



Περίληψη διαδικτυακής παρουσίασης

Διαχείριση των μηνυμάτων email με ασφάλεια

Η δημιουργία διεύθυνσης email είναι η πύλη σας στον διαδικτυακό κόσμο. Σας επιτρέπει να διατηρείτε επαφή με την οικογένεια και τους φίλους σας και να έχετε πρόσβαση σε υπηρεσίες, όπως ηλεκτρονικές αγορές και τραπεζικές συναλλαγές. Είναι σημαντικό να διατηρείτε τον λογαριασμό email σας όσο το δυνατόν πιο ασφαλή, χρησιμοποιώντας έναν ισχυρό κωδικό πρόσβασης και έλεγχο ταυτότητας πολλαπλών παραγόντων.



Τρόποι πρόσβασης σε email

Υπάρχουν πολλοί τρόποι πρόσβασης στα email σας. Μπορείτε να το κάνετε αυτό μέσω:

Μιας εφαρμογής

- χρησιμοποιήστε την εφαρμογή του παρόχου email που μπορείτε να κατεβάσετε από το App Store για συσκευές Apple ή το Play Store για συσκευές Android
- συνδέστε τον λογαριασμό email σας με:
 - την προεγκατεστημένη εφαρμογή αλληλογραφίας στην έξυπνη συσκευή σας
 - την εφαρμογή Mail ή Outlook στον υπολογιστή σας.

Ιστοσελίδα

- συνδεθείτε στην ιστοσελίδα του παρόχου email σας από ένα πρόγραμμα περιήγησης στον υπολογιστή ή την έξυπνη συσκευή σας.

Παρόχων υπηρεσιών email

Υπάρχουν πολλοί πάροχοι υπηρεσιών email που προσφέρουν τόσο δωρεάν όσο και πληρωμένες επιλογές λογαριασμού email, όπως:



Gmail Google



Πρόγραμμα Outlook της Microsoft



Yahoo Mail Yahoo



iCloud Apple



ProntonMail Proton AG

Επισκεφθείτε την ιστοσελίδα Be Connected για [αναλυτικούς οδηγούς](#) σχετικά με τον τρόπο ρύθμισης και χρήσης του Gmail, Outlook και Yahoo.

Συμβουλή: Μπορεί να θέλετε να δημιουργήσετε έναν λογαριασμό email μόνο για τις τραπεζικές σας συναλλαγές ή να τον χρησιμοποιήσετε μόνο για ηλεκτρονικές αγορές για να βοηθήσετε στη διαχείριση ανεπιθύμητων μηνυμάτων email.

Διαχείριση του λογαριασμού email σας

Ρύθμιση φακέλων και ετικετών

Η ρύθμιση φακέλων στα εισερχόμενά σας είναι ένας πολύ καλός τρόπος για να διατηρήσετε τον λογαριασμό σας οργανωμένο και να διευκολύνετε τον εντοπισμό σημαντικών μηνυμάτων email όταν τα χρειάζεστε. Οι φάκελοι ονομάζονται μερικές φορές ετικέτες, ανάλογα με την υπηρεσία email που χρησιμοποιείτε.

Οργάνωση και αρχειοθέτηση των μηνυμάτων email σας

Η υπηρεσία email σας διαθέτει εύχρηστα στοιχεία ελέγχου που σας βοηθούν να αρχειοθετήσετε μηνύματα email με διαφορετικούς τρόπους και να περιορίσετε τα παραπλανητικά και τα ανεπιθύμητα μηνύματα στο ελάχιστο. Όταν φτάσει ένα νέο μήνυμα email και το ανοίξετε για να το διαβάσετε, ορισμένα στοιχεία ελέγχου εμφανίζονται στο επάνω μέρος της οθόνης. Μπορείτε να κάνετε κλικ σε αυτά τα στοιχεία ελέγχου για:

- **Διαγραφή:** μετακινήστε το μήνυμα email στον φάκελο Bin/Trash
- **Αρχειοθέτηση:** μετακινήστε το email στο αρχείο
- **Επισήμανση ως μη αναγνωσμένου:** κάντε το μήνυμα email να εμφανιστεί εκ νέου
- **Ετικέτες/Φάκελος:** επισημάνετε το email ή μετακινήστε το σε έναν φάκελο.

