



Australian Government



Ενεργήστε Τώρα.
Παραμείνετε Ασφαλείς.

Πώς μπορείτε να παραμείνετε ασφαλείς στο διαδίκτυο

Συνοπτική έκδοση



Πώς να χρησιμοποιήσετε αυτόν τον οδηγό



Είμαστε η αυστραλιανή κυβέρνηση.

Γράψαμε αυτόν τον οδηγό.



Γράψαμε μερικές λέξεις με **έντονα γράμματα**.

Εξηγούμε τι σημαίνουν αυτές οι λέξεις.

Υπάρχει επίσης μια λίστα με αυτές τις λέξεις στη σελίδα 28.



Μπορείτε να ζητήσετε υποστήριξη από κάποιον που εμπιστεύεστε:

- διαβάστε αυτόν τον οδηγό
- βρείτε περισσότερες πληροφορίες.



Αυτή είναι μια συνοπτική περίληψη ενός άλλου οδηγού

Περιλαμβάνει μόνο τις πιο σημαντικές ιδέες.



Μπορείτε να βρείτε τον άλλο οδηγό στην ιστοσελίδα μας.

www.actnowstaysecure.gov.au

Τι περιέχει αυτός ο Οδηγός;

Σχετικά με αυτόν τον οδηγό	4
Διατηρήστε τους λογαριασμούς σας ασφαλείς	6
Ελέγξτε τις ρυθμίσεις σας για να προστατεύσετε τις πληροφορίες σας	10
Προστατέψτε τις συσκευές σας	16
Απάτες	20
Μιλήστε	25
Λίστα λέξεων	28
Επικοινωνήστε μαζί μας	30

Σχετικά με αυτόν τον οδηγό



Όλοι πρέπει να σκεφτούμε πώς μπορούμε να παραμείνουμε ασφαλείς στο διαδίκτυο.

Αυτό το ονομάζουμε ασφάλεια **στον κυβερνοχώρο**.



Κυβερνοχώρος σημαίνει ότι κάτι έχει να κάνει με το διαδίκτυο.



Αυτός ο οδηγός εξηγεί ορισμένα πράγματα που μπορείτε να κάνετε για να προστατευτείτε στο διαδίκτυο.

Για παράδειγμα, από **το έγκλημα στον κυβερνοχώρο**.

Το έγκλημα στον κυβερνοχώρο είναι όταν οι εγκληματίες χρησιμοποιούν το διαδίκτυο για έγκλημα.



Για παράδειγμα, μπορεί να χρησιμοποιούν το διαδίκτυο για να:

- κλέψουν τα προσωπικά σας στοιχεία
- αναλάβουν τους διαδικτυακούς λογαριασμούς ή τα προφίλ σας.

Το έγκλημα στον κυβερνοχώρο μπορεί να συμβεί σε οποιαδήποτε συσκευή.



Αυτό περιλαμβάνει:

- υπολογιστή
- έξυπνο τηλέφωνο
- έξυπνο ρολόι.



Υπάρχουν πράγματα που μπορείτε να κάνετε για να παραμείνετε ασφαλείς από το έγκλημα στον κυβερνοχώρο.



Εξηγούμε τι μπορείτε να κάνετε στις επόμενες σελίδες.

Διατηρήστε τους λογαριασμούς σας ασφαλείς



Θα πρέπει να σκεφτείτε πώς μπορείτε να διατηρήσετε ασφαλείς τους διαδικτυακούς σας λογαριασμούς.

Χρησιμοποιήστε ισχυρούς και διαφορετικούς κωδικούς πρόσβασης



Η **φράση πρόσβασης** είναι ένας ισχυρότερος τύπος κωδικού πρόσβασης.

Είναι πολύ δύσκολο για τους άλλους να μαντέψουν.



Η χρήση ισχυρών και διαφορετικών φράσεων πρόσβασης είναι ένας από τους καλύτερους τρόπους για την προστασία των λογαριασμών σας.



