ΚΑΤΑΓΓΕΛΛΕΤΕ ΕΠΙΘΕΣΕΙΣ ΚΑΙ ΠΕΡΙΣΤΑΤΙΚΑ ΣΤΟΝ ΚΥΒΕΡΝΟΧΩΡΟ ΓΙΑ ΝΑ ΔΙΑΤΗΡΕΙΤΑΙ Η ΑΥΣΤΡΑΛΙΑ ΑΣΦΑΛΗΣ.

ΕΓΓΡΑΦΕΙΤΕ

Στην υπηρεσία μας για δωρεάν προειδοποιήσεις

cyber.gov.au

ΑΝΑΦΕΡΕΤΕ

Έγκλημα κυβερνοχώρου στο REPORTCYBER:

cyber.gov.au/report

ΕΠΙΚΟΙΝΩΝΙΑ

Καλέστε το 1300 CYBER1 ή επισκεφτείτε το cyber.gov.au

Ο αριθμός αυτός διατίθεται προς χρήση μόνο εντός της Αυστραλίας.

ΑΚΟΛΟΥΘΗΣΤΕ ΜΑΣ

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

5. ΠΡΟΣΕΧΕΤΕ ΤΙΣ ΑΠΑΤΕΣ

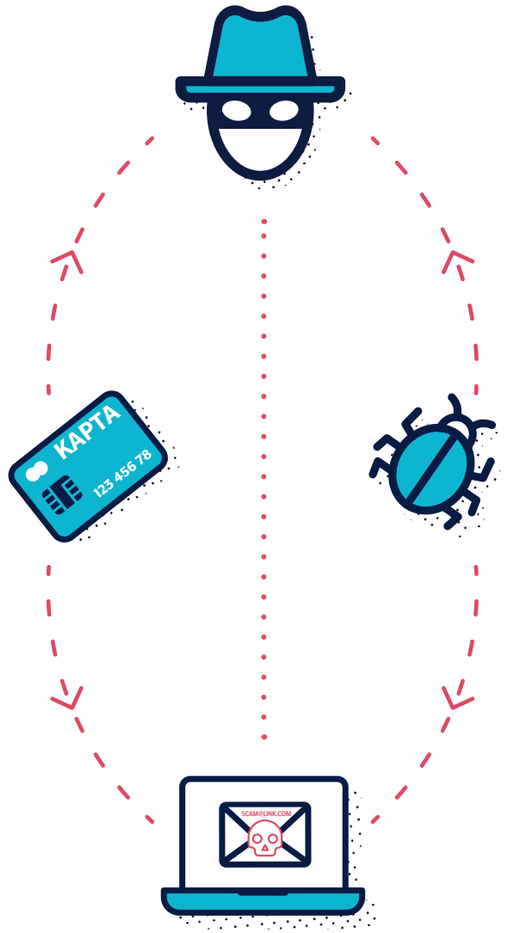
Οι εγκληματίες του κυβερνοχώρου χρησιμοποιούν μηνύματα ηλεκτρονικού ταχυδρομείου, SMS, τηλεφωνικές κλήσεις και μέσα κοινωνικής δικτύωσης για να σας ξεγελάσουν ώστε να ανοίξετε ένα συνημμένο, να επισκεφτείτε μια ιστοσελίδα, να αποκαλύψετε στοιχεία σύνδεσης λογαριασμού, να φανερώσετε ευαίσθητες πληροφορίες ή να κάνετε μεταφορά χρημάτων ή δωροκαρτών. Αυτά τα μηνύματα εμφανίζονται επίτηδες σαν να έχουν σταλεί από άτομα ή οργανισμούς που νομίζετε ότι γνωρίζετε ή πιστεύετε ότι θα πρέπει να τους εμπιστευτείτε.

