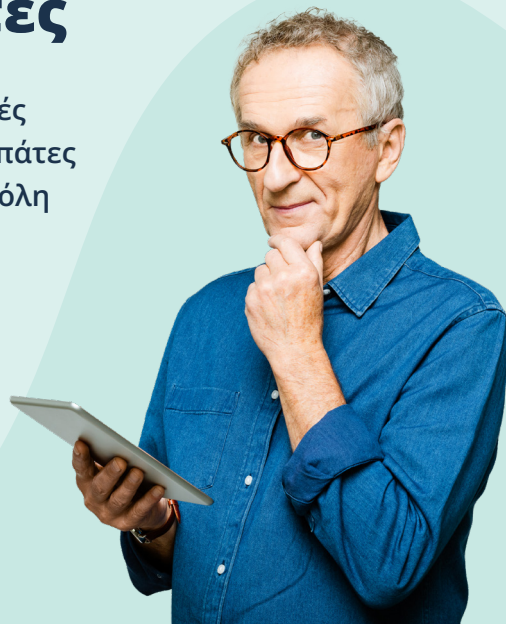


Προστατευθείτε από τις απάτες

Οι απατεώνες γίνονται όλο και πιο εξελιγμένοι στις προσπάθειές τους να πάρουν τα χρήματα ή τα προσωπικά σας στοιχεία. Οι απάτες στοχεύουν άτομα κάθε καταγωγής, ηλικίας και εισοδήματος σε όλη την Αυστραλία. Οι διαδικτυακές απάτες συνήθως γίνονται από κάποιον με ψεύτικο προφίλ ή επιχείρηση ή προσποιούνται ότι είναι από κάποιον γνωστό οργανισμό. Έτσι ενώ το διαδίκτυο μπορεί να είναι ένα θαυμάσιο μέρος για εξερεύνηση, είναι καλό να είστε προσεκτικοί! Να είστε προσεκτικοί και προστατευθείτε από τις απάτες ακολουθώντας τις παρακάτω συμβουλές μας.



Προστατέψτε τα προσωπικά σας στοιχεία

Οι απατεώνες προσποιούνται ότι εργάζονται σε οργανισμούς που γνωρίζετε και εμπιστεύεστε, όπως επιχειρήσεις με τις οποίες συναλλάσσετε, κρατικές υπηρεσίες ή υπηρεσία καταπολέμησης απατών για να προσπαθήσουν να σας κάνουν να αποκαλύψετε σημαντικά προσωπικά και οικονομικά στοιχεία. Ενδέχεται να επικοινωνήσουν μαζί σας τηλεφωνικά, με email, γραπτό μήνυμα ή με τα μέσα κοινωνικής δικτύωσης. Οι απατεώνες θα χρησιμοποιήσουν τα προσωπικά σας στοιχεία για να κλέψουν τα χρήματά σας ή να διαπράξουν κάποια άλλη παράνομη πράξη.

Για να σας εξαπατήσουν να δώσετε τα προσωπικά ή οικονομικά στοιχεία σας, οι απατεώνες μπορεί να σας ζητήσουν:

- να επιβεβαιώσετε την ταυτότητά σας ή να ενημερώσετε τα στοιχεία σας
- να κάνετε κλικ σ' έναν σύνδεσμο
- να τους δώσετε εξ αποστάσεως πρόσβαση στον υπολογιστή σας
- να πληρώσετε ένα χρέος
- να αγοράσετε κάποιο κουπόνι για να πληρώσετε ένα πρόστιμο
- να μεταφέρετε ή να στείλετε χρήματα στο εξωτερικό.



Ενδείξεις ότι μπορεί να είναι απάτη

- email, μηνύματα ή κλήσεις που δεν τα περιμένατε ή έρχονται από κάποιον που δεν γνωρίζετε
- υποσχέσεις για οικονομικό όφελος
- απειλές για επιβολή προστίμου ή χρέους
- απειλές να κλείσουν ή να "κλειδώσουν" τον λογαριασμό σας
- σύνδεσμοι που δεν φαίνονται γνήσιοι, όπως αν έχει ασυνήθιστη διεύθυνση ιστοσελίδας
- μια ασυνήθιστη αίσθηση επείγουσας ανάγκης ή προθεσμίας.

