



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN
SIGNALS
DIRECTORATE
ACSC Australian
Cyber Security
Centre



ΠΩΣ ΝΑ ΧΡΗΣΙΜΟΠΟΙΕΙΤΕ ΤΟ ΔΙΑΔΙΚΤΥΟ ΜΕ ΑΣΦΑΛΕΙΑ ΟΔΗΓΟΣ ΓΙΑ ΗΛΙΚΙΩΜΕΝΟΥΣ

cyber.gov.au

Εισαγωγή

Η διαδικτυακή σύνδεση σας επιτρέπει να διατηρείτε επαφή με τους φίλους και την οικογένειά σας, να μαθαίνετε για διάφορα θέματα, ακόμη και να παίζετε παιχνίδια.

Όπως ακριβώς δένετε τη ζώνη ασφαλείας σας πριν οδηγήσετε, έτσι θα πρέπει να λαμβάνετε μέτρα και πριν χρησιμοποιήσετε το διαδίκτυο για να είστε πιο ασφαλείς.

Το Αυστραλιανό Κέντρο Ασφάλειας Κυβερνοχώρου (ACSC) θέλει να διασφαλίσει ότι είναι όλοι ασφαλείς όταν συνδέονται στο διαδίκτυο. Αυτό το έγγραφο καλύπτει ορισμένες βασικές πρακτικές ασφάλειας κυβερνοχώρου, τις οποίες μπορείτε να χρησιμοποιείτε για να προστατεύσετε όταν κάνετε πρόσβαση στο διαδίκτυο.



Το Αυστραλιανό Κέντρο Ασφάλειας Κυβερνοχώρου (ACSC), ως μέρος της Αυστραλιανής Διεύθυνσης Σημάτων (ASD), παρέχει συμβουλές, βοήθεια και πρακτικές απαντήσεις για την πρόληψη, τον εντοπισμό και την αποτελεσματική αντιμετώπιση απειλών του κυβερνοχώρου στην Αυστραλία. Το ACSC είναι στη διάθεσή σας για να βοηθήσει να κάνουμε την Αυστραλία το πιο ασφαλές μέρος για σύνδεση στο διαδίκτυο.

Για περισσότερες πληροφορίες σχετικά με την ασφάλεια στον κυβερνοχώρο, οδηγίες και συμβουλές επισκεφτείτε το [cyber.gov.au](https://www.cyber.gov.au)

Ασφάλεια στον κυβερνοχώρο για ηλικιωμένους

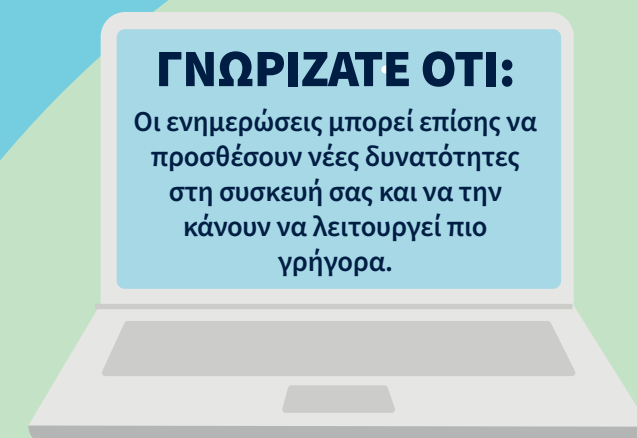


Συμβουλή 1: Ενημερώστε τη συσκευή σας

Η ενημέρωση του λογισμικού σας είναι σαν να κάνετε σέρβις στο αυτοκίνητό σας. Βελτιώνει την απόδοση της συσκευής σας και την καθιστά πιο ασφαλή.

Οι εγκληματίες του κυβερνοχώρου βρίσκουν πάντα νέους τρόπους για να παραβιάσουν (χακάρουν) συσκευές. Η ρύθμιση της συσκευής σας για αυτόματη εγκατάσταση ενημερώσεων μπορεί να διορθώσει τυχόν αδυναμίες του λογισμικού σας και να κρατήσει τους χάκερ μακριά.

