

Μπορείς να εντοπίσεις μια απάτη;

Στο διαδίκτυο, δεν μπορούμε να είμαστε πάντα σίγουροι ότι οι άνθρωποι είναι αυτοί που λένε ότι είναι. Αν συνειδητοποιήσετε ότι υπάρχουν απατεώνες στο διαδίκτυο είναι ένα από τα πιο σημαντικά πράγματα που μπορείτε να κάνετε για τους αποφύγετε. Όταν μάθετε τα κόλπα τους, θα πρέπει να είναι ευκολότερο να εντοπίσετε μια απάτη όταν τη δείτε.



Απάτες με ηλεκτρονικό "ψάρεμα"

Οι απάτες με ηλεκτρονικό "ψάρεμα" (Phishing) είναι η συνηθέστερη μορφή απάτης στο διαδίκτυο. Μπορεί να φαίνονται ότι είναι από κάποιον αξιόπιστο οργανισμό και είναι σχεδιασμένες να σας εξαπατήσουν για να δώσετε τα προσωπικά σας στοιχεία όπως τραπεζικός λογαριασμός, αριθμός της πιστωτικής κάρτας, όνομα χρήστη και κωδικούς πρόσβασης.

Μπορεί να εμφανιστούν σε πολλές μορφές:

- απροσδόκητα email, γραπτά μηνύματα ή τηλεφωνικές κλήσεις που σας ζητούν να επιβεβαιώσετε, να ενημερώσετε ή να καταχωρίσετε ξανά τα προσωπικά σας στοιχεία
- επείγοντα ή απειλητικά μηνύματα που σας λένε κάτι περίεργο συμβαίνει με το λογαριασμό σας ή ότι ο λογαριασμός σας θα κλείσει ώστε να αναγκαστείτε να κάνετε κλικ σ' ένα σύνδεσμο για να το διορθώσετε
- απροσδόκητα email που σας ζητάνε να ανοίξετε ή να κατεβάσετε κάποιο αρχείο σε μορφή '.exe' ή '.zip'.

Χρήσιμη συμβουλή: Εάν δεν είστε σίγουροι για ένα μήνυμα που λάβατε, κάντε μια αναζήτηση στο διαδίκτυο για την εταιρεία που φαίνεται ότι έστειλε το μήνυμα και επικοινωνήστε απευθείας με την εταιρεία αυτή.

Μη βιάζεστε. Ξαναδιαβάστε το μήνυμα.

- Ποιος είναι ο αποστολέας; Είναι μια επίσημη διεύθυνση email ή μια περίεργη διεύθυνση;
- Σε ποιον απευθύνεται; Να υποπτευθείτε ότι κάτι συμβαίνει αν γράφει «Αγαπητέ πελάτη» αντί το όνομά σας.
- Είναι κακογραμμένο με ορθογραφικά λάθη; Αυτό μπορεί να είναι ένα σημάδι ότι το έχει στείλει κάποιος απατεώνας.

Μην:

- κάνετε κλικ σε κανένα σύνδεσμο
- ανοίγετε κανένα συνημμένο γιατί μπορεί να κατεβάσει ιό στον υπολογιστή σας
- χρησιμοποιείτε τα στοιχεία επικοινωνίας που αναφέρονται στο μήνυμα, μπορεί να είναι ψεύτικα.



Απάτες που αφορούν την Εφορία και το Medicare

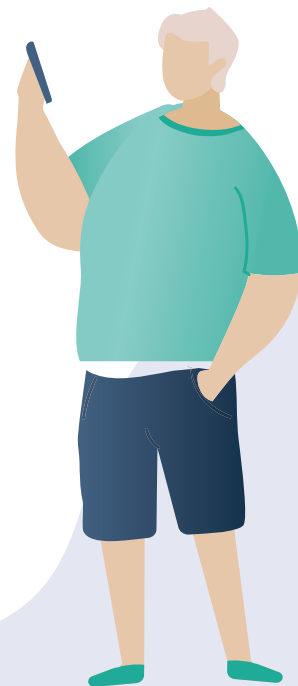
Οι απατεώνες μιμούνται την Αυστραλιανή Εφορία, το Medicare και άλλους κρατικούς οργανισμούς για να πάρουν χρήματα και προσωπικά στοιχεία από θύματα μέσω ψεύτικων ιστότοπων, email, γραπτών μηνυμάτων και τηλεφωνικών κλήσεων.