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.

Πώς να προστατευθείτε

- Να γνωρίζετε για το γεγονός ότι όντως υπάρχουν απάτες και να εξετάζετε πάντα την πιθανότητα ότι ένα μήνυμα, email ή τηλεφώνημα μπορεί να είναι απάτη.
- Μάθετε με ποιον έχετε να κάνετε. Αν δεν είστε βέβαιοι αν ένα γραπτό μήνυμα ή κλήση είναι γνήσια, μην χρησιμοποιήσετε τα στοιχεία επικοινωνίας που παρέχονται, αλλά κάντε μια αναζήτηση στο διαδίκτυο για τον αριθμό ή email του οργανισμού.
- Μη δίνετε προσωπικά ή οικονομικά στοιχεία.
- Μην ανοίγετε ύποπτα κείμενα, αναδυόμενα παράθυρα και μην κάνετε κλικ σε συνδέσμους ή συνημμένα στα email – διαγράψτε τα.
- Μην απαντάτε σε τηλεφωνήματα που αφορούν τον υπολογιστή σας που ζητούν εξ αποστάσεως πρόσβαση - κλείστε το τηλέφωνο - ακόμα κι αν λένε μια γνωστή εταιρεία όπως η Telstra.

Να είστε προσεκτικοί όταν κάνετε φιλίες στο διαδίκτυο

Οι απατεώνες επικοινωνούν με ανθρώπους, συνήθως με τα μέσα κοινωνικής δικτύωσης, ενός ιστότοπου γνωριμιών ή ακόμα και μέσω ενός διαδικτυακού παιχνιδιού. Θα είναι πολύ φιλικοί και θα δείξουν ενδιαφέρον και μεγάλη προθυμία πριν ξεκινήσουν μια φιλία ή σχέση μαζί σας. Οι απατεώνες μπορεί να είναι υπερβολικά υπομονετικοί. Η απατηλή σχέση μπορεί να συνεχιστεί για εβδομάδες ή ακόμα κι ένα χρόνο, ώστε να κερδίσουν την εμπιστοσύνη σας και να σας ζητήσουν χρήματα, προσωπικά στοιχεία, προσωπικές φωτογραφίες ή να σας εξαπατήσουν να κάνετε κάτι παράνομο.

Ενδείξεις ότι μπορεί να είναι απάτη

Προσέχετε για άτομα τα οποία:

- εκφράζουν γρήγορα βαθιά τρυφερότητα και επικοινωνούν συχνά μαζί σας
- δεν μπορούν να συναντηθούν προσωπικά μαζί σας ή μπορεί να σας ζητήσουν χρήματα για να ταξιδέψουν ώστε να σας συναντήσουν
- προσπαθούν να σας κάνουν να αφήσετε την πλατφόρμα ή εφαρμογή όπου συναντηθήκατε και να πάτε σ' ένα πιο προσωπικό κανάλι επικοινωνίας, όπως με απευθείας μηνύματα ή email
- ισχυρίζονται ότι είναι οικονομικά σταθεροί, αλλά σας ζητούν χρήματα
- σας λένε περίτεχνες ιστορίες για οικονομικά προβλήματα
- ρωτάνε για την οικονομική σας κατάσταση
- λένε ότι είναι σε απόγνωση, γίνονται επίμονοι, πιο άμεσοι ή ακόμα και επιθετικοί όταν δεν στέλνετε χρήματα
- φαίνεται να έχουν ασυνέπειες στις ιστορίες τους και στο διαδικτυακό τους προφίλ - για παράδειγμα, η φωτογραφία τους φαίνεται διαφορετική από την περιγραφή που σας δίνουν
- κάνουν ορθογραφικά και γραμματικά λάθη
- σας λένε ότι εργάζονται στο εξωτερικό (π.χ. εργάζονται σε φιλανθρωπικό οργανισμό βοήθειας ή στο στρατό).

