

10 κορυφαίες συμβουλές για να προστατευτείτε από

Απάτες Πλαστοπροσωπίας

Greek | Ελληνικά



Be Connected
Every Australian online.



SCAMWATCH

Οι σημερινές απάτες γίνονται όλο και πιο περίπλοκες. Στο παρελθόν, λάθη στην ορθογραφία και τη γραμματική διευκόλυναν τον εντοπισμό τους, αλλά η νέα τεχνολογία σημαίνει ότι η αναγνώριση απάτης γίνεται όλο και πιο δύσκολη.



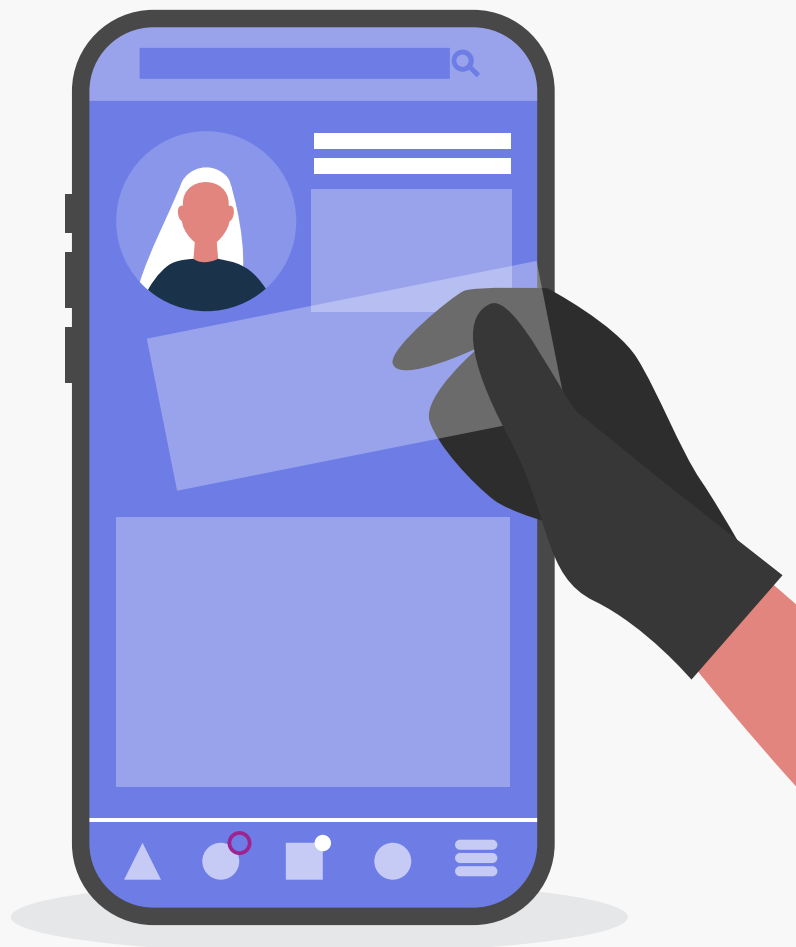
Το Εθνικό Κέντρο κατά της Απάτης έχει ενώσει τις δυνάμεις του με την κυβέρνηση, τους εμπειρογνώμονες του τομέα, τους φορείς επιβολής του νόμου και τους κοινοτικούς οργανισμούς για την καταπολέμηση της απάτης. Αλλά υπάρχουν επίσης μέτρα που μπορείτε να πάρετε για να προστατεύσετε τον εαυτό σας από την απάτη. Μία από τις καλύτερες δικλίδες ασφαλείας είναι να μένετε ενήμεροι για νέες και αναδυόμενες απάτες, ώστε να μπορείτε να αναγνωρίζετε τα σημάδια.

Η Be Connected σε συνεργασία με το National Anti-Scam Centre's Scamwatch σας προσφέρει αυτόν τον οδηγό για να σας βοηθήσει να εντοπίζετε τις απάτες πλαστοπροσωπίας, να προστατεύεστε από αυτές και να γνωρίζετε πού να πάτε για βοήθεια σε περίπτωση που πέσετε ποτέ θύμα απάτης.

Όλα τα παραδείγματα που παρέχονται σε αυτόν τον οδηγό είναι πραγματικές απάτες.

Σε αυτόν τον οδηγό

- [Τι είναι απάτη πλαστοπροσωπίας;](#)
- [Τι είναι παραπλάνηση/πλαστογράφιση;](#)
- [Συχνές απάτες πλαστοπροσωπίας](#)
- [Οι 10 κορυφαίες συμβουλές για την προστασία σας](#)
- [Πού να πάτε για βοήθεια](#)



Τι είναι απάτη πλαστοπροσωπίας;

Οι απάτες πλαστοπροσωπίας έχουν σχεδιαστεί για να φαίνονται σαν να προέρχονται από νόμιμους οργανισμούς που γνωρίζετε. Μπορεί να φαίνονται ότι προέρχονται από την τράπεζά σας, τον πάροχο υπηρεσιών διαδικτύου, έναν κυβερνητικό οργανισμό, έναν λιανοπωλητή, ή ακόμη και έναν απατεώνα που προσποιείται ότι είναι φίλος ή μέλος της οικογένειας.