Για να βρείτε περισσότερες πληροφορίες, αναζητήστε πληκτρολογώντας 'Updates' στο [cyber.gov.au](https://www.cyber.gov.au).





Συμβουλή 2: Ενεργοποιήστε τον έλεγχο ταυτότητας πολλαπλών παραγόντων

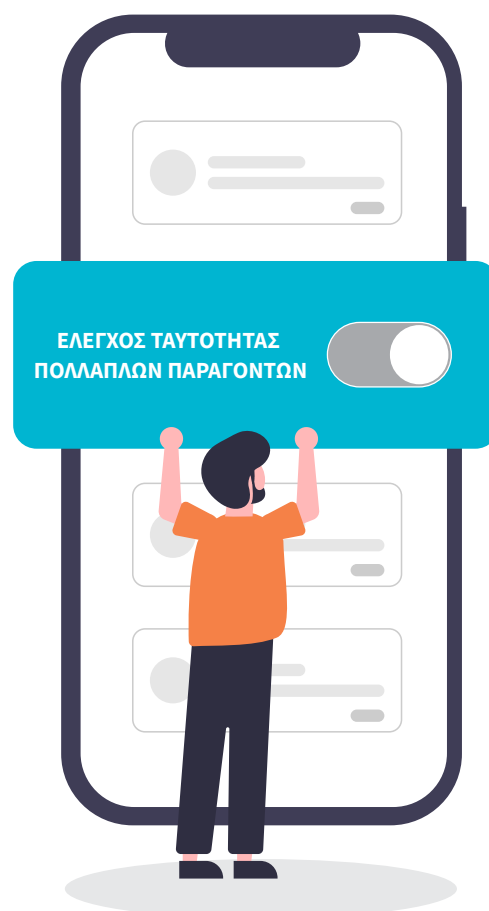
Ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) στο λογαριασμό σας λειτουργεί όπως μια καγκελόπορτα ασφαλείας στο σπίτι σας.

Σας προστατεύει από εγκληματίες που προσπαθούν να σας διαρρήξουν.

Με ενεργοποιημένο τον έλεγχο ταυτότητας πολλαπλών παραγόντων, χρειάζεται να δώσετε πολλαπλές πληροφορίες για να αποκτήσετε πρόσβαση στο λογαριασμό σας. Για παράδειγμα, ίσως χρειαστεί να εισαγάγετε τον κωδικό πρόσβασής σας και έναν κωδικό που θα λάβετε μέσω μηνύματος κειμένου για να συνδεθείτε με το προφίλ σας στα μέσα κοινωνικής δικτύωσης.

Τα πολλαπλά στρώματα δυσκολεύουν τους εγκληματίες του κυβερνοχώρου να παραβιάσουν τη συσκευή σας. Μπορεί να καταφέρουν να αποκρυπτογραφήσουν κάτι, όπως τον κωδικό πρόσβασής σας, αλλά θα χρειαστεί να βρουν και άλλα στοιχεία του παζλ για πρόσβαση στο λογαριασμό σας.

Για να βρείτε περισσότερες πληροφορίες, αναζητήστε πληκτρολογώντας 'Multi-factor authentication' ή 'MFA' στο [cyber.gov.au](https://www.cyber.gov.au)



ΝΑ ΘΥΜΑΣΤΕ:

Αν χρειάζεστε βοήθεια για να ενεργοποιήσετε τον έλεγχο ταυτότητας πολλαπλών παραγόντων, ζητήστε βοήθεια από ένα φίλο ή συγγενή σας.



