



Το Μικρό Μαύρο Βιβλίο για τις Απάτες

Ένας οδηγός τσέπης για να μπορείτε να αναγνωρίζετε, να αποφεύγετε και να προστατευθείτε από τις απάτες





Το Μικρό Μαύρο Βιβλίο για τις Απάτες

Ένας οδηγός τσέπης για να μπορείτε να αναγνωρίζετε, να αποφεύγετε και να προστατευθείτε από τις απάτες

ISBN 978 1 920702 00 7

Αυστραλιανή Επιτροπή Ανταγωνισμού και Προστασίας Καταναλωτών
(Australian Competition and Consumer Commission)

23 Marcus Clarke Street, Canberra, Australian Capital Territory, 2601

© Κοινοπολιτεία της Αυστραλίας 2016

Το παρόν έργο προστατεύεται από πνευματικά δικαιώματα. Εκτός από οποιαδήποτε χρήση που επιτρέπεται βάσει του Νόμου περί Πνευματικής Ιδιοκτησίας 1968, όλο το υλικό που περιέχεται σ' αυτό το έργο παρέχεται με άδεια της Creative Commons Attribution 3.0 Australia, με εξαίρεση:

- το εθνόσημο της Κοινοπολιτείας
- τα λογότυπα ACCC και AER
- οποιοσδήποτε εικονογραφήσεις, διαγράμματα, φωτογραφίες ή γραφικά για τα οποία η Αυστραλιανή Επιτροπή Ανταγωνισμού και Προστασίας Καταναλωτών δεν έχει τα πνευματικά δικαιώματα, αλλά τα οποία ενδέχεται να αποτελούν μέρος του παρόντος εντύπου.

Οι λεπτομέρειες των σχετικών όρων της άδειας διατίθενται στον ιστότοπο της Creative Commons, καθώς και ο πλήρης νομικός κωδικός για την άδεια CC BY 3.0 AU.

Τα αιτήματα και η ζήτηση πληροφοριών σχετικά με την αναπαραγωγή και τα δικαιώματα θα πρέπει να απευθύνονται στον: Director, Corporate Communications, ACCC, GPO Box 3131, Canberra ACT 2601, ή publishing.unit@accc.gov.au.

ACCC 12/16_1129

www.accc.gov.au

Περιεχόμενα

Εισαγωγή	2
Οι πιο διαδεδομένες απάτες για αποφυγή	3
Απάτες που αφορούν γνωριμίες και ειδύλλια	4
Απάτες που αφορούν γνωριμίες και ειδύλλια	6
Απάτες που αφορούν απειλές και πρόστιμα	8
Απάτες που αφορούν απροσδόκητα χρήματα	10
Απάτες που αφορούν δώρα και λαχεία	12
Απάτες που αφορούν αγορές από το διαδίκτυο, μικρές αγγελίες και δημοπρασίες	14
Απάτες που στοχεύουν υπολογιστές και κινητές συσκευές	16
Κλοπή ταυτότητας	18
Απάτες που αφορούν θέσεις εργασίας και απασχόληση	20
Απάτες που αφορούν φιλανθρωπικά ιδρύματα και ιατρικά ζητήματα	22
Επιχειρηματικές απάτες	24
Πώς λειτουργούν οι απάτες – η ανατομία μιας απάτης	26
Οι χρυσοί κανόνες για να προστατευθείτε	32
Πού να αποταθείτε για βοήθεια ή υποστήριξη	34
Πού να καταγγείλετε μια απάτη	36

Εισαγωγή

Κάθε χρόνο, οι απάτες κοστίζουν στους Αυστραλούς, στις επιχειρήσεις και την οικονομία εκατοντάδες εκατομμύρια δολάρια και προκαλούν συναισθηματική βλάβη στα θύματα και τις οικογένειές τους.

Ο καλύτερος τρόπος για να προστατευθείτε είναι μέσω της επίγνωσης και της επιμόρφωσης. Αυτή η νέα έκδοση του *Μικρού Μαύρου Βιβλίου για τις Απάτες* είναι μια παρουσίαση για εσάς από την Αυστραλιανή Επιτροπή Ανταγωνισμού και Προστασίας Καταναλωτών (ACCC), η εθνική υπηρεσία προστασίας καταναλωτών. Το Μικρό Μαύρο Βιβλίο για τις Απάτες αναγνωρίζεται διεθνώς ως ένα σημαντικό εργαλείο για τους καταναλωτές και τις μικρές επιχειρήσεις για να μάθουν για τις απάτες και περιλαμβάνει:

- τις πιο συνήθεις απάτες που θα πρέπει να προσέχετε
- τους διαφορετικούς τρόπους με τους οποίους οι απατεώνες μπορούν να επικοινωνήσουν μαζί σας
- τα εργαλεία που χρησιμοποιούν οι απατεώνες για να σας ξεγελάσουν
- τις προειδοποιητικές ενδείξεις
- πώς να προστατευθείτε, και
- πού να αποταθείτε για βοήθεια.

Το *Μικρό Μαύρο Βιβλίο για τις Απάτες* διατίθεται στο διαδίκτυο: www.accc.gov.au/littleblackbookofscams.

Προστατευθείτε—εγγραφείτε στο Scamwatch

Για να είστε ένα βήμα μπροστά από τους απατεώνες, μάθετε περισσότερα μέσω του ιστότοπου Scamwatch της ACCC - www.scamwatch.gov.au - όπου μπορείτε να εγγραφείτε για δωρεάν προειδοποιήσεις με email σχετικά με τις καινούριες απάτες που στοχεύουν καταναλωτές και μικρές επιχειρήσεις. Μπορείτε επίσης να ακολουθήσετε το Scamwatch στο Twitter στο [@scamwatch_gov](https://twitter.com/scamwatch_gov) ή στο http://twitter.com/scamwatch_gov.

Οι πιο διαδεδομένες απάτες για αποφυγή

Όλοι είναι ευάλωτοι στις απάτες, οπότε όλοι χρειάζονται πληροφορίες για τον τρόπο αναγνώρισης και αποφυγής από τις απάτες. Μερικοί άνθρωποι πιστεύουν ότι μόνο οι αφελείς και οι άπληστοι πέφτουν θύματα απάτης. Η αλήθεια είναι ότι οι απατεώνες είναι έξυπνοι κι αν δεν ξέρετε τι να προσέχετε, οποιοσδήποτε μπορεί να πέσει θύμα απάτης.

Λάβετε μια προσφορά που φαίνεται ότι είναι πολύ ωραία για να είναι αληθινή, ίσως ένα τηλεφώνημα για να σας βοηθήσουν να επιδιορθώσετε τον υπολογιστή σας ή μια απειλή για να πληρώσετε χρήματα που δεν χρωστάτε, μια ειδοποίηση από την τράπεζα ή την εταιρεία τηλεπικοινωνιών σας για ένα πρόβλημα με το λογαριασμό σας ή ακόμα και μια πρόσκληση να «γίνετε φίλοι» ή να διασυνδεθείτε στο διαδίκτυο; Οι απατεώνες ξέρουν να πατούν τα κουμπιά σας για να πάρουν αυτό που θέλουν.

Γίνονται πιο έξυπνοι, κινούνται με τους καιρούς για να επωφεληθούν από τη νέα τεχνολογία, τα νέα προϊόντα ή υπηρεσίες και τις μεγάλες εκδηλώσεις για να δημιουργήσουν πιστευτές ιστορίες που θα σας πείσουν να αποχωριστείτε τα χρήματα ή τα προσωπικά σας στοιχεία.

Ωστόσο, χάρη στις δεκάδες χιλιάδες καταγγελίες απάτης που υποβάλλονται κάθε χρόνο, η ACCC έχει ετοιμάσει μια λίστα με συνήθεις απάτες για να αποκαλύψει τα μυστικά και τις τακτικές που οι απατεώνες δεν θέλουν να γνωρίζετε.

Απάτες που αφορούν γνωριμίες και ειδύλλια



Οι απάτες που αφορούν γνωριμίες και ειδύλλια κοστίζουν στους Αυστραλούς εκατομμύρια κάθε χρόνο και μπορούν να καταστρέψουν άτομα και οικογένειες.

Πώς λειτουργεί αυτή η απάτη

Οι απατεώνες των **γνωριμιών και ειδυλλίων** δημιουργούν ψεύτικα προφίλ σε νόμιμες ιστοσελίδες γνωριμιών, σε εφαρμογές για κινητά ή πλατφόρμες μέσω κοινωνικής δικτύωσης όπως το Facebook χρησιμοποιώντας φωτογραφίες και ταυτότητες που συχνά έχουν κλέψει από άλλα άτομα. Χρησιμοποιούν αυτά τα προφίλ σε μια προσπάθεια να ξεκινήσουν μια σχέση μαζί σας που μπορεί να κρατήσει μήνες ή και χρόνια, απλά για να μπορέσουν να πάρουν τα χρήματά σας. Ο απατεώνας θα ζητήσει χρήματα για βοήθεια με κάποια ασθένεια, τραυματισμό, έξοδα ταξιδιού ή οικογενειακή κρίση. Είναι άκαρδοι και θα σας πουν ψέματα για να επωφεληθούν από την καλή, ανθρώπινη φύση σας.

Οι απατεώνες συνήθως είναι στο εξωτερικό κι έχουν κάποια δικαιολογία για το λόγο που είναι εκεί, όπως λόγω στρατιωτικής θητείας, εργάζονται ως μηχανικοί ή φροντίζουν κάποιο φίλο ή συγγενή. Ποτέ δεν είναι αυτοί που λένε ότι είναι και μερικοί πονηροί απατεώνες είναι ακόμη διατεθειμένοι να στείλουν και δωράκια. Αυτό είναι μόνο ένα μέρος του μεγαλεπήθολου σχεδίου τους για να σας πάρουν ακόμα περισσότερα χρήματα αργότερα.

Προστατευθείτε

- Ποτέ μη στέλνετε χρήματα και μη δίνετε τα προσωπικά σας στοιχεία σε κάποιον που συναντήσατε μόνο στο διαδίκτυο.
- Προσέχετε εάν κάποιος διαδικτυακός θαυμαστής ζητήσει να επικοινωνήσει εκτός της ιστοσελίδας γνωριμιών ή της πλατφόρμας μέσω κοινωνικής δικτύωσης μετά από λίγες «επαφές» ή συνομιλίες - θα μπορούσε να είναι απατεώνας.
- Κάντε μια αναζήτηση της εικόνας του θαυμαστή σας για να σας βοηθήσει να καταλάβετε εάν πραγματικά είναι αυτός που λέει ότι είναι. Μπορείτε να χρησιμοποιήσετε υπηρεσίες αναζήτησης εικόνων όπως Google ή TinEye.
- Να είστε προσεκτικοί όταν μοιράζεστε πολύ προσωπικές φωτογραφίες ή βίντεο στο διαδίκτυο. Είναι γνωστό ότι οι απατεώνες συχνά εκβιάζουν το στόχο τους χρησιμοποιώντας δικές σας εικόνες ή βίντεο που δεν θέλετε να δει κανείς άλλος.