Με το να προσποιούνται ότι είναι από κάποιον που εμπιστεύεστε, οι απατεώνες χρησιμοποιούν την αίσθηση του επείγοντος για να σας ξεγελάσουν να πληρώσετε χρήματα ή να δώσετε προσωπικά στοιχεία, όπως σημαντικούς κωδικούς πρόσβασης και στοιχεία πιστωτικών καρτών ή τραπεζικών λογαριασμών.

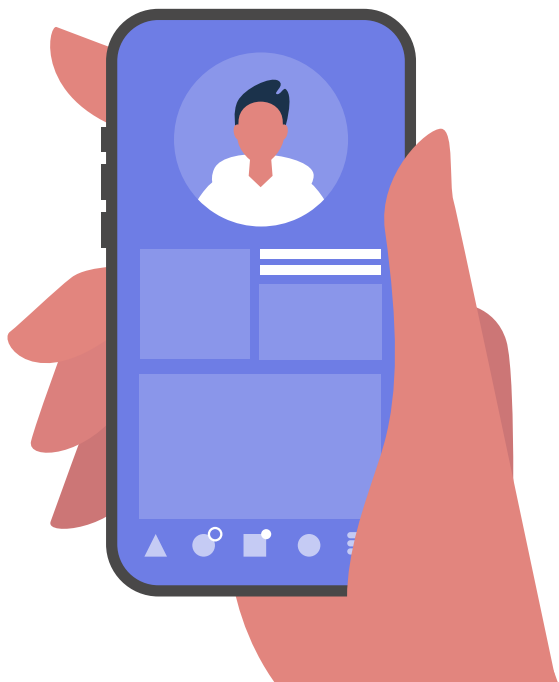
Οι απατεώνες χρησιμοποιούν μια σειρά μεθόδων για να έρθουν σε επαφή μαζί σας, συμπεριλαμβανομένων μηνυμάτων κειμένου, τηλεφωνικών κλήσεων, μηνυμάτων ηλεκτρονικού ταχυδρομείου, αναρτήσεων στα μέσα κοινωνικής δικτύωσης και ψεύτικων ιστότοπων που μοιάζουν απόλυτα με επίσημες ιστοσελίδες.



Τι είναι η παραπλάνηση/ πλαστογράφηση [spoofing];

Οι απατεώνες μπορούν να υποδυθούν οργανισμούς που γνωρίζετε χρησιμοποιώντας την τεχνολογία για να κάνουν την κλήση ή το μήνυμά τους να φαίνεται ότι προέρχεται από αξιόπιστη πηγή. Αυτό είναι γνωστό ως spoofing.

Να είστε σε εγρήγορση για την πιθανότητα απάτης και επιφυλακτικοί με την ανεπιθύμητη επαφή που ζητά προσωπικά στοιχεία, όπως κωδικό πρόσβασης ή κάποιο είδος πληρωμής. Επικοινωνήστε απευθείας με τον οργανισμό από όπου ισχυρίζεται ότι προέρχεται για να είστε σίγουροι.



Υπάρχουν διάφοροι τύποι τεχνικών spoofing, που συμπεριλαμβάνουν:

- 01. Παραπλανητική ταυτότητα καλούντος:** Οι απατεώνες αλλάζουν το αναγνωριστικό καλούντος για να εμφανίσουν έναν διαφορετικό αριθμό από αυτόν που χρησιμοποιείται, κάνοντας την κλήση να φαίνεται ότι προέρχεται από νόμιμο αριθμό.
- 02. Παραπλανητικό μήνυμα SMS (ή ετικέτες άλφα):** Οι απατεώνες αλλάζουν τον αριθμό τηλεφώνου τους για να φαίνεται ως το όνομα επιχείρησης (για παράδειγμα, AusPost). Μπορεί να κάνει ένα μήνυμα κειμένου να εμφανίζεται στην ίδια συνομιλία ή νήμα ως γνήσια μηνύματα από έναν οργανισμό.
- 03. Παραπλανητικά email:** Οι απατεώνες αλλάζουν τη διεύθυνση email ή το όνομα του αποστολέα τους για να κάνουν ένα μήνυμα email να φαίνεται ότι προέρχεται από αξιόπιστη πηγή. Μπορεί να παραποιήσουν το όνομα εμφάνισης "Από" ή τη διεύθυνση email, συχνά αλλάζοντας ή προσθέτοντας ένα γράμμα ή έναν αριθμό σε ένα νόμιμο όνομα τομέα (για παράδειγμα, @amazon.com αντί για @amazon.com).

