

Προφυλαχθείτε από τις απάτες

Η εμπιστοσύνη και η ασφάλεια αποτελούν κορυφαία προτεραιότητα για εμάς στην CommBank. Βλέπουμε όλο και περισσότερες περιπτώσεις πελατών που πιέζονται ή εξαπατώνται από απατεώνες για να τους στείλουν χρήματα. Αυτές οι απάτες μπορεί να είναι περίπλοκες και να έχουν διάφορες μορφές. Είναι σημαντικό να προσέχετε και να μας ενημερώνετε αν κάτι δεν πάει καλά. Για να μάθετε περισσότερα για το πώς να προστατευθείτε και να καταγγείλετε μια απάτη, ρίξτε μια ματιά στην ιστοσελίδα commbank.com.au/safe.

Ταυτοποίηση και επαλήθευση

- Κάντε τον έλεγχο ασφάλειας στην εφαρμογή της CommBank.
- Ενεργοποιήστε την πολυπαραγοντική ταυτοποίηση (multi-factor authentication), η οποία προσθέτει έναν επιπλέον έλεγχο για να αποδείξετε την ταυτότητά σας.
- Χρησιμοποιήστε το **CallerCheck** (Έλεγχος Καλούντος) για να επαληθεύσετε την ταυτότητα των καλούντων που ισχυρίζονται ότι είναι από την τράπεζα.
- Χρησιμοποιήστε το **CustomerCheck** (Έλεγχος Πελάτη) στο υποκατάστημα για να επαληθεύσετε την ταυτότητά σας στο προσωπικό μας.
- **NameCheck** (Έλεγχος Ονόματος) θα σας ειδοποιήσει αν τα στοιχεία του λογαριασμού σε μια πληρωμή που κάνετε για πρώτη φορά δεν φαίνονται σωστά.

Ασφάλεια συσκευής και πληρωμών

- Διατηρήστε ενημερωμένο το λογισμικό προστασίας από ιούς και προστατέψτε τον υπολογιστή σας από συνήθεις απειλές.
- Χρησιμοποιήστε ασφαλείς μεθόδους πληρωμής, όπως επαφή ή εισαγωγή της κάρτας σας.
- Μην μοιράζετε συσκευές που έχουν πρόσβαση στο ψηφιακό σας πορτοφόλι.

Κωδικός πρόσβασης & Προσωπικά στοιχεία

- Μην κοινοποιείτε ποτέ τους κωδικούς πρόσβασης ή PIN και να είστε προσεκτικοί όταν μοιράζεστε προσωπικά στοιχεία.
- Μη δίνετε ποτέ τον κωδικό σας NetCode σε κανέναν, συμπεριλαμβανομένου του προσωπικού της CommBank.
- Μπορείτε να αλλάξετε τον κωδικό σας πρόσβασης στο NetBank και στην εφαρμογή CommBank ανά πάσα στιγμή.
- Δημιουργήστε ισχυρούς κωδικούς πρόσβασης και να τους αλλάζετε τακτικά. Για τις χρήσιμες συμβουλές μας σχετικά με τη δημιουργία κωδικού πρόσβασης, επισκεφθείτε την ιστοσελίδα commbank.com.au/password-security.

Email, SMS και διαδίκτυο

- Μην κάνετε κλικ σε συνδέσμους σε ύποπτα email ή SMS.
- Αν δεν είστε σίγουροι για ένα μήνυμα, συζητήστε το με κάποιον που εμπιστεύεστε ή επικοινωνήστε απευθείας με τον οργανισμό μέσω των επίσημων στοιχείων επικοινωνίας.
- Κλείστε το τηλέφωνο σε αυτοματοποιημένες, ύποπτες ή απειλητικές τηλεφωνικές κλήσεις από τρίτους.
- Να είστε προσεκτικοί με τις άγνωστες επαφές στα μέσα κοινωνικής δικτύωσης και τις διαδικτυακές πλατφόρμες.

Σταματήστε. Ελέγξτε. Απορρίψτε.

Σταματήστε. Νομίζετε ότι κάτι δεν πάει καλά; Αν έχετε αμφιβολίες, το καλύτερο που έχετε να κάνετε είναι να σταματήσετε. Πάρτε μια ανάσα. **Ελέγξτε.** Ρωτήστε κάποιον που εμπιστεύεστε ή επικοινωνήστε απευθείας με τον οργανισμό, χρησιμοποιώντας τα επίσημα στοιχεία επικοινωνίας του.

Απορρίψτε Κλείστε το τηλέφωνο στον καλούντα, διαγράψτε το email, μπλοκάρτε τον αριθμό τηλεφώνου. Αλλάξτε τους κωδικούς σας πρόσβασης.

Αν πιστεύετε ότι πέσατε θύμα απάτης, επικοινωνήστε αμέσως με την CommBank στο **13 22 21**, ή στο **+61 2 9999 3283** από το εξωτερικό.