Επενδυτικές απάτες



«Επένδυση μηδενικού ρίσκου»
ή ευκαιρία για συμφορά;

Πώς λειτουργεί αυτή η απάτη

Οι **επενδυτικές απάτες** παρουσιάζονται σε πολλές μορφές, συμπεριλαμβανομένων της αγοράς κρυπτονομισμάτων, συναλλαγών δυαδικών δικαιωμάτων προαίρεσης, επιχειρηματικών εγχειρημάτων, προγραμμάτων επαγγελματικής συνταξιοδότησης, διαχειριζόμενων κεφαλαίων και αγοροπωλησία μετοχών ή ακινήτων. Οι απατεώνες στολίζουν τις «ευκαιρίες» με επαγγελματικά φυλλάδια και ιστότοπους για να καμουφλάρουν τις δόλιες δουλειές τους. Οι απατεώνες συχνά ξεκινούν μ' ένα τηλεφώνημα ή email από το πουθενά που προσφέρουν μια «ευκαιρία που δεν πρέπει να χάσετε», μια «ευκαιρία με υψηλή απόδοση» ή μια «εγγυημένη» ευκαιρία. Ο απατεώνας συνήθως λειτουργεί από το εξωτερικό και δεν έχει Αυστραλιανή Άδεια Χρηματοπιστωτικών Υπηρεσιών (Australian Financial Services).

Οι **απάτες υπολογιστικού λογισμικού πρόβλεψης** υπόσχονται να προβλέπουν επακριβώς τις κινήσεις των χρηματιστηρίων, τα αποτελέσματα των ιπποδρομιών, των αθλητικών εκδηλώσεων ή κληρώσεων λαχείων. Απλά είναι μια μορφή τζόγου μεταμφιεσμένη σε επένδυση. Τα περισσότερα συστήματα ή προγράμματα δεν λειτουργούν και οι αγοραστές δεν μπορούν να πάρουν πίσω τα χρήματά τους. Σε πολλές περιπτώσεις ο προμηθευτής απλώς εξαφανίζεται.

Οι **απάτες επαγγελματικής συνταξιοδότησης** σας προσφέρουν έγκαιρη πρόσβαση στα χρήματα που έχετε στο επαγγελματικό συνταξιοδοτικό ταμείο σας, συχνά μέσω ενός αυτοδιαχειριζόμενου ταμείου συνταξιοδότησης ή έναντι αμοιβής. Ο απατεώνας μπορεί να σας ζητήσει να συμφωνήσετε με μια ιστορία που θα επιτρέψει την έγκαιρη απελευθέρωση των χρημάτων σας και στη συνέχεια, ενεργώντας ως ο οικονομικός σας σύμβουλος, θα εξαπατήσει το ταμείο σας επαγγελματικής σύνταξης για να καταβάλλει τις συνταξιοδοτικές παροχές σας απευθείας σε αυτόν. Μόλις πάρει τα χρήματά σας, ο απατεώνας ενδέχεται να πάρει μεγάλες «αμοιβές» ή να σας αφήσει χωρίς τίποτα.

Προστατευθείτε

- Μην αφήσετε κανέναν να σας πιέσει να πάρετε αποφάσεις σχετικά με τα χρήματα ή τις επενδύσεις σας - ειδικά εάν η προσφορά σας ήρθε από το πουθενά.
- Πριν αποχωριστείτε από τα χρήματά σας, κάντε τη δική σας έρευνα σχετικά με την επενδυτική εταιρεία και επισκεφθείτε τον ιστότοπο www.moneysmart.gov.au για να δείτε αν έχει Αυστραλιανή Άδεια Χρηματοπιστωτικών Υπηρεσιών. Ρωτήστε τον εαυτό σας: εάν κάποιος άγνωστος γνώριζε το μυστικό για να κάνει χρήματα, γιατί να το μοιραζόταν αυτό το μυστικό;

Εάν είστε κάτω της ηλικίας συνταξιοδότησης, προσέξτε για προσφορές που προωθούν την εύκολη πρόσβαση στις συσσωρευμένες παροχές επαγγελματικής συνταξιοδότησης. Εάν πάρετε παράνομα τα χρήματα της επαγγελματικής συνταξιοδότησής σας νωρίς, ενδέχεται να σας επιβληθούν κυρώσεις βάσει του φορολογικού νόμου.

Απάτες που αφορούν απειλές και πρόστιμα

Αν μια κρατική αρχή ή μια αξιόπιστη εταιρεία σας λέει να αποπληρώσετε, σταματήστε, σκεφτείτε και ελέγξτε διπλά.

Πώς λειτουργεί αυτή η απάτη

Αντί να προσφέρουν ένα δώρο, χρήμα ή επιστροφή χρημάτων, αυτές οι απάτες χρησιμοποιούν απειλές με σκοπό να σας φοβίσουν να δώσετε τα χρήματά σας. Ο απατεώνας μπορεί να σας καλέσει και να σας απειλήσει με **σύλληψη** ή να σας στείλει email ισχυριζόμενος ότι χρωστάτε χρήματα για κάποιο **πρόστιμο παράβασης ορίου ταχύτητας, χρέος στην εφορία** ή κάποιον **απλήρωτο λογαριασμό**.

Κατά τη διάρκεια του τηλεφωνήματος, οι απατεώνες θα σας ασκήσουν πίεση να πληρώσετε αμέσως και θα σας πουν ότι εάν αρνηθείτε θα στείλουν την αστυνομία στο σπίτι σας. Είναι γνωστό ότι οι απατεώνες στοχεύουν ευάλωτα άτομα στην κοινωνία μας, όπως νεοαφιθέντες μετανάστες. Υποκρίνονται ότι είναι υπάλληλοι του Υπουργείου Μετανάστευσης και απειλούν τα θύματα με **απέλαση**, εκτός αν καταβάλλουν αμοιβές για διόρθωση σφαλμάτων στις βίζες τους. Σε μια πολύ παρόμοια απάτη ο απατεώνας προσποιείται ότι είναι από την Αυστραλιανή Εφορία και λέει στα θύματά του ότι έχουν μια εκκρεμή φορολογική οφειλή.

Οι απατεώνες προσποιούνται επίσης ότι είναι **αξιόπιστες εταιρείες** όπως η τράπεζά σας, η εταιρεία φυσικού αερίου, ηλεκ. ρεύματος, ύδρευσης ή τηλεφώνου. Απειλούν να ακυρώσουν την σύνδεσή σας ή να σας χρεώσουν υπερβολικές χρεώσεις εάν δεν πληρώσετε αμέσως τον λογαριασμό. Μερικές φορές μπορεί να μιμηθούν μια επιχείρηση όπως τα Αυστραλιανά Ταχυδρομεία (Australian Post) λέγοντάς σας ότι έχετε ένα δέμα για παραλαβή διαφορετικά θα χρεωθείτε χρέωση φύλαξης για κάθε μέρα που δεν πληρώνετε. Όποια κι αν είναι η περίπτωση, προσπαθούν να σας κάνουν να ανησυχήσετε και να ενεργήσετε χωρίς να σταματήσετε να σκεφτείτε και να ελέγξετε αν η ιστορία αυτή είναι πραγματική.

Εάν η απάτη αποστέλλεται με email, πιθανώς να περιλαμβάνει συνημμένο έγγραφο ή σύνδεσμο σε κάποιον ψεύτικο ιστότοπο όπου θα σας ζητηθεί να κατεβάσετε αποδεικτικά στοιχεία για το «λογαριασμό», «πρόστιμο» ή «λεπτομέρειες παράδοσης». Το άνοιγμα του συνημμένου ή το κατέβασμα του αρχείου θα έχει ως αποτέλεσμα τη μόλυνση του υπολογιστή σας από κακόβουλο λογισμικό (δείτε σελίδα 16).

Προστατευθείτε

- Μην αφήνετε το απειλητικό άτομο που σας τηλεφωνεί να σας ασκήσει πίεση. Σταματήστε, σκεφθείτε και ελέγξτε αν η ιστορία του είναι αληθινή.
- Μια κρατική υπηρεσία ή μια αξιόπιστη εταιρεία δεν θα σας ζητήσει ποτέ να πληρώσετε με ασυνήθιστες μεθόδους, όπως με δωροκάρτα, τραπεζικό έμβασμα ή Μπίτκοϊν (Bitcoins).
- Επαληθεύστε την ταυτότητα του καλούντος τηλεφωνώντας απευθείας στον σχετικό οργανισμό – βρείτε τον οργανισμό μέσω μιας ανεξάρτητης πηγής, όπως τηλεφωνικός κατάλογος, προηγούμενος λογαριασμός ή αναζήτηση στο διαδίκτυο.
- Μην χρησιμοποιείτε τα στοιχεία επικοινωνίας που παρέχονται στα email ή που σας δίνονται κατά τη διάρκεια του τηλεφωνήματος. Και πάλι, βρείτε τα στοιχεία του μέσω μιας ανεξάρτητης πηγής.

Απάτες που αφορούν απροσδόκητα χρήματα



Εάν σας ζητηθεί να κάνετε πληρωμές πριν λάβετε αγαθά ή χρήματα, σκεφτείτε το διπλά.

Πώς λειτουργεί αυτή η απάτη

Οι απατεώνες σας λένε ότι εντελώς ξαφνικά δικαιούστε κάποια χρήματα, πολύτιμα πετράδια, χρυσό ή πολύτιμες μετοχές αλλά πρέπει να κάνετε **προκαταβολικές πληρωμές** για να τα πάρετε. Δεν θα λάβετε ποτέ αυτά που σας υποσχέθηκαν και πάντα θα υπάρχει μια δικαιολογία γιατί πρέπει να πληρώσετε περισσότερα. Αν πληρώσετε τις χρεώσεις, θα χάσετε τα χρήματά σας.

Οι απάτες που αφορούν **επιστροφή ή ανάκτηση χρημάτων** σημαίνει ότι ένας απατεώνας σας λέει ότι σας οφείλουν χρήματα για λόγους όπως υπερπληρωμένος φόρος, τραπεζικά τέλη ή κάποιο είδος αποζημίωσης. Πριν όμως πάρετε τα χρήματά σας, σας ζητάνε να πληρώσετε ένα μικρό διοικητικό τέλος.

Στις **απάτες κληρονομιάς**, οι απατεώνες προσποιούνται ότι είναι δικηγόροι, τραπεζίτες ή ανώτεροι υπάλληλοι ξένων χωρών και σας λένε ότι δικαιούστε μια μεγάλη κληρονομιά ή σας προσφέρουν μερίδιο σ' ένα πλάνο επειδή έχετε το ίδιο όνομα με κάποιον που πέθανε. Συχνά χρησιμοποιούν πλαστά νομικά έγγραφα και σας ζητούν να κάνετε πληρωμές για τέλη και φόρους για να λάβετε την κληρονομιά. Μπορεί επίσης να σας ζητήσουν τα προσωπικά σας στοιχεία για να συμπληρώσουν τα «επίσημα έγγραφα». Αυτό σημαίνει ότι ενδέχεται να σας κλέψουν την ταυτότητα καθώς και τα χρήματά σας.

Οι κοινώς ονομαζόμενες **Νιγηριανές απάτες** μπορεί να προέρχονται από τη Δυτική Αφρική, αλλά μπορεί να προέρχονται από οπουδήποτε στον κόσμο. Περιλαμβάνουν απατεώνες που σας λένε ότι χρειάζονται τη βοήθειά σας για

να εξασφαλίσουν μια μεγάλη περιουσία την οποία προσπαθούν απεγνωσμένα να τη βγάλουν από τη χώρα τους. Μπορεί να ισχυριστούν ότι η περιουσία είναι ένα μεγάλο κατακωνιασμένο ποσό χρημάτων, χρυσός ή περιουσιακά στοιχεία που εγκαταλείφθηκαν από μια διεφθαρμένη κυβέρνηση ή αξιωματούχο κι αν συμφωνήσετε να τη λάβετε, θα σας δώσουν ένα μεγάλο μερίδιο όταν είναι ασφαλές να γίνει αυτό. Όπως όλες αυτές οι απάτες, θα σας πουν ότι πρέπει πρώτα να πληρώσετε φόρους, τραπεζικές χρεώσεις ή τέλη για ελέγχους κατά της τρομοκρατίας και ξεπλύματος χρήματος, προτού μπορέσουν να σας στείλουν τα χρήματα.