Κοινές απάτες πλαστοπροσωπίας

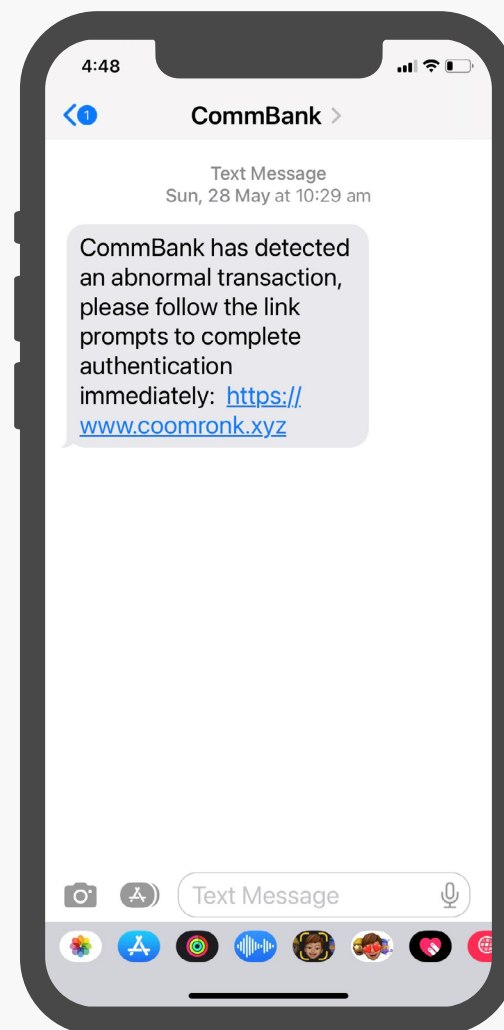
Απάτες πλαστοπροσωπίας Τράπεζας

- Λαμβάνετε μια κλήση ή ένα μήνυμα από κάποιον που ισχυρίζεται ότι είναι από το τμήμα ασφάλειας της τράπεζάς σας. Σας ενημερώνει για μια ύποπτη συναλλαγή, ισχυριζόμενος ότι ο λογαριασμός σας έχει παραβιαστεί. Σας παροτρύνει να μεταφέρετε χρήματα σε διαφορετικό λογαριασμό για να τα «κρατήσετε ασφαλή» ή για «περαιτέρω διερεύνηση».
- Λαμβάνετε ένα μήνυμα κειμένου ή email που σας ζητά να κάνετε κλικ σε έναν σύνδεσμο για να επαληθεύσετε τα στοιχεία του λογαριασμού σας. Ο σύνδεσμος σάς μεταφέρει σε έναν ψεύτικο ιστότοπο που έχει σχεδιαστεί για να συλλέξει το όνομα χρήστη, τον κωδικό πρόσβασής σας και άλλα προσωπικά στοιχεία.

i Πώς ξέρετε ότι αυτό είναι απάτη;

Ενώ η τράπεζά σας μπορεί να επικοινωνήσει μαζί σας εάν υπάρχει ύποπτη δραστηριότητα στον λογαριασμό σας, δεν θα σας ζητήσει ποτέ να μεταφέρετε κεφάλαια σε άλλον λογαριασμό. Ούτε θα ζητήσει οποιαδήποτε στοιχεία λογαριασμού ή προσωπικά στοιχεία, συμπεριλαμβανομένων, του κωδικού πρόσβασης, του PIN ή του μοναδικού κωδικού πρόσβασης με ανεπιθύμητο μήνυμα κειμένου, email ή τηλεφωνική κλήση.

Οι απατεώνες μπορούν να κάνουν έναν αριθμό τηλεφώνου να μοιάζει με το αναγνωριστικό κλήσης από την τράπεζά σας, αλλά μην το θεωρήσετε αυτό ως απόδειξη του με ποιον μιλάτε. Μπορεί επίσης να φαίνεται ότι έχουν πληροφορίες σχετικά με εσάς, αλλά οποιαδήποτε στοιχεία έχουν, είναι πιθανό ότι τα έχουν αποκτήσει με δόλο.



Παράδειγμα μηνύματος κειμένου που προσποιείται ότι προέρχεται από τράπεζα από πλαστογραφημένο αριθμό που σας ζητά να κάνετε κλικ σε έναν σύνδεσμο για να επαληθεύσετε τα στοιχεία σας.

