Ciberseguridad para principiantes

Consejos generales y errores que se deben evitar

1. Reconocer el origen de los correos electrónicos, SMS y llamadas telefónicas fraudulentas

La mayoría de las estafas en línea se transmiten a través de llamadas telefónicas, correos electrónicos y SMS que parecen provenir de organismos conocidos y fuentes confiables, a menudo grandes empresas, bancos e incluso organismos públicos. Así que lo primero que hay que hacer es verificar el origen de las comunicaciones, en particular las que piden datos personales, credenciales, códigos de dispositivos o que invitan a hacer clic en un enlace.

- Verifique la dirección desde la que provienen los correos electrónicos y los números de teléfono desde los que provienen las llamadas y los mensajes de texto.
- Compruebe cuidadosamente la dirección del remitente de los correos electrónicos y el texto de los enlaces que contienen: los estafadores suelen utilizar textos que difieren poco de los oficiales de las empresas.
- El texto de los correos electrónicos y mensajes también puede darle una indicación de su naturaleza fraudulenta, ya que a menudo contienen errores ortográficos y de sintaxis.
- Por último, recuerde que las estafas a veces son complejas, ya que los estafadores pueden coordinarse y actuar en varios canales (por ejemplo, haciendo una llamada telefónica después de enviar un SMS).

2. No te apresures

Muy a menudo, las estafas se basan en un sentido de urgencia y una invitación a actuar de inmediato. Por ejemplo, la comunicación avisa de la caducidad de un servicio, de un pago fallido o de la posibilidad de que se bloquee una cuenta corriente y invita a actuar con rapidez o incluso de inmediato.

- En cualquier contexto regular, siempre tiene tiempo para renovar un servicio o para intervenir en una transacción de pago.
- No actúe por impulso y tómese el tiempo para verificar, por ejemplo, a través de una llamada telefónica a la empresa que le brinda el servicio o una verificación en su área reservada, la veracidad de la comunicación.

3. Preste atención a las propuestas o promesas particularmente ventajosas de dinero o ganancias fáciles

Las ofertas a precios de ganga, los préstamos extrañamente ventajosos y las propuestas sospechosas de comercio en línea podrían resultar estafas.

- Comprueba siempre la bondad de la oferta comparándola con ofertas similares y buscando información sobre el proveedor.

4. Revisa las páginas web en las que realizas tus compras

En las páginas web que ofrecen compras, siempre es bueno prestar atención a la presencia de algunos elementos básicos, como: la dirección "https", la presencia del candado en la barra de direcciones (que indica que el sitio está protegido por sistemas de seguridad internacionales) y los datos del vendedor, como el número de IVA, el domicilio social de la empresa, datos de contacto, condiciones generales de venta, o un sistema de pago seguro que indique claramente los gastos de envío.

- Recuerda también que, en la página web de la Agencia Tributaria, puedes consultar los datos fiscales reportados en la página web.

5. Extremar la precaución al manejar datos, información y documentos personales

Si se le pide que comunique datos personales o sensibles o que envíe copias de documentos personales, debe tener mucho cuidado: envíe copias de sus documentos solo si es necesario y en un contexto fiable y asegúrese de la identidad del interlocutor.

6. Mantén tu software y contraseñas actualizados

Además de cambiar periódicamente las contraseñas, es necesario que los sistemas operativos y las aplicaciones de los PC y teléfonos inteligentes estén siempre actualizados.

- En particular, compruebe que el navegador que utiliza está actualizado y elimine periódicamente las cookies y los archivos temporales utilizando las herramientas adecuadas de su navegador.

He sido víctima de una estafa, ¿qué puedo hacer?

Ser víctima de una estafa es una eventualidad que le puede pasar a cualquiera. Si, a pesar de todas las precauciones implementadas, ha sido víctima de una estafa, siempre es posible tomar medidas para denunciar lo sucedido a la policía. En el caso de una estafa que tuvo lugar en línea, es recomendable consultar a la Policía Postal que tiene jurisdicción sobre delitos informáticos.