Αυτές οι απάτες συνήθως προέρχονται από το εξωτερικό και ζητούν πληρωμή μέσω τραπεζικού εμβάσματος, αλλά ενδέχεται επίσης να ζητήσουν τραπεζική εντολή μεταβίβασης χρημάτων ή άλλες μεθόδους πληρωμής.

Εάν ξεγελαστείτε απ' αυτές τις απάτες, ποτέ δεν θα λάβετε κάτι από τον απατεώνα και θα χάσετε τα χρήματα που στείλατε.

Προστατευθείτε

- Να θυμάστε ότι δεν υπάρχουν πλάνα γρήγορου πλουτισμού: αν κάτι φαίνεται ότι παραείναι καλό για να είναι αληθινό, τότε μάλλον συμβαίνει αυτό ακριβώς».
- Αποφεύγετε κάθε συμφωνία με κάποιον άγνωστο που ζητάει προκαταβολική πληρωμή με εντολή πληρωμής, τραπεζικό έμβασμα, διεθνής μεταβίβαση χρημάτων, προπληρωμένη κάρτα ή ηλεκτρονικό νόμισμα. Είναι σπάνιο να ανακτήσετε χρήματα που αποστέλλονται με τέτοιον τρόπο.
- Εάν ένα ανεπιθύμητο email φαίνεται ύποπτο, απλά διαγράψτε το. Μην κάνετε κλικ σε κανέναν σύνδεσμο.
- Κρατικές υπηρεσίες, τράπεζες ή επιχειρήσεις κοινής ωφέλειας ποτέ δεν επικοινωνούν μαζί σας ζητώντας να πληρώσετε προκαταβολικά χρήματα για να πάρετε πίσω κάποια χρέωση ή επιστροφή χρημάτων.
- Εάν δεν είστε βέβαιοι, ελέγξτε ανεξάρτητα την ταυτότητα του ατόμου που έρχεται σε επαφή μαζί σας. Μην χρησιμοποιείτε τα στοιχεία επικοινωνίας που παρέχονται στο μήνυμα που σας στάλθηκε - πάρτε τα σωστά στοιχεία επικοινωνίας μέσω μιας ανεξάρτητης πηγής, όπως τηλεφωνικός κατάλογος ή αναζήτηση στο διαδίκτυο.
- Κάντε μια αναζήτηση στο διαδίκτυο χρησιμοποιώντας την ακριβή διατύπωση της προσφοράς - πολλές απάτες μπορούν να αναγνωριστούν με αυτόν τον τρόπο.

Απάτες που αφορούν δώρα και λαχεία



Μη δελεάζεστε από την προοπτική να κερδίσετε ξαφνικά το λαχείο - μόνο ο απατεώνας αποκομίζει απροσδόκητα κέρδη.

Πώς λειτουργεί αυτή η απάτη

Με τις απάτες αυτές προσπαθούν να σας εξαπατήσουν να δώσετε προκαταβολικά χρήματα ή τα προσωπικά σας στοιχεία ώστε να πάρετε ένα δώρο από λαχείο, στοίχημα ή διαγωνισμό που ποτέ δεν συμμετείχατε. Οι απατεώνες ισχυρίζονται ότι πρέπει να πληρώσετε αμοιβές ή φόρους πριν αποδεσμευθούν τα «κέρδη» ή το δώρο σας. Μπορεί επίσης να χρειαστεί να καλέσετε ή να στείλετε γραπτό μήνυμα σε έναν αριθμό τηλεφώνου με υψηλή χρέωση για να διεκδικήσετε το δώρο σας.

Στις **απάτες με τα ξυστά** λαβαίνετε ταχυδρομικώς μια επιστολή που περιέχει φανταχτερά φυλλάδια και αρκετά ξυστά, ένα από τα οποία κερδίζει. Για να γίνει πιο πιστευτό, συχνά θα υπάρχει και δεύτερο ή τρίτο δώρο. Όταν καλέσετε να διεκδικήσετε το δώρο σας, οι απατεώνες θα σας ζητήσουν να πληρώσετε τέλη ή φόρους για να πάρετε τα κέρδη σας.

Οι **απάτες με τα λαχεία** ενδέχεται να χρησιμοποιούν ονόματα πραγματικών λαχείων του εξωτερικού για να ισχυριστούν ότι έχετε κερδίσει μετρητά, παρόλο που δεν έχετε αγοράσει ποτέ λαχείο. Οι απατεώνες συνήθως ζητούν αμοιβές ή φόρους για να αποδεσμεύσουν τα χρήματα. Θα σας πουν επίσης ότι χρειάζονται τα προσωπικά σας στοιχεία για να αποδείξουν ότι είστε ο σωστός νικητής, στη συνέχεια όμως χρησιμοποιούν αυτά τα στοιχεία για να κλέψουν την ταυτότητα ή τα χρήματά σας από τον τραπεζικό σας λογαριασμό.

Με τα **πλαστά κουπόνια και τις δωροκάρτες** οι απατεώνες σάς στέλνουν μήνυμα με email ή γραπτό μήνυμα στο κινητό ή μήνυμα στα μέσα κοινωνικής δικτύωσης και ισχυρίζονται ότι έχετε κερδίσει δωροκάρτα για κάποιο πασίγνωστο κατάστημα, αλλά πρέπει να δώσετε μερικά στοιχεία για να το διεκδικήσετε. Αυτή είναι μια προσπάθεια να αποσπάσουν προσωπικά στοιχεία τα οποία μπορούν να χρησιμοποιηθούν για κλοπή ταυτότητας ή να σας στοχεύσουν με μια άλλη απάτη. Επίσης είναι γνωστό ότι προσφορές σαν αυτές προσβάλλουν τη συσκευή σας με λυτρισμικό λογισμικό (ransomware) (δείτε σελίδα 17).

Στις **απάτες με ταξιδιωτικά δώρα** οι απατεώνες ισχυρίζονται ότι έχετε κερδίσει δωρεάν διακοπές ή αεροπορικά εισιτήρια. Στην πραγματικότητα, αυτό που έχετε κερδίσει είναι η ευκαιρία να αγοράσετε κουπόνια για κατάλυμα ή πτήσεις. Αυτά τα ταξιδιωτικά κουπόνια συχνά έχουν κρυφές χρεώσεις και προϋποθέσεις, ή μπορεί να είναι πλαστά και άχρηστα. Παρομοίως, οι απατεώνες μπορεί να σας προσφέρουν καταπληκτικά πακέτα διακοπών με έκπτωση που απλά είναι ανύπαρκτα.

Προστατευθείτε

- Να θυμάστε: δεν μπορείτε να κερδίσετε χρήματα σε κλήρωση ή διαγωνισμό, εκτός αν έχετε λάβει μέρος.
- Στους διαγωνισμούς και τα λαχεία δεν χρειάζεται να καταβάλετε κάποια χρέωση για να πάρετε τα κέρδη σας – κάντε μια αναζήτηση στο διαδίκτυο χρησιμοποιώντας την ακριβή διατύπωση της προσφοράς. Μπορεί να σας βοηθήσει να επιβεβαιώσετε ότι είναι μια απάτη.
- Σκεφτείτε το προσεκτικά πριν καλέσετε ή στείλετε γραπτό μήνυμα σε αριθμό τηλεφώνου που αρχίζει με '19' - χρεώνονται με υψηλά τέλη.

Απάτες που αφορούν αγορές από το διαδίκτυο, μικρές αγγελίες και δημοπρασίες



Και οι απατεώνες αγαπούν την ευκολία που προσφέρουν οι αγορές από το διαδίκτυο.

Πώς λειτουργεί αυτή η απάτη

Καταναλωτές και επιχειρήσεις αγοράζουν και πωλούν όλο και περισσότερο στο διαδίκτυο. Δυστυχώς, οι απατεώνες προτιμούν να ψωνίζουν θύματα στο διαδίκτυο.

Οι απατεώνες μπορούν να δημιουργήσουν πολύ πειστικές **πλαστές ιστοσελίδες λιανικής πώλησης** που μοιάζουν με πραγματικές, συμπεριλαμβανομένων στα μέσα κοινωνικής δικτύωσης όπως το Facebook. Η μεγαλύτερη προειδοποίηση ότι μια ιστοσελίδα λιανικής πώλησης είναι απάτη είναι ο τρόπος πληρωμής - να είστε προσεκτικοί αν σας ζητηθεί να πληρώσετε με τραπεζικό έμβασμα ή άλλες ασυνήθιστες μεθόδους.

Η **απάτη της διαδικτυακής δημοπρασίας** περιλαμβάνει έναν απατεώνα που ισχυρίζεται ότι έχετε μια δεύτερη ευκαιρία να αγοράσετε ένα αντικείμενο στο οποίο βάλατε μια προσφορά, επειδή ο νικητής αποχώρησε. Ο απατεώνας θα σας ζητήσει να πληρώσετε έξω από την ασφαλή εγκατάσταση πληρωμής της ιστοσελίδας δημοπρασιών· αν το κάνετε, θα χάσετε τα χρήματά σας, δεν θα πάρετε αυτά που πληρώσατε και η ιστοσελίδα της δημοπρασίας δεν θα μπορέσει να σας βοηθήσει.

Η **απάτη με τις διαδικτυακές μικρές αγγελίες** είναι μια συνήθης απάτη που στοχεύει τόσο αγοραστές όσο και πωλητές. Οι αγοραστές θα πρέπει να προσέχουν τους απατεώνες που δημοσιεύουν ψεύτικες διαφημίσεις σε νόμιμες ιστοσελίδες με μικρές αγγελίες. Οι διαφημίσεις μπορούν να είναι για

ο,τιδήποτε από ενοικιαζόμενα ακίνητα έως κατοικίδια ζώα, μεταχειρισμένα αυτοκίνητα ή φωτ. μηχανές και συχνά θα έχουν φθηνή τιμή. Αν δείξετε ενδιαφέρον στο αντικείμενο, ο απατεώνας μπορεί να ισχυριστεί ότι ταξιδεύει ή ότι έχει φύγει για το εξωτερικό και ότι ένας πράκτορας θα παραδώσει τα αγαθά μετά την παραλαβή της πληρωμής. Μετά την πληρωμή δεν θα λάβετε τα αγαθά ή δεν θα μπορέσετε να επικοινωνήσετε με τον πωλητή.

Για τους πωλητές, ένας απατεώνας μικρών αγγελιών θα απαντήσει στη διαφήμισή σας με μια γενναιόδωρη προσφορά. Εάν τη δεχτείτε, ο απατεώνας θα πληρώσει με επιταγή ή με εντολή πληρωμής. Ωστόσο, το ποσό που θα λάβετε είναι μεγαλύτερο από τη συμφωνημένη τιμή. Σ' αυτή την **απάτη υπερπληρωμής**, ο «αγοραστής» ενδέχεται να σας πει ότι αυτό ήταν λάθος και θα σας ζητήσει να επιστρέψετε το επιπλέον ποσό με μεταβίβαση χρημάτων. Ο απατεώνας ελπίζει ότι θα μεταφέρετε τα χρήματα πριν ανακαλύψετε ότι η επιταγή του ήταν ακάλυπτη ή ότι η εντολή πληρωμής ήταν ψεύτικη. Θα χάσετε τα χρήματα, καθώς και το αντικείμενο που πουλήσατε, αν ήδη το στείλατε.