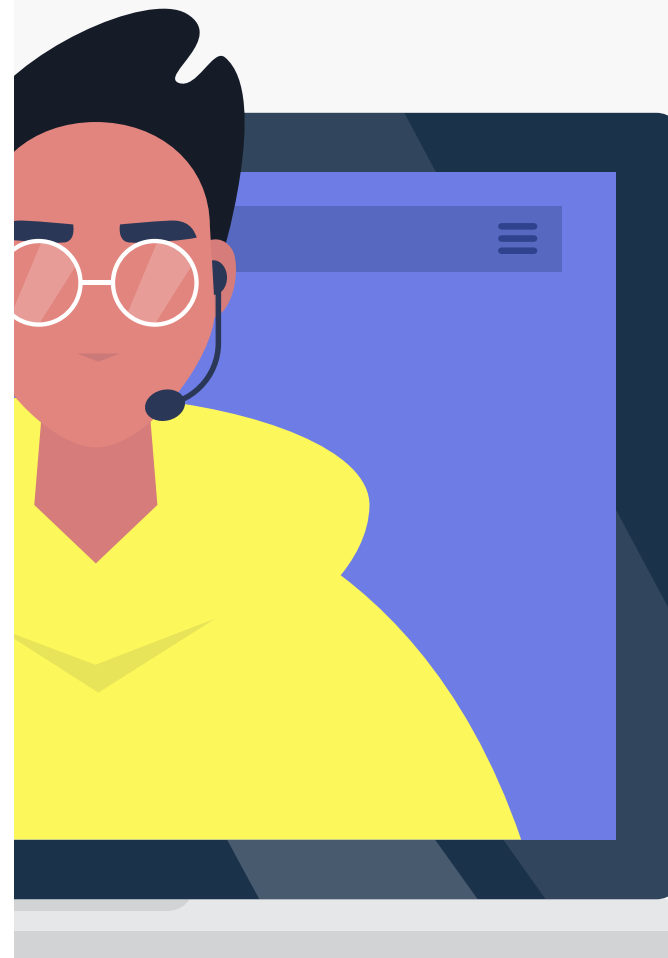
Απάτες τεχνικής υποστήριξης

- Ένας τηλεφωνητής που ισχυρίζεται ότι προέρχεται από έναν πάροχο διαδικτυακών υπηρεσιών, εταιρεία τηλεπικοινωνιών ή εταιρεία υπολογιστών, σας ενημερώνει ότι υπάρχει πρόβλημα με το διαδίκτυο ή τον υπολογιστή σας. Μπορεί να πει ότι κάποιος τον χάκαρε (μπήκε στο λογισμικό του), έχει έναν ιό, τρέχει αργά ή πρόκειται να αποσυνδεθεί. Σας καθοδηγεί να κατεβάσετε μια εφαρμογή ή λογισμικό για να του δώσετε πρόσβαση εξ αποστάσεως στον υπολογιστή σας, ώστε να μπορέσει να τον «διορθώσει».
- Ένα προειδοποιητικό μήνυμα εμφανίζεται στην οθόνη του υπολογιστή σας και σας προτρέπει να καλέσετε αμέσως τον αναφερόμενο αριθμό για βοήθεια με ένα πρόβλημα που έχει εντοπιστεί.

i Πώς ξέρετε ότι αυτό είναι απάτη;

Οι νόμιμες εταιρείες δεν θα σας καλέσουν ποτέ για να σας πουν ότι υπάρχει πρόβλημα με τη σύνδεση στο διαδίκτυο ή τον υπολογιστή σας (αναμένουν ότι εσείς θα επικοινωνήσετε μαζί τους όταν υπάρχει πρόβλημα). Δεν θα σας ζητήσουν ποτέ να κατεβάσετε οποιοδήποτε λογισμικό ή εφαρμογή που τους δίνει πρόσβαση στη συσκευή σας.

Κλείστε ύποπτα αναδυόμενα μηνύματα κάνοντας κλικ στο "x" στην επάνω δεξιά γωνία του πλαισίου. Αν αυτό δεν λειτουργεί, δοκιμάστε να κάνετε κλικ έξω από το πλαίσιο ή να κλείσετε την ιστοσελίδα στην οποία εμφανίζεται. Εάν το αναδυόμενο παράθυρο δεν έχει εξαφανιστεί ακόμα, δοκιμάστε να πατήσετε τα πλήκτρα ALT και F4 στον υπολογιστή Windows για να κλείσετε το πρόγραμμα περιήγησης ιστού. Σε υπολογιστή Apple, επιλέξτε Force Quit από το μενού Apple και επιλέξτε το πρόγραμμα περιήγησης που θέλετε να κλείσετε.