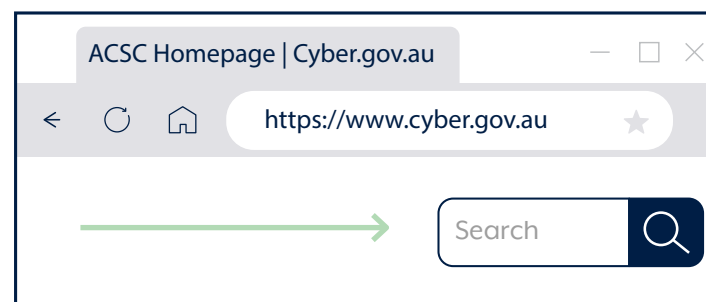
Συμβουλή 3: Δημιουργήστε αντίγραφα ασφαλείας της συσκευής σας

Δημιουργία αντιγράφου ασφαλείας ('backup') είναι όταν κάνετε αντίγραφα των σημαντικών αρχείων σας και τα τοποθετείτε σε κάποιο ασφαλές μέρος. Είναι σαν να φωτοτυπείτε πολύτιμες φωτογραφίες για να τις φυλάξετε με ασφάλεια σε περίπτωση που χάσετε τα πρωτότυπα.

Όταν δημιουργείτε αντίγραφα ασφαλείας του υπολογιστή, τηλεφώνου ή tablet σας, τα αντίγραφα των αρχείων σας αποθηκεύονται στο διαδίκτυο ή σε μια ξεχωριστή συσκευή. Η ύπαρξη αντιγράφων ασφαλείας των σημαντικών αρχείων και των αγαπημένων φωτογραφιών σας θα σας προσφέρει ψυχική ηρεμία.

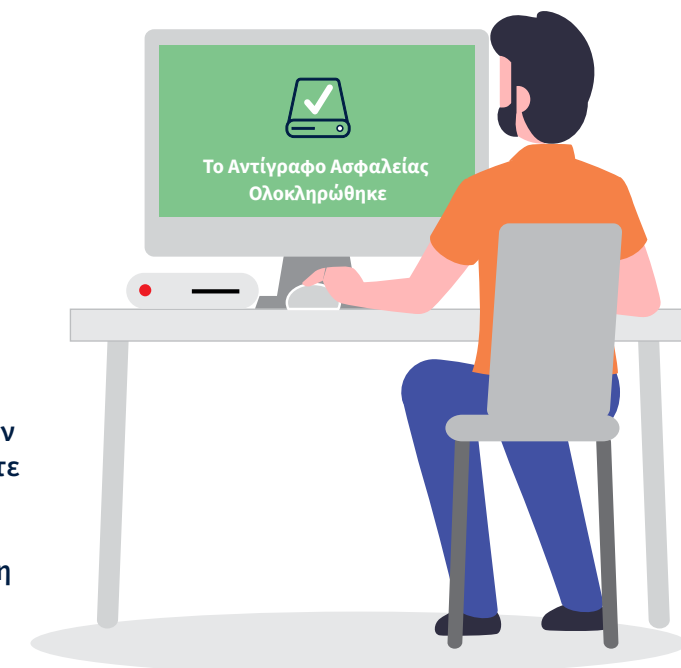
Εάν κάτι δεν πάει καλά με τη συσκευή σας ή την παραβιάσουν εγκληματίες του κυβερνοχώρου, μπορείτε εύκολα να επαναφέρετε τα αρχεία σας από τα αντίγραφα ασφαλείας σας.

Για να βρείτε περισσότερες πληροφορίες, αναζητήστε πληκτρολογώντας 'Backups' στο [cyber.gov.au](https://www.cyber.gov.au)



ΓΝΩΡΙΖΑΤΕ ΟΤΙ:

Η τακτική δημιουργία αντιγράφων ασφαλείας της συσκευής σας σημαίνει ότι θα έχετε πάντα πρόσβαση στα πιο ενημερωμένα αρχεία σας.



Συμβουλή 4: Χρησιμοποιήστε μια φράση πρόσβασης

Εάν ένας κωδικός πρόσβασης κλειδώσει το λογαριασμό σας, μια φράση πρόσβασης παρέχει το δικό της σύστημα ασφαλείας! Οι φράσεις είναι ισχυρότερες και ασφαλέστερες εκδοχές των κωδικών πρόσβασης.