Προστατευθείτε

- Βρείτε με ποιον ακριβώς συναλλάσσετε. Εάν πρόκειται για αυστραλιανό λιανοπωλητή, είστε σε πολύ καλύτερη θέση να λύσετε το πρόβλημα εάν κάτι πάει στραβά.
- Ελέγξτε αν ο πωλητής είναι αξιόπιστος, έχει πολιτική επιστροφής χρημάτων και υπηρεσίες χειρισμού παραπόνων.
- Να αποφεύγετε οποιαδήποτε ρύθμιση που απαιτεί προκαταβολική πληρωμή μέσω εντολής πληρωμής, τραπεζικό έμβασμα, διεθνής μεταβίβαση χρημάτων, προπληρωμένη κάρτα ή ηλεκτρονικό νόμισμα. Είναι σπάνιο να ανακτήσετε χρήματα που αποστέλλονται μ' αυτόν τον τρόπο. Ποτέ μην στέλνετε χρήματα και μη δίνετε τα στοιχεία πιστωτικής κάρτας ή διαδικτυακού λογαριασμού σε οποιοδήποτε άτομο που δεν γνωρίζετε ή δεν εμπιστεύεστε και ποτέ μέσω email.
- Να πληρώνετε μόνο μέσω της ασφαλούς μεθόδου πληρωμής στην ιστοσελίδα- αναζητήστε τη διεύθυνση στην ιστοσελίδα που αρχίζει με «https» κι ένα σύμβολο κλειδωμένου λουκέτου.
- Μη δεχτείτε ποτέ μια επιταγή ή εντολή πληρωμής που είναι παραπάνω απ' αυτό που συμφωνήσατε και μην προωθήσετε χρήματα για οποιονδήποτε.

Απάτες που στοχεύουν υπολογιστές και κινητές συσκευές



Να θυμάστε: ο,τιδήποτε συνδέεται με το ίντερνέτ είναι ευάλωτο.

Πώς λειτουργεί αυτή η απάτη

Οι **απατεώνες που χρησιμοποιούν απομακρυσμένη πρόσβαση** σας καλούν στο τηλέφωνο ισχυριζόμενοι ότι ο υπολογιστής σας έχει μολυνθεί από ιούς. Αν ακολουθήσετε τις οδηγίες τους, θα τους επιτρέψει να έχουν πρόσβαση και να ελέγχουν τον υπολογιστή σας απ' όπου μπορούν να κλέψουν πληροφορίες ή να εγκαταστήσουν κακόβουλο λογισμικό. Μπορεί επίσης να προσπαθήσουν να σας πείσουν να αγοράσετε λογισμικό κατά των ιών «anti-virus», το οποίο συνθήως αποδεικνύεται υπερτιμημένο ή διατίθεται δωρεάν στο διαδίκτυο.

Κακόβουλο λογισμικό είναι ένας όρος για οποιοδήποτε κακόβουλο λογισμικό που μπορεί να εγκατασταθεί στον υπολογιστή σας ή σε άλλες συσκευές και περιλαμβάνει ιούς, λογισμικό κατασκοπίας (spyware), λογισμικό λυτρισισμού (ransomware), δούρειοι ίπποι (trojan horses) και συστήματα καταγραφής πληκτρολόγησης.

Το **σύστημα καταγραφής πληκτρολόγησης και το λογισμικό κατασκοπίας** επιτρέπουν στους απατεώνες να καταγράφουν ακριβώς αυτά που πληκτρολογείτε στο πληκτρολόγιό σας για να μάθουν κωδικούς πρόσβασης και τραπεζικά στοιχεία ή να αποκτήσουν πρόσβαση σε προσωπικά στοιχεία και να τα στείλουν όπου θέλουν. Μόλις εγκατασταθεί, οι απατεώνες μπορούν να ελέγχουν τους λογαριασμούς σας email και μέσω των κοινωνικών δικτύων και να αρπάξουν οποιοδήποτε πληροφορίες υπάρχουν στη συσκευή σας, συμπεριλαμβανομένων κωδικών πρόσβασης. Μπορούν επίσης

να χρησιμοποιήσουν τους λογαριασμούς σας για να στείλουν περισσότερες απάτες στους φίλους και την οικογένειά σας.

Το **λογισμικό λυτρισμού** είναι ένας άλλος τύπος κακόβουλου λογισμικού που κρυπτογραφεί ή κλειδώνει τη συσκευή σας για να σας εμποδίσει να τη χρησιμοποιήσετε μέχρι να γίνει μια πληρωμή για να την ξεκλειδώσουν. Η πληρωμή δεν εγγυάται ότι θα ξεκλειδωθεί ή ότι θα απαλλαγεί από κρυμμένους ιούς, οι οποίοι μπορούν επίσης να εξαπλωθούν και να μολύνουν άλλους υπολογιστές ή συσκευές στο δίκτυό σας.

Το κακόβουλο λογισμικό συνήθως παρέχεται μέσω email και μπορεί να φαίνεται ότι προέρχεται από νόμιμες πηγές, όπως η εταιρεία σας κοινής ωφέλειας, μια κρατική υπηρεσία ή ακόμα και η αστυνομία που δήθεν εκδίδει κάποιο πρόστιμο. Μην κάνετε κλικ στο σύνδεσμο και μην ανοίξετε οποιαδήποτε συνημμένα για τα οποία δεν είστε απολύτως βέβαιοι. Αντιθέτως μπορεί να κατεβάσετε κακόβουλο λογισμικό. Αυτές οι απάτες στοχεύουν τόσο ιδιώτες όσο και επιχειρήσεις.

Προστατευθείτε

- Να είστε προσεκτικοί για δωρεάν λήψεις από το διαδίκτυο που προσφέρουν μουσική, παιχνίδια, ταινίες και πρόσβαση σε ιστότοπους για ενήλικες. Μπορεί να εγκαταστήσουν επιβλαβή προγράμματα εν αγνοία σας.
- Να διατηρείτε τα δίκτυα του γραφείου σας, τους υπολογιστές και τις κινητές συσκευές σας ασφαλή. Να ενημερώνετε το λογισμικό ασφαλείας, να αλλάζετε τους κωδικούς πρόσβασης και να κάνετε αντίγραφα ασφαλείας των δεδομένων σας τακτικά. Να αποθηκεύετε τα αντίγραφα ασφαλείας εκτός δικτύου και εκτός διαδικτύου. Η ιστοσελίδα www.staysmartonline.gov.au εξηγεί πώς μπορείτε να κάνετε αντίγραφα ασφαλείας των δεδομένων σας και να προστατεύετε τις κινητές συσκευές σας.
- Μην ανοίγετε συνημμένα και μην κάνετε κλικ σε συνδέσμους στα email ή σε μηνύματα στα μέσα κοινωνικής δικτύωσης που έχετε λάβει από αγνώστους - απλά πατήστε delete (διαγραφή).

Κλοπή ταυτότητας



Όλες οι απάτες έχουν τη δυνατότητα κλοπής ταυτότητας. Η προστασία από τις απάτες σημαίνει επίσης να διατηρείτε τα προσωπικά σας στοιχεία ασφαλή.

Η κλοπή ταυτότητας αποτελεί απειλή σε κάθε απάτη

Οι περισσότεροι άνθρωποι συνδέουν τις απάτες με προσπάθειες παραπλάνησης για να σας πάρουν τα χρήματά σας. Ωστόσο, τα στοιχεία σας είναι επίσης πολύτιμα για τους απατεώνες. Οι απατεώνες κλέβουν τα προσωπικά σας στοιχεία για να διαπράξουν δόλιες δραστηριότητες όπως να κάνουν μη εξουσιοδοτημένες αγορές με την πιστωτική σας κάρτα ή κάνουν χρήση της ταυτότητάς σας για να ανοίξουν τραπεζικούς ή τηλεφωνικούς λογαριασμούς. Μπορεί να πάρουν δάνεια ή να διαπράξουν άλλες παράνομες δραστηριότητες στο όνομά σας. Ενδέχεται ακόμη και να πουλήσουν τα στοιχεία σας σε άλλους απατεώνες για περαιτέρω παράνομη χρήση.

Η κλοπή της ταυτότητάς σας μπορεί να είναι οικονομικά αλλά και συναισθηματικά καταστροφική. Μπορεί να χρειαστούν μήνες για να ξαναπάρετε την ταυτότητά σας και οι συνέπειες της κλοπής αυτής μπορεί να διαρκέσουν χρόνια.

Ηλεκτρονικό «ψάρεμα» (phishing) - ένας απατεώνας έρχεται ξαφνικά σε επαφή μαζί σας με email, τηλεφωνικά, με μήνυμα στο Facebook ή γραπτό μήνυμα στο κινητό προσποιούμενος ότι προέρχεται από μια νόμιμη επιχείρηση όπως τράπεζα, εταιρεία τηλεπικοινωνιών ή διαδικτύου. Σας κατευθύνουν σε μια ψεύτικη έκδοση της ιστοσελίδας της επιχείρησης ζητώντας τα προσωπικά σας στοιχεία για να επαληθεύσουν το αρχείο πελατών λόγω κάποιου τεχνικού σφάλματος. Μπορεί να καλέσουν μιμούμενοι κατάσταση ειδών πολυτελείας και ισχυρίζονται ότι κάποιος προσπαθεί να χρησιμοποιήσει την πιστωτική σας κάρτα. Σας συμβουλεύουν να επικοινωνήσετε με την τράπεζά σας, αλλά δεν κλείνουν τη γραμμή από τη δική τους πλευρά και διατηρούν τη γραμμή ανοιχτή. Όταν προσπαθήσετε να καλέσετε την τράπεζα, εξακολουθείτε να μιλάτε με τους απατεώνες που προσομοιώνουν μια πραγματική κλήση μιμούμενοι τραπεζικό υπάλληλο και ζητούν στοιχεία για το λογαριασμό

και τους κωδικούς σας ασφάλειας. Και στις δύο περιπτώσεις, ο απατεώνας αποθηκεύει τα στοιχεία που του δίνετε και στη συνέχεια τα χρησιμοποιεί για πρόσβαση στους λογαριασμούς σας.

Ψεύτικες έρευνες - Οι απατεώνες προσφέρουν δώρα ή ανταμοιβές, όπως δωροκάρτες για πασίγνωστα καταστήματα σε αντάλλαγμα να συμπληρώσετε μια διαδικτυακή έρευνα. Η έρευνα σας ζητάει να απαντήσετε διάφορες ερωτήσεις συμπεριλαμβανομένης της αποκάλυψης σημαντικών στοιχείων αναγνώρισης της ταυτότητας ή τραπεζικών στοιχείων.

Ως μέρος οποιασδήποτε απάτης - Οι απατεώνες συχνά ζητούν προσωπικά στοιχεία σε άλλες απάτες. Σε μια απάτη λαχειών, οι απατεώνες συχνά ζητούν τον αριθμό της άδειας οδήγησης ή διαβατηρίου για να «αποδείξουν την ταυτότητά σας προτού μπορέσουν να αποδεσμεύσουν το χρηματικό δώρο». Σε απάτες που αφορούν γνωριμίες ή ειδύλλια μπορεί να ζητήσουν στοιχεία «για να σπηρίξουν την αίτησή τους για βίζα ώστε να σας επισκεφθούν στην Αυστραλία».

Να θυμάστε: Η αποκάλυψη προσωπικών στοιχείων σε κάποιον απατεώνα μπορεί να είναι εξίσου κακή με το να δίνετε χρήματα. Κρατήστε τα προσωπικά σας στοιχεία για τον εαυτό σας και κρατήστε τα ασφαλή.