Απάτες αναστολής λογαριασμού

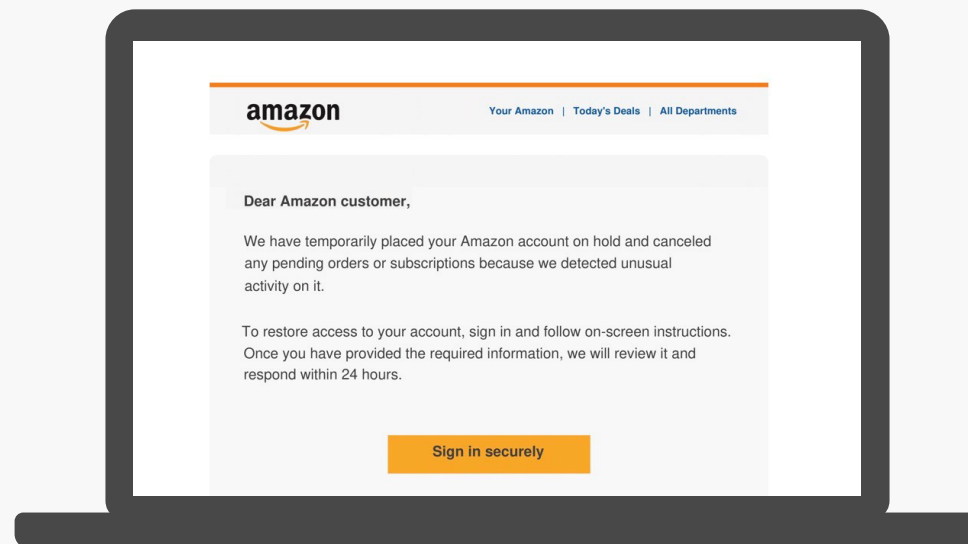
Λαμβάνετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου ή ένα μήνυμα κειμένου που ισχυρίζεται ότι προέρχεται από έναν οργανισμό που γνωρίζετε, όπως το Amazon, το PayPal ή το Netflix. Σας ενημερώνει ότι ο λογαριασμός σας έχει ανασταλεί λόγω ύποπτης δραστηριότητας και ότι θα πρέπει να κάνετε κλικ σε έναν σύνδεσμο για να επιβεβαιώσετε την ταυτότητά σας, ώστε να γνωρίζουν ότι είστε πραγματικά εσείς.

Οι απατεώνες χρησιμοποιούν τακτικές εκφοβισμού για να σας κατευθύνουν σε έναν ψεύτικο ιστότοπο που συλλέγει προσωπικά στοιχεία όπως το όνομα χρήστη, τον κωδικό πρόσβασης και τα στοιχεία τραπεζικών λογαριασμών ή της πιστωτικής κάρτας σας.

i Πώς ξέρετε ότι αυτό είναι απάτη;

Το Amazon, το PayPal και το Netflix δεν θα ζητήσουν ποτέ προσωπικά στοιχεία όπως κωδικούς πρόσβασης, στοιχεία τραπεζικών λογαριασμών ή της πιστωτικής κάρτας σας μέσω ενός συνδέσμου σε ανεπιθύμητο email ή μήνυμα κειμένου. Ενώ οι οργανισμοί διαφέρουν στην προσέγγισή τους στην επικοινωνία με τους πελάτες, είναι καλύτερο να είστε επιφυλακτικοί και πάντα να αντιμετωπίζετε αυτά τα είδη email, μηνυμάτων κειμένου ή κλήσεων με προσοχή.

Εάν δεν είστε σίγουροι αν ένα μήνυμα προέρχεται πραγματικά από την επιχείρηση από την οποία ισχυρίζεται ότι προέρχεται, επικοινωνήστε με την επιχείρηση απευθείας με αναζήτηση των στοιχείων επικοινωνίας στο διαδίκτυο. Μην χρησιμοποιείτε ποτέ τα στοιχεία επικοινωνίας που παρέχονται στο μήνυμα κειμένου, το email ή το τηλέφωνο.



Παράδειγμα απάτης μέσω email που ισχυρίζεται ότι προέρχεται από το Amazon και σας προτρέπει να κάνετε κλικ στον σύνδεσμο για να δώσετε τα προσωπικά σας στοιχεία.

Προσοχή στις τακτικές εκφοβισμού

Οι απατεώνες χρησιμοποιούν τακτικές εκφοβισμού για να δημιουργήσουν μια αίσθηση του επείγοντος ώστε να σας κάνουν να ενεργήσετε. Εδώ είναι μερικά πράγματα που μπορεί να πουν για να τραβήξουν την προσοχή σας:

- Εντοπίστηκε ασυνήθιστη δραστηριότητα στον λογαριασμό
- Μη εξουσιοδοτημένες απόπειρες σύνδεσης
- Ο λογαριασμός σας είναι αποκλεισμένος / κλειδωμένος
- Η πληρωμή σας απορρίφθηκε
- Δεν είμαστε σε θέση να επικυρώσουμε τις πληροφορίες χρέωσης σας

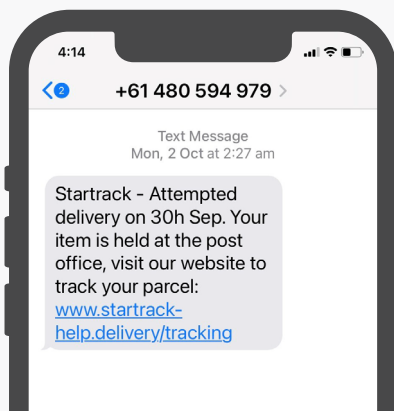
Απάτες για αποτυχημένες απόπειρες παράδοσης