Όταν δεν μπορείτε να ενεργοποιήσετε το MFA, χρησιμοποιήστε μια φράση πρόσβασης για να ασφαλίσετε το λογαριασμό σας. Οι φράσεις πρόσβασης χρησιμοποιούν τέσσερις ή περισσότερες τυχαίες λέξεις ως κωδικό πρόσβασης. Αυτό δυσκολεύει τους εγκληματίες του κυβερνοχώρου να τις μαντέψουν, αλλά διευκολύνει εσάς να τις θυμάστε.

Όταν δημιουργείτε μια φράση πρόσβασης, φτιάχντέ την:

- **Μακροσκελή.** Όσο μεγαλύτερη, τόσο το καλύτερο. Βάλτε στόχο να αποτελείται τουλάχιστον από 14 χαρακτήρες. Θα ήταν καλά να διαλέξετε τέσσερις ή περισσότερες τυχαίες λέξεις που θα τις θυμάστε. Για παράδειγμα, «μωβ πάπια πατάτα βάρκα».
- **Απρόβλεπτη.** Όσο λιγότερο προβλέψιμη είναι η φράση πρόσβασής σας, τόσο το καλύτερο. Οι προτάσεις μπορούν να είναι καλές φράσεις πρόσβασης, αλλά είναι πιο εύκολο να τις μαντέψει κάποιος. Ένας συνδυασμός τεσσάρων ή περισσότερων τυχαίων λέξεων θα δημιουργήσει μια ισχυρότερη φράση πρόσβασης.
- **Μοναδική.** Μην ανακυκλώνετε τις φράσεις πρόσβασής σας. Χρησιμοποιήστε διαφορετικές φράσεις πρόσβασης για διαφορετικούς λογαριασμούς. Αν δυσκολεύεστε να θυμάστε όλες τις φράσεις πρόσβασής σας, σκεφτείτε να χρησιμοποιήσετε έναν διαχειριστή κωδικών πρόσβασης. Με έναν διαχειριστή κωδικών πρόσβασης, χρειάζεται να θυμάστε μόνο έναν κωδικό πρόσβασης, καθώς ο διαχειριστής κωδικών πρόσβασης φροντίζει για τα υπόλοιπα. Αναζητήστε πληκτρολογώντας 'password manager' στο cyber.gov.au για περισσότερες συμβουλές.



Μάθετε περισσότερα για τη δημιουργία ασφαλών φράσεων πρόσβασης, αναζητώντας 'Passphrases' στο cyber.gov.au

Συμβουλή 5: Αναγνωρίζετε και καταγγέλλετε απάτες

Όσο πιο γρήγορα αναφέρετε μια απάτη, τόσο πιο γρήγορα μπορούμε να δράσουμε.

Εάν πιστεύετε ότι προσπαθεί κάποιος να χρησιμοποιήσει το διαδίκτυο για να σας εξαπατήσει, είναι καλύτερα να δράσετε προνοητικά και να είστε προσεκτικοί αντί να κινδυνέψετε να πέσετε θύμα εκμετάλλευσης.

Αν ακούγεται απίστευτο, μάλλον δεν είναι αληθινό. Αν και ένα μήνυμα μπορεί να λέει ότι κερδίσατε ένα βραβείο ή ότι ο υπολογιστής σας περιέχει ιό, αυτό το μήνυμα δεν απευθύνεται μόνο σ' εσάς.

Μπορεί να προέρχεται από έναν απατεώνα που θέλει να σας εκμεταλλευτεί.

Να θυμάστε, οι απατεώνες συχνά προσποιούνται ότι είναι πρόσωπο ή οργανισμός που εμπιστεύεστε. Να είστε καχύποπτοι αν λάβετε ένα μήνυμα που φαίνεται να προέρχεται από κάποιον που εμπιστεύεστε αλλά χρησιμοποιεί νέο αριθμό τηλεφώνου, ηλεκτρονική διεύθυνση ταχυδρομείου (email) ή προφίλ στα μέσα κοινωνικής δικτύωσης. Πριν απαντήσετε, βεβαιωθείτε ότι το άτομο ή ο οργανισμός που σας στέλνει μήνυμα είναι πραγματικά αυτό που λέει ότι είναι, επικοινωνώντας μαζί του με τρόπο που εμπιστεύεστε. Για παράδειγμα, αν λάβετε ένα γραπτό μήνυμα που μοιάζει να είναι από ένα από τα παιδιά σας, αλλά προέρχεται από έναν νέο αριθμό, μην απαντήσετε. Στείλτε του πρώτα ένα μήνυμα στα μέσα κοινωνικής δικτύωσης για να ελέγξετε ότι όντως έχει αλλάξει τον αριθμό τηλεφώνου του.