Θα πρέπει να χρησιμοποιείτε διαφορετική φράση πρόσβασης για κάθε έναν από τους διαδικτυακούς λογαριασμούς σας.



Οι ισχυρές φράσεις πρόσβασης περιλαμβάνουν:

- 4 ή περισσότερες τυχαίες λέξεις
- 15 ή περισσότερα γράμματα και αριθμούς.



Μπορείτε να συμπεριλάβετε μερικά κεφαλαία γράμματα.



Μπορείτε επίσης να χρησιμοποιήσετε σύμβολα όπως:

- μια παύλα
- σύμβολο δολαρίου
- ένα σύμβολο email @.



Δεν πρέπει να χρησιμοποιείτε προσωπικά στοιχεία στις φράσεις πρόσβασής σας.



Για παράδειγμα:

- τα γενέθλιά σας
- τα ονόματα των μελών της οικογένειάς σας ή των κατοικίδιών σας.

Προσθέστε επιπλέον βήματα για να συνδεθείτε στους λογαριασμούς σας



Μπορείτε να προστατεύσετε τους διαδικτυακούς σας λογαριασμούς με **έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA)**.

MFA είναι όταν χρησιμοποιείτε 2 ή περισσότερους διαφορετικούς τρόπους για να συνδέεστε στον λογαριασμό σας κάθε φορά.



Για παράδειγμα, ίσως χρειαστεί να εισαγάγετε πρώτα τη φράση πρόσβασης.

Στη συνέχεια, εισάγετε έναν κωδικό που λαμβάνετε στο τηλέφωνό σας.

Μπορεί να έχετε την επιλογή:



- να αποκτήσετε μια εφαρμογή στο τηλέφωνό σας για να σας δώσει τον κωδικό



- να λάβετε τον κωδικό σε ένα email



- να λάβετε τον κωδικό σε ένα μήνυμα κειμένου (SMS).



Το MFA καθιστά πιο δύσκολο για άλλα άτομα να μπουν στους διαδικτυακούς σας λογαριασμούς.

Ακόμα κι αν μάθουν τη φράση πρόσβασής σας.

Ελέγξτε τις ρυθμίσεις σας για να προστατεύσετε τις πληροφορίες σας



Μπορείτε να ελέγξετε ότι οι ρυθμίσεις σας προστατεύουν τις πληροφορίες σας στο διαδίκτυο.



Αυτό περιλαμβάνει ρυθμίσεις για:

- διαδικτυακούς λογαριασμούς
- συσκευές
- εφαρμογές.



Μπορείτε:

- να αλλάξετε τις ρυθμίσεις σας
- να επιλέξετε ποιες εφαρμογές μπορούν να χρησιμοποιούν τις πληροφορίες σας.

Μπορείτε να βρείτε ρυθμίσεις στη συσκευή σας με τους εξής τρόπους:



- αναζητώντας το εικονίδιο «γραναζιού»
ή
- πληκτρολογώντας «Ρυθμίσεις» στη γραμμή αναζήτησης της συσκευής σας.



Μπορείτε να βρείτε ρυθμίσεις σε μια εφαρμογή ή έναν διαδικτυακό λογαριασμό ανοίγοντας το μενού.

Το μενού συχνά μοιάζει με 3 ευθείες γραμμές.



Ορισμένες από αυτές τις ρυθμίσεις μπορούν να κοινοποιούν πληροφορίες σχετικά με τα εξής:

- ποιος είστε
- πού βρίσκεστε
- πού ζείτε.



Η κοινή χρήση αυτών των πληροφοριών στο διαδίκτυο μπορεί να σας θέσει σε κίνδυνο εγκλημάτων στον κυβερνοχώρο.



Οι εγκληματίες του κυβερνοχώρου μπορούν να χρησιμοποιήσουν τις πληροφορίες σας για να προσποιηθούν ότι είστε εσείς.

Για παράδειγμα, μπορεί να χρησιμοποιούν πληροφορίες όπως:



- πού ζείτε



- τα ονόματα των μελών της οικογένειάς σας



- τα ονόματα των κατοικίδιών σας.



Μπορείτε να ρυθμίσετε τους λογαριασμούς σας έτσι ώστε μόνο άτομα που γνωρίζετε να μπορούν να βλέπουν τα προφίλ σας στα μέσα κοινωνικής δικτύωσης.

Για παράδειγμα, το προφίλ σας στο Facebook.



Αυτές οι ρυθμίσεις ονομάζονται συνήθως ρυθμίσεις απορρήτου.



Μπορείτε επίσης να ελέγξετε **τις ρυθμίσεις τοποθεσίας** σας.

Οι ρυθμίσεις τοποθεσίας δείχνουν πού βρίσκεται η συσκευή σας.



Μπορείτε να ενεργοποιήσετε ή να απενεργοποιήσετε τις ρυθμίσεις τοποθεσίας.

Μπορείτε επίσης να επιλέξετε ποιες εφαρμογές μπορούν να χρησιμοποιούν τις ρυθμίσεις τοποθεσίας σας.



Μπορείτε να το κάνετε αυτό για:

- διαδικτυακούς λογαριασμούς
- συσκευές
- εφαρμογές.

Ορισμένες εφαρμογές μπορεί επίσης να σας ρωτήσουν εάν μπορούν:



- να χρησιμοποιήσουν τη φωτογραφική σας μηχανή



- να δουν τις φωτογραφίες σας.



Θα πρέπει να επιτρέπετε μόνο σε εφαρμογές με τις οποίες είστε εξοικειωμένος να χρησιμοποιούν την φωτογραφική μηχανή και τις φωτογραφίες σας.

Προστατέψτε τις συσκευές σας



Θα πρέπει να σκεφτείτε πώς μπορείτε να προστατεύσετε τις συσκευές σας για να παραμείνετε ασφαλής στο διαδίκτυο.

Για παράδειγμα, το τηλέφωνο ή το «έξυπνο» ρολόι σας.



Αυτό είναι σημαντικό για συσκευές που συνδέονται στο διαδίκτυο.

Ενημερώστε τις συσκευές σας



Μπορείτε να ενημερώσετε τις συσκευές σας για να τις διατηρήσετε ασφαλείς στο διαδίκτυο.

Για παράδειγμα, το τηλέφωνο και ο φορητός υπολογιστής σας.



Η συσκευή σας μπορεί να το ονομάσει αυτό ενημέρωση λογισμικού.



Οι ενημερώσεις βοηθούν μια συσκευή να προστατεύεται από το έγκλημα στον κυβερνοχώρο.



Μπορείτε να ρυθμίσετε μια συσκευή ώστε να ενημερώνεται μόνη της.



Μπορείτε να μάθετε περισσότερα σχετικά με τον τρόπο ενημέρωσης των συσκευών σας στον ιστότοπό μας.

www.actnowstaysecure.gov.au/cyber-safe-actions

Δημόσια δίκτυα Wi-Fi



Θα πρέπει να είστε προσεκτικός όταν χρησιμοποιείτε **δημόσιο Wi-Fi**.



Το δημόσιο Wi-Fi είναι δωρεάν ασύρματο Διαδίκτυο που μπορείτε να χρησιμοποιήσετε σε δημόσιους χώρους.



Για παράδειγμα, σε:

- καφετέρια
- αεροδρόμιο
- ξενοδοχείο.



Θα πρέπει να είστε προσεκτικός σχετικά με τις πληροφορίες που εισάγετε σε έναν ιστότοπο χρησιμοποιώντας δημόσιο Wi-Fi.



Για παράδειγμα:

- τραπεζικά στοιχεία
- λογαριασμούς email
- προφίλ στα μέσα κοινωνικής δικτύωσης.



Ορισμένοι εγκληματίες του κυβερνοχώρου μπορούν να χρησιμοποιήσουν δημόσιο Wi-Fi για:

- να δουν τι κάνετε στο διαδίκτυο
- να κλέψουν τις πληροφορίες σας.

Αυτό συμβαίνει επειδή:



- οποιοσδήποτε μπορεί να το χρησιμοποιήσει



- είναι πιο δύσκολο να προστατεύσετε τις συσκευές σας.



Μπορείτε να μάθετε πώς να παραμένετε ασφαλής χρησιμοποιώντας δημόσιο Wi-Fi στον ιστότοπό μας.

www.actnowstaysecure.gov.au/cyber-safe-actions

Απάτες



Το ονομάζουμε **απάτη** όταν κάποιος προσπαθεί:

- να σας ξεγελάσει
- να πάρει τα χρήματά σας.



Απατεώνας είναι κάποιος που κάνει απάτες.

Οι απατεώνες μπορεί να προσπαθήσουν να σας εξαπατήσουν:



- με ένα μήνυμα κειμένου ή ένα τηλεφώνημα
- με ένα email
- από τα μέσα κοινωνικής δικτύωσης
- μέσω ενός ιστότοπου.



Μπορεί να φαίνονται φιλικοί.

Αλλά μπορεί να σας ξεγελάσουν για να τους δώσετε τις πληροφορίες σας.

Μπορούν να τις χρησιμοποιήσουν για:



- να μπουν στους διαδικτυακούς σας λογαριασμούς



- να προσποιηθούν ότι είστε εσείς



- να κλέψουν τα χρήματά σας.

Οι απατεώνες μπορεί επίσης:



- να δημιουργήσουν ψεύτικους λογαριασμούς για να σας ξεγελάσουν



- να μοιραστούν συνδέσμους και διαφημίσεις για να κάνετε κλικ.

Πώς να εντοπίσετε μια απάτη

Μπορεί να είναι απάτη εάν:



- σας ζητά να κάνετε κάτι γρήγορα



- σας προσφέρει πολλά χρήματα



- σας ζητάει χρήματα



- σας ζητά να κάνετε κλικ σε έναν σύνδεσμο.



Οι απατεώνες μπορεί επίσης να προσποιούνται ότι είναι ένας οργανισμός που γνωρίζετε και εμπιστεύεστε.

Για παράδειγμα, η τράπεζά σας.



Οι απατεώνες το κάνουν αυτό για να μοιραστείτε τα προσωπικά σας στοιχεία μαζί τους.



Θα πρέπει να σταματήσετε να μιλάτε με το άτομο εάν πιστεύετε ότι είναι απατεώνας.



Θα πρέπει να ελέγξετε ότι το άτομο είναι αυτό που λέει ότι είναι.

Μπορείτε να επικοινωνήσετε με το άτομο ή τον οργανισμό χρησιμοποιώντας στοιχεία που εμπιστεύεστε και έχετε βρει μόνοι σας.



Ενεργήστε γρήγορα για να προστατεύσετε τον εαυτό σας εάν κάτι δεν πάει καλά.

Αναφορά απάτης



Το Scamwatch βοηθά τους Αυστραλούς:

- να κατανοήσουν τις απάτες
- να αναφέρουν απάτες.



Το Scamwatch βοηθά επίσης τους Αυστραλούς που έχουν βιώσει απάτες.



Μπορείτε να αναφέρετε μια απάτη στον ιστότοπο του Scamwatch.

www.scamwatch.gov.au/report-a-scam

Μιλήστε



Θα πρέπει να μιλήσετε για το πώς οι άλλοι μπορούν να προστατευτούν στο διαδίκτυο.

Αυτό περιλαμβάνει:



- την αναφορά ενός εγκλήματος στον κυβερνοχώρο



- τη μοιρασιά όσων που γνωρίζετε με την οικογένεια και τους φίλους σας.



Θα εξηγήσουμε πώς μπορείτε να μιλήσετε στις επόμενες σελίδες.