Λαμβάνετε ένα email ή μήνυμα κειμένου που ισχυρίζεται ότι προέρχεται από την Αυστραλιανή Ταχυδρομική Υπηρεσία ή μια εταιρεία ταχυμεταφορών όπως η FedEx, που σας ενημερώνει ότι υπάρχει πρόβλημα ή καθυστέρηση με την παράδοση. Για να λάβετε το πακέτο σας, θα πρέπει να πληρώσετε ένα κόστος αποστολής ή «να επικαιροποιήσετε τα στοιχεία σας».

i Πώς ξέρετε ότι αυτό είναι απάτη;

Η Australia Post, η FedEx και άλλες νόμιμες εταιρείες ταχυμεταφορών δεν θα στείλουν ποτέ μηνύματα κειμένου, μηνύματα ηλεκτρονικού ταχυδρομείου ή κλήσεις για να ζητήσουν προσωπικά στοιχεία ή πληρωμές. Εάν περιμένετε μια παράδοση, είναι καλύτερο να παρακολουθείτε την παράδοσή σας μέσω της ασφαλούς εφαρμογής τους ή μέσω της διαδικτυακής υπηρεσίας παρακολούθησης στο email επιβεβαίωσης της παραγγελίας σας. Αν δεν έχετε κανένα απ' αυτά, καλέστε την εταιρεία ταχυμεταφορών απευθείας για να ρωτήσετε πού βρίσκεται το πακέτο σας.

Παράδειγμα
μηνύματος κειμένου
που ισχυρίζεται
ότι προέρχεται
από εταιρεία
ταχυμεταφορών.



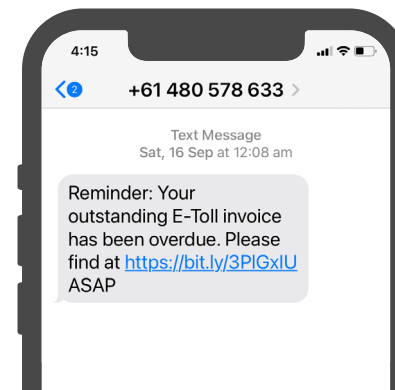
Απάτες διοδίων

Λαμβάνετε μήνυμα από διαχειριστή διοδίων που σας ενημερώνει ότι η πληρωμή των τελών σας έχει καθυστερήσει. Πρέπει να λάβετε άμεσα μέτρα για να αποφύγετε να πληρώσετε πρόστιμο, οπότε περιλαμβάνει έναν σύνδεσμο για να κανονίσετε την πληρωμή, αλλά σας μεταφέρει σε έναν ψεύτικο ιστότοπο που έχει σχεδιαστεί για να κλέψει τα οικονομικά σας στοιχεία.

i Πώς ξέρετε ότι αυτό είναι απάτη;

Εάν έχετε λάβει ένα μήνυμα που ισχυρίζεται ότι έχετε έναν ληξιπρόθεσμο λογαριασμό ή ανεπαρκή κεφάλαια για τα διόδια, μπορεί να είναι απάτη. Επισκεφθείτε τον ιστότοπο ή την εφαρμογή του υπεύθυνου φορέα διοδίων για να συνδεθείτε στον λογαριασμό σας και να ελέγξετε την πρόσφατη δραστηριότητά σας.

Παράδειγμα
μηνύματος κειμένου
απάτης διοδίων.



Απάτες ψεύτικων επενδύσεων

Βλέπετε μια καταπληκτική επενδυτική ευκαιρία που φαίνεται να υποστηρίζεται από διασημότητα ή άτομο που ασκεί επιρροή σε χρηματοοικονομικά θέματα. Υπόσχεται εγγυημένη υψηλή απόδοση με ελάχιστο ή κανένα ρίσκο. Όταν ζητάτε περισσότερες πληροφορίες, μεταβαίνετε σε έναν επαγγελματικό ιστότοπο και λαμβάνετε προσεγμένο διαφημιστικό υλικό.

i Πώς ξέρετε ότι αυτό είναι απάτη;

Αν μια προσφορά ακούγεται πολύ καλή για να είναι αληθινή, πιθανότατα είναι. Οι απατεώνες χρησιμοποιούν τακτικές υψηλής πίεσης για να σας πείσουν να δράσετε γρήγορα ώστε να μην «χάσετε την ευκαιρία». Προσοχή σε μηνύματα ηλεκτρονικού ταχυδρομείου, ιστότοπους ή διαφημίσεις με μαρτυρίες και υπερβολικές υποσχέσεις μεγάλων κερδών.

Ο «σύμβουλος» που σας βοηθά μπορεί να ισχυριστεί ότι δεν χρειάζεται άδεια Australian Financial Services [Αυστραλιανών Οικονομικών Υπηρεσιών] (AFS). Αν σας τη δώσει, πάντα να ελέγχετε ότι το άτομο με το οποίο επικοινωνείτε είναι ο πραγματικός κάτοχος της άδειας.