Για να εντοπίζετε μηνύματα απάτης, σταματήστε και σκεφτείτε:

- **Εγκυρότητα:** Το μήνυμα ισχυρίζεται ότι προέρχεται από κάποιον αξιωματούχο;
- **Επείγον:** Σας λένε ότι έχετε περιορισμένο χρόνο για να απαντήσετε;
- **Συναίσθημα:** Μήπως το μήνυμα σας προξενεί πανικό, φόβο, ελπίδα ή περιέργεια;
- **Σπάνιο:** Το μήνυμα προσφέρει κάτι δυσεύρετο;
- **Επικαιρότητα:** Το μήνυμα σχετίζεται με επίκαιρες ειδήσεις, σημαντικά γεγονότα ή συγκεκριμένες περιόδους του έτους (όπως όταν κάνετε φορολογικές δηλώσεις);

Για να ελέγξετε εάν ένα μήνυμα είναι αυθεντικό:

- Ανατρέξτε σε κάτι που μπορείτε να εμπιστευτείτε. Επισκεφτείτε την επίσημη ιστοσελίδα, συνδεθείτε στο λογαριασμό σας ή τηλεφωνήστε στο διαφημιζόμενο αριθμό τηλεφώνου της υπηρεσίας. Μη χρησιμοποιείτε τους συνδέσμους ή τα στοιχεία επικοινωνίας στο μήνυμα που σας έχουν στείλει ή σας έχουν δώσει από τηλεφώνου.
- Ελέγξτε αν η επίσημη πηγή σάς έχει ήδη πει τι δεν θα σας ρωτήσουν ποτέ. Για παράδειγμα, η τράπεζά σας μπορεί να σας έχει πει ότι δεν θα ζητήσει ποτέ τον κωδικό πρόσβασής σας.



Για περισσότερες πληροφορίες σχετικά με τον εντοπισμό μηνυμάτων απάτης, ανατρέξτε στη δημοσίευση Detecting Socially Engineered Messages (Ανίχνευση Κοινωνικά Κατασκευασμένων Μηνυμάτων) του Αυστραλιανού Κέντρου Ασφάλειας Κυβερνοχώρου (ACSC) και παραμένετε ενημερωμένοι κάνοντας εγγραφή στην Υπηρεσία Προειδοποιήσεων (Alert Service) του ACSC στο **cyber.gov.au.**

ΑΠΛΑ ΒΗΜΑΤΑ

ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ ΤΩΝ ΣΥΣΚΕΥΩΝ ΚΑΙ ΤΩΝ ΛΟΓΑΡΙΑΣΜΩΝ ΣΑΣ

ΜΕΙΩΣΤΕ ΤΟΝ ΚΙΝΔΥΝΟ ΝΑ ΓΙΝΕΤΕ ΣΤΟΧΟΣ ΕΓΚΛΗΜΑΤΙΩΝ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ ΑΚΟΛΟΥΘΩΝΤΑΣ ΑΥΤΑ ΤΑ ΒΗΜΑΤΑ

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

1. ΕΝΗΜΕΡΩΝΕΤΕ ΤΙΣ ΣΥΣΚΕΥΕΣ ΣΑΣ

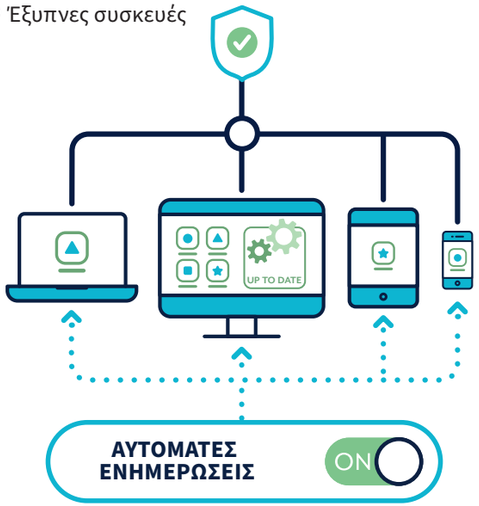
Οι εγκληματίες του κυβερνοχώρου παραβιάζουν (χακάρουν) συσκευές χρησιμοποιώντας γνωστές αδυναμίες σε συστήματα ή εφαρμογές. Οι ενημερώσεις περιέχουν αναβαθμίσεις ασφαλείας για να διορθώνουν αυτές τις αδυναμίες. Ενεργοποιήστε τις αυτόματες ενημερώσεις, έτσι ώστε να μη χρειάζεται να τις κάνετε εσείς.