Αναφορά εγκλήματος στον κυβερνοχώρο

Η αναφορά του εγκλήματος στον κυβερνοχώρο βοηθά την κυβέρνηση:



- να μάθει πώς οι εγκληματίες του κυβερνοχώρου προσπαθούν να επιτεθούν σε ανθρώπους



- να προστατεύει περισσότερους ανθρώπους.



Μπορείτε να αναφέρετε το έγκλημα στον κυβερνοχώρο στον ιστότοπο ReportCyber.

www.cyber.gov.au/report

Μιλήστε με την οικογένεια και τους φίλους σας για να παραμείνετε ασφαλείς στο διαδίκτυο



Θα πρέπει να μοιραστείτε τις συμβουλές σας για να παραμείνετε ασφαλείς στο διαδίκτυο με την οικογένεια και τους φίλους σας.

Μπορείτε να μάθετε και από αυτούς.



Μπορείτε να προστατεύσετε τον εαυτό σας και τους ανθρώπους γύρω σας κοινοποιώντας όσα γνωρίζετε για να παραμείνετε ασφαλείς στο διαδίκτυο.



Αυτό είναι επίσης σημαντικό εάν μοιράζεστε συσκευές με άλλους.

Λίστα ορολογίας

Αυτή η λίστα εξηγεί τι σημαίνουν οι **έντονες** λέξεις σε αυτόν τον οδηγό.



Κυβερνοχώρος

Κυβερνοχώρος σημαίνει ότι κάτι έχει να κάνει με το διαδίκτυο.

Έγκλημα στον κυβερνοχώρο

Το έγκλημα στον κυβερνοχώρο είναι όταν οι εγκληματίες χρησιμοποιούν το διαδίκτυο για έγκλημα.



Για παράδειγμα, μπορεί να χρησιμοποιούν το διαδίκτυο για:

- να κλέψουν τα προσωπικά σας στοιχεία
- κλέψουν τους διαδικτυακούς σας λογαριασμούς.



Ρυθμίσεις τοποθεσίας

Οι ρυθμίσεις τοποθεσίας δείχνουν πού βρίσκεται η συσκευή σας.



Έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA)

MFA είναι όταν χρησιμοποιείτε 2 ή περισσότερους διαφορετικούς τρόπους για να συνδέεστε στον λογαριασμό σας κάθε φορά.



Φράση πρόσβασης

Η φράση πρόσβασης είναι ένας ισχυρότερος τύπος κωδικού πρόσβασης.

Είναι πολύ δύσκολο για τους άλλους να μαντέψουν.



Δημόσιο Wi-Fi

Το δημόσιο Wi-Fi είναι δωρεάν ασύρματο διαδίκτυο που μπορείτε να χρησιμοποιήσετε σε δημόσιους χώρους.



Απάτες

Το ονομάζουμε απάτη όταν κάποιος προσπαθεί:

- να σας ξεγελάσει
- να πάρει τα χρήματά σας.



Απατεώνες

Απατεώνας είναι κάποιος που κάνει απάτες.

Για περισσότερες πληροφορίες



Μπορείτε να καλέσετε την Αυστραλιανή
Γραμμή Κυβερνοασφάλειας.

1300 292 371



Μπορείτε να επισκεφτείτε την ιστοσελίδα
μας.

www.actnowstaysecure.gov.au



Μπορείτε να αναφέρετε το έγκλημα στον
κυβερνοχώρο στον ιστότοπο ReportCyber.

www.cyber.gov.au/report



Η Ομάδα Πρόσβασης Πληροφοριών δημιούργησε
αυτό το έγγραφο Easy Read χρησιμοποιώντας
φωτογραφίες αρχείου και προσαρμοσμένες εικόνες.

Οι εικόνες δεν επιτρέπεται να
επαναχρησιμοποιηθούν χωρίς άδεια. Για
οποιαδήποτε απορία σχετικά με τις εικόνες,
επισκεφθείτε www.informationaccessgroup.com.
Αναφέρετε τον αριθμό εργασίας 6342.