Απάτες ψεύτικων ιστοσελίδων

Βλέπετε στο Facebook μια διαφήμιση πασίγνωστης μάρκας BBQ που πωλείται για \$100 όταν συνήθως κοστίζει \$900. Κάνετε κλικ στον σύνδεσμο στον ιστότοπο του λιανοπωλητή και βλέπετε ότι οι πληρωμές με πιστωτική κάρτα περιλαμβάνουν επιπλέον χρέωση 2,99%, οπότε επιλέγετε να πληρώσετε με άμεση τραπεζική μεταφορά για να λάβετε μια πρόσθετη έκπτωση 5%. Θα λάβετε ένα email επιβεβαίωσης, αλλά όχι το BBQ.

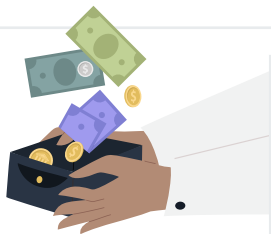
i Πώς ξέρετε ότι αυτό είναι απάτη;

Οι ψεύτικες ιστοσελίδες έχουν τιμές που είναι πολύ καλές για να είναι αληθινές, ασυνήθιστες μεθόδους πληρωμής και άλλα προειδοποιητικά σημάδια, όπως μια διεύθυνση URL που προσπαθεί να μοιάζει με τη διεύθυνση URL ενός επίσημου καταστήματος (για παράδειγμα, webberbbqs.com έναντι του πραγματικού weber.com).

Οι απατεώνες μπορούν επίσης να πληρώσουν για διαφημίσεις στα μέσα κοινωνικής δικτύωσης και τις μηχανές αναζήτησης όπως η Google (γνωστές ως χορηγούμενες διαφημίσεις), γι' αυτό να είστε προσεκτικοί όταν κάνετε κλικ σε αυτούς τους τύπους διαφημίσεων.

10 κορυφαίες συμβουλές για να προστατεύσετε τον εαυτό σας

- 01.** Προσοχή στις κλήσεις από αγνώστους. Αφήστε κλήσεις από αριθμούς τηλεφώνου που δεν αναγνωρίζετε να πάνε στο φωνητικό ταχυδρομείο.



- 02.** Σταματήστε και σκεφτείτε πριν δώσετε προσωπικά ή οικονομικά στοιχεία σε επικοινωνίες με αγνώστους. Αναρωτηθείτε: μπορεί να είναι ψεύτικο;

- 03.** Προσοχή σε email που χρησιμοποιούν τακτικές εκφοβισμού. Ελέγξτε το όνομα και τη διεύθυνση email. Ταιριάζουν αυτά; Για παράδειγμα, το πεδίο 'Από' δείχνει «Υποστήριξη απ' το Amazon», αλλά η διεύθυνση email είναι amazonsupport830@gmail.com



- 04.** Μην εμπιστεύεστε ένα μήνυμα κειμένου μόνο και μόνο επειδή φαίνεται να είναι στο ίδιο νήμα με άλλα μηνύματα από έναν οργανισμό που γνωρίζετε. Θα μπορούσε, παρ' όλα αυτά, να είναι απάτη.

- 05.** Αν δεν είστε σίγουροι για ένα μήνυμα ή μια κλήση που έχετε λάβει, επικοινωνήστε με τον οργανισμό από τον οποίο φαίνεται ότι προέρχεται. Επικοινωνήστε μέσω της επίσημης ιστοσελίδας τους ή ασφαλούς εφαρμογής στο έξυπνο τηλέφωνο ή το tablet σας.

- 06.** Ποτέ μη δίνετε τον κωδικό πρόσβασης, τον κωδικό PIN ή τον κωδικό μίας χρήσης σε κανέναν μέσω τηλεφώνου, ακόμη και αν ισχυρίζεται ότι προέρχεται από την τράπεζά σας ή από κυβερνητικό οργανισμό και διαβάζει πληροφορίες σχετικά με τον λογαριασμό σας.



- 07.** Ποτέ μην κάνετε κλικ σε συνδέσμους που βρίσκονται σε μηνύματα κειμένου. Ενώ είναι πιθανόν ότι μερικοί είναι ακίνδυνοι, είναι καλύτερο να είστε επιφυλακτικοί. Το ίδιο ισχύει και για συνημμένα έγγραφα και συνδέσμους σε email, εκτός αν είστε σίγουροι για τον αποστολέα.

- 08.** Ποτέ μην ακολουθείτε οδηγίες από άγνωστο καλούντα που θέλει να κατεβάσετε μια εφαρμογή ή να εγκαταστήσετε λογισμικό, το οποίο του παρέχει πρόσβαση στη συσκευή σας. Κλείστε το τηλέφωνο αμέσως.

- 09.** Ποτέ μην συνδέεστε στους διαδικτυακούς λογαριασμούς σας μέσω ενός συνδέσμου σε email ή μήνυμα κειμένου. Αντ' αυτού, εισαγάγετε τη διεύθυνση URL της εταιρείας στο πρόγραμμα περιήγησης ή χρησιμοποιήστε την ασφαλή εφαρμογή της για να αποκτήσετε πρόσβαση στον λογαριασμό σας.