Ενεργοποιήστε τις αυτόματες ενημερώσεις σε όλες τις συσκευές σας:

- Κινητό τηλέφωνο
- Φορητό υπολογιστή (Laptop)
- Επιτραπέζιο υπολογιστή (Desktop)

Ελέγχετε τακτικά αν υπάρχουν ενημερώσεις για:

- Εφαρμογές
- Προγράμματα
- Έξυπνες συσκευές



2. ΕΝΕΡΓΟΠΟΙΗΣΤΕ ΤΟΝ ΕΛΕΓΧΟ ΤΑΥΤΟΤΗΤΑΣ ΠΟΛΛΑΠΛΩΝ ΠΑΡΑΓΟΝΤΩΝ (MFA)

Το MFA βελτιώνει την ασφάλειά σας αυξάνοντας τη δυσκολία πρόσβασης των εγκληματιών κυβερνοχώρου στα αρχεία ή στο λογαριασμό σας.

Ενεργοποιήστε το MFA, ξεκινώντας με τους πιο σημαντικούς λογαριασμούς σας:

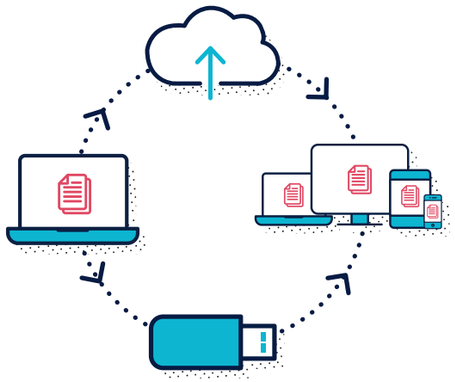
- Λογαριασμούς email
- Ηλεκτρονικές τραπεζικές συναλλαγές και λογαριασμούς με αποθηκευμένα στοιχεία πληρωμής
- Μέσα κοινωνικής δικτύωσης

3. ΔΗΜΙΟΥΡΓΗΣΤΕ ΑΝΤΙΓΡΑΦΑ ΑΣΦΑΛΕΙΑΣ ΤΩΝ ΣΥΣΚΕΥΩΝ ΣΑΣ

Το αντίγραφο ασφαλείας (backup) είναι ένα ψηφιακό αντίγραφο των πληροφοριών που είναι αποθηκευμένες στη συσκευή σας, όπως φωτογραφίες, έγγραφα, βίντεο και δεδομένα από εφαρμογές. Μπορεί να αποθηκευτεί σε μια εξωτερική συσκευή αποθήκευσης ή στο cloud. Δημιουργία αντιγράφων ασφαλείας σημαίνει ότι μπορείτε να αποκαταστήσετε τα αρχεία σας σε περίπτωση τυχόν απώλειας, κλοπής ή φθοράς της συσκευής σας.

Δημιουργείτε τακτικά αντίγραφα ασφαλείας των συσκευών σας:

- Κινητό τηλέφωνο
- Φορητός υπολογιστής
- Επιτραπέζιος υπολογιστής
- Τάμπλετ



4. ΟΡΙΖΕΤΕ ΑΣΦΑΛΕΙΣ ΦΡΑΣΕΙΣ ΠΡΟΣΒΑΣΗΣ

Σε περιπτώσεις όπου δεν είναι διαθέσιμο το MFA, μια ασφαλής φράση πρόσβασης (passphrase) μπορεί συχνά να είναι το μόνο πράγμα που προστατεύει τις πληροφορίες και τους λογαριασμούς σας από εγκληματίες.

Μια φράση πρόσβασης χρησιμοποιεί τέσσερις ή περισσότερες τυχαίες λέξεις ως κωδικό πρόσβασης. Αλλάζετε τους κωδικούς σας σε φράσεις πρόσβασης, διασφαλίζοντας ότι είναι:

- Μακροσκελείς: Όσο μεγαλύτερη είναι η φράση πρόσβασης, τόσο το καλύτερο. Πρέπει να αποτελείται από τουλάχιστον 14 χαρακτήρες
- Απρόβλεπτοι: Χρησιμοποιήστε έναν τυχαίο συνδυασμό άσχετων μεταξύ τους λέξεων
- Μοναδικοί: Μη χρησιμοποιείτε ξανά φράσεις πρόσβασης σε πολλαπλούς λογαριασμούς