- Reúna todo el material que pueda probar lo sucedido.
- Además, si te preocupa haber sido víctima de una estafa bancaria, ponte en contacto con tu banco para bloquear tus tarjetas de pago y comprobar que no ha habido instrucciones de pago fraudulentas.

Conceptos erróneos sobre la ciberseguridad

Mito: Hacer clic en los enlaces "cancelar suscripción" en los correos electrónicos no deseados los detendrá.

Hecho: Al hacer clic en dichos enlaces, su dirección de correo electrónico puede ser confirmada por los spammers, lo que podría aumentar la cantidad de spam.

- Estas son algunas formas más seguras de darse de baja y lidiar con los correos electrónicos no deseados:
    - Configure filtros en su cliente de correo electrónico para mover automáticamente los correos electrónicos no deseados a la carpeta de correo no deseado o spam.
    - Utilice la opción "Reportar spam" en su cliente de correo electrónico para entrenar a su filtro de spam para que reconozca y bloquee correos electrónicos similares.
    - Utilice el enlace "cancelar suscripción" solo si reconoce al remitente y confía en el correo electrónico. Para otros correos electrónicos, es más seguro eliminarlos sin hacer clic en ningún enlace.

Mito: El restablecimiento de fábrica borra por completo todos los datos de mi dispositivo.

Hecho: Después de un restablecimiento de fábrica, aún puede recuperar sus datos, a menos que los sobrescriba correctamente con software especializado.

Mito: Mi dispositivo es seguro si nunca me conecto a Internet.

Realidad: Incluso los dispositivos sin conexión pueden ser vulnerables al malware a través de unidades USB u otras conexiones físicas.

Mito: Cerrar la tapa de tu portátil es lo mismo que desconectar.

Hecho: Cerrar la tapa solo suspende el sistema. No cierra la sesión, lo que hace que la sesión sea vulnerable al acceso no autorizado. Se recomienda que cierre la sesión de su computadora.

Mito: El modo avión es suficiente para proteger tu dispositivo durante el vuelo.

Realidad: Aunque el modo avión desactiva las señales inalámbricas, no protege contra el malware preinstalado o el acceso no autorizado si accedes físicamente a tu dispositivo.

Proteger la seguridad y la privacidad de tus redes sociales

Recomendaciones:

- **Utilice contraseñas seguras y únicas:** Cree contraseñas seguras y diferentes para cada cuenta. Utilice un administrador de contraseñas para almacenarlos de forma segura.
- **Habilite la autenticación de dos factores (2FA):** agregue una capa adicional de seguridad al requerir un segundo factor de verificación además de su contraseña.
- **Comprueba tu configuración de privacidad:** revisa y actualiza tu configuración de privacidad con regularidad para limitar quién puede ver tu información y tus publicaciones.
- **Desconfíe de los enlaces sospechosos:** No haga clic en enlaces sospechosos o de fuentes no confiables, ya que pueden ser intentos de phishing.
- **Limite la información personal compartida:** Evite compartir detalles confidenciales como dirección, número de teléfono o información financiera.
- **Usa redes Wi-Fi seguras:** Evita conectarte a redes Wi-Fi públicas no seguras para acceder a tus cuentas de redes sociales.
- **Comprueba los permisos de las aplicaciones:** controla los permisos que concedes a las aplicaciones de redes sociales y limita el acceso a los datos innecesarios.
- **Supervise la actividad sospechosa:** esté atento a la actividad inusual en sus cuentas e informe cualquier problema de inmediato.
- **Edúcate a ti mismo y a los demás:** Edúcate sobre las mejores prácticas de seguridad y comparte esta información con amigos y familiares.

Errores a evitar:

- **Usa la misma contraseña para varias cuentas:** si una cuenta se ve comprometida, todas las demás con la misma contraseña corren peligro.
- **Ignorar las actualizaciones de seguridad:** No actualizar regularmente las aplicaciones y los dispositivos puede dejar vulnerabilidades aprovechables.
- **Aceptar solicitudes de amistad de extraños**: Podrían ser perfiles falsos creados para recopilar información personal.
- **Comparte tu ubicación en tiempo real:** Evita compartir tu ubicación actual, especialmente en publicaciones públicas.
- **No cierres sesión en dispositivos compartidos:** dejar tu cuenta abierta en dispositivos compartidos puede permitir que otras personas accedan a tu información.
- **No supervises si hay actividad sospechosa:** ignorar los signos de actividad inusual en tus cuentas puede provocar problemas de seguridad.
- **Compartir demasiada información personal:** Publicar detalles confidenciales puede facilitar el robo de identidad.
- **No educarse sobre las prácticas de seguridad:** La falta de conocimiento puede dejarlo vulnerable a los ataques.

Examen

1. ¿Cómo puedo verificar el origen de un correo electrónico sospechoso?

a) Haciendo clic directamente en los enlaces del correo electrónico.

b) Comprobar cuidadosamente la dirección del remitente y el texto de los enlaces.

c) Respondiendo inmediatamente al correo electrónico para solicitar la confirmación.

d) Reenviar el correo electrónico a todos los contactos para notificarles.

2. ¿Qué es una señal de advertencia en las comunicaciones fraudulentas?

a) La presencia de ofertas especialmente ventajosas.

b) La ausencia de errores ortográficos y sintácticos.

c) La petición de actuar con serenidad y sin prisas.

d) El origen de un número de teléfono conocido.

3. ¿Qué hacer ante una propuesta sospechosa de comercio en línea?

a) Invertir de inmediato para no perder la oportunidad.

b) Comprobar la bondad de la oferta comparándola con otras similares.

c) Proporcionar sus datos financieros para recibir más información.

d) Compartir la oferta en las redes sociales para obtener opiniones.

4. ¿Qué elementos indican la fiabilidad de una página web de compras?

a) La presencia de ofertas a precios de ganga.

b) La dirección "https" y el candado en la barra de direcciones.

c) La ausencia de datos del vendedor.

d) La solicitud de pago por transferencia bancaria.

5. ¿Cómo gestionar la solicitud de comunicación de datos personales/sensibles?

a) Presentar todos los documentos requeridos de inmediato.

b) Enviar documentos solo si es necesario y en un contexto confiable.

c) Compartir datos en las redes sociales para mayor seguridad.

d) Ignorar la solicitud para evitar riesgos.

6. ¿Por qué es importante mantener actualizados el software y las contraseñas?

a) Recibir notificaciones publicitarias personalizadas.

b) Para protegerse contra vulnerabilidades y riesgos de seguridad.

c) Para acelerar la navegación por Internet.

d) Aumentar el espacio de almacenamiento del dispositivo.

7. ¿Qué hacer en caso de una estafa en línea?

a) Enviar un correo electrónico de protesta al estafador.

b) Ponerse en contacto con la Policía Postal y recopilar todo el material probatorio.

c) Elimine todas sus cuentas en línea.

d) Compartir el incidente en las redes sociales para alertar a otros usuarios.

8. ¿Cuál de las siguientes es una buena práctica para la seguridad en línea?

a) Utilice la misma contraseña para todas las cuentas.

b) Hacer clic en enlaces sospechosos por curiosidad.

c) Habilitar la autenticación de dos factores (2FA).

d) Comparte tu ubicación en tiempo real en las redes sociales.

9. ¿Qué error común aumenta el riesgo de ser víctima de estafas?

a) Actualice sus aplicaciones y dispositivos con regularidad.

b) Verifique los permisos de la aplicación.

c) Utilizar redes Wi-Fi públicas no seguras.

d) Utilizar contraseñas seguras y únicas.

10. ¿Qué se entiende por phishing?

a) Una técnica para mejorar la conexión a internet.

b) Intento de obtener información sensible a través de enlaces sospechosos.

c) Un método de actualización automática del software.

d) Un sistema seguro de pago en línea.

Soluciones:

1. b
2. en
3. b
4. b
5. b
6. b
7. b
8. c
9. c
10. b