Publicado en Madrid el 07/04/2020

Diez consejos para detectar y evitar el fraude online en tiempos de uso intensivo de Internet

El boom del comercio online, con crecimientos de hasta el 55% desde que comenzó el aislamiento por coronavirus, de la socialización digital y de las fake news han propiciado un aumento de las estafas, según Biocryptology

En las últimas semanas el cambio de hábitos y el afán de información y solidaridad consecuencia del coronavirus han multiplicado las estafas y los ciberataques. Entre otros, los ataques online a centros hospitalarios, supuestas páginas web creadas para promover donaciones o emails y mensajes aparentemente reales cuyo objetivo es el robo de credenciales (phishing).

La actividad de los e-commerce ha crecido entre un 20 y un 55% desde que comenzó la crisis del coronavirus, particularmente en los sectores de alimentación, deportes y farmacia, según datos de Biocryptology. La compañía de software para identificación en base a los datos biométricos de las personas ha lanzado una serie de recomendaciones a tener en cuenta para para evitar a hackers y desaprensivos:

- Si se compra online por primera vez, usar páginas conocidas. Buscar comentarios de otros consumidores sobre la empresa, informarse sobre su política de devoluciones, plazo de entrega, gastos de envío y comprobar que lleva a una página segura para hacer el pago.

- Usar sitios web con cifrado (certificados HTTPS), que ayuda a proteger la información más confidencial de los asistentes, como es el caso de las tarjetas de crédito. Es importante diferenciar las páginas que utilizan cifrado (identificadas con un candado cerrado en el navegador) de las que no (candado abierto). Se debe desconfiar de sitios web que no cifren la información y nunca incluir datos sensibles

- Comprobar los correos electrónicos. Durante estos días se reciben una avalancha de mails de e-commerces, apps, entidades bancarias, seguros, etc. que ofrecen premios, ganancias o propuestas laborales durante el confinamiento. Es muy importante comprobar la autoría de los mismos y extremar la precaución ante correos de empresas o personas que no se conocen. En muchas ocasiones, detrás de un beneficio fácil suele haber una estafa escondida.

- Phishing. El robo de credenciales para suplantación de identidad es uno de los delitos más extendidos en la red. Para evitarlo hay que asegurarse de que los correos que se abren corresponden a los sitios oficiales desde donde se escribe. El phishing se esconde en páginas y correos que parecen ser de la propia compañía y que, en realidad, son de un tercero que simula su apariencia. En ocasiones es muy difícil de detectar, porque los estafadores utilizan logos de la marca, un lenguaje similar y un mensaje más o menos coherente. Comprobar que el correo no tenga errores gramaticales, que las direcciones o enlaces del email llevan a la página oficial de la compañía y no a una parecida, que no contengan ficheros sospechosos o que demanden una respuesta inmediata o urgente.

Desconfiar si piden nuevamente información que ellos ya deberían conocer.

- Proteger las credenciales de identificación web (usuario y contraseña). Una alerta de peligro clara es que alguien quiera que se envíe la contraseña por cualquier motivo, aunque parezca razonable. Los datos de acceso a cualquier servicio son personales y secretos y nadie debe requerírtelos. Los sistemas de identificación que utilizan la biometría de las personas (huella, rostro o iris), como es Biocryptology, pueden ayudar en este aspecto, al evitar la suplantación de identidad.

- Acudir directamente a las empresas. Las compañías tienen normalmente servicios de atención telefónica, direcciones de email oficiales de consulta y chats online. Si se duda de la veracidad del mensaje, confirmarlo con el proveedor oficial.

- Las tarjetas de crédito. Son otra fuente de riesgo permanente. En breve mejorará la seguridad al imponerse la obligación para que las entidades utilicen sistemas de autenticación reforzada de clientes (SCA). Entre tanto y como norma general, se debe seguir las recomendaciones de la entidad emisora y asegurarnos de introducir los datos sólo en páginas seguras.

- Redes sociales. Las redes sociales se están convirtiendo en un e-commerce más. A través de ellas se pueden adquirir productos. Es importante pagar de forma segura y tomar una serie de precauciones, por ejemplo, asegurarse de no dejar los datos de la tarjeta guardados en los perfiles, ya que alguien podría acceder a ellas y adquirir productos.

- Extremar la seguridad. No se debe enviar a nadie las claves personales y bancarias por email, WhatsApp ni otros sistemas online. Si se necesita dar los datos personales a una tienda o un amigo, lo mejor es hacerlo por teléfono.

- Evitar la difusión de un mensaje sin contrastar previamente. El deseo de ayudar hace a la gente vulnerable porque baja la guardia. Es importante detener la cadena de difusión de mentiras, fraudes o falsas oportunidades laborales como las que están llegando por WhatsApp. La mejor manera de informarse es acudir a fuentes oficiales y a los medios de comunicación. La difusión de mentiras y bulos contribuye al aumento de la crispación.

Javier González, director de Biocryptology, asegura que estas prácticas fraudulentas están cada vez más extendidas porque los ciberdelincuentes aprovechan estos tiempos de incertidumbre para actuar. “Nadie, ni los más experimentados usuarios, están libres de caer en una estafa, una trampa digital o participar en la propagación de un bulo o de fake news. De igual forma, nuestros datos personales y bancarios pueden verse comprometidos, por lo que es importante extremar la precaución”.

Para ampliar información, y ante cualquier duda o confusión, se puede recurrir al Instituto Nacional de Ciberseguridad (INCIBE), que entre otras labores presta servicios de información y de difusión de alertas de seguridad. En el caso de padecer alguna estafa, se debe denunciar cuanto antes a los cuerpos y fuerzas de seguridad del Estado. Aunque se considere que la pérdida individual pueda ser

pequeña, ten en cuenta que los ciberdelincuentes pueden haber estafado a centenares o miles de personas. Al igual que con los bulos, hay que detener la cadena.

Datos de contacto:
Círculo de Comunicación
910001948

Nota de prensa publicada en: Madrid

Categorías: Nacional E-Commerce Ciberseguridad Recursos humanos Consumo

NotasdePrensa
https://www.notasdeprensa.es