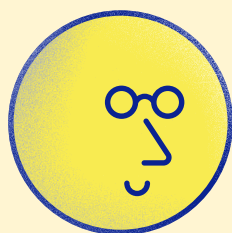


Πώς να εντοπίσετε και να αποφύγετε απάτες



Ο οδηγός σας για να
προστατευτείτε από απάτες



Australian Government



National
Anti-Scam
Centre



ScamWatch
Stop. Better safe than scammed.

Αναγνώριση της χώρας των Ιθαγενών

Η ACCC αναγνωρίζει τους παραδοσιακούς ιδιοκτήτες και θεματοφύλακες της Χώρας σε όλη την Αυστραλία και αναγνωρίζει τη συνεχή σύνδεσή τους με τη γη, τη θάλασσα και την κοινότητα τους. Αποτίνουμε φόρο τιμής σε αυτούς και στους πολιτισμούς τους· και στους Πρεσβύτερους τους του παρελθόντος, του παρόντος και του μέλλοντος.

Australian Competition and Consumer Commission
Ngunnawal
23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

© Κοινοπολιτεία της Αυστραλίας 2023

Αυτό το έργο απολαύει των δικαιωμάτων πνευματικής ιδιοκτησίας. Εκτός από οποιαδήποτε χρήση επιτρέπεται βάσει του νόμου περί πνευματικών δικαιωμάτων του 1968, όλο το υλικό που περιέχεται σε αυτό το έργο παρέχεται υπό την άδεια Creative Commons Australia 4.0 με Αναφορά δημιουργού:

- το Εθνόσημο της Κοινοπολιτείας
- τα λογότυπα ACCC και AER
- οποιαδήποτε απεικόνιση, διάγραμμα, φωτογραφία ή γραφικό επί των οποίων η Αυστραλιανή Επιτροπή Ανταγωνισμού και Καταναλωτών δεν κατέχει πνευματικά δικαιώματα, αλλά το οποίο μπορεί να αποτελεί μέρος ή να περιέχεται σε αυτή την έκδοση.

Οι λεπτομέρειες των σχετικών όρων αδειοδότησης είναι διαθέσιμες στον ιστότοπο Creative Commons, όπως και ο πλήρης νομικός κώδικας για την άδεια CC BY 4.0 AU.

Τα αιτήματα και οι ερωτήσεις σχετικά με την αναπαραγωγή και τα δικαιώματα πρέπει να απευθύνονται στον Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

Προσοχή

Οι πληροφορίες στην παρούσα έκδοση προορίζονται μόνο για γενική καθοδήγηση. Δεν αποτελεί νομική ή άλλη επαγγελματική συμβουλή και δεν πρέπει να χρησιμοποιείται ως δήλωση του νόμου σε οποιαδήποτε δικαιοδοσία. Επειδή προορίζεται μόνο ως γενικός οδηγός, μπορεί να περιέχει γενικεύσεις. Ας πρέπει να λάβετε επαγγελματικές συμβουλές εάν έχετε κάποια συγκεκριμένη αμφιβολία.

Η ACCC έχει καταβάλει κάθε εύλογη προσπάθεια για την παροχή ενημερωμένων και ακριβών πληροφοριών, αλλά δεν παρέχει καμία εγγύηση σχετικά με την ακρίβεια, την επικαιρότητα ή την πληρότητα αυτών των πληροφοριών.

Άτομα που επιθυμούν να αναδημοσιεύσουν ή να χρησιμοποιήσουν με άλλο τρόπο τις πληροφορίες αυτής της δημοσίευσης πρέπει να ελέγξουν αυτές τις πληροφορίες για την επικαιρότητα και την ακρίβειά τους πριν από τη δημοσίευση. Αυτό θα πρέπει να γίνεται πριν από κάθε έκδοση δημοσίευσης, καθώς οι κατευθυντήριες γραμμές της ACCC και η σχετική μεταβατική νομοθεσία αλλάζουν συχνά. Τυχόν απορίες που μπορεί να έχετε θα πρέπει να απευθύνονται στον Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601.

ACCC 05/24_24-13

www.accc.gov.au

Περιεχόμενα

Παρέχουμε και βοήθεια	1
Τι είναι μια απάτη	3
Απλά βήματα για να εντοπίσετε και να αποφύγετε τις απάτες	4
Απάτες email ή SMS	7
Απάτες μέσω email	11
Τηλεφωνικές απάτες	15
Απάτες στον ιστότοπο	19
Απάτες κοινωνικών μέσων, εφαρμογών και διαδικτυακών μηνυμάτων	23
Κορυφαίες απάτες που πρέπει να γνωρίζετε	27
Πού να αναφέρετε απάτες	31
Περισσότερη βοήθεια και υποστήριξη	33



Αυτός ο οδηγός έχει συνταχθεί από το Εθνικό Κέντρο Καταπολέμησης της Απάτης και θα σας βοηθήσει να εντοπίσετε και να προστατευτείτε από τη ζημιά που προκαλείται από απάτες.

Μια απάτη είναι έγκλημα και οι άνθρωποι που κάνουν απάτες είναι εγκληματίες. Πολλοί άνθρωποι στην Αυστραλία εξαπατώνται και χάνουν τα χρήματά τους, μερικές φορές ακόμη και τις αποταμιεύσεις της ζωής τους. Οι απάτες βλάπτουν τις ζωές των ανθρώπων.

Οι απάτες γίνονται όλο και πιο δύσκολο να εντοπιστούν, επομένως πρέπει να συνεργαστούμε για να τις σταματήσουμε.

Το Εθνικό Κέντρο Καταπολέμησης της Απάτης εργάζεται για να κρατήσει τους Αυστραλούς ασφαλείς από απάτες.

