Australian Banking Association

Κρατήστε τον εαυτό σας ασφαλή: προσέξτε τις απάτες

Είναι πιθανό να αυξηθούν τους επόμενους μήνες οι απάτες με θέμα τον COVID-19.

Οι απατεώνες χρησιμοποιούν ψεύτικα μηνύματα email, τηλεφωνικές κλήσεις ή SMS για να προσπαθήσουν να αποκτήσουν προσωπικές πληροφορίες. Προσποιούνται ότι είναι από την τράπεζά σας, τον Παγκόσμιο Οργανισμό Υγείας, την κυβέρνηση, φιλανθρωπικούς οργανισμούς ή νόμιμες επιχειρήσεις, όπως ταξιδιωτικοί πράκτορες, πάροχοι υπηρεσιών ηλεκτρισμού, τηλεφωνίας ή διαδικτύου ή το τοπικό σας σούπερ μάρκετ.

Προστατεύστε τον Εαυτό σας

Η τράπεζά σας δε θα στείλει ΠΟΤΕ email ή SMS να σας ζητήσει τυχόν στοιχεία λογαριασμού ή οικονομικά, και αυτό περιλαμβάνει ενημέρωση της διεύθυνσής σας ή κωδικούς για Τηλεφωνικό, Κινητό ή Διαδικτυακό Banking.

Η κυβέρνηση και άλλοι νόμιμοι οργανισμοί δε θα σας ζητήσουν ΠΟΤΕ να ενημερώσετε στοιχεία σας κάνοντας κλικ σε έναν σύνδεσμο. Σε περίπτωση αμφιβολίας, μιλήστε σε ένα φίλο ή μέλος της οικογένειας ή επικοινωνήστε απευθείας με τον οργανισμό και ρωτήστε τους.

Εάν λάβετε τηλεφώνημα από κάποιον που δε γνωρίζετε και σας ζητά προσωπικές πληροφορίες, ΚΛΕΙΣΤΕ το τηλέφωνο. Καλέστε απευθείας την εταιρεία και ελέγξτε αν σας κάλεσαν.

Μην ανοίγετε ΠΟΤΕ συνημμένα από άτομα ή οργανισμούς που δεν γνωρίζετε. Να είστε πάντα προσεκτικοί με προσφορές που ακούγονται πολύ καλές για να είναι αληθινές ή που ζητάνε πάρα πολλές πληροφορίες.

Η τράπεζά σας μπορεί να βοηθήσει, επικοινωνήστε μαζί της αμέσως εάν:

- μοιραστήκατε τα τραπεζικά σας στοιχεία απαντώντας σε τηλεφωνική κλήση, email ή σε κείμενο απάτης
- κάνατε κατά λάθος κλικ σε συνδέσμους ή κατεβάσατε συνημμένα
- παρατηρήσατε ασυνήθιστες συναλλαγές στους λογαριασμούς σας.

Πώς να εντοπίσετε μια απάτη

- Σας ζητείται να ενημερώσετε ή να επιβεβαιώσετε προσωπικά στοιχεία, όπως διεύθυνση, ημερομηνία γέννησης, στοιχεία τραπεζικού λογαριασμού, αριθμό φορολογικού μητρώου ή οποιοδήποτε PIN ή κωδικό πρόσβασης.
- Το μήνυμα email ή SMS περιέχει συνδέσμους που φαίνονται ύποπτοι. Εάν δεν είστε σίγουροι, ζητήστε βοήθεια από ένα φίλο ή μέλος της οικογένειας.
- Σας ζητείται άμεση πληρωμή ή προκαταβολή.
- Εάν η προσφορά ακούγεται πολύ καλή για να είναι αληθινή, μάλλον είναι.
- Η διεύθυνση email δεν ταιριάζει με την εταιρεία.
- Ο καλών ζητά να αποκτήσει πρόσβαση στον υπολογιστή σας εξ αποστάσεως.

Australian Banking Association

www.ausbanking.org.au

Οι καλύτερες συμβουλές να προστατεύσετε τις οικονομικές σας πληροφορίες από απάτες

- Να κλείνετε το τηλέφωνο σε ύποπτες τηλεφωνικές κλήσεις, αλλιώς μεταβείτε στον ιστότοπο της εταιρείας ή βρείτε τον αριθμό της και καλέστε την απευθείας.
- Να μη μοιράζεστε ποτέ κωδικούς πρόσβασης ή PIN. Προστατεύστε τις συσκευές σας με κωδικό πρόσβασης. Εάν χρησιμοποιείτε κοινόχρηστο υπολογιστή, μην αποθηκεύετε ποτέ κωδικούς πρόσβασης και να αποσυνδέεστε πάντα από τον λογαριασμό σας.
- Ελέγχετε τακτικά τους τραπεζικούς λογαριασμούς σας, ώστε να προσέξετε γρήγορα ύποπτες συναλλαγές.
- Αποφεύγετε να σύρετε την κάρτα σας για να πραγματοποιήσετε αγορές. Η ανέπαφη συναλλαγή και η εισαγωγή της κάρτας είναι συχνά ασφαλέστερα.
- Μπλοκάρετε τις προκαταβολές σε μετρητά σε πιστωτικές κάρτες.
- Συζητήστε με την τράπεζά σας για τον καλύτερο τρόπο προστασίας του λογαριασμού σας.
- Εάν πιστεύετε ότι έχετε πέσει θύμα απάτης, αναφέρετέ το αμέσως στην τράπεζά σας.

