Περίληψη διαδικτυακής παρουσίασης

Australian Government

Be Connected
Every Australian online.

Μπορείς να εντοπίσεις μια απάτη;

Αν γνωρίζετε ότι υπάρχουν απάτες και πώς λειτουργούν είναι ένα από τα πιο σημαντικά πράγματα που μπορείτε να κάνετε για να τις αποφύγετε. Κάθε χρόνο ηλικιωμένοι Αυστραλοί χάνουν εκατομμύρια δολάρια από απάτες. Ενώ το διαδίκτυο είναι ένα θαυμάσιο μέρος να εξερευνήσετε και να συνδεθείτε με άλλους, δεν μπορούμε πάντα να είμαστε σίγουροι ότι οι άνθρωποι είναι αυτοί που λένε ότι είναι. Όταν γνωρίζετε τα κόλπα ενός απατεώνα, είναι πιθανότερο να εντοπίσετε μια απάτη.

Απάτες με ηλεκτρονικό 'ψάρεμα'

Οι απάτες με ηλεκτρονικό ψάρεμα (phishing) είναι απόπειρες απατεώνων να σας εξαπατήσουν ώστε να πιστέψετε ότι προέρχονται από έναν αξιόπιστο οργανισμό ή άτομο που γνωρίζετε για να σας κάνουν να δώσετε προσωπικά στοιχεία, όπως αριθμό τραπεζικού λογαριασμού, κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών.

Τα μηνύματα ηλεκτρονικού ψαρέματος έχουν σχεδιαστεί για να φαίνονται αυθεντικά και συχνά αντιγράφουν τη μορφή που χρησιμοποιείται από τον οργανισμό που ο απατεώνας προσποιείται ότι αντιπροσωπεύει, συμπεριλαμβανομένης της επωνυμίας και το λογότυπό του. Αυτές οι απάτες μπορεί να εμφανιστούν σε πολλές μορφές, όπως email, γραπτά μηνύματα ή τηλεφωνικές κλήσεις. Για παράδειγμα, μπορεί να λάβετε:

- ένα γραπτό μήνυμα από την τράπεζά σας που σας ζητάει να επιβεβαιώσετε τον κωδικό σας πρόσβασης
- ένα email από εταιρεία τηλεπικοινωνιών που σας ζητάει να ενημερώσετε τα στοιχεία σας
- ένα γραπτό μήνυμα από άτομο της οικογένειας που χρησιμοποιεί έναν καινούργιο αριθμό τηλεφώνου και σας λέει ότι έχει χάσει το τηλέφωνό του και χρειάζεται να του στείλετε χρήματα επειγόντως
- ένα τηλεφώνημα από την τράπεζά σας για να σας προειδοποιήσει για μια «μη εξουσιοδοτημένη ή ύποπτη δραστηριότητα στον λογαριασμό σας» ή ότι ο λογαριασμός σας θα κλείσει αν δεν ενημερώσετε τα στοιχεία σας
- μια ειδοποίηση μέσω του Facebook απ' ένα άτομο που γνωρίζετε που σας προτείνει έναν ιστότοπο.

Απάτες που αφορούν την Εφορία και το Medicare

Οι απατεώνες υποδύονται ότι είναι από την Αυστραλιανή Εφορία (ATO), το Medicare και άλλους κρατικούς οργανισμούς για να προσπαθήσουν να σας εξαπατήσουν ώστε να πληρώσετε χρήματα και να κοινοποιήσετε προσωπικά στοιχεία. Αυτοί οι απατεώνες δημιουργούν ψεύτικες ιστοσελίδες και στέλνουν email, γραπτά μηνύματα και σας τηλεφωνούν προσποιούμενοι ότι είναι από κάποιον κρατικό οργανισμό.

Η Εφορία (ATO) δεν στέλνει ποτέ email, γραπτό μήνυμα ή τηλεφώνημα ζητώντας από εσάς:

- να δώσετε προσωπικά στοιχεία όπως ο αριθμός φορολογικού μητρώου, στοιχεία για την πιστωτική κάρτα ή τον τραπεζικό σας λογαριασμό
- να πληρώσετε μια χρέωση για να πάρετε την επιστροφή του φόρου σας ή να αποφύγετε τη σύλληψή σας για φοροδιαφυγή
- να κάνετε κλικ σ' έναν σύνδεσμο για να εισαγάγετε τα προσωπικά σας στοιχεία
- να κατεβάσετε αρχεία ή να εγκαταστήσετε λογισμικό.

Αν δεν είστε σίγουροι ότι η επικοινωνία προέρχεται από την Εφορία (ATO), καλέστε τη γραμμή πληροφοριών για Απάτες της ATO στο1800 008 540 ή επισκεφθείτε το ato.gov.au/scams.