Συνεργαζόμαστε με την κυβέρνηση και τη βιομηχανία για να βρούμε νέους τρόπους για να εμποδίσουμε τους απατεώνες να κλέβουν χρήματα και προσωπικές πληροφορίες από τους Αυστραλούς. Σας παρουσιάζουμε μερικούς από τους τρόπους με τους οποίους το επιτυγχάνουμε αυτό.

Σας βοηθάμε να εντοπίζετε και να αποφεύγετε τις απάτες

Μέσω του Scamwatch μοιραζόμαστε ενημερωμένες πληροφορίες σχετικά με απάτες και τρόπους με τους οποίους μπορείτε να προστατευτείτε από απάτες.

Σταματάμε τους απατεώνες

Με το να συλλέγουμε και να κοινοποιούμε πληροφορίες σε ολόκληρο τον κυβερνητικό και τον εμπορικό χώρο, δυσκολεύουμε τους απατεώνες να συνεχίσουν τα εγκλήματά τους και διευκολύνουμε τα θύματα απατών να αναφέρουν απάτες.



Παρέχουμε και βοήθεια

Εάν διαβάζετε αυτό, πιθανότατα είτε εσείς ή κάποιος που γνωρίζετε έχει εξαπατηθεί. Δυστυχώς, δεν είστε ούτε ο μόνος ούτε η μόνη. Οι απάτες είναι όλο και πιο έξυπνες, πράγμα που σημαίνει ότι ο καθένας μας μπορεί να εξαπατηθεί.

Εάν έχετε πέσει θύμα απάτης, είναι απαραίτητο να ενεργήσετε γρήγορα.

Αν έχετε χάσει χρήματα από κάποιον απατεώνα, επικοινωνήστε με την τράπεζα ή τον πάροχο της κάρτας σας.

Επικοινωνήστε με την IDCARE, **1800 595 160**, www.idcare.org.

Οι απάτες πετυχαίνουν επειδή μοιάζουν με την πραγματικότητα. Οι απατεώνες βασίζονται στο ότι δεν αναγνωρίζετε προειδοποιητικά σημάδια επειδή βιάζεστε, δε θέλετε να χάσετε κάποια καλή ευκαιρία ή επειδή φαίνεται ότι προέρχεται από άτομο που εμπιστεύεστε.

Προστατευτείτε από απάτες ακολουθώντας αυτά τα τρία (3) βήματα:

ΣΤΑΜΑΤΗΣΤΕ Μην δίνετε χρήματα ή προσωπικές πληροφορίες σε κανέναν εάν δεν είστε σίγουροι.



Οι απατεώνες θα προσφερθούν να σας βοηθήσουν ή να σας ζητήσουν να επαληθεύσετε την ταυτότητά σας. Θα προσποιηθούν ότι προέρχονται από οργανισμούς που γνωρίζετε και εμπιστεύεστε, όπως οι πάροχοι υπηρεσιών, η αστυνομία, η τράπεζά σας ή οι κυβερνητικές υπηρεσίες.

ΕΛΕΓΞΤΕ



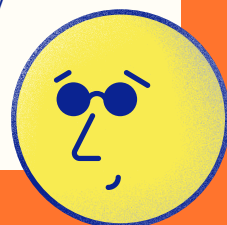
Ρωτήστε τον εαυτό σας - θα μπορούσε το μήνυμα ή η κλήση να είναι ψεύτικη;

Μην κάνετε ποτέ κλικ σε σύνδεσμο σε ένα μήνυμα. Επικοινωνήστε μόνο με επιχειρήσεις ή κυβερνήσεις χρησιμοποιώντας τα στοιχεία επικοινωνίας που βρίσκετε από τον επίσημο ιστότοπο ή στην εφαρμογή τους. Εάν δεν είστε βέβαιοι, πείτε «όχι», κλείστε το τηλέφωνο ή διαγράψτε το μήνυμα.

ΑΝΑΦΕΡΕΤΕ Ενεργήστε γρήγορα αν κάτι σας φαίνεται ύποπτο.



Επικοινωνήστε με την τράπεζά σας εάν παρατηρήσετε ασυνήθιστη δραστηριότητα ή εάν ένας απατεώνας πάρει τα χρήματα ή τα στοιχεία σας. Ζητήστε βοήθεια και αναφέρετε την απάτη στο ReportCyber και στο Scamwatch. Όταν αναφέρετε απάτες, βοηθάτε όλους τους Αυστραλούς ενισχύοντας έτσι την άμυνά μας εναντίον απατών.



Τι είναι μια απάτη

Μια απάτη είναι όταν κάποιος σας εξαπατά για να κλέψει τα χρήματα ή τα προσωπικά σας στοιχεία.

Οι απάτες είναι οικονομικά εγκλήματα που διαπράττονται από εγκληματίες που είναι συχνά πολύ οργανωμένοι και τεχνικά εξελιγμένοι.

Απάτες:

-  διαπράττονται από
-  εγκληματίες
-  φαίνονται αληθινές
-  παρουσιάζονται με πιστευτές ιστορίες σας πιέζουν να προβείτε σε κάποια ενέργεια

Μια απάτη ΔΕΝ είναι:

-  Ηλεκτρονική πειρατεία
-  Καταχρηστικές συμβατικές ρήτρες (unfair contract terms)
-  Παρενοχλητικές προσεγγίσεις μάρκετινγκ

Έχετε πάντα υπόψη ότι οι αρνητικές εμπειρίες δεν είναι όλες απάτες. Μπορεί να έχετε πληρώσει για ένα προϊόν που ποτέ δεν λάβατε ή αγοράσατε κάτι και διαπιστώσατε ότι η ποιότητα ήταν κακή. Αν και αυτό είναι απογοητευτικό, δεν πρόκειται απαραίτητα για απάτη. Ο Νόμος περί Καταναλωτών Αυστραλίας προσφέρει προστασία στους Αυστραλούς καταναλωτές για τέτοιου είδους ζητήματα.

