Scotiabank: ¿Cómo proteger tu dinero de fraudes y robos?

La pandemia de la COVID-19 ha generado que muchas personas opten por realizar sus compras a través de canales digitales para anteponer la seguridad y cuidar su salud. Desde pedir comida, comprar ropa, regalos, hasta paquetes de entrenamiento en línea, son ahora una realidad cada vez más frecuente en las familias peruanas. En el 2020, **58% de las compras en el Perú se pagaron a través de medios digitales,** según Lineo.

Sin embargo, es importante tener en cuenta que personas inescrupulosas están aprovechando el aumento del comercio electrónico para crear modalidades de estafa en aplicaciones y páginas web falsas, de las cuales obtienen información personal. Por esa razón, **Scotiabank te brinda algunos consejos para identificar y proteger tus ahorros** de este tipo de situaciones.

Sitios web falsos

Si recibes un correo electrónico de una empresa conocida o ves un anuncio de esta en redes sociales, cuestiona la veracidad del remitente, no siempre estos mensajes o publicaciones son verídicos. Los estafadores crean páginas y redes falsas y se hacen pasar por empresas de tu confianza con la finalidad de obtener datos de tus tarjetas.

 Siete acciones clave para gestionar los riesgos de ciberseguridad

 Sunarp autoriza emisión vía internet de copias informativas de títulos archivados

Pero ¿cómo saber si una empresa o un sitio web es real o no? Hazte las siguientes preguntas:

- ¿Hay errores de ortografía y gramática?
- ¿Te llegaron enlaces desde correos o SMS desconocidos o no confiables?
- ¿El sitio web se ve mal diseñado o tiene enlaces que no funcionan?
- ¿No muestra la dirección y/o el número de teléfono de la empresa?
- ¿No ofrece políticas de venta, devolución y privacidad claras?
- ¿El sitio web pide datos de la tarjeta de crédito mucho antes de efectuar una compra?

Si notas alguna de estas características, evita realizar la transacción o colocar cualquier tipo de información personal. Es preferible abrir una nueva página en el navegador y acceder al sitio web de la empresa a través de una búsqueda en el explorador de tu preferencia.

Seguros para proteger sus finanzas

Muchos bancos tienen programas de seguros para proteger tus ahorros de posibles fraudes y estafas e incluso promueven campañas para que sus clientes sigan ahorrando.

Por ejemplo, **Scotiabank premia a las personas que se preocupan por su futuro y ahorran** responsablemente; por eso sorteará entre quienes abran sus cuentas y compren seguros 9 camisetas del **FC Barcelona** autografiadas por estrellas del club como **Messi.**

“En Scotiabank, buscamos acompañar a nuestros clientes con la mejor oferta de productos financieros que ya les ofrecemos, pero también recompensarlos por su disciplina financiera con un premio que sabemos que les interesará”, expresó **Ignacio Quintanilla, Vicepresidente Senior de Banca Retail de Scotiabank.**

Cuidado con las app falsas

Son cada vez más las tiendas y proveedores de servicios que optan por una aplicación propia e invitan a sus clientes a descargarlas y realizar sus compras por este medio.

Sin embargo, **las aplicaciones también pueden ser falsas.** Si bien App Store de Apple y Play Store de Google constantemente

controlan las aplicaciones que aparecen en sus catálogos para evitar la aparición de algunas que son utilizadas para estafas, hay la posibilidad de que una app fraudulenta pueda burlar estos monitoreos.

Pero ¿qué debemos verificar antes de descargar y utilizar alguna aplicación? De acuerdo a un estudio de la Asociación Bancaria Canadiense debemos tener en cuenta lo siguiente:

- ¿El nombre del editor de la app no es el mismo que el de la aplicación que aparece para descarga? ¿Es incorrecta la ortografía?
- ¿No presenta evaluaciones y un puntaje asignado por los usuarios?
- ¿Requiere de un número significativo de permisos para su instalación?
- ¿Tiene múltiples avisos publicitarios emergentes o pide constantemente información personal?

Si percibes alguna de las señales anteriores, mejor no descargar la aplicación o desinstalarla por completo. Para reconocer una aplicación verídica, visita el sitio web de la empresa y haz clic en el enlace directo a su aplicación y así puedes asegurarte de descargar la correcta.