Προστατευθείτε

- **Σκεφτείτε το προσεκτικά τι λέτε και τι κάνετε σ' ένα διαδικτυακό περιβάλλον**

Προσέχετε όταν μοιράζεστε προσωπικές πληροφορίες στο διαδίκτυο, συμπεριλαμβανομένων μέσων κοινωνικής δικτύωσης, ιστολογίων και άλλων διαδικτυακών φόρουμ. Σταματήστε και σκεφτείτε πριν συμπληρώσετε έρευνες, πριν συμμετάσχετε σε διαγωνισμούς, πριν κάνετε κλικ σε συνδέσμους ή συνημμένα, ή ακόμα και πριν «κάνετε φίλο», «μου αρέσει» ή «μοιραστείτε» κάτι στο διαδίκτυο.

- **Προσέχετε οποιοδήποτε αίτημα για τα στοιχεία ή τα χρήματά σας**

Οι απατεώνες θα προσπαθήσουν να σας εξαπατήσουν για να τους δώσετε τα δεδομένα σας χρησιμοποιώντας ονόματα γνωστών εταιρειών ή κρατικών υπηρεσιών. Αν πιστεύετε ότι είναι απάτη, μην απαντάτε. Χρησιμοποιήστε τον τηλεφωνικό κατάλογο ή μια αναζήτηση στο διαδίκτυο για να ελέγξετε τα στοιχεία επικοινωνίας του οργανισμού. Ποτέ μην χρησιμοποιήσετε τα στοιχεία επικοινωνίας που παρέχονται στο αρχικό αίτημα.

Αν δώσατε προσωπικά στοιχεία ταυτοποίησης σε απατεώνες, επικοινωνήστε με το IDCARE στο 1300 432 273.

Απάτες που αφορούν θέσεις εργασίας και απασχόληση



Μεγάλο εισόδημα – εγγυημένο; Απίθανο!

Πώς λειτουργεί αυτή η απάτη

Οι **απάτες που αφορούν θέσεις εργασίας και απασχόλησης** περιλαμβάνουν προσφορές για εργασία από το σπίτι ή σύσταση και επένδυση σε μια «επιχειρηματική ευκαιρία». Οι απατεώνες υπόσχονται θέση εργασίας, υψηλό μισθό ή μεγάλη επενδυτική απόδοση μετά την καταβολή προκαταβολικών πληρωμών. Αυτές οι πληρωμές ενδέχεται να αφορούν κάποιο «επιχειρηματικό σχέδιο», πρόγραμμα τεχνικής κατάρτισης, λογισμικό, στολές, διαπίστευση ασφαλείας, φόρους ή τέλη. Εάν πληρώσετε τη χρέωση ενδέχεται να μη λάβετε τίποτα ή όχι αυτό που περιμένατε ή αυτό που σας υποσχέθηκαν.

Ορισμένες προσφορές θέσεων εργασίας μπορεί να αποτελούν προκάλυψη για παράνομες δραστηριότητες **ξεπλύματος βρώμικου χρήματος**, όπου σας ζητείται να ενεργήσετε ως «διαχειριστής λογαριασμού» ή «προσωπικός βοηθός» για να λαβαίνετε πληρωμές στον τραπεζικό σας λογαριασμό με την απολαβή προμήθειας και στη συνέχεια να μεταβιβάσετε τα χρήματα σε ξένα εταιρεία.

Οι απάτες με τις θέσεις εργασίας συχνά προωθούνται μέσω ανεπιθύμητων μηνυμάτων email ή διαφημίσεων σε γνωστές ιστοσελίδες μικρών αγγελιών και αναζήτησης εργασίας - ακόμα και σε κρατικές ιστοσελίδες αναζήτησης εργασίας.

Ένας μεγάλος κίνδυνος με αυτές τις απάτες θέσεων εργασίας είναι ότι μπορεί να σας ζητήσουν πολλά προσωπικά στοιχεία που δεν θα πρέπει να δίνετε, συμπεριλαμβανομένου του αριθμού φορολογικού μητρώου σας και αντιγράφων του διαβατηρίου σας ή της άδειας οδήγησης. Αυτά τα στοιχεία θα μπορούσαν αργότερα να χρησιμοποιηθούν για κλοπή ταυτότητας.

Προστατευθείτε

- Προσέχετε τις προσφορές ή πλάνα που ισχυρίζονται εγγυημένο εισόδημα ή απαιτούν προκαταβολική πληρωμή.
- Ποτέ μην συμφωνήσετε να μεταβιβάσετε χρήματα για κάποιον άλλο - αυτό είναι ξέπλυμα βρώμικου χρήματος και είναι παράνομο.
- Μη δίνετε τον αριθμό του φορολογικού μητρώου, της άδειας οδήγησης ή διαβατηρίου σας όταν κάνετε αίτηση για μια θέση εργασίας. Ίσως χρειαστεί να δώσετε αυτά τα στοιχεία αλλά μόνο αφού αρχίσετε να εργάζεστε.

Το ξέπλυμα βρώμικου χρήματος αποτελεί ποινικό αδίκημα: μην συμφωνήσετε να μεταβιβάσετε χρήματα για κάποιον άγνωστο.

Απάτες που αφορούν φιλανθρωπικά ιδρύματα και ιατρικά ζητήματα



Οι απατεώνες είναι άκαρδοι και μπορεί να χτυπήσουν κατά τη διάρκεια απεγνωσμένων περιόδων ανάγκης.

Πώς λειτουργεί αυτή η απάτη

Οι απατεώνες επωφελούνται από άτομα που θέλουν να δωρίσουν για κάποιον καλό σκοπό ή να βρουν μια απάντηση σ' ένα πρόβλημα υγείας.

Στις **απάτες που αφορούν φιλανθρωπικά ιδρύματα** οι απατεώνες συγκεντρώνουν χρήματα προσποιούμενοι ότι εργάζονται για κάποιο νόμιμο σκοπό ή φιλανθρωπικό ίδρυμα ή κάποιο πλασματικό ίδρυμα που δημιούργησαν. Συχνά οι απατεώνες εκμεταλλεύονται μια πρόσφατη φυσική καταστροφή ή κρίσιμη κατάσταση που ήταν στις ειδήσεις.

Αυτές οι απάτες εκτρέπουν τις πολύ απαραίτητες δωρεές μακριά από τα νόμιμα φιλανθρωπικά ιδρύματα. Τα φιλανθρωπικά ιδρύματα πρέπει να είναι εγγεγραμμένα στο κράτος – μπορείτε να κάνετε δωρεά με σιγουριά ελέγχοντας πρώτα την εγγραφή τους.

Οι **απάτες με τις θαυματουργικές γιατρείες** προσφέρουν διάφορα προϊόντα και υπηρεσίες που φαινομενικά μοιάζουν να είναι νόμιμα εναλλακτικά φάρμακα, συνήθως υπόσχονται γρήγορες και αποτελεσματικές θεραπείες για σοβαρές ιατρικές παθήσεις. Οι θεραπείες συχνά προωθούνται χρησιμοποιώντας ψευδείς μαρτυρίες από άτομα που έχουν «γιατρευτεί».

Οι **απάτες αδυνατίσματος** υπόσχονται εντυπωσιακή απώλεια βάρους με ελάχιστη ή καμία προσπάθεια. Αυτό το είδος απάτης μπορεί να περιλαμβάνει μια ασυνήθιστη ή περιοριστική δίαιτα, μια επαναστατική άσκηση, μια συσκευή «διάλυσης των λιπών», πρωτοποριακά χάπια, επιθέματα ή κρέμες. Μπορεί να χρειαστεί να καταβάλετε μια μεγάλη προκαταβολή ή να συνάψετε μακροπρόθεσμη συμφωνία για να λαβαίνετε συνεχείς προμήθειες.

Τα **ψεύτικα διαδικτυακά φαρμακεία** προσφέρουν παραποιημένα φάρμακα και φάρμακα σε πολύ φθηνές τιμές και μερικές φορές τα παρέχουν χωρίς ιατρική συνταγή. Αυτά τα φάρμακα μπορεί να έχουν περιορισμένα ή καθόλου δραστικά συστατικά, τα οποία μπορεί να έχουν θανατηφόρες συνέπειες για τους χρήστες.

Προστατευθείτε

- Εάν σας προσεγγίσει συλλέκτης για φιλανθρωπικό ίδρυμα στο δρόμο, ζητήστε να δείτε την ταυτότητά του. Αν έχετε αμφιβολίες για το ποιος είναι, μη δώσετε χρήματα.
- Ελέγξτε τον κατάλογο των εγγεγραμμένων φιλανθρωπικών ιδρυμάτων της Ένωσης Αυστραλιανών Μη Κερδοσκοπικών Φιλανθρωπικών Ιδρυμάτων (Australian Charities Not for Profit Association).
- Συμβουλευτείτε το γιατρό σας αν σκέφτεστε να πάρετε φάρμακα, συμπληρώματα ή άλλες θεραπείες που ισχυρίζονται ότι είναι «θαυματουργά» ή «άμεσες γιατρείας».
- Ρωτήστε τον εαυτό σας: εάν αυτή είναι πραγματικά μια θαυματουργική θεραπεία, δεν θα έπρεπε να σας το είχε πει ο γιατρός σας;

Επιχειρηματικές απάτες



Οι απατεώνες επωφελούνται από την πολυάσχολη φύση πολλών επιχειρήσεων για να τις εξαπατήσουν.

Πώς λειτουργεί αυτή η απάτη

Οι απάτες που στοχεύουν επιχειρήσεις έχουν πολλά προσωπεία και πιθανόν να χτυπήσουν στις πιο πολυάσχολες περιόδους, όπως στο τέλος του οικονομικού έτους.

Η απάτη της **πλαστικής τιμολόγησης** είναι το πιο συνηθισμένο τέχνασμα που χρησιμοποιούν οι απατεώνες κατά των επιχειρήσεων. Οι απατεώνες εκδίδουν πλαστούς λογαριασμούς για ανεπιθύμητες ή μη εξουσιοδοτημένες καταχωρίσεις, διαφημίσεις, προϊόντα ή υπηρεσίες. Η **απάτη που αφορά τον κατάλογο επιχειρήσεων** είναι ένα πολύ γνωστό παράδειγμα, όπου λαβαίνετε λογαριασμό για την καταχώριση σ' έναν δήθεν πολύ γνωστό κατάλογο. Οι απατεώνες σας εξαπατούν να εγγραφείτε, καμουφλάροντας την προσφορά ως απλήρωτο τιμολόγιο ή ως δωρεάν εγγραφή, αλλά με μια κρυφή συμφωνία συνδρομής στα ψιλά γράμματα.

Η **απάτη του ονόματος τομέα (domain name)** είναι ένα άλλο είδος τεχνάσματος που χρησιμοποιούν οι απατεώνες, με το οποίο σας εξαπατούν να εγγραφείτε για μια αυτόκλητη εγγραφή σε ονομασία τομέα διαδικτύου πολύ παρόμοιο με το δικό σας. Μπορεί επίσης να λάβετε μια πλαστή ειδοποίηση ανανέωσης για το πραγματικό σας όνομα τομέα και να πληρώσετε χωρίς να το συνειδητοποιήσετε.

Η **απάτη εφοδιασμού γραφείου** σημαίνει ότι λαβαίνετε και χρεώνεστε για προϊόντα που δεν έχετε παραγγείλει. Αυτές οι απάτες συχνά περιλαμβάνουν προϊόντα ή υπηρεσίες που παραγγέλνεται τακτικά όπως χαρτικά και είδη καθαρισμού. Οι απατεώνες συνήθως καλούν την επιχείρησή σας προσποιούμενοι ότι έχει ήδη παραγγελθεί μια υπηρεσία ή προϊόν.

