Recebi uma mensagem eletrónica suspeita, o que devo fazer?

Reporte-a enviando uma mensagem eletrónica para info@centreantifraude.ca ou ao entrar em contacto com a instituição financeira com a qual a mensagem parece vir.

Se recebeu uma das mensagens eletrónicas suspeitas e forneceu, sem o saber, os dados pessoais ou financeiros, faça o seguinte:

- **Fase 1.** Comunique com o seu banco, instituição financeira ou a empresa emissora do seu cartão de crédito.
- **Fase 2.** Comunique com as agências de avaliação do crédito e peça-lhes que sejam inscritas alertas de fraude nos seus relatórios de crédito.
    - Equifax Canada
      Número gratuito: 1 800 465-7166
    - TransUnion Canada
      Número gratuito: 1 877 525-3823
- **Fase 3.** Comunique com o serviço de polícia.
- **Fase 4.** Denuncie sempre o phishing. Se respondeu a uma mensagem eletrónica suspeita, reporte-o enviando uma mensagem eletrónica para

info@centreantifraude.ca

AUTORITÉ DES MARCHÉS FINANCIERS

ACCÉSSS

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

O QUE SIGNIFICA A FRAUDE NA WEB OU PHISHING?

O que significa a fraude na WEB ou phishing?

Recebe uma mensagem eletrónica duma sociedade com a qual faz negócios. Pedem-lhe para atualizar imediatamente os seus dados pessoais. O correio eletrónico informa-vos, geralmente, que:

- A sociedade foi vítima de fraude;
- Alguém tenta ter acesso à sua conta;
- Uma nova lei obriga a instituição a pedir-vos para atualizar os seus dados pessoais.
- Etc.

Chamamos, igualmente, este crime de «usurpação de marca» (exemplo: um correio eletrónico proveniente, supostamente, das Caixas Desjardins).

Como reconhecer uma mensagem deste tipo e diferenciá-la de uma mensagem autêntica?

- O conteúdo dum correio eletrónico ou de um SMS-alvo visa provocar uma reação impulsiva do seu lado. Estas mensagens eletrónicas anunciam-vos uma notícia excitante ou perturbante e pedem-vos uma resposta imediata sob um falso pretexto. As mensagens eletrónicas-alvo não são normalmente personalizadas e contêm erros ortográficos.
- Regra geral, as mensagens deste género pediram para atualizar, validar ou confirmar os dados pessoais da sua conta, caso contrário as consequências poderão ser prejudiciais. Poderão também pedir-vos para fazer uma chamada telefónica.

Atenção! Frequentemente, a mensagem ou o site WEB inclui os logotipos que parecem autênticos, bem como outras informações de identificação retiradas dos sites WEB legítimos. Os organismos governamentais, as instituições financeiras e os serviços de pagamento eletrónico são alvos comuns de violação da marca.

O que procuram os fraudadores?

O seu número de segurança social, o seu nome completo, a sua data de nascimento, a sua morada completa, o nome de solteira da sua mãe, os seus nomes de utilizador e palavras-passe dos serviços da internet, o número da sua carta de condução, os números da sua identificação pessoal, os dados dos seus cartões de crédito (números, datas de expiração e os últimos três números que estão no verso do cartão) e os números das suas contas bancárias.

Para que poderão servir os seus dados?

Graças à sua informaçao, os fraudadores poderão ter acesso às suas contas bancárias, abrir novas contas, transferir o saldo das suas contas, pedir empréstimos, cartões de crédito e outros bens ou serviços, realizar compras, aceder à sua conta eletrónica pessoal, ocultar atividades criminosas, receber os benefícios do governo ou obter um passaporte.