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 φωτογραφίας για να δείτε αν πραγματικά είναι το άτομο που λέει ότι είναι. Πηγαίνετε 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.
- Προσέχετε αν βλέπετε πράγματα όπως ορθογραφικά και γραμματικά λάθη, ασυνέπειες στις ιστορίες τους.
- Μην συμφωνήσετε να μεταφέρετε πακέτα στο εξωτερικό ή να μεταφέρετε χρήματα για κάποιον άλλο, επειδή μπορεί να διαπράττετε παράνομη πράξη.
- Μην ανταλλάσσετε προσωπικές φωτογραφίες ή βίντεο. Είναι γνωστό ότι οι απατεώνες εκβιάζουν τα θύματά τους χρησιμοποιώντας ταπεινωτικό υλικό.
- Διακόψτε κάθε επικοινωνία αν το άτομο αρχίσει να σας ζητάει κάποια χάρη ή χρήματα.
- Αποφύγετε οποιαδήποτε συμφωνία με κάποιον άγνωστο που ζητάει πληρωμή μέσω χρηματικής εντολής, τραπεζικού εμβάσματος, διεθνή μεταφορά χρημάτων, προπληρωμένης κάρτας ή ηλεκτρονικού νομίσματος, όπως το Bitcoin. Είναι σπάνιο να πάρετε πίσω τα χρήματά σας που στείλατε μ' αυτόν τον τρόπο.

Προσέχετε τις απάτες που αφορούν επενδύσεις

Οι επενδυτικές απάτες περιλαμβάνουν υποσχέσεις για μεγάλες πληρωμές, γρήγορο χρήμα ή εγγυημένες αποδόσεις. Να είστε πάντα καχύποπτοι για τυχόν επενδυτικές ευκαιρίες που υπόσχονται υψηλή απόδοση με μικρό ή καθόλου κίνδυνο.

Αυστραλοί χάνουν περισσότερα χρήματα από επενδυτικές απάτες από οποιουδήποτε άλλους. Μπορεί να είναι δύσκολο να εντοπιστούν, καθώς οι απατεώνες καταβάλλουν μεγάλη προσπάθεια να δημιουργήσουν πειστικές ιστορίες και να κάνουν επαγγελματικές ιστοσελίδες και διαφημιστικό υλικό. Πριν επενδύσετε να ζητάτε πάντα ανεξάρτητες νομικές ή οικονομικές συμβουλές από χρηματοοικονομικό σύμβουλο που είναι εγγεγραμμένος στην Αυστραλιανή Επιτροπή Κεφαλαιαγοράς και Επενδύσεων (ASIC).

Μερικοί από τους πιο συνηθισμένους τρόπους με τους οποίους μπορούν να λειτουργήσουν οι επενδυτικές απάτες περιλαμβάνουν:

- επικοινωνώντας μαζί σας με email ή τηλεφωνικά για μια ειδική ευκαιρία για γρήγορο ή εγγυημένο κέρδος
- χρησιμοποιώντας ψεύτικες εγκρίσεις διάσημων ατόμων για να κάνουν μια απάτη να φαίνεται νόμιμη
- προσπαθούν να σας πείσουν να πάρετε τα συντάξιά σας νωρίς ή με εφάπαξ πληρωμή
- επενδυτικά σεμινάρια (συχνά μέσω διαδικτυακού βίντεο, Zoom ή κάτι παρόμοιο) που είναι δωρεάν ή χρεώνουν υψηλή τιμή για να τα παρακολουθήσετε.



Συνταξιοδοτική ασφάλεια

Οι απάτες που αφορούν τα συντάξιμα (Superannuation) προσφέρουν έγκαιρη πρόσβαση στο ασφαλιστικό σας ταμείο, συχνά μέσω αυτασφάλισης ή έναντι αμοιβής. Η προσφορά μπορεί να προέρχεται από κάποιον απατεώνα που υποκρίνεται ότι είναι οικονομικός σύμβουλος.