Είναι σημαντικό να θυμάστε ότι η Αυστραλιανή Εφορία (ATO) δεν πρόκειται ποτέ:

- να σας στείλει email ή γραπτό μήνυμα για να ζητήσει τα προσωπικά σας στοιχεία, συμπεριλαμβανομένου του Αριθμού Φορολογικού Μητρώου (TFN), της πιστωτικής κάρτας ή των τραπεζικών σας στοιχείων
- να σας ζητήσει να πληρώσετε μια χρέωση για να πάρετε την επιστροφή του φόρου σας ή να αποφύγετε τη σύλληψή σας για φοροδιαφυγή
- να σας στείλει email με έναν σύνδεσμο για μια διαδικτυακή υπηρεσία που ζητάει τα προσωπικά σας στοιχεία
- να στείλει αρχεία που μπορείτε να κατεβάσετε ή να σας δώσει οδηγίες για να εγκαταστήσετε κάποιο λογισμικό.

Τι μπορείτε να κάνετε για να είστε ενήμεροι και ασφαλείς;

- Μην κάνετε κλικ σε οποιονδήποτε σύνδεσμο και μην κατεβάζετε κανένα συνημμένο.
- Μη δίνετε προσωπικά στοιχεία όπως ο αριθμός του φορολογικού σας μητρώου (TFN), η ημερομηνία γέννησής σας, ο τραπεζικός σας λογαριασμός ή τα στοιχεία της πιστωτικής σας κάρτας.
- Εάν δεν είστε βέβαιοι αν ένα τηλεφωνικό μήνυμα είναι πραγματικό, μην χρησιμοποιήσετε τα στοιχεία επικοινωνίας που παρέχονται, αλλά κάντε μια αναζήτηση στο διαδίκτυο για τον αριθμό του οργανισμού.
- Να είστε ενήμεροι για την κατάσταση των φορολογικών υποθέσεών σας - υπάρχει πιθανότητα να σας επιστραφεί φόρος ή να χρωστάτε κάποια πληρωμή;
- Συνδεθείτε με τον επίσημο λογαριασμό σας στο myGov πληκτρολογώντας τη διεύθυνση μόνοι σας αντί να κάνετε κλικ σε κάποιον σύνδεσμο.
- Ελέγξτε αν το email που λάβατε προέρχεται από πραγματική διεύθυνση της Εφορίας που λήγει σε @ato.gov.au
- Ακόμα κι αν φαίνεται ότι βρίσκεστε σε ιστοσελίδα της Εφορίας ή myGov, ελέγξτε αν η διεύθυνση τελειώνει σε .gov.au (αντί για παράδειγμα .com.au, .org.au ή .net.au).
- Κοιτάξτε αν είναι κακογραμμένο με ορθογραφικά λάθη.
- Να υποπτευθείτε ότι κάτι συμβαίνει αν δεν απευθύνετε σε εσάς προσωπικά.



Απάτες που αφορούν γνωριμίες και ειδύλλια

Οι απατεώνες δημιουργούν ψεύτικα διαδικτυακά προφίλ στα μέσα κοινωνικής δικτύωσης ή ιστοσελίδες γνωριμιών για να έρθουν σε επαφή με τα θύματα. Σκοπός τους είναι να κερδίσουν την εμπιστοσύνη σας πριν σας ζητήσουν χρήματα.

Τι μπορείτε να κάνετε για να είστε ενήμεροι και ασφαλείς;

Προσέχετε για:

- άτομα που εκφράζουν πολύ γρήγορα τη βαθιά αγάπη τους για σας πριν σας ζητήσουν χρήματα ή "δάνειο"
- άτομα που αποφεύγουν να σας συναντήσουν προσωπικά και βρίσκουν δικαιολογίες για το λόγο που δεν μπορούν να ταξιδέψουν να σας δουν
- άτομα των οποίων το προφίλ στο διαδίκτυο δεν ταιριάζει με αυτά που σας έχουν πει για τον εαυτό τους.

Τι πρέπει να κάνετε:

- ελέγξτε εάν οι φωτογραφίες τους είναι πραγματικά δικές τους ή αν τις έχουν πάρει από κάπου αλλού στο διαδίκτυο κάνοντας μια αναζήτηση φωτογραφιών στο Google. Πηγαίστε στο images.google.com και κάντε κλικ στο εικονίδιο της κάμερας
- να υποπτευθείτε ότι κάτι συμβαίνει όταν αρχίζουν να αναφέρουν για οικονομικά προβλήματα ή χρειάζονται χρήματα για μια «έκτακτη» ανάγκη.