Για περισσότερες πληροφορίες επισκεφθείτε www.accc.gov.au/consumers

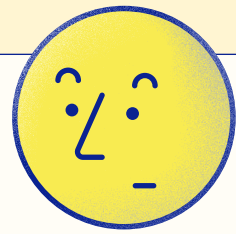
Απλά βήματα για να εντοπίσετε και να αποφύγετε τις απάτες

Οι απάτες μπορούν να συμβούν σε όλους μας. Οι απάτες πετυχαίνουν επειδή οι απατεώνες δημιουργούν πιστευτές ιστορίες για να κλέψουν τα χρήματά σας και να αποκτήσουν τα προσωπικά σας στοιχεία.

Οι απατεώνες γίνονται όλο και πιο έξυπνοι και εκμεταλλεύονται τη νέα τεχνολογία, τα προϊόντα, τις υπηρεσίες και τα σημαντικότερα γεγονότα για να σας πείσουν ότι οι απάτες τους είναι πραγματικές.

Μπορεί να είναι πολύ δύσκολο να εντοπίσετε μια απάτη. Ακολουθούν ορισμένες περιστάσεις που πρέπει να προσέχετε. Μερικές φορές οι απατεώνες χρησιμοποιούν έναν συνδυασμό αυτών των τακτικών.

- 1. Ευκαιρίες για να κερδίσετε ή να εξοικονομήσετε χρήματα:** Οι απατεώνες θα σας εξαπατήσουν να πιστέψετε ότι θα πάρετε μια απίστευτη ευκαιρία ή προσφορά. Θα σας ασκήσουν πίεση να ενεργήσετε γρήγορα, ώστε να μην χάσετε. Θυμηθείτε, οι προσφορές που φαίνονται εξαιρετικά καλές, συνήθως δεν είναι αληθινές.
- 2. Θλιβερές ιστορίες και κραυγές για βοήθεια:** Οι απατεώνες θα προσπαθήσουν να χρησιμοποιήσουν τον καλό σας χαρακτήρα εναντίον σας. Θα μοιραστούν μαζί σας ιστορίες αποτυχίας και τραγωδίας και θα σας εξηγήσουν γιατί χρειάζονται τη βοήθειά και τα χρήματά σας.
- 3. Σύνδεσμοι και συνημμένα:** Οι απατεώνες χρησιμοποιούν συνδέσμους για να σας στείλουν σε ιστότοπους απάτης που έχουν σχεδιαστεί για να κλέψουν τις πληροφορίες και τα χρήματά σας. Οι απατεώνες μπορεί επίσης να σας ζητήσουν να ανοίξετε τα συνημμένα. Αυτά μπορούν να εγκαταστήσουν ιούς που κλέβουν τις πληροφορίες σας.



4. **Πίεση για να ενεργήσετε γρήγορα:** Οι απατεώνες δεν θέλουν να ζητήσετε χρόνο και να σκεφτείτε καλά τα πράγματα. Θέλουν να σας πιέσουν να ενεργήσετε γρήγορα. Μεταξύ άλλων, μπορεί να σας απειλήσουν ότι κάτι κακό θα συμβεί αν δεν ενεργήσετε γρήγορα.
5. **Αιτήματα για πληρωμή με ασυνήθιστους ή συγκεκριμένους τρόπους:** Οι απατεώνες συχνά σας ζητούν να πληρώσετε χρησιμοποιώντας ασυνήθιστες μεθόδους, όπως προφορτωμένες χρεωστικές κάρτες, κάρτες iTunes ή εικονικό νόμισμα όπως το Bitcoin. Μόλις δαπανηθούν αυτά τα χρήματα, δεν μπορείτε να τα πάρετε πίσω.
6. **Αίτημα να δημιουργήσετε καινούριους λογαριασμούς ή PayID:** Οι απατεώνες μπορεί να σας ζητήσουν να δημιουργήσετε έναν καινούριο τραπεζικό λογαριασμό ή PayID για να τους πληρώσετε (ή να πληρωθείτε από αυτούς). Μπορεί να προσποιούνται ότι είναι από την τράπεζά σας και να σας λένε να μεταφέρετε τα χρήματά σας σε καινούριους λογαριασμούς για την εξασφάλισή τους.

Εάν οι απατεώνες καταφέρουν να πάρουν τα χρήματά σας, θα προσπαθήσουν να πάρουν περισσότερα χρήματα από εσάς. Δυστυχώς, το ένα στα τρία θύματα απάτης έχει εξαπατηθεί περισσότερες από μία φορές. Εάν έχετε χάσει χρήματα από μια απάτη, να είστε σε επιφυλακή για απατεώνες που προσφέρονται να σας βοηθήσουν να πάρετε τα χρήματά σας πίσω. Αυτό αποτελεί άλλο είδος επακόλουθης απάτης.



Απάτες email ή SMS

Οι απατεώνες στέλνουν μηνύματα που προσποιούνται ότι προέρχονται από την κυβέρνηση, τις διωκτικές αρχές, αξιόπιστες επιχειρήσεις ή ακόμα και την οικογένεια ή τους φίλους σας.

Αυτά τα μηνύματα θα φαίνονται επείγοντα και θα προσπαθήσουν να σας κάνουν να ενεργήσετε γρήγορα. Συχνά θα έχουν έναν σύνδεσμο που θα σας μεταφέρει σε έναν ιστότοπο απάτης. Οι απατεώνες μπορούν να κλέψουν τυχόν προσωπικές πληροφορίες που εισάγονται σε αυτούς τους ιστότοπους απάτης και να τις χρησιμοποιήσουν για να πάρουν τα χρήματά σας ή να διαπράξουν απάτη στο όνομά σας.

Για να φαίνονται αληθινά αυτά τα μηνύματα, οι απατεώνες αντιγράφουν ή συγκαλύπτουν τον αριθμό τηλεφώνου τους πίσω από τον αριθμό τηλεφώνου και την αναγνώριση κλήσης νόμιμων επιχειρήσεων ή ατόμων που γνωρίζετε.