Μπορεί να σας ζητήσουν να συμφωνήσετε σε μια ιστορία για να διασφαλίσουν την πρόωρη αποδέσμευση των χρημάτων σας και μετά ενεργούν ως ο οικονομικός σας σύμβουλος, εξαπατώντας έτσι το ασφαλιστικό σας ταμείο για να μεταβιβάσουν τα χρήματα της συνταξιοδοτικής σας ασφάλειας απευθείας σε αυτούς. Μόλις πάρει τα χρήματά σας, ο απατεώνας μπορεί να πάρει μια μεγάλη «προμήθεια» από τα αποδεσμευμένα χρήματα ή να μην αφήσει τίποτα για εσάς.

Σημείωση: Συνήθως δεν μπορείτε να πάρετε νόμιμα το δεσμευμένο τμήμα των συντάξιμών σας έως ότου είστε μεταξύ 55 και 60 ετών, ανάλογα το έτος που γεννηθήκατε. Υπάρχουν ορισμένες εξαιρέσεις όπως σοβαρές οικονομικές δυσκολίες ή παρηγορητικοί λόγοι - αλλά σε αντίθετη περίπτωση αν κάποιος προσφέρει πρόωρη πρόσβαση στα συντάξιμά σας τότε ενεργεί παράνομα. Για περισσότερες πληροφορίες επισκεφθείτε το: moneysmart.gov.au/how-super-works/superannuation-scams

Προσφορές για μετοχές και χρήσιμες συμβουλές

Οι απατεώνες μπορεί να επικοινωνήσουν μαζί σας μέσω email, με τα μέσα κοινωνικής δικτύωσης ή να αναρτήσουν ένα μήνυμα σ' ένα φόρουμ για να σας ενθαρρύνουν να αγοράσετε μετοχές σε μια εταιρεία που προβλέπουν ότι πρόκειται να αυξηθεί σε αξία. Το μήνυμα μοιάζει ότι στάλθηκε από κάποιον μέσα από την εταιρεία και συνήθως τονίζει ότι πρέπει να ενεργήσετε γρήγορα. Ο απατεώνας προσπαθεί να σας κάνει να αγοράσετε μετοχές για να αυξήσει την τιμή της μετοχής, ώστε να μπορέσει να πουλήσει τις μετοχές που έχει ήδη αγοράσει και να αποκομίσει τεράστιο κέρδος. Στη συνέχεια, η αξία της μετοχής θα μειωθεί δραματικά.

Απάτες με την έγκριση διασημοτήτων

Οι απατεώνες χρησιμοποιούν τη φωτογραφία, το όνομα και τα προσωπικά χαρακτηριστικά γνωστών διασημοτήτων χωρίς την άδειά τους για να σας δελεάσουν να επενδύσετε καθώς έχει την στήριξη κάποιου που εμπιστεύεστε. Αυτές οι απάτες εμφανίζονται συχνά ως διαφημίσεις στο διαδίκτυο ή διαφημιστικές καμπάνιες σε αναρτήσεις στα μέσα κοινωνικής δικτύωσης ή φαινομενικά νόμιμοι, αξιόπιστοι ιστότοποι.



Προειδοποιητικά σημάδια επενδυτικής απάτης

Επικοινωνεί κάποιος μαζί σας ξαφνικά τηλεφωνικά, με γραπτό μήνυμα, email ή μήνυμα στα μέσα κοινωνικής δικτύωσης που προσφέρει επενδυτικές συμβουλές που δεν έχετε ζητήσει και:

