αυτό μπορεί να περιλαμβάνει τα εξής:

- Τόπος και ημερομηνία γέννησης.
- Διεύθυνση και αριθμός τηλεφώνου.
- Εργοδότης και ιστορικό εργασίας.
- Πού πήγατε σχολείο.
- Οποιαδήποτε άλλη προσωπική πληροφορία που μπορεί να χρησιμοποιηθεί για να σας στοχοποιήσει.

Συνοπτική λίστα ελέγχου

Έχετε ολοκληρώσει τα πάντα σε αυτόν τον οδηγό;

Χρησιμοποιήστε αυτήν την εύχρηστη λίστα ελέγχου για να παρακολουθείτε την πρόοδό σας:

- **Έχω ενεργοποιήσει τις αυτόματες ενημερώσεις για όλες τις συσκευές μου:**
  - Υπολογιστή (επιτραπέζιο και φορητό υπολογιστή).
  - Κινητό τηλέφωνο.
  - Tablet.
- **Έχω ενεργοποιήσει τον έλεγχο ταυτότητας πολλαπλών παραγόντων στους πιο σημαντικούς λογαριασμούς μου:**
  - όλους τους διαδικτυακούς τραπεζικούς και χρηματοοικονομικούς λογαριασμού μου (π.χ. η τράπεζά σας, PayPal).
  - Όλους τους λογαριασμούς ηλεκτρονικού ταχυδρομείου μου (π.χ. Gmail, Outlook, Hotmail, Yahoo!).
- **Δημιουργώ τακτικά αντίγραφα ασφαλείας των συσκευών μου::**
  - Υπολογιστή (επιτραπέζιο και φορητό υπολογιστή).
  - Κινητό τηλέφωνο.
  - Tablet.
- **Χρησιμοποιώ μοναδικές ισχυρές φράσεις πρόσβασης στους πιο σημαντικούς λογαριασμούς μου που δεν προστατεύονται από MFA:**
  - Ηλεκτρονικές τραπεζικές συναλλαγές και χρηματοοικονομικούς λογαριασμούς
  - Λογαριασμοί ηλεκτρονικού ταχυδρομείου.
- **Έχω ασφαλίσει τις κινητές μου συσκευές:**
  - Φορητός υπολογιστής.
  - Κινητό τηλέφωνο.
  - Tablet.
- **Χρησιμοποιώ την ασφαλή σκέψη στον κυβερνοχώρο καθημερινά:**
  - Μπορώ να αναγνωρίζω μηνύματα απάτης.
  - Ξέρω τι πρέπει να κάνω αν λάβω ένα μήνυμα απάτης.
  - Ξέρω πώς να ελέγξω αν ένα μήνυμα είναι απάτη αν δεν είμαι σίγουρος/η.
  - Σκέφτομαι πριν κάνω κλικ σε συνδέσμους και συνημμένα αρχεία.
  - Σκέφτομαι πριν μοιραστώ κάτι στα μέσα κοινωνικής δικτύωσης.
- **Ξέρω πού μπορώ να ζητήσω βοήθεια αν είμαι θύμα ηλεκτρονικού εγκλήματος ή απάτης.**

ΓΛΩΣΣΑΡΙ

Ανάκτηση λογαριασμού
Διαδικασία κατά την οποία χρησιμοποιείται ένα σύνολο ερωτήσεων ή άλλες μέθοδοι επαλήθευσης για την ανάκτηση ή την επανάκτηση πρόσβασης σε έναν λογαριασμό ή για την αλλαγή μιας φράσης/ενός κωδικού πρόσβασης λογαριασμού.

Κακόβουλο λογισμικό
Κακόβουλο λογισμικό που χρησιμοποιείται για να αποκτήσει μη εξουσιοδοτημένη πρόσβαση και έλεγχο του υπολογιστή ενός χρήστη, να κλέψει πληροφορίες και να διαταράξει ή να απενεργοποιήσει δίκτυα.