Τα μηνύματα απάτης μπορούν ακόμη και να εμφανίζονται στην ίδια αλυσίδα μηνυμάτων με τα πραγματικά μηνύματα από τον οργανισμό, καθιστώντας ακόμη πιο δύσκολο τον εντοπισμό τους.

Ενδείξεις ότι ένα μήνυμα μπορεί να είναι απάτη

Το μήνυμα:



Σας ζητά να προβείτε σε άμεσες ενέργειες, να πραγματοποιήσετε μια πληρωμή ή να μεταφέρετε χρήματα.



Σας ζητά να κάνετε κλικ σε έναν σύνδεσμο ή να καλέσετε έναν αριθμό που στέλνεται με το μήνυμα.



Σας ζητά να συνδεθείτε σε έναν ηλεκτρονικό λογαριασμό με το όνομα χρήστη και τον κωδικό πρόσβασής σας ή να δώσετε άλλες προσωπικές πληροφορίες.



Προέρχεται από μέλος της οικογένειας ή φίλο σας που λέει ότι τα στοιχεία επικοινωνίας τους έχουν αλλάξει.



Απειλεί να διακόψει μια υπηρεσία ή να σας χρεώσει εάν δεν ενεργήσετε.



Υποδηλώνει ότι εσείς ή οι λογαριασμοί σας έχετε παραβιαστεί ή έχετε εμπλακεί σε απάτη.



Υποδηλώνει ότι υπάρχει πρόβλημα με την πληρωμή σας ή την παράδοση του πακέτου σας.

Βήματα για να προστατευτείτε από απάτες μηνυμάτων

1. Αν κάποιος γνωστός σας στείλει μήνυμα για να πει ότι έχει καινούριο αριθμό τηλεφώνου:



- α. προσπαθήστε να τον καλέσετε στον υπάρχοντα αριθμό που έχετε για το άτομο αυτό, και
- β. στείλτε του μήνυμα στον καινούριο αριθμό με μια ερώτηση στην οποία μόνο αυτός θα ξέρει την απάντηση, για να βεβαιωθείτε ότι είναι όντως ο ίδιος.



2. Ποτέ μην κάνετε κλικ σε συνδέσμους σε μηνύματα.



3. Εάν ένα μήνυμα οδηγεί σε έναν ιστότοπο, μην κάνετε κλικ στον σύνδεσμο. Αναζητήστε καλύτερα τον ιστότοπο μόνος σας ή χρησιμοποιήστε την επίσημη εφαρμογή.



4. Μην απαντάτε σε μήνυμα τηλεφώνου χρησιμοποιώντας τον αριθμό τηλεφώνου που παρέχεται.



5. Καλέστε ξανά τον οργανισμό ή το άτομο σε έναν αριθμό τηλεφώνου που βρήκατε, όπως από τον ιστότοπο του οργανισμού.



Απάτες μέσω email

Οι απατεώνες στέλνουν μηνύματα email που προσποιούνται ότι προέρχονται από την κυβέρνηση, τις διωκτικές αρχές και από επιχειρήσεις. Παρουσιάζουν το θέμα ως επείγον για να σας κάνουν να δράσετε γρήγορα.

Οι απατεώνες χρησιμοποιούν το ίδιο λογότυπο και παρόμοια διεύθυνση email με τον πραγματικό οργανισμό. Οι απατεώνες μπορούν επίσης να αντιγράψουν ή να κρύψουν τη διεύθυνση email τους πίσω από τη διεύθυνση email ενός οργανισμού ή μιας επιχείρησης για να κάνουν το μήνυμα email απάτης να φαίνεται πιο ρεαλιστικό.

Ενδείξεις ότι ένα email μπορεί να είναι απάτη

Το email:



Ζητά πληρωμή, αλλά τα στοιχεία του λογαριασμού είναι καινούρια ή έχουν αλλάξει από την τελευταία πληρωμή που κάνατε.



Σας ζητά να συνδεθείτε σε έναν ηλεκτρονικό λογαριασμό με το όνομα χρήστη και τον κωδικό πρόσβασής σας ή να δώσετε άλλες προσωπικές πληροφορίες.



Ήταν απρόσμενο και περιλαμβάνει ένα συνημμένο με πρόσκληση να το ανοίξετε.



Σας ζητά να επιβεβαιώσετε τα τραπεζικά σας στοιχεία για να λάβετε επιστροφή χρημάτων ή χρήματα που δεν περιμένατε.



Ισχυρίζεται ότι έχει πληροφορίες σχετικά με εσάς ή εικόνες σας και απειλεί να τις δημοσιοποιήσει.



Σας προσφέρει βοήθεια για να ανακτήσετε χρήματα ή να πάρετε αποζημίωση για παραβίαση δεδομένων ή κλοπή ταυτότητας.

Βήματα που μπορείτε να ακολουθήσετε για να προστατευτείτε από απάτες μέσω email

1. Βεβαιωθείτε ότι το μήνυμα email είναι πραγματικό ως εξής:



- α. επικοινωνώντας απευθείας με το πρόσωπο ή τον οργανισμό χρησιμοποιώντας τα στοιχεία επικοινωνίας που βρήκατε, όπως από τον ιστότοπο του οργανισμού ή
- β. κάνοντας πρόσβαση σε έναν οργανισμό μέσω της επίσημης εφαρμογής του (ποτέ μέσω συνδέσμου).



2. Διακόψτε αμέσως την επαφή με οποιοδήποτε άτομο που προσπαθεί να σας απειλήσει ή να σας εκφοβίσει.



3. Ποτέ μην δίνετε προσωπικά στοιχεία και μην πληρώνετε κανέναν που σας προσφέρει:
 - α. αποζημίωση ή βοήθεια για την ανάκτηση από προηγούμενη απάτη ή παραβίαση δεδομένων ή,
 - β. κέρδη, δώρα ή κληρονομιά.