Αν τα αγγλικά δεν είναι η μητρική σας γλώσσα, η δωρεάν κρατική υπηρεσία Μεταφραστών και Διερμηνέων μπορεί να σας βοηθήσει να επικοινωνήσετε μαζί μας. Αυτή η υπηρεσία διατίθεται σε περισσότερες από 150 γλώσσες. Μπορούμε να κανονίσουμε αυτή την υπηρεσία όταν μας καλέσετε ή μας επισκεφθείτε σε υποκατάστημα.

Πράγματα που πρέπει να γνωρίζετε: Δεν θα σας στείλουμε ποτέ email ή SMS ζητώντας από εσάς τραπεζικά στοιχεία όπως το Αναγνωριστικό Πελάτη NetBank, τον κωδικό πρόσβασης ή το NetCode, ή να συμπεριλάβουμε έναν σύνδεσμο για να συνδεθείτε απευθείας από ένα email ή SMS. Να πληκτρολογείτε πάντοτε commbank.com.au σε ένα πρόγραμμα περιήγησης ή χρησιμοποιήστε την εφαρμογή CommBank για ασφαλή πρόσβαση στις τραπεζικές σας συναλλαγές. Αν κάτι σας φαίνεται ύποπτο από την CommBank, προωθήστε το στο hoax@cba.com.au και διαγράψτε το. Commonwealth Bank of Australia ABN 48 123 123 124 AFSL και Αυστραλιανή πιστωτική άδεια 2349 45.



Σημαντικές πληροφορίες που αφορούν συνήθειες απάτες



Επενδύσεις (Συμπεριλαμβανομένων κρυπτονομισμάτων)

Απατεώνες δеляάζουν άτομα με την υπόσχεση υψηλών κερδών, που συχνά περιλαμβάνουν κρυπτονομίσματα ή άλλες επενδυτικές ευκαιρίες. Οι απατεώνες ενδέχεται να επιχειρήσουν να επικοινωνήσουν μαζί σας τηλεφωνικά, με email ή μέσω πλατφορμών μέσων κοινωνικής δικτύωσης.

Χρήσιμες συμβουλές για να προστατευθείτε:

- Αν κάτι ακούγεται πολύ καλό για να είναι αληθινό, μάλλον δεν είναι.
- Να είστε προσεκτικοί με τις αυτόκλητες προσφορές και πείση να επενδύσετε ή να ενεργήσετε γρήγορα.
- Επαληθεύστε πρώτα τη νομιμότητα της εταιρείας ή του μεσίτη στον ιστότοπο ASIC.



Εξ αποστάσεως πρόσβαση

Στην περίπτωση όπου ένας απατεώνας σας καλεί και προσπαθεί να αποκτήσει πρόσβαση στους λογαριασμούς ή τη συσκευή σας, προσποιούμενος ότι είναι από μια αξιόπιστη εταιρεία ή οργανισμό.

Χρήσιμες συμβουλές για να προστατευθείτε:

- Ποτέ μην κατεβάζετε λογισμικό για εξ αποστάσεως πρόσβαση μετά από αίτημα ή υπό πείση από τρίτα πρόσωπα που σας καλούν.
- Μπορείτε πάντοτε να καλέσετε πίσω έναν οργανισμό μέσω των νόμιμων στοιχείων επικοινωνίας του, που βρίσκονται στον επίσημο ιστότοπό του.
- Αν λάβετε μια κλήση που ισχυρίζεται ότι είναι κάποιος από την CommBank, μπορείτε πάντοτε να μας ζητήσετε να επαληθεύσουμε την κλήση μέσω της λειτουργίας CallerCheck (Έλεγχος Καλούντος) μέσω της εφαρμογής.

Παραβίαση επιχειρηματικών email



Απατεώνες μπορεί να στοχεύσουν επιχειρήσεις με email από μια παραβιασμένη διεύθυνση ή email που μοιάζουν σαν να προέρχονται από μια αξιόπιστη επαφή, όπως: βοηθός, πελάτης, δικηγόρος, διευθυντής ή προμηθευτής σας.

Χρήσιμες συμβουλές για να προστατευθείτε:

- Προτού προβείτε σε πληρωμές για πρώτη φορά ή αλλάξετε τα στοιχεία πληρωμής, καλέστε τον οργανισμό στον επίσημο αριθμό επικοινωνίας του για να επιβεβαιώσετε πρώτα τα στοιχεία.
- Χρησιμοποιήστε τη λειτουργία NameCheck (Έλεγχος Ονόματος) όταν κάνετε πληρωμές, για να δείτε αν το όνομα λογαριασμού ταιριάζει με το BSB και τον αριθμό λογαριασμού που σας δόθηκαν.
- Εκπαιδεύστε τους υπαλλήλους να αναγνωρίζουν και να αναφέρουν απόπειρες ηλεκτρονικού ψαρέματος (phishing).

Ηλεκτρονικό ψάρεμα και παραπλανητικά μηνύματα



Οι απατεώνες χρησιμοποιούν παραπλανητικά email ή γραπτά μηνύματα που μπορεί να περιλαμβάνουν έναν σύνδεσμο που σας κατευθύνει σ' ένα πλαστό ιστότοπο ή ζητούν ευαίσθητα προσωπικά στοιχεία.

