Έλαβα ένα ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου, τι μπορώ να κάνω;

Να το αναφέρετε, στέλνοντας ένα email στο info@centreantifraude.ca ή επικοινωνώντας με το χρηματοπιστωτικό ίδρυμα από το οποίο το μήνυμα φαίνεται να έρχεται.

Εάν λάβατε ένα από αυτά τα ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου και έχετε δώσει εν αγνοία σας προσωπικές ή οικονομικές πληροφορίες, κάντε τα εξής:

- **Βήμα 1.** Επικοινωνήστε με την τράπεζα ή με το χρηματοπιστωτικό ίδρυμα ή την εταιρεία της πιστωτικής σας κάρτας.
- **Βήμα 2.** Επικοινωνήστε με τα πρακτορεία εκτίμησης της χρηματοπιστωτικής σας ικανότητας και ζητήσετε να μπει άμεσα συναγερμός στις εκθέσεις φερεγγυότητας σας για πιθανές παράνομες εγγραφές.
    - Equifax Καναδά: 1 800 465-7166 (χωρίς χρέωση)
    - TransUnion Καναδά : 1 877 525-3823 (χωρίς χρέωση)
- **Βήμα 3.** Επικοινωνήστε με το τοπικό σας αστυνομικό τμήμα.
- **Βήμα 4.** Πάντα να αναφέρετε τα μηνύματα δολώματα. Αν έχετε απαντήσει σε ένα ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου, να το αναφέρετε στέλνοντας ένα e-mail στο

info@centreantifraude.ca

AUTORITÉ DES MARCHÉS FINANCIERS

ACCÉSSS

Alliance des Communautés Culturelles pour l'Égalité dans la Santé et les Services Sociaux

ΤΙ ΣΗΜΑΙΝΕΙ Η ΑΠΑΤΗ ΣΤΟ WEB Η ΤΟ FISHING

Τι σημαίνει η απάτη στο Web ή το fishing

Λαμβάνετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου από μια εταιρεία με την οποία ήδη έχετε συνεργασία. Σας ζητούν να ενημερώσετε αμέσως τα προσωπικά σας στοιχεία. Συνήθως το μήνυμα ηλεκτρονικού ταχυδρομείου σας ενημερώνει ότι:

- Η εταιρεία υπήρξε θύμα απάτης
- Κάποιος προσπαθεί να αποκτήσει πρόσβαση στο λογαριασμό σας
- Ένας νέος νόμος απαιτεί από το ίδρυμα να σας ζητήσει να ενημερώσετε τα στοιχεία σας
- Άλλος λόγος

Αυτή η απάτη ονομάζεται επίσης και «σφετερισμός εμπορικού σήματος» (π.χ.: ένα μήνυμα ηλεκτρονικού ταχυδρομείου που προέρχεται δήθεν από τη τράπεζα Caisses Desjardins).

Πώς να αναγνωρίσετε ένα τέτοιο μήνυμα και τις διαφορές από ένα αυθεντικό μήνυμα;

- Το περιεχόμενο των e-mail ή των μηνυμάτων κειμένου που αποτελούν δόλωμα έχει σχεδιαστεί για να προκαλέσει μια παρορμητική αντίδραση από εσάς. Αυτά τα μηνύματα σας ανακοινώνουν συναρπαστικά νέα που απαιτούν άμεση απάντηση με ψευδείς ισχυρισμούς. Το e-mail δόλωμα δεν είναι γενικά εξατομικευμένο και περιέχει ορθογραφικά λάθη.
- Σε γενικές γραμμές, αυτά τα μηνύματα σας ζητούν να ενημερώσετε, να επικυρώσετε ή να επιβεβαιώσετε τις πληροφορίες του λογαριασμού σας, διαφορετικά οι συνέπειες θα είναι δυσάρεστες. Μπορούν επίσης να σας ζητήσουν να κάνετε ένα τηλεφώνημα.

Προσοχή! Συχνά, το μήνυμα ή η ιστοσελίδα περιλαμβάνουν λογότυπα που φαίνονται αυθεντικά, καθώς και άλλες πληροφορίες αναγνώρισης που πάρθηκαν από νόμιμες ιστοσελίδες. Οι κρατικές υπηρεσίες, τα χρηματοπιστωτικά ιδρύματα και οι υπηρεσίες ηλεκτρονικών πληρωμών είναι συνηθισμένοι στόχοι για την παραβίαση του εμπορικού σήματος.

Τι ψάχνουν οι απατεώνες ;

Τον αριθμό της κοινωνικής σας ασφάλισης, το ονοματεπώνυμό σας, την ημερομηνία γέννησης, την πλήρη διεύθυνση, το πατρικό όνομα της μητέρας σας, ονόματα χρηστών και κωδικούς πρόσβασης σε ηλεκτρονικές υπηρεσίες, τον αριθμό της άδειας οδήγησής σας, προσωπικούς αριθμούς αναγνώρισης (PIN), πληροφορίες για τις πιστωτικές σας κάρτες (αριθμούς, ημερομηνίες λήξης και τα τρία τελευταία ψηφία στο πίσω μέρος της κάρτας σας) και αριθμούς τραπεζικών σας λογαριασμών.

Για ποιό σκοπό μπορούν να χρησιμοποιηθούν οι πληροφορίες σας;

Χάρη στις πληροφορίες σας, οι απατεώνες μπορούν να έχουν πρόσβαση σε τραπεζικούς σας λογαριασμούς, να ανοίξουν νέους λογαριασμούς, να μεταφέρουν το υπόλοιπο των λογαριασμών σας, να ζητούν δάνεια, πιστωτικές κάρτες και άλλες υπηρεσίες, να κάνουν αγορές, να έχουν πρόσβαση στο προσωπικό σας λογαριασμό, να κρύβουν εγκληματικές δραστηριότητες, να λαμβάνουν παροχές της κυβέρνησης ή να αποκτήσουν διαβατήριο.