Πώς να προστατευθείτε

- Μη βιάζεστε. Ξαναδιαβάστε το μήνυμα. Αναρωτηθείτε: μπορεί το μήνυμα ή η κλήση να είναι ψεύτικα;
- Είναι μια επίσημη διεύθυνση email ή είναι κάτι ύποπτο;
- Σε ποιον απευθύνεται; Να υποπτευθείτε ότι κάτι συμβαίνει αν γράφει «Αγαπητέ πελάτη» αντί το όνομά σας.
- Περιέχει τυπογραφικά ή γραμματικά λάθη; Αυτό μπορεί να είναι ένα σημάδι ότι το έχει στείλει κάποιος απατεώνας.
- Μην χρησιμοποιείτε τα στοιχεία επικοινωνίας που αναφέρονται στο μήνυμα, μπορεί να είναι ψεύτικα. Κάντε μια αναζήτηση στο διαδίκτυο για τον αριθμό τηλεφώνου και τον επίσημο ιστότοπο του οργανισμού.
- Μην κάνετε κλικ σε συνδέσμους και μην ανοίγετε συνημμένα επειδή μπορεί να κατεβάσουν έναν ιό στη συσκευή σας – απλά πατήστε το πλήκτρο Delete (Διαγραφή).
- Μη δίνετε προσωπικά στοιχεία όπως ο αριθμός του φορολογικού σας μητρώου (TFN), η ημερομηνία γέννησής σας, στοιχεία του τραπεζικού λογαριασμού ή της πιστωτικής σας κάρτας.

Να θυμάστε: Οι απατεώνες μπορεί να προσπαθήσουν να παίξουν με τα συναισθήματά σας για να σας κάνουν να αντιδράσετε και να μην έχετε χρόνο να σκεφτείτε προσεκτικά την κατάσταση. Οι τακτικές τους μπορεί να περιλαμβάνουν χρήση απειλών ή προστίμων, να σας λένε ότι έχουν γίνει μη εξουσιοδοτημένες αγορές από τον λογαριασμό σας ή να προσποιούνται ότι είναι κάποιο άτομο της οικογένειας που χρειάζεται βοήθεια.

Απάτες φιλίας και ρομαντικών σχέσεων

Οι απατεώνες εκμεταλλεύονται άτομα που αναζητούν φίλους ή ρομαντικούς συντρόφους, συχνά μέσω ιστοσελίδων γνωριμιών, εφαρμογών, μέσων κοινωνικής δικτύωσης ή ακόμα και διαδικτυακών παιχνιδιών, προσποιούμενοι τους υποψήφιους συντρόφους. Στόχος τους είναι να κερδίσουν την εμπιστοσύνη σας για να σας κάνουν να τους δώσετε χρήματα, δώρα, προσωπικές φωτογραφίες ή προσωπικά στοιχεία.

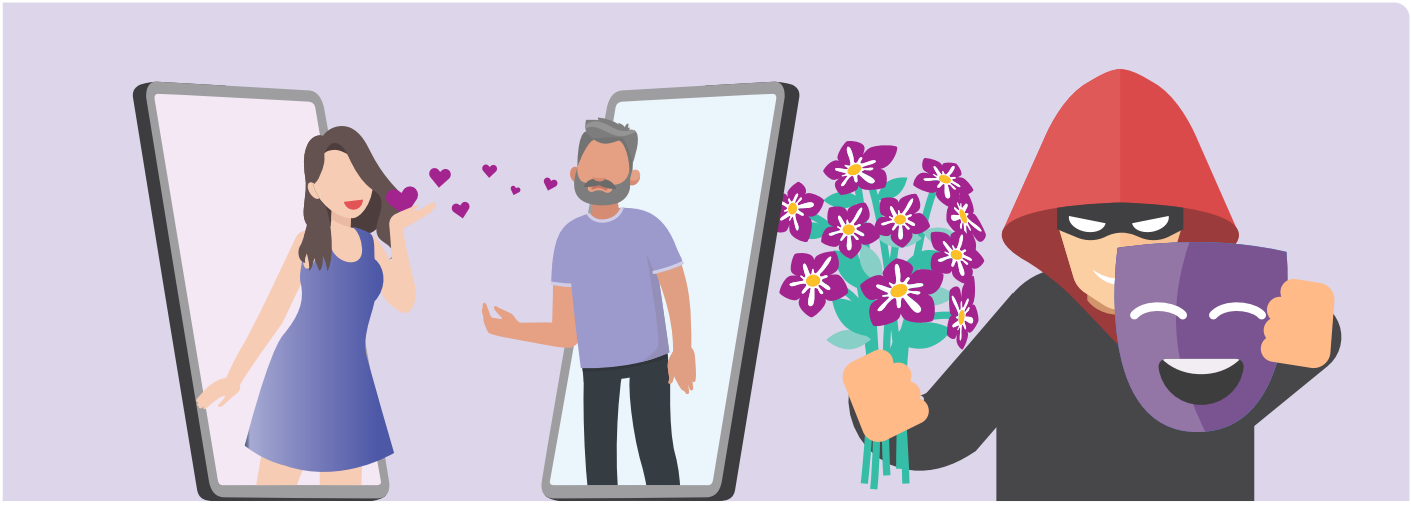
Τι μπορείτε να κάνετε για να είστε ενήμεροι και ασφαλείς;