Οι **απάτες επαναποστολής πληρωμής** σημαίνει ότι ένας απατεώνας χρησιμοποιεί πληροφορίες που απέκτησε παράνομη πρόσβαση (hacking) στα συστήματά σας πληροφορικής. Μετά παριστάνει έναν από τους τακτικούς προμηθευτές σας και σας λέει ότι τα τραπεζικά του στοιχεία άλλαξαν. Μπορεί να σας πει ότι πρόσφατα άλλαξε τράπεζα και μπορεί να χρησιμοποιεί επιστολόχαρτα ή λογότυπα που έχει αντιγράψει για να σας πείσει ότι είναι νομότυπα. Θα σας δώσει έναν καινούριο αριθμό τραπεζικού λογαριασμού και θα σας ζητήσει όλες οι μελλοντικές πληρωμές να διεκπεραιώνονται ανάλογα. Η απάτη συχνά εντοπίζεται μόνο όταν ο τακτικός προμηθευτής σας ρωτήσει γιατί δεν έχει πληρωθεί.

Το **λογισμικό λυτρίσμου** μπορεί να είναι εξαιρετικά επιζήμιο για οποιαδήποτε επιχείρηση. Η καλύτερη άμυνα είναι να κάνετε αντίγραφα ασφαλείας των δεδομένων σας τακτικά και να αποθηκεύετε τα αντίγραφα ασφαλείας εκτός δικτύου και εκτός διαδικτύου. Δείτε περισσότερες λεπτομέρειες στη σελίδα 17.

Προστατευθείτε

- Μην συμφωνήσετε με προσφορές ή συμφωνίες αμέσως - πάντα να ζητάτε την προσφορά γραπτώς και ζητήστε ανεξάρτητες συμβουλές εάν η συμφωνία αφορά χρήματα, χρόνο ή μακροπρόθεσμη δέσμευση.
- Ποτέ μη δίνετε τραπεζικά, οικονομικά και λογιστικά στοιχεία για την επιχείρησή σας σε κάποιον που επικοινωνεί μαζί σας απροσδόκτα τον οποίο ούτε γνωρίζετε ούτε εμπιστεύεστε.
- Οι αποτελεσματικές διαχειριστικές διαδικασίες δύνανται να συμβάλλουν σημαντικά στην αποτροπή της απάτης - να έχετε σαφώς καθορισμένες διαδικασίες επαλήθευσης και πληρωμής λογαριασμών και τιμολογίων και να εξετάζετε πολύ προσεκτικά τα αιτήματα για αλλαγή τραπεζικών στοιχείων.
- Εκπαιδεύστε το προσωπικό σας να αναγνωρίζει τις απάτες.
- Να αποθηκεύετε τα αντίγραφα ασφαλείας της επιχείρησής σας εκτός δικτύου και εκτός διαδικτύου.
- Να προσέχετε τα email στα οποία σας ζητούν να κάνετε αλλαγές στα στοιχεία πληρωμής. Να επαληθεύετε πάντοτε τις αλλαγές στις λεπτομέρειες πληρωμής απευθείας με την επιχείρηση ή το μεμονωμένο άτομο.

Πώς λειτουργούν οι απάτες – η ανατομία μιας απάτης

Οι περισσότερες απάτες ακολουθούν το ίδιο πρότυπο και μόλις το καταλάβετε τα τεχνάσματα του απατεώνα γίνονται πιο εύκολα αντιληπτά.

Αν κοιτάξετε προσεκτικά όλα τα διαφορετικά είδη απάτης που περιγράφονται σ' αυτό το βιβλίο, θα παρατηρήσετε σύντομα ότι οι περισσότερες απάτες περνούν από τρία στάδια: (1) προσέγγιση, (2) επικοινωνία και (3) πληρωμή.

Η κατανόηση των βασικών συστατικών μιας απάτης θα σας βοηθήσει να αποφύγετε την τρέχουσα σοδειά απατών και να είστε σε επιφυλακή για τις νέες απάτες που θα εμφανιστούν στο μέλλον.

1. Η προσέγγιση: μέθοδος επαφής

Όταν σας προσεγγίζουν οι απατεώνες πάντοτε συνοδεύεται από κάποια ιστορία που έχει ως σκοπό να σας κάνει να πιστέψετε ένα ψέμα. Ο απατεώνας θα προσποιηθεί ότι είναι κάτι που δεν είναι, ένας κρατικός υπάλληλος, ένας εξειδικευμένος επενδυτής, ένας υπάλληλος εταιρείας λαχείων ή ακόμα κι ένας ρομαντικός θαυμαστής.

Για να περάσει αυτά τα ψέματα σε εσάς, οι απατεώνες χρησιμοποιούν διάφορες μεθόδους επικοινωνίας.

Από το διαδίκτυο



Οι απατεώνες παραμονεύουν μέσα στο ανώνυμο περιβάλλον του διαδικτύου.

Το **email** είναι μια προτιμώμενη μέθοδος επαφής της απάτης, παρέχοντας έναν φθινό και απλό τρόπο επικοινωνίας σε μεγάλη κλίμακα. Τα email του ηλεκτρονικού «ψαρέματος» που «ψαρεύουν» για τα προσωπικά σας στοιχεία είναι το πιο συνηθισμένο είδος απάτης με email.

Οι **πλατφόρμες των μέσων κοινωνικής δικτύωσης, οι ιστοσελίδες γνωριμιών και τα διαδικτυακά φόρουμ** επιτρέπουν στους απατεώνες να σας «κάνουν φίλους» και να εισέλθουν στην προσωπική σας ζωή για να αποκτήσουν πρόσβαση στα προσωπικά σας στοιχεία, τα οποία στη συνέχεια μπορούν να τα χρησιμοποιήσουν εναντίον σας ή εναντίον της οικογένειας και των φίλων σας.

Οι **αγορές από το διαδίκτυο, οι μικρές αγγελίες και οι ιστοσελίδες δημοπρασιών** χρησιμοποιούνται από απατεώνες για να βάλουν στόχο αγοραστές και πωλητές, και η αρχική επικοινωνία συχνά γίνεται μέσω ευυπόληπτων και αξιόπιστων ιστοσελίδων ή ψεύτικων ιστοσελίδων που μοιάζουν με πραγματικές. Αναζητήστε τις ασφαλείς επιλογές πληρωμής και προσέχετε τις ασυνήθιστες μεθόδους πληρωμής, όπως εμβάσματα, Bitcoins ή προπληρωμένες κάρτες χρημάτων. Συνήθως οι πιστωτικές κάρτες προσφέρουν κάποια προστασία.

Από το τηλέφωνο



Οι απατεώνες τηλεφωνούν και επίσης στέλνουν γραπτά μηνύματα SMS.

Γίνονται **τηλεφωνήματα** από απατεώνες σε σπίτια και επιχειρήσεις για μια μεγάλη ποικιλία απατών, από απειλητικές απάτες φορολογίας έως προσφορές δώρων ή «βοήθεια» για ιούς υπολογιστών. Η διαθεσιμότητα φτηνών τηλεφωνικών κλήσεων φωνής μέσω πρωτοκόλλου ιντερνέτ (Voice Over Internet Protocol - VOIP) σημαίνει ότι τα κέντρα κλήσεων μπορούν να λειτουργούν από το εξωτερικό με αριθμούς τηλεφώνων που μοιάζουν με τοπικούς αριθμούς. Η αναγνώριση του αριθμού κλήσης μπορεί εύκολα να συγκαλυφθεί και είναι ένα από τα πολλά τεχνάσματα που χρησιμοποιούν οι απατεώνες για να σας κάνουν να πιστέψετε ότι είναι κάποιος άλλος.

Τα **γραπτά μηνύματα SMS** χρησιμοποιούνται από τους απατεώνες για να στείλουν μια μεγάλη ποικιλία απατών, συμπεριλαμβανομένων απατών που αφορούν διαγωνισμούς ή δώρα. Εάν απαντήσετε, μπορεί να χρεωθείτε με υψηλές τιμές ή να καταλήξετε να εγγραφείτε σε μια συνδρομητική υπηρεσία. Είναι ασφαλέστερο να μην απαντήσετε ή να κάνετε κλικ σε συνδέσμους που υπάρχουν στα γραπτά μηνύματα, εκτός αν γνωρίζετε από ποιον προέρχονται. Μπορεί επίσης να περιέχουν συνημμένα ή συνδέσμους για κακόβουλα λογισμικά με τη μορφή φωτογραφιών, τραγουδιών, παιχνιδιών ή εφαρμογών.

Στην πόρτα σας



Προσοχή - μερικοί απατεώνες θα έρθουν ως την πόρτα σας για να προσπαθήσουν να σας εξαπατήσουν.

Οι **απάτες από πόρτα σε πόρτα** συνήθως περιλαμβάνουν έναν απατεώνα που προωθεί αγαθά ή υπηρεσίες που δεν παραδίδονται ή έχουν πολύ κακή ποιότητα. Μπορεί ακόμη και να χρεωθείτε για εργασία που δεν θέλετε ή δεν είχατε συμφωνήσει. Μια συνηθισμένη απάτη από πόρτα σε πόρτα γίνεται από επιτήδειους εμπόρους που μετακινούνται από τόπο σε τόπο και κάνουν κακής ποιότητας επισκευές στο σπίτι ή απλά παίρνουν τα χρήματά σας και εξαφανίζονται.

Νόμιμες επιχειρήσεις μπορούν να πωλούν από πόρτα σε πόρτα αλλά πρέπει να αναφέρουν επακριβώς το όνομά τους και την ταυτότητα της εταιρείας τους και να συμμορφώνονται με άλλους κανόνες. Έχετε συγκεκριμένα δικαιώματα όταν πρόκειται για πρακτικές πώλησης από πόρτα σε πόρτα, συμπεριλαμβανομένης της επιλογής να αλλάξετε γνώμη - μάθετε περισσότερα στο www.accc.gov.au/doortodoor.

Οι απατεώνες μπορεί να παριστάνουν **ψεύτικους εργαζόμενους φιλανθρωπικών ιδρυμάτων** για να συλλέγουν δωρεές. Επωφελούνται από πρόσφατα γεγονότα όπως πλημμύρες και δασικές πυρκαγιές. Πριν κάνετε κάποια δωρεά ζητήσετε την ταυτότητά τους και δείτε το επίσημο μπλοκ αποδείξεών τους.

Η **μαζική αλληλογραφία** χρησιμοποιείται ακόμη για να αποστέλλονται **απάτες** που αφορούν **λαχεία και κληρώσεις, επενδυτικές ευκαιρίες, Νιγηριανές απάτες και πλαστές επιστολές κληρονομιάς**. Το φανταχτερό φυλλάδιο δεν αποτελεί εγγύηση ότι μια προσφορά είναι νόμιμη.

Ανεξάρτητα από τη μέθοδο παράδοσης που χρησιμοποιούν, η ιστορία τους είναι πάντα το δόλωμα κι αν τσιμπήσετε, ο απατεώνας θα προσπαθήσει να σας πάει στο επόμενο στάδιο.

2. Επικοινωνία και προπαρασκευή



Εάν τους δώσετε την ευκαιρία να μιλήσουν μαζί σας, οι απατεώνες θα αρχίσουν να χρησιμοποιούν τεχνάσματα που έχουν στην τσέπη τους για να σας πείσουν να αποχωριστείτε τα χρήματά σας.