4. Χρησιμοποιήστε έλεγχο ταυτότητας πολλών παραγόντων όταν μπορείτε. Παρέχει ένα επιπλέον επίπεδο προστασίας και σημαίνει ότι ένας απατεώνας πρέπει να γνωρίζει τον κωδικό πρόσβασης email σας και έναν αριθμό PIN που αποστέλλεται στο τηλέφωνό σας για να αποκτήσει πρόσβαση στο λογαριασμό email σας.



Τηλεφωνικές απάτες

Οι απατεώνες τηλεφωνούν, ισχυριζόμενοι ότι είναι από γνωστούς οργανισμούς.

Αυτό περιλαμβάνει κυβερνητικούς οργανισμούς, διωκτικές αρχές, επενδυτικές και δικηγορικές εταιρείες, τράπεζες και παρόχους τηλεπικοινωνιών.

Σας το παρουσιάζουν με τρόπο που να φαίνεται επείγον να σας κάνουν να ενεργήσετε γρήγορα. Μπορεί να προσπαθήσουν να σας πείσουν να τους δώσετε τα προσωπικά ή τραπεζικά σας στοιχεία ή πρόσβαση στον υπολογιστή σας.

Ο καλών μπορεί να έχει ήδη κάποιες λεπτομέρειες σχετικά με εσάς, όπως το όνομα ή τη διεύθυνσή σας, κάνοντας την κλήση να φαίνεται πραγματική.

Ενδείξεις ότι μια τηλεφωνική κλήση μπορεί να είναι απάτη

Αυτός που καλεί:



Ζητά πληρωμή ή σας ζητά να μεταφέρετε χρήματα σε καινούριο λογαριασμό.



Σας ζητά τον κωδικό πρόσβασης, το PIN, τον κωδικό μίας χρήσης ή ορισμένες άλλες πληροφορίες ασφαλείας.



Σας ζητά τα οικονομικά σας στοιχεία, όπως στοιχεία της πιστωτικής σας κάρτας ή τα τραπεζικά σας στοιχεία.



Σας ζητά να ολοκληρώσετε μια ενέργεια στο κινητό τηλέφωνο ή τον υπολογιστή σας, όπως η εγκατάσταση λογισμικού ή πρόσβαση σε ασφαλή λογαριασμό.



Ισχυρίζεται ότι προέρχεται από τις διωκτικές αρχές και σας απειλεί με άμεση σύλληψη ή απέλαση.



Λέει ότι η τράπεζά σας ή άλλοι διαδικτυακοί λογαριασμοί έχουν παραβιαστεί ή έχουν εμπλακεί σε απάτη.

Βήματα που μπορείτε να ακολουθήσετε για να προστατευτείτε από τηλεφωνικές απάτες

1. Βεβαιωθείτε ότι η κλήση είναι πραγματική είτε:



- α. επικοινωνώντας απευθείας με το πρόσωπο ή τον οργανισμό χρησιμοποιώντας τα στοιχεία επικοινωνίας που βρήκατε, όπως από τον ιστότοπο του οργανισμού ή
- β. κάνοντας πρόσβαση σε έναν οργανισμό μέσω της επίσημης εφαρμογής του (ποτέ μέσω συνδέσμου).



2. Εάν δεν είστε σίγουροι ποιος είναι ο καλών ή αν σας απειλεί ή σας εκφοβίζει, κλείστε αμέσως το τηλέφωνο.



3. Ποτέ μην εγκαθιστάτε λογισμικό που επιτρέπει σε κάποιον να έχει πρόσβαση στον υπολογιστή ή τη συσκευή σας.



4. Αγνοήστε κλήσεις από αριθμούς που δεν γνωρίζετε ή αφήστε τις κλήσεις να πηγαίνουν στον τηλεφωνητή.



Καλό είναι να γνωρίζετε!

Μπορεί να εξακολουθείτε να δέχετε κλήσεις απάτης ακόμα κι αν έχετε ιδιωτικό αριθμό τηλεφώνου ή είστε στο μητρώο Do Not Call.



Απάτες στον ιστότοπο

Οι απατεώνες μπορούν να προσποιηθούν ότι είναι οποιοσδήποτε που δρα στο διαδίκτυο, συμπεριλαμβανομένης της κυβέρνησης, μιας πραγματικής επιχείρησης, διασημοτήτων ή φίλων ή της οικογένειάς σας.

Μπορούν να δημιουργήσουν ψεύτικους ιστότοπους για να μοιάζουν με αυτούς των γνωστών εταιρειών. Μπορεί να υποδύονται διάσημους ανθρώπους και να φαίνεται ότι εγκρίνουν αγαθά ή υπηρεσίες. Αυτοί οι ιστότοποι μπορεί να περιέχουν ψευδείς κριτικές για να σας κάνουν να τους εμπιστευέστε.

Μπορεί να δείτε ψεύτικα διαφημιστικά banner ή αναδυόμενα παράθυρα που περιέχουν ψεύτικες προειδοποιήσεις ή μηνύματα σφάλματος όταν είστε συνδεδεμένοι στο διαδίκτυο.

Ενδείξεις ότι ένας ιστότοπος μπορεί να είναι απάτη

Ο ιστότοπος:



Προσφέρει είδη προς πώληση σε σημαντικά χαμηλότερες τιμές από τη συνηθισμένη ή σε σύγκριση με άλλους ιστότοπους.



Σας λέει για έναν τρόπο να κερδίσετε χρήματα γρήγορα, εύκολα και με ελάχιστο κίνδυνο ή προσπάθεια.



Περιέχει μια επείγουσα προειδοποίηση ή ένα μήνυμα σφάλματος που σας ζητά να κάνετε κλικ σ' έναν σύνδεσμο.



Ζητά πληρωμή με ασυνήθιστους ή συγκεκριμένους τρόπους, όπως δωροκάρτες ή κρυπτονομίσματα όπως το Bitcoin.