Προσέχετε τα άτομα τα οποία:

- εκφράζουν πολύ γρήγορα μια βαθιά τρυφερότητα
- αφού κερδίσουν την εμπιστοσύνη σας - συχνά περιμένοντας εβδομάδες, μήνες ή και χρόνια - σας λένε μια περίτεχνη ιστορία και ζητάνε χρήματα ή δάνειο, δώρα ή τα στοιχεία του τραπεζικού λογαριασμού ή της πιστωτικής σας κάρτας
- αποφεύγουν να σας συναντήσουν προσωπικά και λένε δικαιολογίες για το λόγο που δεν μπορούν να ταξιδέψουν να σας δουν
- έχουν ένα διαδικτυακό προφίλ που δεν ταιριάζει με αυτά που σας λένε για τον εαυτό τους.

Πώς να προστατευθείτε

- Μην στέλνετε ποτέ χρήματα και μη δίνετε στοιχεία πιστωτικής κάρτας, στοιχεία λογαριασμού στο διαδίκτυο ή αντίγραφα σημαντικών προσωπικών εγγράφων σε κάποιον που δεν έχετε γνωρίσει προσωπικά.
- Κάντε μια αναζήτηση φωτογραφιών στο Google για τις φωτογραφίες του ατόμου για να δείτε αν είναι πραγματικά το άτομο που λένε ότι είναι ή αν έχει πάρει τις φωτογραφίες από κάπου αλλού στο διαδίκτυο. Πηγαίνετε στο images.google.com και κάντε κλικ στο εικονίδιο της κάμερας.
- Να υποπτευθείτε ότι κάτι συμβαίνει όταν αρχίζει να αναφέρει για οικονομικά προβλήματα ή χρειάζεται χρήματα για μια «έκτακτη» ανάγκη.
- Προσέχετε αν βλέπετε πράγματα όπως ορθογραφικά και γραμματικά λάθη και ασυνέπειες στις ιστορίες τους.
- Μην ανταλλάσσετε προσωπικές φωτογραφίες ή βίντεο. Είναι γνωστό ότι οι απατεώνες εκβιάζουν τα θύματά τους χρησιμοποιώντας ταπεινωτικό υλικό.



Απάτες που αφορούν τεχνική υποστήριξη

Αυτές οι απάτες συνήθως αρχίζουν με μια κλήση ή email που φαίνεται να προέρχεται από μια μεγάλη εταιρεία τηλεπικοινωνιών ή υπολογιστών, όπως Telstra, NBN ή Microsoft και σας λέει ότι έχετε κάποιο πρόβλημα με τον υπολογιστή ή το διαδίκτυο και μπορούν να το διορθώσουν. Μετά ζητούν εξ αποστάσεως πρόσβαση στον υπολογιστή σας για να «μάθουν ποιο είναι το πρόβλημα» ή θα προσπαθήσουν να σας πείσουν να αγοράσετε μη αναγκαίο λογισμικό ή μια υπηρεσία για να «διορθώσετε» τον υπολογιστή.

Πώς να προστατευθείτε

- Αν λάβετε ένα απροσδόκητο τηλεφώνημα για τον υπολογιστή σας και σας ζητηθεί εξ αποστάσεως πρόσβαση - κλείστε το τηλέφωνο.
- Μη δίνετε εξ αποστάσεως πρόσβαση στον υπολογιστή σας.
- Μην τους δίνετε προσωπικά στοιχεία, όπως στοιχεία για τον τραπεζικό λογαριασμό ή την πιστωτική σας κάρτα.
- Μην αγοράζετε λογισμικό από αυθαίρετη κλήση ή email.
- Αγνοήστε τα αναδυόμενα μηνύματα που σας λένε να καλέσετε για τεχνική υποστήριξη.

Σημαντικές συμβουλές για να αποφύγετε τις απάτες

Σταματήστε

- Μη βιαστείτε να δώσετε χρήματα ή προσωπικές πληροφορίες σε οποιονδήποτε.
- Οι απατεώνες θα προσφερθούν να σας βοηθήσουν ή θα σας ζητήσουν να επαληθεύσετε την ταυτότητά σας. Θα προσποιηθούν ότι εργάζονται σε οργανισμό που γνωρίζετε και εμπιστεύεστε, όπως μια επιχείρηση με την οποία συναλλάσσεστε ή αστυνομία, κυβέρνηση ή υπηρεσία καταπολέμησης απατών.