Διαχείριση ανεπιθύμητων μηνυμάτων

Η υπηρεσία email σας εντοπίζει αυτόματα και ανακατευθύνει γνωστά ανεπιθύμητα μηνύματα email, αλλά ορισμένα ανεπιθύμητα μηνύματα μπορούν ακόμα να περάσουν.

Εάν θεωρείτε ότι ένα μήνυμα email στα εισερχόμενά σας είναι ανεπιθύμητο ή παραπλανητικό, μπορείτε:

- **Να καταγγείλετε τα παραπλανητικά μηνύματα:** ενημερώστε τον πάροχο email ότι το μήνυμα είναι παραπλανητικό
- **Αποκλείσετε μηνύματα email:** σταματήστε να λαμβάνετε μηνύματα email από τον αποστολέα
- **Απεγγραφείτε:** σταματήστε να λαμβάνετε ενημερωτικά δελτία ή μηνύματα email μάρκετινγκ στα οποία έχετε εγγραφεί.

Εάν πιστεύετε ότι έχετε απεγγραφεί, αλλά συνεχίζετε να λαμβάνετε ανεπιθύμητα παραπλανητικά μηνύματα email, μπορείτε να υποβάλετε καταγγελία στην [Australian Communications and Media Authority \[Αυστραλιανή Αρχή Επικοινωνιών και Μέσων Ενημέρωσης\]](#).

Συμβουλή: Για να αποφύγετε ανεπιθύμητα μηνύματα email, να είστε επιφυλακτικοί όταν παρέχετε τα στοιχεία σας για διαγωνισμούς και τυχόν προεπιλεγμένα πλαίσια για να λαμβάνετε μηνύματα email μάρκετινγκ όταν αγοράζετε προϊόντα ή υπηρεσίες.

Διατηρήστε τον λογαριασμό email σας ασφαλή

Φράσεις πρόσβασης

Διατηρήστε τους λογαριασμούς σας ασφαλείς με ισχυρές φράσεις πρόσβασης. Οι φράσεις πρόσβασης είναι η πιο ασφαλής έκδοση των κωδικών πρόσβασης και αποτελούνται από τέσσερις ή περισσότερες τυχαίες λέξεις.

Δοκιμάστε να σκεφτείτε μια διαφορετική φράση πρόσβασης για κάθε λογαριασμό σας και μην ανακυκλώνετε τμήματα παλαιών.

Όταν επιλέγετε τη φράση πρόσβασης, κάντε την:

- **Μεγάλη** - τουλάχιστον 14 χαρακτήρες
- **Απρόβλεπτη** - χρησιμοποιήστε τέσσερις ή περισσότερες τυχαίες λέξεις με αριθμούς, σύμβολα και κεφαλαία και μικρά γράμματα
- **Μοναδική** - μην επαναχρησιμοποιείτε τις φράσεις πρόσβασης.

Π.χ. *Yellow So Hey Plant* > *Yell*w-S0heyPl@nt!*

Συμβουλή: Μια εφαρμογή διαχείρισης κωδικών πρόσβασης μπορεί επίσης να σας βοηθήσει να δημιουργήσετε και να αποθηκεύσετε σύνθετους κωδικούς πρόσβασης που είναι δύσκολο για άλλους να μαντέψουν ή να παραβιάσουν. Μπορείτε να βρείτε πληροφορίες σχετικά με τους [διαχειριζόμενους κωδικούς πρόσβασης](#) και τον τρόπο ρύθμισής τους στην ιστοσελίδα Be Connected.

