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

AUTORITÉ DES MARCHÉS FINANCIERS

**¿Qué significa el fraude por el Internet o el «*phishing*»?**

Vd. recibe un mensaje electrónico de una compañía con la que tiene negocios. Se le pide que ponga al día inmediatamente sus datos personales. Por lo general, dicho mensaje le informaría que:

- La compañía ha sido estafada;
- Alguien trataría de acceder a su cuenta;
- Una nueva ley exige que la institución le pida a Vd. que revise todos sus datos personales;
- Etcétera

A este tipo de crimen se le llama también « usurpación de marca » (por ejemplo: un mensaje electrónico que pretende venir de una sucursal del Banco Desjardins).

**¿Cómo percatarse que un mensaje es falso a diferencia de uno auténtico?**

- El contenido de un mensaje electrónico o de tipo *texting* fraudulento intenta desatar una reacción impulsiva de su parte. Dicho tipo de mensaje le hace una advertencia dramática o alarmante, y le exige una respuesta inmediata bajo un pretexto falso. Por lo general, los mensajes de tipo *phishing* no son personalizados, y tienden a contener faltas de ortografía.
- Por regla general, los mensajes de esta índole le piden que ponga al día, o que valide o confirme los datos de su cuenta o, si nó, le advierte que las consecuencias pudieran ser muy desagradables. También se le pediría quizás de hacer una llamada telefónica a un número de los mismos estafadores.

**¡Atención!** A menudo, el mensaje o el sitio Web contienen emblemas corporativos que parecen ser auténticos u otros datos de identificación que han sido copiados de sitios Web legítimos. Las agencias gubernamentales, las instituciones financieras y los servicios de paga electrónicos constituyen generalmente blancos ideales para la usurpación de marcas.

**¿Qué tratan de obtener los estafadores?**

Su número del seguro social, su nombre completo, su fecha de nacimiento, su dirección postal completa, el apellido de soltera de su madre, sus apelaciones de utilizador de correos electrónicos y su contraseña de acceso al Web, su número de licencia de conducir automóviles, sus números de identificación personales (NIP) para las cajas de banco automáticas, información sobre sus tarjetas de crédito (números, fechas de expiración y las tres últimas cifras inscritas al verso de su tarjeta) y sus números de cuentas de banco.

**¿Para qué les sirven sus datos a los estafadores?**

Gracias a sus datos, los estafadores pueden acceder a sus cuentas de banco, abrir nuevas cuentas, trasferir sus fondos bancarios, agenciar préstamos, obtener tarjetas de crédito y otros bienes o servicios, hacer compras, acceder a su cuenta electrónica personal, esconder actividades criminales, recibir subsidios del gobierno u obtener un pasaporte.

**¿Si he recibido un mensaje electrónico sospechoso, qué puedo hacer?**

Denúncielo enviándole un mensaje a info@centreantifraude.ca o llamando a la institución financiera de la que pretende originarse.

**Si Vd. ha recibido un mensaje electrónico sospechoso y ha transmitido datos personales o financieros sin darse cuenta, haga lo siguiente:**

- **Etapa 1.** Comuníqueselo inmediatamente a su banco, institución bancaria o a la compañía que le emitió su tarjeta de crédito.
- **Etapa 2.** Comuníquese con las agencias de evaluación de crédito; y pídales que alertas al fraude sean inscritas en sus reportes de solvencia.
    - Equifax Canada
      Número gratuito: 1 800 465-7166
    - TransUnion Canada
      Número gratuito: 1 877 525-3823
- **Etapa 3.** Comuníqueselo a su cuartel de policía local.
- **Etapa 4.** Denuncie siempre las estafas de tipo «*phishing*». Si Vd. responde a cualquier mensaje electrónico sospechoso, denúncielo enviando un mensaje a **info@centreantifraude.ca**