- χρησιμοποιεί τακτικές υψηλής πίεσης, συμπεριλαμβανομένης της επανειλημμένης επικοινωνίας μαζί σας και πίεσης να πάρετε γρήγορα μια απόφαση.
- υπόσχεται χαμηλούς κινδύνους με υψηλές ή εγγυημένες αποδόσεις.
- δεν έχει αυστραλιανή άδεια παροχής χρηματοοικονομικών υπηρεσιών (Australian financial services - AFS) ή ότι δεν χρειάζεται άδεια.
- έχει επενδυτικό προσπέκτους που δεν είναι καταχωρημένο στην ASIC.
- χρησιμοποιεί εγκρίσεις ή φωτογραφίες διασημοτήτων: Συνήθως είναι ψεύτικες. Οι διασημότητες σπάνια συζητούν δημόσια για τις επενδύσεις ή τις οικονομικές τους αποφάσεις.
- σας κατευθύνει σε μια ψεύτικη ιστοσελίδα.
- προσπαθεί να σας σταματήσει για να μην αποσυρθείτε από τη συμφωνία.

Πώς να προστατευθείτε

- Να υποπτευθείτε ότι κάτι συμβαίνει όταν ακούτε για ευκαιρίες που φαίνονται πολύ καλές για να είναι αληθινές.
- Να υποπτευθείτε ότι κάτι συμβαίνει όταν ακούτε για διαφημίσεις ή ιστορίες που τις έχουν εγκρίνει διασημότητες.
- Μην αφήνετε κανέναν να σας πιέσει.
- Αν είστε κάτω των 55 ετών, να προσέχετε τις προσφορές που προωθούν την εύκολη πρόσβαση στα συντάξιμά σας.
- Κάντε την έρευνά σας και ψάξτε για αξιόπιστες ή ανεξάρτητες οικονομικές ή νομικές συμβουλές.
- Μη δίνετε προσωπικά ή οικονομικά στοιχεία έως ότου:
 - ελέγξετε αν ο οικονομικός σύμβουλος και η εταιρεία που εργάζεται είναι καταχωρημένη στην ιστοσελίδα του ASIC asic.gov.au/online-services/search-asics-registers/
 - ελέγξετε τη λίστα των εταιρειών που διατηρεί το ASIC με τις οποίες δεν πρέπει να έχετε συναλλαγές moneysmart.gov.au/scams/companies-you-should-not-deal-with

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 συναλλάσσετε ή αστυνομία, κυβέρνηση ή υπηρεσία καταπολέμησης απατών.

Σκεφτείτε

- Αναρωτηθείτε, μπορεί το μήνυμα ή το τηλεφώνημα να είναι ψεύτικο;
- 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.

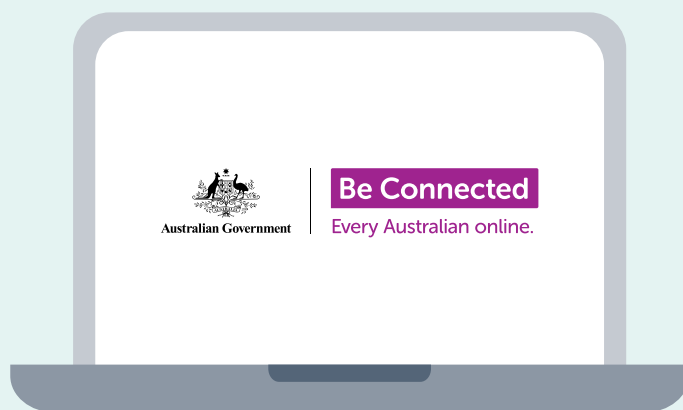
- Επικοινωνήστε με την τράπεζα ή το χρηματοοικονομικό σας ίδρυμα και σταματήστε τυχόν περαιτέρω πληρωμές στον απατεώνα.
- Αν πέσατε θύμα παράνομης πράξης στον κυβερνοχώρο και χάσατε χρήματα στο διαδίκτυο, μπορείτε να το καταγγείλετε στην αστυνομία μέσω του [ReportCyber](#) ή επισκεφθείτε το: [cyber.gov.au](#)
- 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.



επισκεφθείτε το
[beconnected.esafety.gov.au](#)



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