ΓΝΩΡΙΖΑΤΕ ΟΤΙ:

Οι εγκληματίες του κυβερνοχώρου είναι πανούργοι και μπορεί να χρησιμοποιούν ένα γνώριμο όνομα και διεύθυνση ηλεκτρονικού ταχυδρομείου.

Να είστε προσεκτικοί εάν:

- σας ζητήσουν να πληρώσετε επείγοντως ένα λογαριασμό
- σας ζητήσουν να αλλάξετε τα στοιχεία σας ή τον κωδικό σας
- σας ζητήσουν να κάνετε κλικ σε ένα σύνδεσμο ή να ανοίξετε ένα συνημμένο.



Συμπέρασμα

Τώρα που είστε εξοπλισμένοι με τις γνώσεις να χρησιμοποιείτε το διαδίκτυο με μεγαλύτερη ασφάλεια, μπορείτε να περιηγείστε με σιγουριά και να συνεχίσετε να απολαμβάνετε την απασχόλησή σας στο διαδίκτυο.

Απλά να θυμάστε ότι οι εγκληματίες του κυβερνοχώρου συνεχώς μηχανεύονται νέους τρόπους για να στοχεύουν τον κόσμο.

Δεν βλέπτε να φρεσκάρετε κατά καιρούς την τεχνογνωσία σας για την ασφάλειά σας στον κυβερνοχώρο και να μαθαίνετε νέους τρόπους για να παραμένετε ασφαλείς.

Πρόσθετες συμβουλές

Θέλετε να μάθετε περισσότερους τρόπους για να παραμείνετε ασφαλείς στο διαδίκτυο; Ελέγξτε τις παρακάτω συμβουλές.

Σκεφτείτε τι αναρτήσεις δημοσιεύετε.

Σκεφτείτε προσεκτικά τις πληροφορίες που μοιράζεστε στο διαδίκτυο και ποιος θα τις δει. Να δέχεστε αιτήματα φιλίας μόνο από άτομα που γνωρίζετε στην πραγματική ζωή.

Λαμβάνετε προειδοποιήσεις για νέες απειλές.

Εγγραφείτε για τις δωρεάν προειδοποιήσεις της υπηρεσίας μας. Έτσι, θα ενημερώνεστε κάθε φορά που εντοπίζουμε μια νέα απειλή στον κυβερνοχώρο.

Θα λαμβάνετε επίσης συμβουλές σχετικά με το τι να κάνετε σε περίπτωση επίθεσης.

Μιλήστε για την ασφάλεια στον κυβερνοχώρο με την οικογένεια και τους φίλους σας.

Τώρα που έχετε αποκτήσει δεξιότητες για την ασφάλεια στον κυβερνοχώρο, μοιραστείτε ό,τι μάθατε με την οικογένεια και τους φίλους σας. Οι γνώσεις σας θα μπορούσαν να τους βοηθήσουν να μη βρεθούν σε δύσκολη θέση στο μέλλον!