Έλεγχος ταυτότητας με πολλαπλούς παράγοντες

Είναι πάντα καλή ιδέα να ενεργοποιείτε τον έλεγχο ταυτότητας πολλαπλών παραγόντων για τους λογαριασμούς σας. Ο έλεγχος ταυτότητας πολλαπλών παραγόντων (γνωστός και ως έλεγχος ταυτότητας 2 βημάτων) προσθέτει ένα επιπλέον επίπεδο ασφάλειας. Αυτό σημαίνει ότι όταν συνδέεστε σε έναν λογαριασμό με τον κωδικό πρόσβασής σας, μπορεί να σας ζητηθεί να κάνετε ένα επιπλέον βήμα για να επιβεβαιώσετε ότι είστε εσείς - όπως να εισαγάγετε έναν κωδικό από ένα μήνυμα κειμένου ή να χρησιμοποιήσετε αναγνώριση προσώπου.

Χρησιμοποιήστε την ασφάλεια της συσκευής

Η χρήση λογισμικού ασφαλείας στον υπολογιστή σας είναι ένας από τους απλούστερους τρόπους για να ασφαλίσετε τους λογαριασμούς και τις συσκευές σας. Η καλή ασφάλεια του υπολογιστή περιλαμβάνει την εγκατάσταση αξιόπιστων σαρωτών προστασίας από ιούς και κακόβουλο λογισμικό, και λογισμικού τείχους προστασίας. Θα πρέπει επίσης να διατηρείτε επικαιροποιημένα τα διαδικτυακά εργαλεία ασφαλείας και τις εφαρμογές σας ενεργοποιώντας τις αυτόματες ενημερώσεις.

Χρησιμοποιήστε μια ασφαλή σύνδεση

Όταν χρειάζεται να αποκτήσετε πρόσβαση στους λογαριασμούς σας, να στείλετε ευαίσθητες πληροφορίες ή να εισαγάγετε κωδικούς πρόσβασης, συνδεθείτε σε μια αξιόπιστη σύνδεση στο διαδίκτυο, όπως στο σπίτι, στην εργασία ή χρησιμοποιώντας τα δικά σας δεδομένα κινητής τηλεφωνίας, εάν είναι διαθέσιμα. Το δημόσιο Wi-Fi δεν είναι τόσο ασφαλές όσο το Wi-Fi στο σπίτι ή στην εργασία σας.

Επιλογές ανάκτησης λογαριασμού

Βεβαιωθείτε ότι έχετε ρυθμίσει έναν αριθμό τηλεφώνου ανάκτησης ή μια εναλλακτική διεύθυνση email για όλους τους λογαριασμούς email σας. Εάν χάσετε την πρόσβαση στον λογαριασμό σας ή έχει παραβιαστεί, μπορείτε να επαναφέρετε τον κωδικό πρόσβασής σας χρησιμοποιώντας την επιλογή ανάκτησης.

Ηλεκτρονικές απάτες (Scams emails)

Τα παραπλανητικά μηνύματα email έχουν σχεδιαστεί για να μοιάζουν σαν να προέρχονται από νόμιμους οργανισμούς που γνωρίζετε. Μπορεί να φαίνονται αληθινά, χρησιμοποιώντας λογότυπα και παρόμοια διεύθυνση email με τον οργανισμό που πλαστογραφούν. Τα παραπλανητικά μηνύματα email μπορεί να φαίνεται ότι προέρχονται από την τράπεζά σας, τον πάροχο υπηρεσιών Διαδικτύου, μια κυβερνητική υπηρεσία, λιανοπωλητή, ή ακόμα και έναν απατεώνα που προσποιείται ότι είναι φίλος ή μέλος της οικογένειας. Προσποιούμενοι ότι προέρχονται από κάποιον που εμπιστεύεστε, οι απατεώνες χρησιμοποιούν την αίσθηση του επείγοντος για να σας εξαπατήσουν να πληρώσετε χρήματα ή να παρέχετε προσωπικά στοιχεία, όπως σημαντικούς κωδικούς πρόσβασης, πιστωτικές κάρτες ή τραπεζικά στοιχεία.