Χρήσιμες συμβουλές για να προστατευθείτε:

- Μην κάνετε κλικ σε συνδέσμους σε ύποπτα email ή SMS.
- Μπορείτε να επιβεβαιώσετε την αυθεντικότητα ενός μηνύματος επικοινωνώντας απευθείας με τον οργανισμό, χρησιμοποιώντας τις επίσημες διαθέσιμες μεθόδους επικοινωνίας του.
- Καταγγείτε τυχόν ύποπτα μηνύματα από την CommBank στο hoax@cba.com.au

Σημαντικές πληροφορίες που αφορούν συνήθειες απάτες



Προσωπικές σχέσεις

Απατεώνες δημιουργούν πλαστά προφίλ για να δημιουργήσουν προσωπικές σχέσεις και να παραπλανήσουν τα θύματα ώστε να τους στείλουν χρήματα ή προσωπικά στοιχεία.

Χρήσιμες συμβουλές για να προστατευθείτε:

- Ποτέ μην στέλνετε χρήματα και μη δίνετε κωδικούς πρόσβασης, στοιχεία πιστωτικής κάρτας ή λογαριασμού σε κάποιον που δεν εμπιστεύεστε.
- Κάντε μια έρευνα για τον πιθανό σύντροφό σας στο διαδίκτυο μέσω του Google ή εφαρμογών των μέσων κοινωνικής δικτύωσης. Δοκιμάστε να κάνετε μια αντίστροφη αναζήτηση φωτογραφίας για να δείτε αν οι φωτογραφίες που σας στάλθηκαν ανήκουν σε κάποιο άλλο άτομο.
- Μιλήστε στην οικογένεια και τους φίλους σας για τη διαδικτυακή σας σχέση. Ίσως μπορέσουν να σας προσφέρουν μια γνώμη και να εντοπίσουν προειδοποιητικά σημάδια που μπορεί εσείς να μην έχετε παρατηρήσει.

Ευκαιρίες απασχόλησης

Στις περιπτώσεις όπου μια προσφορά για θέση εργασίας φαίνεται να απαιτεί λίγη έως καθόλου προσπάθεια για υψηλό οικονομικό κέρδος ή υπόσχεται ότι θα βγάλετε γρήγορο χρήμα.



Χρήσιμες συμβουλές για να προστατευθείτε:

- Επταληθεύστε την εταιρεία και την προσφορά μέσω επίσημων καναλιών και κάντε μια έρευνα για την εταιρεία για να βεβαιωθείτε ότι είναι νόμιμη και ότι τώρα λειτουργεί.
- Να είστε προσεκτικοί στις προσφορές θέσεων εργασίας μέσω μέσων κοινωνικής δικτύωσης, κρυπτογραφημένης συνομιλίας, email, τηλεφώνου ή επιστολής από άτομα που δεν έχετε συναντήσει ή εταιρείες που δεν γνωρίζετε.
- Μια νόμιμη εταιρεία δεν θα απαιτήσει ποτέ να δώσετε μια προκαταβολή ή να χρησιμοποιήσει τα προσωπικά τραπεζικά στοιχεία σας για τη μεταφορά εταιρικών κεφαλαίων ή συναλλαγών.



Αγορές στο διαδίκτυο

Απατεώνες δημιουργούν διαδικτυακά καταστήματα ή διαφημίσεις για να δελιάσουν τους αγοραστές να αγοράσουν ανύπαρκτα ή πλαστά προϊόντα.

Χρήσιμες συμβουλές για να προστατευθείτε:

- Να ψωνίζετε μόνο από αξιόπιστους και ασφαλείς ιστότοπους και να είστε προσεκτικοί με οποιαδήποτε προσφορά που φαίνεται πολύ καλή για να είναι αληθινή.
- Χρησιμοποιήστε ασφαλείς μεθόδους πληρωμής και αποφύγετε την άμεση μεταφορά χρημάτων σε πωλητές.
- Μη βιάζεστε και μην πιέζεστε από διαφημίσεις που λένε «περιορισμένη προσφορά» ή «αντίστροφη μέτρηση» για το τέλος των εκπτώσεων.

Απειλές και πρόστιμα

Απατεώνες υποδύονται αρχές ή έμπιστους οργανισμούς για να αποσπάσουν χρήματα μέσω απειλών προστίμων ή νομικών ενεργειών.



Χρήσιμες συμβουλές για να προστατευθείτε:

- Κλείστε το τηλέφωνο σε άτομα που σας απειλούν και επικοινωνήστε απευθείας με τον οργανισμό.
- Ένας νόμιμος οργανισμός δεν θα σας ζητήσει ποτέ να πληρώσετε με ασυνήθιστες μεθόδους, όπως με δωροκάρτες ή κάρτες καταστήματος, κουπόνια iTunes, τραπεζικά εμβάσματα ή κρυπτονομίσματα Bitcoin.
- Αν ανησυχείτε για την ασφάλειά σας, τηλεφωνήστε στη γραμμή βοήθειας της αστυνομίας.