Σκεφτείτε

- Αναρωτηθείτε, μπορεί το μήνυμα ή η κλήση να είναι ψεύτικα;
- Μην κάνετε ποτέ κλικ σ' έναν σύνδεσμο που υπάρχει σε μήνυμα και ρωτήστε έναν έμπιστο φίλο ή μέλος της οικογένειας για το τι θα έκαναν εκείνοι. Επικοινωνήστε μόνο με επιχειρήσεις ή δημόσια υπηρεσία χρησιμοποιώντας τα στοιχεία επικοινωνίας από τον επίσημο ιστότοπο ή μέσω των ασφαλών εφαρμογών τους. Αν δεν είστε σίγουροι πείτε όχι, κλείστε το τηλέφωνο ή διαγράψτε το μήνυμα.

Προστατευθείτε

- Ενεργήστε γρήγορα αν κάτι σας φαίνεται ύποπτο.
- Επικοινωνήστε αμέσως με την τράπεζά σας αν χάσετε χρήματα ή προσωπικά στοιχεία ή αν παρατηρήσετε κάποια ασυνήθιστη δραστηριότητα στις κάρτες ή τους λογαριασμούς σας. Ζητήστε βοήθεια από οργανισμούς όπως IDCARE και καταγγείλετε κάποια διαδικτυακή παράνομη πράξη στο ReportCyber. Βοηθήστε άλλους καταγγέλοντας απάτες στο Scamwatch.

Βοήθεια, υποπτεύομαι ότι έπεσα θύμα απάτης

Αν νομίζετε ότι πέσατε θύμα απάτης, μη ντρέπεστε και μην το κρατάτε μυστικό. Υπάρχουν βήματα που μπορείτε να ακολουθήσετε για να διορθώσετε το πρόβλημα.

- Επικοινωνήστε με την τράπεζα ή το χρηματοοικονομικό σας ίδρυμα και σταματήστε τυχόν περαιτέρω πληρωμές στον απατεώνα.
- Αν πέσατε θύμα παράνομης πράξης στον κυβερνοχώρο και χάσατε χρήματα στο διαδίκτυο, μπορείτε να το καταγγείλετε στην αστυνομία μέσω του ReportCyber ή επισκεφθείτε το: cyber.gov.au
- Αν ανησυχείτε ότι τα προσωπικά σας στοιχεία έχουν εκτεθεί και χρησιμοποιηθεί παράνομα, επικοινωνήστε με την Αυστραλιανή Εθνική Υπηρεσία Ταυτοποίησης και Στήριξης στον Κυβερνοχώρο (National Identity and Cyber Support Service) IDCARE στο 1300 432 273 ή στο idcare.org
- Καταγγείλετε την απάτη στην ACCC μέσω της ιστοσελίδας scamwatch.gov.au/report-a-scam. Αυτό βοηθάει στην προειδοποίηση του κόσμου για τις τρέχουσες απάτες, στην παρακολούθηση των τάσεων και στη διακοπή της απάτης όπου είναι εφικτό.
- Διαδώστε το μήνυμα στους φίλους και την οικογένειά σας για να τους προστατέψετε.

Να θυμάστε: Πάντοτε υπάρχει κάποιος που μπορεί να σας βοηθήσει - είτε είναι οι υπάλληλοι στο cyber.gov.au ή scamwatch.gov.au, κάποιος τεχνογνώστης φίλος ή μέλος της οικογένειας, ή ακόμα κι ένας σύλλογος χρηστών υπολογιστών στην περιοχή σας.

Για να είστε ενημερωμένοι σχετικά με τις πιο πρόσφατες απάτες για να τις αποφύγετε, εγγραφείτε να λαβαίνετε προειδοποιήσεις με email στο Scamwatch email alerts.

Αφιερώστε χρόνο για να ανακαλύψετε το πρόγραμμα Be Connected

Be Connected είναι ένας ολοκληρωμένος ιστότοπος με δωρεάν ενημερωτικό υλικό ειδικά σχεδιασμένο για να βοηθάει ηλικιωμένους Αυστραλούς να συνδέονται με ασφάλεια στο διαδίκτυο και να περιηγηθούν με σιγουριά στον ψηφιακό κόσμο. Ο ιστότοπος είναι επίσης χρήσιμος για οικογένειες και κοινοτικούς συλλόγους που θέλουν να βοηθήσουν τα ηλικιωμένα μέλη να έχουν πρόσβαση σε όλα τα οφέλη του διαδικτύου.

visit beconnected.esafety.gov.au

Australian Government | eSafety Commissioner

Το πρόγραμμα αυτό αναπτύχθηκε από το eSafety (ηλεκτρονική ασφάλεια και προστασία) ως μέρος της πρωτοβουλίας Be Connected.