- 10.** Πριν κάνετε μια πληρωμή στο διαδίκτυο, να ελέγχετε πάντοτε τη διεύθυνση URL του ιστότοπου (είναι ο επίσημος ιστότοπος;), να προσέχετε για ασυνήθιστες μεθόδους πληρωμής και κακώς διατυπωμένες ή ελλιπείς πληροφορίες στο About Us [Σχετικά με Εμάς], Shipping and Returns [Αποστολή και Επιστροφές] και άλλες ενότητες που βρίσκονται στο κάτω μέρος του ιστότοπου.

Εάν έχετε ποτέ αμφιβολίες, κάντε μια αναζήτηση στο διαδίκτυο εισάγοντας το όνομα του συγκεκριμένου οργανισμού ή του ιστότοπου και τη λέξη «απάτη».

Πιστεύετε ότι έχετε εξαπατηθεί; Πού να πάτε για βοήθεια

Η απάτη μπορεί να έχει οικονομικό και συναισθηματικό κόστος, γι' αυτό είναι σημαντικό να ζητήσετε βοήθεια και να ενεργήσετε γρήγορα. Υπάρχουν διάφορα βήματα που μπορείτε να ακολουθήσετε:

1. Επικοινωνήστε αμέσως με την τράπεζά σας για να σταματήσετε τυχόν περαιτέρω συναλλαγές.
2. Επικοινωνήστε με το IDCARE, μια δωρεάν υπηρεσία υποστήριξης για άτομα που έχουν πέσει θύματα εξαπάτησης ή κλοπής ταυτότητας. Καλέστε το 1800 595 160 ή επισκεφθείτε το idcare.org
3. Αλλάξτε αμέσως τους κωδικούς σας και βεβαιωθείτε ότι είναι ισχυροί.
4. Καταγγίλτε την απάτη στο Scamwatch για να προειδοποιήσετε άλλους: scamwatch.gov.au/report-a-scam
5. Βρείτε υποστήριξη για τον εαυτό σας. Αν δεν αισθάνεστε άνετα να μιλήσετε με τους φίλους ή την οικογένεια, επικοινωνήστε με το Lifeline ή το Beyond Blue για μια εμπιστευτική συνομιλία. Και αν έχετε χάσει ένα σημαντικό ποσό χρημάτων, μιλήστε στην National Debt Helpline (Εθνική Γραμμή Βοήθειας Χρέους).

Beyond Blue: 1300 22 4636 (24/7) ή επισκεφθείτε beyondblue.org.au

Lifeline: 13 11 14 (24/7) ή επισκεφθείτε lifeline.org.au

National Debt Helpline: 1800 007 007 (εργάσιμες ημέρες, 9.30 π.μ. έως 4.30 μ.μ.) ή επισκεφθείτε ndh.org.au

Για περισσότερες πληροφορίες

Κάντε κλικ στα πλακίδια παρακάτω για να εξερευνήσετε:



Το [Little Book of Scams](#) είναι ένα διεθνώς αναγνωρισμένο εργαλείο που θα σας βοηθήσει να μάθετε περισσότερα για μια σειρά από συνήθεις απάτες και πώς μπορείτε να προστατευτείτε από αυτές.

Επισκεφθείτε την ιστοσελίδα [Scamwatch](#) για να μένετε ενημερωμένοι για τις τελευταίες απάτες και για συμβουλές για το πώς να προστατευτείτε από αυτές.



Be Connected
Every Australian online.

Σχετικά με το Be Connected

Το **Be Connected** είναι μια πρωτοβουλία της Αυστραλιανής κυβέρνησης που δεσμεύεται να αναπτύξει τις ψηφιακές δεξιότητες, την εμπιστοσύνη και την διαδικτυακή ασφάλεια των ηλικιωμένων Αυστραλών με δωρεάν μαθήματα υπολογιστών, σύντομα μαθήματα χρήσης του διαδικτύου και πολλά άλλα σχετικά με μια σειρά θεμάτων. **Ο Επίτροπος eSafety [Ηλεκτρονικής Ασφάλειας]** διαχειρίζεται τον ιστότοπο Be Connected και το μαθησιακό περιεχόμενο.



Σχετικά με το Scamwatch

Το **Scamwatch** λειτουργεί από το Εθνικό Κέντρο κατά της Απάτης, το οποίο δημιουργήθηκε για να καταστήσει την Αυστραλία πιο δύσκολο στόχο για τους απατεώνες. Αυξάνει την ευαισθητοποίηση σχετικά με τις απάτες εκπαιδεύοντας την κοινότητα σχετικά με τον τρόπο αναγνώρισης, αποφυγής και καταγγελίας απάτης. Το Anti-Scam Centre κοινοποιεί πληροφορίες από καταγγελίες απάτης και συνεργάζεται με την κυβέρνηση, τις αρχές επιβολής του νόμου και τον ιδιωτικό τομέα για να διακόψει και να αποτρέψει τις απάτες.