Περιλαμβάνει μόνο θετικές κριτικές.

Βήματα που μπορείτε να ακολουθήσετε για να αποφύγετε απάτες σε ιστότοπους



1. Συγκρίνετε τις τιμές. Εάν μια προσφορά φαίνεται ότι δεν μπορεί να είναι αληθινή, πιθανό να μην είναι αληθινή.



2. Ερευνήστε τον οργανισμό ή το άτομο με το οποίο κάνετε τη συναλλαγή πριν δώσετε τα χρήματα ή τα προσωπικά σας στοιχεία.



3. Μην βασίζεστε σε κριτικές που αναρτώνται στον ίδιο τον ιστότοπο. Ερευνήστε τον ιστότοπο ή το όνομα της επιχείρησης και τη λέξη «απάτη» ή «κριτικές».



4. Εάν εμφανιστεί μια προειδοποίηση ή ένα μήνυμα σφάλματος στην οθόνη σας, μην κάνετε κλικ, μεταβείτε απευθείας στην εφαρμογή στην οποία αναφέρεται για να βεβαιωθείτε αν είναι πραγματική.



5. Διατηρήστε ενημερωμένη τη συσκευή που χρησιμοποιείτε για ηλεκτρονικές αγορές, ενεργοποιώντας τις «αυτόματες ενημερώσεις» για το λειτουργικό σύστημα και τις εφαρμογές σας.



Καλό είναι να γνωρίζετε!

Θα βρείτε πρακτικούς τρόπους για να προστατευτείτε στο διαδίκτυο στο www.cyber.gov.au



Απάτες κοινωνικών μέσων, εφαρμογών και διαδικτυακών μηνυμάτων

Εάν κάποιος που δεν γνωρίζετε επικοινωνήσει μαζί σας στα μέσα κοινωνικής δικτύωσης, σε μια πλατφόρμα ανταλλαγής μηνυμάτων όπως το WhatsApp ή το WeChat ή μέσω μιας εφαρμογής, θα μπορούσε να είναι απάτη.

Οι απατεώνες που προσποιούνται ότι είναι κάποιος άλλος χρησιμοποιούν συχνά την πραγματική φωτογραφία του ατόμου ή το επίσημο λογότυπο του οργανισμού που προσποιούνται ότι είναι, για να κάνουν την απάτη πιο δύσκολη να εντοπιστεί.

Οι απατεώνες στα μέσα κοινωνικής δικτύωσης θα δημιουργήσουν ψεύτικα προφίλ και θα προσποιηθούν ότι προέρχονται από την κυβέρνηση, μια πραγματική επιχείρηση, εργοδότη, εταιρεία επενδύσεων ή ακόμα και φίλο, ή μέλος της οικογένειας ή κάποιο ρομαντικό ενδιαφέρον.

Μπορεί να υποδύονται διάσημους ανθρώπους και να φαίνεται ότι προωθούν προϊόντα ή υπηρεσίες.

Οι απατεώνες μπορούν επίσης να μάθουν πολλά για εσάς από λεπτομέρειες που μοιράζεστε στους λογαριασμούς σας στα μέσα κοινωνικής δικτύωσης. Μπορούν να χρησιμοποιήσουν αυτές τις πληροφορίες για να μαντέψουν τους κωδικούς πρόσβασης του λογαριασμού σας ή να σας στοχεύσουν με άλλες απάτες.

Ενδείξεις απάτης στα μέσα κοινωνικής δικτύωσης ή σε εφαρμογές

Το προφίλ ή η εφαρμογή μέσων κοινωνικής δικτύωσης:



Σας λέει για έναν τρόπο να κερδίσετε χρήματα γρήγορα, εύκολα και με ελάχιστο κίνδυνο ή προσπάθεια.



Σας προσκαλεί να συμμετάσχετε σε διαγωνισμό ή προσφορά περιορισμένου χρόνου.



Σας ζητά να μεταφέρετε μια συνομιλία από μια εφαρμογή, όπως μια εφαρμογή γνωριμιών, σε ιδιωτική συνομιλία ή email.



Προτείνει ένα διάσημο άτομο να εγκρίνει ή να υποστηρίξει ένα προϊόν ή μια υπηρεσία.



Λέει ότι κάποιος θα αγοράσει κάτι που πουλάτε χωρίς να το δει πρώτα και σε υψηλή τιμή.



Απειλεί να μοιραστεί μια ιδιωτική φωτογραφία σας αν δεν τους πληρώσετε χρήματα.



Επικοινωνεί μαζί σας για να σας προσφέρει δουλειά.



Καλό είναι να γνωρίζετε!

Πληροφορίες σχετικά με το πώς να παραμείνετε ασφαλείς σε διαφορετικές πλατφόρμες κοινωνικών μέσων μπορείτε να βρείτε στο www.esafety.gov.au

Βήματα που μπορείτε να ακολουθήσετε για να αποφύγετε απάτες στα μέσα κοινωνικής δικτύωσης και σε εφαρμογές



1. Ελέγξτε αν το προφίλ μπορεί να είναι ψεύτικο. Είναι ενεργός ο λογαριασμός; Πόσους φίλους/γνωστούς έχουν και πόσο συχνά δημοσιεύουν στο διαδίκτυο;



2. Αναζητήστε το όνομα του προφίλ στο διαδίκτυο μαζί με τη λέξη «απάτη».



3. Ποτέ να μην δεχθείτε μια δουλειά που σας προσφέρθηκε χωρίς συνέντευξη ή συζήτηση σχετικά με την εμπειρία, την καταλληλότητα και τις συστάσεις σας. Ερευνήστε τον υπεύθυνο προσλήψεων και την επιχείρηση ή το άτομο που προσφέρει τη θέση. Επικοινωνήστε με το γραφείο ευρέσεως εργασίας μέσω τηλεφώνων που προέρχονται μετά από ανεξάρτητη αναζήτηση στο διαδίκτυο. Μην πληρώνετε χρήματα εκ των προτέρων μόνο και μόνο για να εξασφαλίσετε μια δουλειά.