Εφαρμογή
Αναφέρεται επίσης ως εφαρμογή για κινητά, η εφαρμογή είναι ένας όρος για λογισμικό που χρησιμοποιείται συνήθως για smartphone ή tablet.

Συνημμένο
Ένα αρχείο που αποστέλλεται με ένα μήνυμα ηλεκτρονικού ταχυδρομείου.

Λειτουργικό σύστημα
Το λογισμικό που είναι εγκατεστημένο στο σκληρό δίσκο ενός υπολογιστή και επιτρέπει στο υλικό του υπολογιστή να επικοινωνεί με τα προγράμματα του υπολογιστή και να τα εκτελεί. Παραδείγματα: Microsoft Windows, Apple macOS, iOS, Android.

Φυσικό σύμβολο
Μια φυσική συσκευή που μπορεί συνήθως να τοποθετηθεί σε ένα μπρελόκ, το οποίο παράγει έναν κωδικό ασφαλείας που χρησιμοποιείται για την επιβεβαίωση της ταυτότητας ενός χρήστη υπολογιστή που χρησιμοποιεί MFA.

Εφαρμογή Πιστοποίησης
Μια εφαρμογή που χρησιμοποιείται για την πιστοποίηση της ταυτότητας ενός χρήστη υπολογιστή για να να επιτρέψει την πρόσβαση μέσω ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA).

Cloud
Ένα δίκτυο απομακρυσμένων διακομιστών που παρέχουν μαζική, κατανεμημένη αποθήκευση και επεξεργαστική ισχύ.

Απομακρυσμένη πρόσβαση
Αποκτήστε πρόσβαση και έλεγχο σε συσκευές και δίκτυα από μια τοποθεσία εκτός του χώρου σας.

Εγκληματίας στον κυβερνοχώρο
Κάθε άτομο που αποκτά παράνομη πρόσβαση σε ένα σύστημα ή λογαριασμό υπολογιστή για να βλάψει ή να κλέψει πληροφορίες.

Συσκευή
Μια συσκευή υπολογιστών ή επικοινωνιών. Για παράδειγμα, υπολογιστής, φορητός υπολογιστής, κινητό τηλέφωνο ή tablet.

Λογισμικό
Συνήθως αναφέρεται ως προγράμματα, συλλογή οδηγιών που επιτρέπουν στο χρήστη να αλληλεπιδρά με έναν υπολογιστή, το υλικό του ή να εκτελεί εργασίες.

Λήξη της υποστήριξης
Η λήξη της υποστήριξης αναφέρεται σε μια κατάσταση κατά την οποία μια εταιρεία παύει να υποστηρίζει ένα προϊόν ή μια υπηρεσία. Αυτό συνήθως εφαρμόζεται σε προϊόντα υλικού και λογισμικού όταν μια εταιρεία κυκλοφορεί μια νέα έκδοση και τερματίζει την υποστήριξη για τις προηγούμενες εκδόσεις.

Αποποίηση ευθύνης
Το υλικό του παρόντος οδηγού είναι γενικής φύσεως και δεν θα πρέπει να εκλαμβάνεται ως νομική συμβουλή ή να βασίζεστε σε αυτή για βοήθεια σε οποιαδήποτε συγκεκριμένη περίσταση ή κατάσταση έκτακτης ανάγκης. Σε κάθε σημαντικό θέμα, θα πρέπει να ζητάτε την κατάλληλη ανεξάρτητη επαγγελματική συμβουλή σε σχέση με τις δικές σας συνθήκες.

Η Κοινοπολιτεία δεν αποδέχεται καμία ευθύνη ή υποχρέωση για οποιαδήποτε ζημία, απώλεια ή έξοδα που προέκυψαν ως αποτέλεσμα της εμπιστοσύνης στις πληροφορίες που περιέχονται στον παρόντα οδηγό.

Για περισσότερες πληροφορίες ή για να αναφέρετε ένα περιστατικό ασφάλειας στον κυβερνοχώρο, επικοινωνήστε μαζί μας:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Ο αριθμός αυτός διατίθεται προς χρήση μόνο εντός της Αυστραλίας.

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre