Phishing: ¿Cómo evitar caer en este tipo de estafa digital?

En el mundo digital no siempre existe total seguridad, por lo que siempre hay que tener cuidado al momento de hacer efectivo el registro de datos personales, realizar transacciones bancarias o simplemente consumir información.

Una de las estafas digitales más comunes es el *phishing*, una modalidad que busca enviar información fraudulenta a las personas para robar sus datos personales.

En ese sentido, Gianncarlo Gómez Morales, profesor del Diploma Internacional en Gestión de la Ciberseguridad y Privacidad de ESAN Graduate School of Business, presenta las principales consideraciones para evitar caer en el phishing, y en este tipo de engaños.

1. Correo electrónico fraudulento

No te sorprendas si resultas ser un presunto ganador de un departamento, auto u otro “gran premio o vale de consumo” porque este tipo de anuncios por correo electrónico se ha vuelto algo común. El ciberdelincuente solicita al usuario ingresar a una página web enlazada al correo enviado que es idéntica a la real.

Una vez allí, solicitan que la persona ingrese sus tarjetas y contraseñas. Desde ese momento, los hackers obtienen tus datos personales. Si recibes un correo de este tipo es necesario que no hagas clic en vínculos ni archivos adjuntos.

2. Llamada telefónica

Las llamadas telefónicas anónimas ocurren todos los días y buscan hacerse pasar por reconocidas empresas, agencias de viajes o negocios similares que otorgan grandes premios o vales de consumo. Por el impacto de la noticia, muchas personas caen en esa trampa y revelan información personal.

Para prevenirlo, es conveniente no contestar números desconocidos ni llamadas de otros países. En caso de contestar, no dar ni corroborar ningún dato.

3. Mensaje de texto

El hacker envía un mensaje de texto al teléfono donde se pide hacer clic en un enlace específico. Una vez que el usuario ingresa, se le pide que rellene los espacios en blanco con información de tarjetas de créditos u otro tipo de información confidencial.

Para evitar estas estafas, es necesario saber que las empresas nunca te van a enviar un SMS con enlaces pidiéndote tus claves para acceder a la cuenta.

4. Sitios web fraudulentos

Es importante recordar que no todo lo que vemos es real. Este fraude ocurre cuando las personas ingresan a una página web y la misma contiene enlaces fraudulentos. En ocasiones muchas plataformas se hacen pasar por una web confiable para poder robar dinero o para obtener la identidad digital.

Debes investigar antes de realizar tus compras y fijarte si en la URL de las páginas en las que navegas aparece el candado de seguridad (certificado SSL que es un protocolo de seguridad que hace que tus datos naveguen por la red de forma segura entre el usuario y la página web).

5. Redes sociales

Este tipo de estafa digital se da cuando se recibe solicitud de amistad de personas desconocidas o de personas que se están haciendo pasar por otra identidad, con el ánimo de robar información.

Para evitar esto, se recomienda no aceptar solicitudes ni ingresar a tus cuentas desde computadoras de terceros. Además, para mayor seguridad, se sugiere no reutilizar tus claves para las distintas plataformas.

En caso de ser víctima de un fraude digital o phishing, es necesario que se notifique a la entidad financiera correspondiente. Adicionalmente, se puede ingresar una denuncia virtual aquí o a través de la División de Investigación de Delitos de Alta Tecnología.