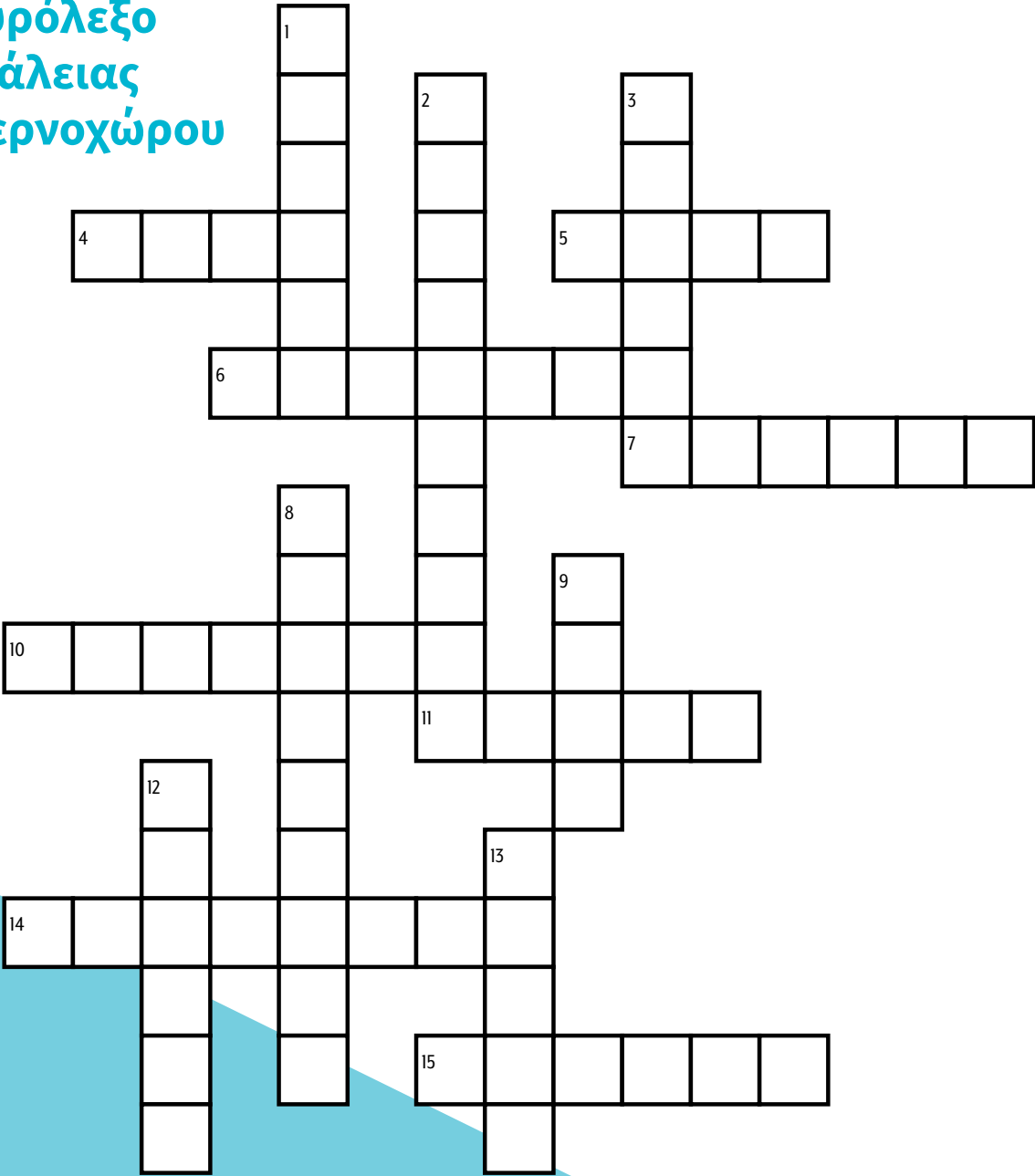
Αποφεύγετε τα δημόσια Wi-Fi όταν κάνετε τραπεζικές συναλλαγές ή αγορές στο διαδίκτυο.

Τα δημόσια Wi-Fi είναι καλά για να βλέπετε βίντεο ή να διαβάσετε ιστοσελίδες, αλλά πραγματοποιείτε οποιαδήποτε διαδικτυακή δραστηριότητα που περιλαμβάνει χρήματα χρησιμοποιώντας την οικιακή σας διαδικτυακή σύνδεση. Το δημόσιο Wi-Fi μπορεί να είναι επικίνδυνο.

Καταγγέλλετε εγκλήματα και περιστατικά στον κυβερνοχώρο για να διατηρείτε ασφαλή την Αυστραλία.