4. Ζητήστε επενδυτικές συμβουλές μόνο από κάποιον με άδεια Αυστραλιανών Χρηματοπιστωτικών Υπηρεσιών και βεβαιωθείτε ότι μια εταιρεία ή ένας ιστότοπος δεν κατονομάζεται στην πύλη ειδοποιήσεων επενδυτών του Διεθνούς Οργανισμού Επιτροπών Κεφαλαιαγοράς (IOSCO).



5. Ποτέ μην δίνετε χρήματα σε ένα άτομο που έχετε γνωρίσει μόνο στο διαδίκτυο. Οι απατεώνες συχνά λένε ότι ζουν στο εξωτερικό και δεν μπορούν να σας συναντήσουν αυτοπροσώπως.



6. Ποτέ μην στέλνετε προσωπικές φωτογραφίες του εαυτού σας σε κάποιον που έχετε γνωρίσει μόνο στο διαδίκτυο.

Για περισσότερες πληροφορίες σχετικά με τις απάτες, συμπεριλαμβανομένων άλλων τρόπων με τους οποίους οι απατεώνες μπορούν να επικοινωνήσουν μαζί σας, όπως αυτοπροσώπως και μέσω ταχυδρομείου, επισκεφτείτε το [Scamwatch](#).



Κορυφαίες απάτες που πρέπει να γνωρίζετε

Ακολουθούν μερικοί από τους πιο συνηθισμένους τύπους απάτης που πρέπει να γνωρίζετε.

Μπορείτε να βρείτε περισσότερες πληροφορίες για καθέναν από αυτούς τους τύπους απάτης, συμπεριλαμβανομένων προειδοποιητικών ενδείξεων και βημάτων για την προστασία σας, στον ιστότοπο [Scamwatch](#).

Απάτες πλαστοπροσωπίας

Οι απατεώνες προσπαθούν να σας πείσουν ότι προέρχονται από αξιόπιστους οργανισμούς όπως η αστυνομία, η κυβέρνηση, οι τράπεζες και γνωστές επιχειρήσεις. Μπορούν ακόμη και να προσποιούνται ότι είναι φίλοι ή μέλη της οικογένειάς σας. Οι απατεώνες αναζητούν πληροφορίες σχετικά με εσάς στέλνοντας email «ψαρέματος» ή μηνύματα ηλεκτρονικού «ψαρέματος». Αυτά έχουν σκοπό να κλέψουν τις πληροφορίες σας. Προσπαθούν να σας πείσουν να τους δώσετε τα προσωπικά σας στοιχεία προσποιούμενοι ότι προέρχονται από κάποιον επίσημο οργανισμό ή κάποιο άτομο που γνωρίζετε και εμπιστεύεστε.

Οι απατεώνες χρησιμοποιούν την τεχνολογία για να κάνουν τις κλήσεις ή τα μηνύματά τους να φαίνονται ότι προέρχονται από έναν νόμιμο αριθμό τηλεφώνου. Μπορούν να κάνουν τα μηνύματα κειμένου να εμφανίζονται στο ίδιο νήμα συνομιλίας με γνήσια μηνύματα από έναν οργανισμό.

Επενδυτικές απάτες

Οι απατεώνες χρησιμοποιούν πειστικό μάρκετινγκ και νέα τεχνολογία για να κάνουν την επενδυτική τους πρόταση να φαίνεται πολύ καλή και για να μη χάσετε την ευκαιρία. Σας υπόσχονται μεγάλα κέρδη με μικρό ή καθόλου κίνδυνο. Συχνά χρησιμοποιούν τακτικές πίεσης για να σας κάνουν να ενεργήσετε γρήγορα, ώστε να μπορούν να κλέψουν τα χρήματά σας.

Απάτες εργασίας και απασχόλησης

Οι απατεώνες προσφέρουν θέσεις εργασίας που πληρώνουν καλά με ελάχιστη προσπάθεια. Προσποιούνται ότι προσλαμβάνουν για λογαριασμό εταιρειών υψηλού προφίλ και διαδικτυακών πλατφορμών αγορών. Μερικές φορές, η δουλειά που περιγράφουν δεν υπάρχει καν. Οι απατεώνες πλαστοπροσωπούν επίσης γνωστά πρακτορεία προσλήψεων. Στόχος τους είναι να κλέψουν τα χρήματα και τα προσωπικά σας στοιχεία. Μπορεί να σας ζητήσουν να πληρώσετε χρήματα εκ των προτέρων για να μπορέσετε να εργαστείτε γι' αυτούς.

Απάτες προϊόντων και υπηρεσιών

Οι απατεώνες παρουσιάζονται ως αγοραστές ή πωλητές για να κλέψουν τα χρήματά σας. Δημιουργούν ψεύτικους ιστότοπους ή προφίλ σε νόμιμους ιστότοπους λιανικής πώλησης που προσφέρουν προϊόντα ή υπηρεσίες σε τιμές που είναι τόσο καλές που αδυνατούν να είναι αληθινές. Δημοσιεύουν ψεύτικες διαφημίσεις και ψεύτικες κριτικές. Μπορεί να χρησιμοποιούν κλεμμένα λογότυπα, ένα όνομα domain .com.au και κλεμμένο Αυστραλιανό Αριθμό Επιχείρησης (ABN). Αυτές οι απάτες είναι δύσκολο να εντοπιστούν.

Οι απατεώνες παρουσιάζονται επίσης ως επιχειρήσεις που γνωρίζετε και εμπιστεύεστε για να σας στείλουν ψεύτικους λογαριασμούς. Μπορούν ακόμη και να αλλάξουν τα στοιχεία των νόμιμων τιμολογίων, έτσι ώστε οι πελάτες να καταλήξουν να πληρώνουν τον απατεώνα αντί για εσάς.