Τα κόλπα ενός απατεώνα μπορεί να περιλαμβάνουν τα παρακάτω:

- Οι απατεώνες πλέκουν περίπλοκες, αλλά **πειστικές ιστορίες** για να πάρουν αυτό που θέλουν.
- Χρησιμοποιούν τα **προσωπικά σας στοιχεία** για να σας κάνουν να πιστέψετε ότι είχατε και παλιά συναλλαγές μαζί τους και να κάνουν την απάτη να φαίνεται νόμιμη.
- Οι απατεώνες ενδέχεται να **επικοινωνούν μαζί σας τακτικά** για να καλλιεργήσουν εμπιστοσύνη και να σας πείσουν ότι είναι φίλοι και συνεργάτες σας ή ενδιαφέρονται ρομαντικά για εσάς.
- **Παίζουν με τα συναισθήματά σας** χρησιμοποιώντας τον ενθουσιασμό μιας νίκης, την υπόσχεση μιας αιώνιας αγάπης, τη συμπάθεια σε μια κακοτυχία, την ενοχή για μη παροχή βοήθειας ή το άγχος και τον φόβο σύλληψης ή πρόστιμου.
- Οι απατεώνες αρέσκονται να δημιουργούν μια **αίσθηση επείγουσας ανάγκης** ώστε να μην έχετε χρόνο να σκεφτείτε σωστά την κατάσταση και να αντιδράσετε στα συναισθήματα και όχι στη λογική.
- Παρομοίως, χρησιμοποιούν **τακτικές πωλήσεων υψηλής πίεσης** λέγοντας ότι είναι μια περιορισμένη προσφορά, οι τιμές θα ανέβουν ή ότι η αγορά θα αλλάξει πορεία και η ευκαιρία θα χαθεί.
- Μια απάτη μπορεί να έχει όλα τα χαρακτηριστικά γνωρίσματα μιας πραγματικής επιχείρησης χρησιμοποιώντας **φανταχτερά φυλλάδια** με τεχνική ορολογία του συγκεκριμένου κλάδου που συνοδεύονται από γραφεία, τηλεφωνικά κέντρα και επαγγελματικές ιστοσελίδες.
- Με την πρόσβαση στο διαδίκτυο και το έξυπνο λογισμικό, είναι εύκολο για τους απατεώνες να δημιουργήσουν παραποιημένα **και επισημοφανή έγγραφα**. Ένα έγγραφο που φαίνεται να έχει εγκριθεί από το κράτος ή είναι γεμάτο με νομική ορολογία μπορεί να δώσει κύρος στην απάτη.

Τα κόλπα του απατεώνα έχουν σχεδιαστεί για να σας κάνουν να εγκαταλείψετε την άμυνα σας, να καλλιεργήσουν εμπιστοσύνη στην ιστορία τους και να σας κάνουν να ενεργήσετε γρήγορα ή παράλογα και να προχωρήσετε στο τελικό στάδιο – να στείλετε τα χρήματά.

3. Αποστολή χρημάτων



Μερικές φορές η μεγαλύτερη ένδειξη που έχετε ότι είναι απάτη είναι ο τρόπος που ο απατεώνας σάς ζητάει να πληρώσετε.

Η ζήτηση χρημάτων μπορεί να έρθει μέσα σε λίγα λεπτά από την απάτη ή μετά από μήνες προσεκτικής προετοιμασίας. Οι απατεώνες έχουν τις προτιμήσεις τους για το πώς να στείλετε τα χρήματά σας.

Είναι γνωστό ότι οι απατεώνες κατευθύνουν τα θύματα στο πλησιέστερο προς αυτούς **μέρος αποστολής χρημάτων** (ταχυδρομείο, υπηρεσία αποστολής εμβασμάτων ή ακόμη και τράπεζα) για να στείλετε χρήματα. Είναι γνωστό ότι παραμένουν στην τηλεφωνική γραμμή, δίνουν συγκεκριμένες οδηγίες και μπορεί ακόμη και να στείλουν ταξί για να σας βοηθήσουν σε αυτό. Οι απατεώνες είναι πρόθυμοι να δεχτούν χρήματα με οποιονδήποτε τρόπο κι αυτό μπορεί να περιλαμβάνει **άμεσες τραπεζικές μεταβιβάσεις χρημάτων, προπληρωμένες χρεωστικές κάρτες, δωροκάρτες, κάρτες Google Play, Steam ή iTunes** ή εικονικό νόμισμα όπως το **Bitcoin**. Κάθε αίτημα για πληρωμή με μια ασυνήθιστη μέθοδο είναι ένα ενδεικτικό σημάδι ότι αποτελεί μέρος μιας απάτης.

Οι πιστωτικές κάρτες συνήθως προσφέρουν κάποια προστασία και θα πρέπει επίσης να αναζητάτε ασφαλείς επιλογές πληρωμής, όπου το «https» εμφανίζεται στη διεύθυνση της ιστοσελίδας και η ιστοσελίδα έχει ένα σύμβολο κλειδωμένου λουκέτου.

Μη στέλνετε χρήματα σε κάποιον που συναντήσατε μόνο στο διαδίκτυο ή μέσω τηλεφώνου - ειδικά εάν είναι στο εξωτερικό.

Να γνωρίζετε ότι οι απατεώνες μπορούν επίσης να ζητήσουν πληρωμή με τη μορφή πολύτιμων αγαθών και ακριβών δώρων, όπως κοσμήματα ή ηλεκτρονικά είδη. Η πληρωμή χρημάτων στους απατεώνες δεν είναι το μόνο πράγμα για το οποίο πρέπει να ανησυχείτε - αν βοηθήσετε στη μεταβίβαση χρημάτων για κάποιον άγνωστο, ενδέχεται να συμμετέχετε εν αγνοία σας σε **παράνομες δραστηριότητες ξηπλύματος βρώμικου χρήματος**.

Οι χρυσοί κανόνες για να προστατευθείτε

Να επαγρυπνείτε για το γεγονός ότι υπάρχουν απάτες. Όταν έχετε να κάνετε με απροσκάλεστες επικοινωνίες από άτομα ή επιχειρήσεις, είτε απ' το τηλέφωνο, με ταχυδρομική επιστολή, email, αυτοπροσώπως είτε από ιστοσελίδα μέσω κοινωνικής δικτύωσης, πάντοτε να σκέφτεστε την πιθανότητα ότι η προσέγγιση μπορεί να είναι απάτη. Να θυμάστε ότι αν κάτι φαίνεται ότι παραείναι καλό για να είναι αληθινό, τότε μάλλον συμβαίνει αυτό ακριβώς.

Μάθετε με ποιον έχετε να κάνετε. Εάν συναντήσατε κάποιον μόνο στο διαδίκτυο ή δεν είστε σίγουροι για τη νομιμότητα μιας επιχείρησης, αφιερώστε λίγο χρόνο να κάνετε κάποια έρευνα. Κάνετε μια αναζήτηση φωτογραφιών στο Google image search (αναζήτηση εικόνων Google) ή αναζητήστε στο διαδίκτυο για άλλους που μπορεί να είχαν συναλλαγές μαζί τους.

Μην ανοίγετε ύποπτα κείμενα, αναδυόμενα παράθυρα ή email - διαγράψτε τα. Εάν έχετε αμφιβολίες, επαληθεύστε την ταυτότητα του ατόμου που ήρθε σε επαφή μαζί σας μέσω μιας ανεξάρτητης πηγής, όπως τηλεφωνικός κατάλογος ή αναζήτηση στο διαδίκτυο. Μην χρησιμοποιείτε τα στοιχεία επικοινωνίας που περιέχονται στο μήνυμα που σας έχει σταλεί.

Να φυλάσσετε με ασφάλεια τα προσωπικά σας στοιχεία. Βάλτε κλειδαριά στο γραμματοκιβώτιό σας και καταστρέψτε τους λογαριασμούς σας και άλλα σημαντικά έγγραφα σε καταστροφή εγγράφων πριν τα πετάξετε. Να κρατάτε τους κωδικούς πρόσβασης και τους προσωπικούς κωδικούς αριθμούς (PIN) σε ασφαλές μέρος. Να είστε πολύ προσεκτικοί για το πόσες προσωπικές πληροφορίες μοιράζεστε στις ιστοσελίδες των μέσων κοινωνικής δικτύωσης. Οι απατεώνες μπορεί να χρησιμοποιήσουν τις πληροφορίες και τις εικόνες σας για να δημιουργήσουν μια πλαστή ταυτότητα ή να σας βάλουν στόχο να σας εξαπατήσουν.

Προσέχετε τις ασυνήθιστες μεθόδους πληρωμής. Οι απατεώνες συχνά ζητούν πληρωμή μέσω εμβασμάτων, προπληρωμένων καρτών ακόμη και κάρτες Google Play, Steam, ή iTunes και Bitcoin. Αυτά σχεδόν πάντοτε αποτελούν ένδειξη ότι είναι μέρος μιας απάτης.

Να φυλάσσετε με ασφάλεια τις κινητές συσκευές και τους υπολογιστές σας. Να χρησιμοποιείτε πάντοτε προστασία με κωδικό πρόσβασης, μην μοιράζετε την πρόσβαση με άλλους (συμπεριλαμβανομένου εξ αποστάσεως), να ενημερώνετε το λογισμικό ασφαλείας και να δημιουργείτε αντίγραφα ασφαλείας. Προστατέψτε το δίκτυό σας WiFi με κωδικό πρόσβασης και αποφεύγετε τη χρήση δημόσιων υπολογιστών ή σημείων ασύρματης πρόσβασης WiFi για πρόσβαση στις διαδικτυακές τραπεζικές συναλλαγές ή για παροχή προσωπικών στοιχείων.

Να επιλέγετε προσεκτικά τους κωδικούς σας πρόσβασης. Να επιλέγετε κωδικούς πρόσβασης που είναι δύσκολο να μαντέψουν οι άλλοι και να τους αλλάζετε τακτικά. Ένας ισχυρός κωδικός πρόσβασης πρέπει να περιλαμβάνει έναν συνδυασμό κεφαλαίων και μικρών γραμμάτων, αριθμών και συμβόλων. Μην χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης για κάθε λογαριασμό/προφίλ και μην αποκαλύπτετε τους κωδικούς πρόσβασης σε κανέναν.

Προσέχετε οποιαδήποτε αιτήματα που ζητούν τα στοιχεία ή τα χρήματά σας. Ποτέ μην στέλνετε χρήματα και μη δίνετε αριθμούς πιστωτικών καρτών, στοιχεία διαδικτυακού λογαριασμού ή αντίγραφα προσωπικών εγγράφων σε οποιοδήποτε άτομο που δεν γνωρίζετε ή δεν εμπιστεύεστε. Μην συμφωνείτε να μεταβιβάσετε χρήματα ή αγαθά για κάποιον άλλο: το ξέπλυμα βρώμικου χρήματος αποτελεί ποινικό αδίκημα.

Να είστε προσεκτικοί όταν ψωνίζετε στο διαδίκτυο. Προσέχετε τις προσφορές που φαίνονται ότι παραείναι καλές για να είναι αληθινές και πάντα να χρησιμοποιείτε μια υπηρεσία διαδικτυακών αγορών που γνωρίζετε και εμπιστεύεστε. Σκεφτείτε προσεκτικά πριν χρησιμοποιήσετε εικονικά νομίσματα (όπως το Bitcoin) - δεν έχουν τις ίδιες προστασίες με άλλες μεθόδους συναλλαγών, πράγμα που σημαίνει ότι δεν μπορείτε να πάρετε πίσω τα χρήματά σας αφού τα στείλετε.