Εάν νομίζετε ότι έχετε πέσει θύμα ηλεκτρονικού εγκλήματος, ενεργήστε γρήγορα. Περισσότερες συμβουλές υπάρχουν στο cyber.gov.au

Σταυρόλεξο ασφάλειας κυβερνοχώρου



ΚΑΘΕΤΑ

1. Connected to the internet
2. A strong password
3. A person who uses computers to steal data
8. Software that destroys viruses
9. A deceptive scheme or trick
12. A copy of your computer's files
13. Relating to, or involving computers

ΟΡΙΖΟΝΤΙΑ

4. Wireless networking technology
5. Australia's lead agency for cyber security
6. A document on the World Wide Web
7. To give information about something
10. New, improved or more secure versions of software
11. Electronic mail
14. The state of being free from danger or threat
15. A tool that can connect to the internet

Συμπληρωματικοί οδηγοί

Για περαιτέρω πληροφορίες, ανατρέξτε στη σειρά εκδόσεων της υπηρεσίας μας *Προσωπική Ασφάλεια στον Κυβερνοχώρο*: τρεις οδηγοί που έχουν σχεδιαστεί για να βοηθήσουν το κοινό της Αυστραλίας να κατανοήσει τα βασικά στοιχεία για την ασφάλεια στον κυβερνοχώρο και πώς μπορείτε να λάβετε μέτρα για να προστατευτείτε από κοινές απειλές στον κυβερνοχώρο.



Μπορείτε να αποκτήσετε πρόσβαση και στους τρεις οδηγούς στο **cyber.gov.au**

Απαντήσεις σταυρόλεξου

1. online, 2. passphrase, 3. hacker, 4. Wi-Fi, 5. ACSC, 6. webpage, 7. report, 8. antivirus, 9. scam, 10. updates, 11. email, 12. backup, 13. cyber, 14. security, 15. device

Σημειώσεις

Blank lined area for notes.

Αποποίηση ευθυνών

Το περιεχόμενο του παρόντος οδηγού είναι γενικού χαρακτήρα και δεν θα πρέπει να θεωρηθεί ως νομική συμβουλή ή ως βάση για βοήθεια σε οποιαδήποτε ιδιαίτερη περίπτωση ή κατάσταση έκτακτης ανάγκης. Σε κάθε σημαντικό θέμα, θα πρέπει να ζητάτε την κατάλληλη ανεξάρτητη επαγγελματική συμβουλή σχετικά με τις δικές σας περιστάσεις.

Η Κοινοπολιτεία δεν αναλαμβάνει καμία ευθύνη ή υποχρέωση για οποιαδήποτε ζημιά, απώλεια ή δαπάνη που προκύπτει από την επίκληση των πληροφοριών που περιέχονται σε αυτόν τον οδηγό.

Πνευματικά δικαιώματα

© Κοινοπολιτεία της Αυστραλίας 2023

Με εξαίρεση το Εθνόσημο και εκτός εάν αναφέρεται διαφορετικά, όλο το υλικό που παρουσιάζεται στην παρούσα δημοσίευση υπόκειται στην άδεια Creative Commons Attribution 4.0 International (www.creativecommons.org/licenses).

Προς αποφυγή αμφιβολιών, αυτό σημαίνει ότι αυτή η άδεια ισχύει μόνο για το υλικό το οποίο περιέχεται στο παρόν έγγραφο.



Οι λεπτομέρειες των σχετικών προϋποθέσεων της άδειας είναι διαθέσιμες στον ιστότοπο του Creative Commons, όπως και ο πλήρης νομικός κώδικας για την άδεια CC BY 4.0 (www.creativecommons.org/licenses).

Χρήση του Εθνόσημου

Οι όροι υπό τους οποίους μπορεί να χρησιμοποιηθεί το Εθνόσημο αναφέρονται λεπτομερώς στον ιστότοπο του Υπουργείου του Πρωθυπουργού και του Υπουργικού Συμβουλίου (www.pmc.gov.au/government/commonwealth-coat-arms).

Για περισσότερες πληροφορίες ή για να αναφέρετε ένα περιστατικό που αφορά την ασφάλεια 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