Ρομαντικές απάτες

Οι απατεώνες χρησιμοποιούν την υπόσχεση της αγάπης, των ραντεβού ή της φιλίας για να κλέψουν τα χρήματά σας. Κάνουν τα πάντα για να σας πείσουν ότι η σχέση είναι πραγματική και σας εκμεταλλεύονται για να τους δώσετε χρήματα.

Οι απατεώνες σας βρίσκουν σε μέσα κοινωνικής δικτύωσης, εφαρμογές γνωριμιών ή παιχνιδιών και σε ιστότοπους. Μπορεί επίσης να σας στείλουν μήνυμα κειμένου ή email. Κρύβονται πίσω από ψεύτικα προφίλ και ταυτότητες, μερικές φορές και διάσημων ανθρώπων. Μόλις τους εμπιστευτείτε, θα έχουν μια «έκτακτη ανάγκη» και θα ζητήσουν τη βοήθειά σας. Συχνά ζητούν χρήματα ή άλλα προϊόντα.

Απειλές και απάτες εκβιασμού

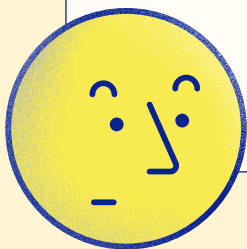
Οι απατεώνες προσποιούνται ότι προέρχονται από έναν αξιόπιστο οργανισμό και ισχυρίζονται ότι πρέπει να πληρώσετε χρήματα, διαφορετικά θα σας συμβεί κάτι κακό. Μπορεί να σας απειλήσουν με σύλληψη, απέλαση ή ακόμα και σωματική βλάβη, εάν δεν συμφωνήσετε να τους πληρώσετε αμέσως.

Μπορούν επίσης να σας εκβιάσουν απειλώντας να κοινοποιήσουν γυμνές φωτογραφίες ή βίντεο που τους έχετε στείλει, εκτός εάν τους στείλετε χρήματα.

Απροσδόκητες απάτες χρημάτων

Οι απατεώνες προσπαθούν να σας πείσουν ότι σας οφείλονται ή δικαιούστε χρήματα ή κέρδη που δεν περιμένατε να λάβετε.

Ο απατεώνας σας ζητά να πληρώσετε ένα τέλος ή να δώσετε τα τραπεζικά σας στοιχεία ή τα στοιχεία ταυτότητάς σας προτού μπορέσετε να πάρετε τα χρήματα ή τα κέρδη. Δυστυχώς, δεν υπάρχουν δωρεάν χρήματα.





Πού να αναφέρετε απάτες

Προσπαθούμε να κάνουμε την Αυστραλία δυσκολότερο στόχο για τους απατεώνες, αυξάνοντας την ευαισθητοποίηση σχετικά με τον τρόπο αναγνώρισης, αποφυγής και αναφοράς των απατών.

Κοινοποιούμε πληροφορίες από αναφορές απάτης και συνεργαζόμαστε με την κυβέρνηση, τις διωκτικές αρχές και τον ιδιωτικό τομέα για να διακόψουμε και να αποτρέψουμε τις απάτες.

Βοηθήστε άλλους υποβάλλοντας αναφορές στο Scamwatch. Αναφέρετε την εμπειρία απάτης σας μέσω της φόρμας αναφοράς στον ιστότοπο Scamwatch www.scamwatch.gov.au

Θυμηθείτε, εάν είστε θύμα απάτης, είναι απαραίτητο να ενεργήσετε γρήγορα.

- Αν έχετε χάσει χρήματα από κάποιον απατεώνα, επικοινωνήστε με την τράπεζα ή τον πάροχο της κάρτας σας.
- Τηλεφωνήστε στο ID CARE: 1800 595 160 | idcare.org



Περισσότερη βοήθεια και υποστήριξη

Το να είσαι θύμα απάτης μπορεί να είναι μια συντριπτική εμπειρία. Είναι απαραίτητο να θυμάστε ότι μπορεί να συμβεί σε οποιονδήποτε αλλά ότι υπάρχει βοήθεια.

Εάν εσείς ή κάποιος που γνωρίζετε έχει πέσει θύμα απάτης, μιλήστε σε κάποιον για αυτό. Μπορείτε να ζητήσετε υποστήριξη από την οικογένεια, τους φίλους, τον γιατρό σας ή μία από τις ακόλουθες υπηρεσίες υποστήριξης.

Lifeline: 13 11 14 | lifeline.org.au

ή διαδικτυακή συνομιλία υποστήριξης κρίσεων (24 ώρες την ημέρα, 7 ημέρες την εβδομάδα)

Beyond Blue: 1300 22 4636 | beyondblue.org.au

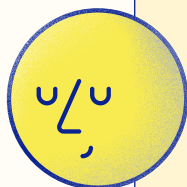
ή διαδικτυακή συνομιλία (24 ώρες την ημέρα, 7 ημέρες την εβδομάδα)

Kids Helpline: 1800 55 1800 | kidshelpline.com.au

(24 ώρες την ημέρα, 7 ημέρες την εβδομάδα)

Οι οικονομικές επιπτώσεις των απατών μπορεί να είναι καταστροφικές και να αλλάξουν τη ζωή σας.

Εάν αντιμετωπίζετε οικονομικές δυσκολίες, μπορείτε να μιλήσετε με έναν οικονομικό σύμβουλο μέσω της Εθνικής Γραμμής Βοήθειας για το Χρέος (**National Debt Helpline**): **1800 007 007** από 9:30πμ – 4:30μμ Δευτέρα έως Παρασκευή ή συνδεθείτε με τη Ζωντανή Συνομιλία από τις 9:00 π.μ. έως τις 8:00 μ.μ. Δευτέρα έως Παρασκευή



scamwatch.gov.au