Πού να αποταθείτε για βοήθεια ή υποστήριξη

Εάν χάσατε χρήματα σε μια απάτη ή δώσατε τα προσωπικά σας στοιχεία σε κάποιον απατεώνα, είναι απίθανο να πάρετε τα χρήματά σας πίσω. Ωστόσο, υπάρχουν βήματα που μπορείτε να πάρετε αμέσως για να περιορίσετε τη ζημιά και να προστατευθείτε από περαιτέρω απώλεια.

Επικοινωνήστε με την τράπεζα ή το πιστωτικό σας ίδρυμα

Αν στείλατε χρήματα ή στοιχεία του προσωπικού σας τραπεζικού λογαριασμού σε κάποιον απατεώνα, επικοινωνήστε αμέσως με την τράπεζα ή το πιστωτικό σας ίδρυμα. Αυτοί ενδέχεται να σταματήσουν μια μεταβίβαση χρημάτων ή επιταγή, ή να κλείσουν τον λογαριασμό σας, αν ο απατεώνας έχει τα στοιχεία του λογαριασμού σας. Ο φορέας της πιστωτικής σας κάρτας ενδέχεται να προβεί σε «επιστροφή χρέωσης» (αντιστροφή συναλλαγής) εάν η πιστωτική σας κάρτα χρεώθηκε δόλια.

Ανάκτηση της κλεμμένης ταυτότητάς σας

Αν υποψιάζεστε ότι πέσατε θύμα κλοπής ταυτότητας, είναι σημαντικό να ενεργήσετε γρήγορα για να μειώσετε τον κίνδυνο οικονομικής απώλειας ή άλλων ζημιών.

Επικοινωνήστε με την υπηρεσία **IDCARE** - μια δωρεάν υπηρεσία που χρηματοδοτείται από το κράτος και παρέχει υποστήριξη στα θύματα εγκληματικής ενέργειας που αφορά ταυτότητα. Η IDCARE μπορεί να σας βοηθήσει να αναπτύξετε ένα σχέδιο ενεργειών για να λάβετε τα κατάλληλα μέτρα για την αποκατάσταση της ζημιάς στην υπόληψή σας, στο πιστωτικό ιστορικό σας και την ταυτότητά σας. Επισκεφθείτε τον ιστότοπο της IDCARE στο www.idcare.org ή καλέστε το 1300 432 273.

Υποβάλετε αίτηση για **Κοινοπολιτειακό Πιστοποιητικό Θύματος (Commonwealth Victims' Certificate)** – αυτό το πιστοποιητικό βοηθάει να τεκμηριώσετε ότι πέσατε θύμα εγκληματικής ενέργειας που αφορά ταυτότητα και μπορεί να χρησιμοποιηθεί για να βοηθήσει στην αποκατάσταση των πιστοποιητικών/χαρτιών σας με κρατικά ή χρηματοπιστωτικά ιδρύματα. Επισκεφθείτε το Υπουργείο Δικαιοσύνης (Attorney-General's Department) στο www.ag.gov.au (ή καλέστε το 02 6141 6666) για περισσότερες πληροφορίες σχετικά με την προστασία και την ανάκτηση της ταυτότητάς σας.

Επικοινωνήστε με μια υπηρεσία συμβουλευτικής ή υποστήριξης

Εάν εσείς ή κάποιο γνωστό σας πρόσωπο πέσατε θύμα απάτης και υποφέρετε από συναισθηματικό άγχος ή κατάθλιψη, μπορείτε να μιλήσετε με τον γενικό γιατρό σας, με επαγγελματία υγείας της περιοχής σας ή με κάποιον που εμπιστεύεστε. Μπορείτε επίσης να επικοινωνήσετε με τις υπηρεσίες παροχής συμβουλών ή υποστήριξης, όπως:

Lifeline (Γραμμή Ζωής) — όταν χρειάζεστε υποστήριξη σε μια κρίσιμη κατάσταση, επικοινωνήστε με την Lifeline στο 13 1114 (24/7) ή επισκεφθείτε το www.lifeline.org.au

Beyondblue (Υπηρεσία ψυχικής υγείας) — για πληροφορίες σχετικά με την κατάθλιψη ή το άγχος, επικοινωνήστε με το beyondblue ή 1300 224 636 ή επισκεφθείτε το www.beyondblue.org.au

Kids helpline (Γραμμή βοήθειας ανηλίκων) — τηλεφωνική και διαδικτυακή υπηρεσία συμβουλευτικής και υποστήριξης για νέους ηλικίας μεταξύ πέντε και 25 ετών. Επικοινωνήστε με τη γραμμή βοήθειας Kids helpline στο 1800 551 800 ή επισκεφθείτε το www.kidshelpline.com.au

Financial Counselling Australia (Οικονομική Συμβουλευτική Υπηρεσία Αυστραλίας) — αν βρίσκεστε σε δυσμενή οικονομική κατάσταση καλέστε το 1800 007 007 για να μιλήσετε δωρεάν με οικονομικό σύμβουλο ή επισκεφθείτε το www.financialcounsellingaustralia.org.au.

Πού να καταγγείλετε μια απάτη

Μπορείτε να βοηθήσετε άλλους καταγγέλλοντας μια απάτη στις αρμόδιες αρχές. Οι πληροφορίες σας θα βοηθήσουν αυτούς τους οργανισμούς να διαμορφώσουν μια καλύτερη εικόνα για τις τελευταίες απάτες και να προειδοποιήσουν άλλους ανθρώπους για το τι θα πρέπει να προσέχουν.

Οι παρακάτω οργανισμοί δέχονται καταγγελίες σχετικά με συγκεκριμένα είδη απάτης.

Scamwatch

Καταγγείλετε απάτες στην ACCC μέσω του Scamwatch — επισκεφθείτε το www.scamwatch.gov.au

Να είστε ένα βήμα μπροστά από τους απατεώνες

Να είστε ένα βήμα μπροστά από τους απατεώνες - επισκεφθείτε τον ιστότοπο Scamwatch για να μάθετε όλες τις πληροφορίες για απάτες που στοχεύουν καταναλωτές και μικρές επιχειρήσεις της Αυστραλίας. Μάθετε περισσότερες πληροφορίες για το πώς λειτουργούν οι απάτες, πώς μπορείτε να προστατευθείτε και τι πρέπει να κάνετε αν έχετε εξαπατηθεί.

Εγγραφείτε στην συνδρομητική υπηρεσία Scamwatch για να λαβαίνετε δωρεάν προειδοποιήσεις με email σχετικά με τις νέες απάτες που κυκλοφορούν.

www.scamwatch.gov.au

Ακολουθήστε το Scamwatch στο Twitter στο @scamwatch_gov ή http://twitter.com/Scamwatch_gov

Αν αντιμετωπίσετε κάποια απάτη σε μια ιστοσελίδα ή πλατφόρμα στα μέσα κοινωνικής δικτύωσης, καταγγείλετε την ιστοσελίδα ώστε να μπορέσουν να τη διερευνήσουν και να την απομακρύνουν. Εάν οι απατεώνες μιμούνται κάποιον νόμιμο οργανισμό όπως υπουργείο ή τράπεζα, ενημερώστε τους ώστε να προειδοποιήσουν τους άλλους.

Άλλες υπηρεσίες

Θα πρέπει επίσης να λάβετε υπόψη σας να καταγγείλετε την απάτη σας σε άλλες υπηρεσίες που ασχολούνται ειδικά για συγκεκριμένα είδη απάτης.

Είδος απάτης	Υπηρεσία
Cybercrime (Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος)	Australian Cybercrime Online Reporting Network (ACORN) (Αυστραλιανό Δίκτυο Καταγγελίας Ηλεκτρονικού Εγκλήματος) — επισκεφθείτε το www.acorn.gov.au
Χρηματοοικονομικές και επενδυτικές απάτες	Australian Securities and Investments Commission (ASIC) (Επιτροπή Κεφαλαιαγοράς Αυστραλίας) — επισκεφθείτε το www.moneysmart.gov.au ή καλέστε τη γραμμή πληροφοριών ASIC infoline στο 1300 300 630
Απάτες και κλοπές	Το αστυνομικό τμήμα της περιοχής σας – καλέστε το 13 1444
Ανεπιθύμητα email και SMS	Australian Communications and Media Authority (ACMA) (Αυστραλιανή Αρχή Επικοινωνιών και Μέσων Μαζικής Ενημέρωσης) — επισκεφθείτε το www.acma.gov.au ή καλέστε το Κέντρο Εξυπηρέτησης Πελατών ACMA στο 1300 850 115
Απάτες που αφορούν τη φορολογία	Australian Taxation Office (ATO) (Αυστραλιανή Εφορία) – για να καταγγείλετε μια φορολογική απάτη ή για να διευκρινίσετε εάν ένα άτομο που επικοινωνήσε μαζί σας από την ATO είναι νόμιμο: <ul style="list-style-type: none">• καλέστε το 1800 008 540 ή προωθήστε το email σας που αφορά φορολογική απάτη στο ReportEmailFraud@ato.gov.au
Τραπεζικές συναλλαγές	Το τραπεζικό ή χρηματοοικονομικό σας ίδρυμα

Επικοινωνήστε με την υπηρεσία προστασίας καταναλωτών της περιοχής σας

Ενώ το ACCC είναι η εθνική υπηρεσία που ασχολείται με γενικά θέματα προστασίας καταναλωτών, οι πολιτειακές αρχές και οι αρχές των επικρατειών μπορούν επίσης να σας βοηθήσουν.

Διεύθυνση Κανονιστικών Υπηρεσιών Επικράτειας Αυστραλιανής Πρωτεύουσας (Australian Capital Territory Office of Regulatory Services)	www.accessscanberra.act.gov.au 13 2281
Υπηρεσία Προστασίας Καταναλωτών Βικτώριας (Consumer Affairs Victoria)	www.consumer.vic.gov.au 1300 558 181
Υπηρεσία Δίκαιων Συναλλαγών Νέας Νότιας Ουαλίας (New South Wales Fair Trading)	www.fairtrading.nsw.gov.au 13 3220
Υπηρεσία Προστασίας Καταναλωτών Βόρειας Επικράτειας (Northern Territory Consumer Affairs)	www.consumeraffairs.nt.gov.au 1800 019 319
Υπηρεσία Δίκαιων Συναλλαγών Κουισλάνδης (Queensland Office of Fair Trading)	www.fairtrading.qld.gov.au 13 7468
Υπηρεσίες Καταναλωτών και Επιχειρήσεων Νότιας Αυστραλίας (South Australia Consumer and Business Services)	www.cbs.sa.gov.au/ 13 1882
Υπηρεσίες Καταναλωτών, Ανοικοδόμησης και Επαγγελματιών Τασμανίας (Tasmania Consumer, Building and Occupational Services)	www.cbos.tas.gov.au/ 1300 654 499
Υπουργείο Ορυχείων, Ρυθμιστική Αρχή Βιομηχανικού Κλάδου και Ασφάλειας Δυτικής Αυστραλίας (Western Australia Department of Mines, Industry Regulation and Safety)	www.consumerprotection.wa.gov.au/ 1300 304 054

Περισσότερες πληροφορίες

Η Αυστραλιανή Κυβέρνηση διαθέτει ορισμένους σημαντικούς πόρους για την προστασία και την ασφάλειά σας στο διαδίκτυο όπως:

- Stay Smart Online Service—www.staysmartonline.gov.au
- CyberSmart website—www.cybersmart.gov.au
- Stay Smart Online guides—διατίθενται στο www.staysmartonline.gov.au/get-involved/guides

www.scamwatch.gov.au