Υπάρχουν πολλοί τρόποι που οι απατεώνες θα προσπαθήσουν να σας κλέψουν, παρακάτω είναι οι κυριότεροι.

Ηλεκτρονικό "ψάρεμα" – Χρησιμοποιείται ένα μήνυμα email ή SMS για την απόκτηση των προσωπικών σας στοιχείων, προσποιούμενο ότι προέρχεται από μια αξιόπιστη πηγή, όπως τράπεζα, φιλανθρωπικό οργανισμό ή κυβέρνηση. Το μήνυμα φαίνεται πραγματικό και συχνά θα σας ζητά να εισαγάγετε προσωπικές πληροφορίες σε πλαστούς ιστοτόπους ή θα σας ζητήσει να κάνετε κλικ σε ένα σύνδεσμο - αυτό θα επιτρέψει στον απατεώνα πρόσβαση στον υπολογιστή σας και τις προσωπικές σας πληροφορίες.

Απάτες διαδικτυακών αγορών – οι απατεώνες προσποιούνται ότι είναι πραγματικά διαδικτυακά καταστήματα, είτε με ψεύτικο ιστότοπο είτε με ψεύτικη διαφήμιση σε γνήσιο ιστότοπο λιανικής. Οι ψεύτικοι ιστότοποι διαδικτυακών αγορών συχνά ζητούν ασυνήθιστους τρόπους πληρωμής, όπως προκαταβολή μέσω τραπεζικής εντολής, τραπεζικού εμβάσματος, διεθνούς μεταφοράς χρημάτων ή δωροκάρτας.

Επενδυτικές απάτες – ο απατεώνας ισχυρίζεται ότι είναι χρηματιστής ή διαχειριστής χαρτοφυλακίου που προσφέρει οικονομικές ή επενδυτικές συμβουλές. Θα σας ζητήσει να δώσετε χρήματα για μια επενδυτική ευκαιρία που μπορεί, ή μπορεί να μην είναι αληθινή, και στη συνέχεια κρατά τα χρήματά σας.

Απάτες πρόσβασης εξ αποστάσεως – ο απατεώνας θα ισχυριστεί ότι υπάρχει κάποιο πρόβλημα με τον υπολογιστή σας ή ότι τη σύνδεσή σας ίντερνετ έχει μολυνθεί από κακόβουλο λογισμικό. Θα προσπαθήσει να σας πείσει να εγκαταστήσει μια εφαρμογή ή να του δώσετε πρόσβαση στον υπολογιστή σας. Θα χρησιμοποιήσει αυτό για να αποκτήσει πρόσβαση στα προσωπικά σας στοιχεία ή θα απαιτήσει «χρέωση» για την επίλυση του προβλήματος.

Απάτες σχέσεων και γνωριμιών – ο απατεώνας δημιουργεί μια σχέση μαζί σας για να σας αφαιρέσει χρήματα ή δώρα. Καλλιεργεί τη σχέση διαχρονικά και ενδέχεται να σας ζητήσει να μεταφέρετε περιουσιακά στοιχεία στο όνομά του/της ή να σας ζητήσει να γίνετε κληρονόμος της διαθήκης σας. Συχνά, θα ζητήσει χρήματα για να διορθώσει ένα πρόβλημα υγείας, ταξιδιού ή οικογενειακό.

ΧΡΗΣΙΜΕΣ ΣΥΝΔΕΣΕΙΣ:

www.ausbanking.org.au/safe-savvy-a-guide-to-help-older-people-avoid-abuse-scams-and-fraud

www.esafety.gov.au/seniors/staying-safer-online

www.scamwatch.gov.au/

Σημαντική σημείωση: Το παρόν πληροφοριακό φυλλάδιο παρέχει πληροφορίες γενικής φύσης και δεν προορίζεται να βασιστείτε σ' αυτό για συμβουλές σε οποιοδήποτε συγκεκριμένο ζήτημα. Θα πρέπει να επικοινωνήσετε με την τράπεζά σας σχετικά με το πώς αυτές οι πληροφορίες ενδέχεται να ισχύουν στις περιστάσεις σας.