Μην:

- μεταφέρετε οποιαδήποτε χρήματα σε κάποιον που έχετε μιλήσει μόνο μέσω τηλεφώνου ή email
- στείλετε προσωπικά στοιχεία όπως ημερομηνία γέννησης, στοιχεία της τράπεζας ή της πιστωτικής σας κάρτας.

Απάτες που αφορούν τεχνική υποστήριξη

Αυτές οι απάτες συνήθως αρχίζουν με μια κλήση ή email που φαίνεται να προέρχεται από έναν μεγάλο, γνωστό οργανισμό που σας λέει ότι έχετε πρόβλημα με τον υπολογιστή ή το διαδίκτυο και μπορούν να το διορθώσουν.

Τι μπορείτε να κάνετε για να είστε ενήμεροι και ασφαλείς;

- Μην παρέχετε απομακρυσμένη πρόσβαση στον υπολογιστή σας.
- Μην τους δίνετε προσωπικά στοιχεία, όπως στοιχεία για τον τραπεζικό λογαριασμό ή την πιστωτική κάρτα σας.
- Μην αγοράζετε λογισμικό από αυθαίρετη κλήση ή email.
- Αγνοήστε τα αναδυόμενα μηνύματα που σας λένε να καλέσετε για τεχνική υποστήριξη.



Οι μεγάλοι οργανισμοί αναμένουν από εσάς να καλέσετε όταν έχετε κάποιο πρόβλημα με το διαδίκτυο ή τον υπολογιστή σας. Δεν σας καλούν αυτοί.

Βοήθεια, υποπτεύομαι ότι με εξαπάτησαν

Εάν νομίζετε ότι έχετε πέσει θύμα απάτης, μη ντρέπεστε και να μην το κρατάτε μυστικό. Μπορείτε να λάβετε μέτρα για να διορθώσετε το πρόβλημα:

- επικοινωνήστε με την τράπεζά σας και σταματήστε τυχόν περαιτέρω πληρωμές στον απατεώνα
- καταγγείλετε την απάτη στην Αυστραλιανή Επιτροπή Ανταγωνισμού και Προστασίας Καταναλωτών (Australian Competition and Consumer Commission) στο scamwatch.gov.au - μπορούν να σας βοηθήσουν με περαιτέρω συμβουλές
- ενημερώστε τους άλλους. Αν υπάρχει κάποιος άλλος που γνωρίζετε ότι μπορεί να έχει πέσει θύμα, ενημερώστε τον.

Εάν δεν είστε σίγουροι ότι το μήνυμα που λάβατε είναι πραγματικά από την Εφορία, ή έχετε πέσει θύμα απάτης φοροδιαφυγής, καλέστε την Άμεση Γραμμή Πληροφοριών ΑΤΟ στο 1800 008 540.

Φροντίστε να είστε ενημερωμένοι για τις απάτες που αφορούν την Εφορία πηγαίνοντας στο ato.gov.au/scams

Αν ανησυχείτε ότι τα προσωπικά σας στοιχεία έχουν εκτεθεί και χρησιμοποιηθεί καταχρηστικά, επικοινωνήστε με την Εθνική Υπηρεσία Ταυτοποίησης και Υποστήριξης στον Κυβερνοχώρο της Αυστραλίας (National Identity and Cyber Support Service) **IDCARE** στο 1300 432 273 ή στο idcare.org

Να θυμάστε ότι:

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

Σκοπός των απατεώνων είναι να αξιοποιήσουν τον καλό σας χαρακτήρα, αλλά το διαδίκτυο μπορεί να είναι ένα ασφαλές μέρος για εξερεύνηση εάν είστε προσεκτικοί σχετικά με την ανταλλαγή προσωπικών στοιχείων στο διαδίκτυο, να χρησιμοποιείτε την κοινή λογική για το πού στέλνετε χρήματα και σε ποιον και να είστε πάντοτε προσεκτικοί.

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 κοινωνικούς συλλόγους που θέλουν να βοηθήσουν τα ηλικιωμένα μέλη να έχουν πρόσβαση σε όλα τα οφέλη του διαδικτύου.

beconnected.esafety.gov.au

