Avete ricevuto una e-mail sospetta: cosa potete fare ?

Segnalatelo tempestivamente inviando una e-mail a info@centreantifraude.ca o comunicandolo all'istituzione finanziaria dalla quale sembra provenire.

Se avete ricevuto messaggi di posta elettronica sospetti e avete inconsapevolmente fornito dati personali o finanziari, effettuate le seguenti operazioni:

- **Step 1.** Informate la vostra banca o istituto bancario o la compagnia emittente la vostra carta di credito.
- **Step 2.** Informate gli agenti di valutazione del credito e chiedete che avvisi di frode sono elencati nei vostri rapporti di credito
    - Equifax Canada
      Numero gratutito: 1 800 465-7166
    - TransUnion Canada
      Numero gratutito: 1 877 525-3823
- **Step 3.** Informate il servizio di polizia locale.
- **Step 4.** Segnalate sempre il tentativo di phishing. Se avete risposto a una e-mail sospetta, segnalatela inviando una e-mail a info@centreantifraude.ca

info@centreantifraude.ca

AUTORITÉ DES MARCHÉS FINANCIERS

ACCÉSSS

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

COS'È LA TRUFFA VIA INTERNET O IL PHISHING?

Cos'è la truffa via internet o il phishing?

L'utente riceve una e-mail che simula, nella grafica e nel contenuto, quello di una istituzione nota al destinatario. Viene richiesto di aggiornare immediatamente i dati personali. La mail di solito informa che:

- La società stessa é stata vittima di una frode;
- Qualcuno sta cercando di accedere al vostro conto internet;
- Una nuova normativa obbliga la società a richiedere l'aggiornamento dei vostri dati;
- Etc.

Viene anche chiamato "brand spoofing" (esempio: una e-mail che proviene presumibilmente da Caisses Desjardins).

Come riconoscere un messaggio falso da un messaggio autentico ?

- Il contenuto di una e-mail o di un messaggio di testo gancio, è progettato per provocare una reazione impulsiva da parte vostra. In queste e-mail "Esca", viene annunciata una notizia entusiasmante o sconvolgente che richiede però una risposta immediata con falsi pretesti. Le e-mail esca solitamente non sono personalizzate e hanno spesso degli errori ortografici.
- In genere, tali messaggi vi chiederanno di aggiornare, convalidare o confermare le informazioni del vostro account, altrimenti le conseguenze potrebbero essere catastrofiche. A volte potrebbero anche chiedervi di effettuare una telefonata.

Attenzione! Spesso il messaggio o il sito web contengono loghi che sembrano autentici così come altre informazioni analoghe a quelle contenute in siti Web legittimi. Le agenzie governative, gli istituti finanziari e i servizi di pagamenti elettronici costituiscono settori facilmente utilizzati per il brand spoofing (usurpazione del marchio).

Che cosa cercano i truffatori?

Il vostro numero di previdenza sociale, il vostro nome, cognome, data di nascita, l'indirizzo completo, il nome da nubile di vostra madre, i vostri nomi utente e le password per i servizi online, il numero di patente di guida, i numeri di identificazione personale (PIN), le informazioni sulla carta di credito (numeri, date di scadenza e le ultime tre cifre sul retro della carta) ed i numeri dei vostri conti bancari.

A cosa servono i vostri dati personali ?

Grazie alle vostre informazioni, i phisher (truffatori) possono accedere ai vostri conti bancari, aprire nuovi conti, trasferire il saldo dei vostri conti ad altri conti correnti, richiedere prestiti, carte di credito e altri beni o servizi, fare acquisti, accedere al vostro account personale, riuscendo a nascondere attività criminali, a ricevere sussidi statali o ottenere un passaporto.