Αυτοί οι τύποι απάτης ονομάζονται απάτες πλαστοπροσωπίας ή email ηλεκτρονικού «ψαρέματος» (phishing emails).

Συμβουλές για την αποφυγή παραπλανητικών μηνυμάτων email

- Προσέξτε τα σημάδια ενός παραπλανητικού email. Τα παραπλανητικά μηνύματα email μπορούν:
 - να δίνουν την αίσθηση του επείγοντος ή να χρησιμοποιούν τακτικές εκφοβισμού, απαιτώντας πληρωμή ή ζητώντας σας να επιβεβαιώσετε προσωπικά στοιχεία
 - να χρησιμοποιούν γενικούς χαιρετισμούς όπως «Αγαπητέ πελάτη», «Αγαπητέ χρήστη» ή κανέναν χαιρετισμό
 - να σας ζητούν να κάνετε κλικ σε έναν σύνδεσμο ή να κατεβάσετε ένα αρχείο, που μπορεί να σας κατευθύνει σε μια ψεύτικη ιστοσελίδα ή να περιέχει ιό ή κακόβουλο λογισμικό.
- Ελέγχετε πάντα ότι η διεύθυνση email του αποστολέα είναι νόμιμη και επικοινωνήστε απευθείας με τον οργανισμό αναζητώντας την επίσημη ιστοσελίδα και τον αριθμό τηλεφώνου του.
- Ποτέ μην συνδέεστε στους διαδικτυακούς λογαριασμούς σας και μην επαληθεύετε λεπτομέρειες μέσω συνδέσμου σε ένα email ή μην κάνετε κλικ σε συνδέσμους ή μην ανοίγετε συνημμένα έγγραφα σε μηνύματα email από άγνωστους ή ύποπτους αποστολείς.
- Διαγράψτε ύποπτα ή πιθανά παραπλανητικά μηνύματα email, χρησιμοποιήστε την επιλογή «καταγγελία παραπλανητικών μηνυμάτων email» για να τα ταξινομήσετε ως ανεπιθύμητα email.

Συμβουλή: Εάν δεν είστε σίγουροι για ένα μήνυμα email, μιλήστε με έναν αξιόπιστο φίλο ή μέλος της οικογένειας και επικοινωνήστε με τον οργανισμό χρησιμοποιώντας τον αριθμό τηλεφώνου στην ιστοσελίδα του.

Επισκεφθείτε την ιστοσελίδα Be Connected για τον δωρεάν [οδηγό απάτης πλαστοπροσωπίας](#) που αναπτύχθηκε με το Scamwatch.

Αφιερώστε χρόνο για να ανακαλύψετε τη Be Connected

Η Be Connected είναι μια ολοκληρωμένη ιστοσελίδα με δωρεάν ενημερωτικούς πόρους ειδικά σχεδιασμένους για να υποστηρίξουν τους ηλικιωμένους Αυστραλούς να συνδέονται με ασφάλεια στο διαδίκτυο και να περιηγούνται στον ψηφιακό κόσμο με αυτοπεποίθηση. Η ιστοσελίδα είναι επίσης χρήσιμη για οικογένειες και κοινοτικούς οργανισμούς που θέλουν να βοηθήσουν τα ηλικιωμένα μέλη της κοινότητας να έχουν πρόσβαση σε όλα τα οφέλη του Διαδικτύου.



Επισκεφθείτε τη διεύθυνση beconnected.esafety.gov.au



Το πρόγραμμα αυτό έχει αναπτυχθεί από τον Επίτροπο eSafety στο πλαίσιο της πρωτοβουλίας Be Connected.