Manténgase alerta:

Estafas y desinformación en internet

Aprenda a reconocer las señales de fraude en línea

Internet ofrece muchos beneficios, pero también es terreno para estafadores y desinformación. Conocer las señales le ayudará a detectar actividades sospechosas fácilmente. Los estafadores siempre mejoran sus técnicas, así que incluso los usuarios más experimentados deben mantenerse actualizados y alerta.

Esta guía le ayudará a identificar las estafas más comunes, le ofrecerá consejos para proteger su información personal, le enseñará a detectar noticias falsas y le explicará cómo puede proteger sus dispositivos y redes personales.

El ciberdelito le costó a los estadounidenses **$12.5 mil millones** en el 2023, según el FBI.

Conozca las estafas más comunes

Los estafadores utilizan diversas tácticas para engañar a las personas y robar su dinero, así como acceder a información personal o a sus dispositivos. Reconocer estas estafas es el primer paso para protegerse del fraude en línea.

Estafas de phishing

El phishing ocurre cuando los estafadores se hacen pasar por instituciones legítimas (como bancos o agencias gubernamentales) para robar información personal como números de seguridad social, contraseñas e información de cuentas bancarias. Estas estafas suelen ocurrir por correo electrónico, pero también pueden suceder a través de mensajes de texto o redes sociales.

SIGNOS DE ALERTA:

- Lenguaje urgente que solicita acción inmediata.
- Solicitudes de información personal como contraseñas o datos bancarios.
- Enlaces a sitios web que parecen legítimos, pero tienen enlaces levemente modificados.

PALABRAS CLAVE DE ALERTA:

- "Verifique su cuenta".
- "Se requiere acción urgente".
- "Confirme su contraseña".

Estafas de pago por adelantado

Estas estafas intentan convencerle de que pague tarifas por adelantado a cambio de servicios o productos que nunca se materializan. Algunos ejemplos comunes incluyen ofertas de trabajo que requieren pago por capacitación o equipos, o mensajes que afirman que usted ha ganado un premio, pero debe pagar impuestos para reclamarlo.

SIGNOS DE ALERTA:

- Solicitudes de dinero para cubrir gastos antes de recibir un producto, servicio o premio.
- Promesas de altos rendimientos por una pequeña inversión inicial.
- Historias que parecen demasiado buenas o extrañas para ser verdad.

PALABRAS CLAVE DE ALERTA:

- "Tarifa de transferencia".
- "Impuesto de herencia".
- "Recargo por procesamiento".

Cerca de **1 de cada 3** estadounidenses reportó ser víctima de un ciberdelito.[1]

Estafas de lotería o sorteo

Al igual que una estafa de pago por adelantado, los estafadores notifican a las víctimas que han ganado una gran suma de dinero en una lotería o sorteo, pero deben pagar una tarifa para desbloquear el premio.

SIGNOS DE ALERTA:

- Notificaciones de loterías o concursos en los que no ha participado.
- Requisitos para pagar una tarifa o proporcionar detalles de cuentas bancarias para reclamar un premio.
- Lenguaje oficial combinado con mala gramática o errores ortografía.

PALABRAS CLAVE DE ALERTA:

- “Usted es el feliz ganador”.
- “Reclame sus ganancias”.
- “Felicidades, ganador”.

Estafas de soporte técnico

Los cibercriminales afirman ofrecer soporte técnico, mientras que su verdadera intención es instalar malware o robar información personal de sus dispositivos.

SIGNOS DE ALERTA:

- Llamadas o alertas no solicitadas en su pantalla afirmando que su computadora tiene un virus.
- Solicitudes de acceso remoto a su computadora.
- Presión para actuar rápidamente y pagar por soporte o descargar un software.

PALABRAS CLAVE DE ALERTA:

- “Virus detectado”.
- “Alerta del sistema”.
- “Se necesita soporte inmediato”.

Estafas románticas (catfishing)

Los estafadores crean perfiles falsos en sitios web de citas o redes sociales para iniciar relaciones a distancia y eventualmente convencer a sus víctimas que envíen dinero.

SIGNOS DE ALERTA:

- Solicitudes para mudar las conversaciones de las plataformas de citas hacia mensajería privada.
- Detalles personales inconsistentes.
- Declaraciones muy súbitas o aceleradas de amor o afecto.
- Solicitudes de dinero citando emergencias, costos de viaje o gastos médicos.

PALABRAS CLAVE DE ALERTA:

“Asistencia financiera”. “No le diga a nadie”. “Confíe en mí”.

RECUERDE LAS 4 R'S:

Para protegerse de los estafadores

Estas cuatro reglas de sentido común le ayudarán a mantener su información segura en línea.

1. **Reduzca lo que comparte:**
   Nunca comparta números de cuenta, contraseñas o números de segruidad social o datos sensibles.

2. **Revise de cerca los URL:**
   ¿La dirección está escrita correctamente? ¿La dirección web comienza con "https://", lo que indica que los mensajes están cifrados usando SSL (Capa de Conexión Segura) para su protección?

3. **Refuerce su seguridad:**
   Usar VPNs y autenticación de dos factores (2FA) dificulta que roben su información privada.

4. **Reavive su intuición:**
   Si una oferta de una persona extraña parece demasiado buena para ser realidad, probablemente lo sea. Tenga mucho cuidado.

Si algo le parece demasiado bueno para ser cierto, deténgase y evalúe la situación. Los delincuentes en línea crean una falsa sensación de urgencia para sorprenderle y hacer que actúe rápidamente.

La importancia del uso del software de seguridad y el firewall

No importa cuán vigilante sea sobre los sitios fraudulentos, a veces puede cometer un error. Si hace clic en el enlace de un estafador o escribe incorrectamente una dirección URL, de repente se convierte en la nueva víctima de un sitio falso. Es por esta razón que se recomienda instalar un software antivirus y antimalware en su computadora y dispositivos en línea. Este software actúa como un filtro que ayuda a evitar que los ciberdelincuentes ingresen, y también le alerta cuando usted está ingresando en territorio peligroso.

Otras prácticas recomendadas para evitar estafadores incluyen:

- Utilizar contraseñas fuertes y software de VPN.
- Habilitar la autenticación de dos factores (2FA).
- Limitar el acceso a su router y red Wi-Fi.

No toda la información que encuentra en línea es confiable

Desinformación, propaganda, insinuaciones, mentiras, engaños, noticias falsas, sea como sea que se llame, el uso de información falsa para manipular y moldear la opinión pública no es nada nuevo. Sin embargo, la era digital ha facilitado y abaratado la creación y difusión de esta información, haciéndola más difícil de detectar.

De hecho, la inteligencia artificial (IA) puede crear "deepfakes" — representaciones falsas generadas por computadora de líderes mundiales, celebridades, eventos y datos — en cuestión de segundos.

Este no es un problema fácil de resolver. Sin embargo, existen tres consejos prácticos que puede usar para evaluar la información que encuentra en línea.

> "No crea todo lo que lee en internet."
>
> —Abraham Lincoln*

3 formas de ser un consumidor de información más astuto:

1. **Verifique la fuente:** Evalúe la credibilidad de la publicación que suministra la información. Busque organizaciones de noticias establecidas, conocidas por su adherencia a los estándares periodísticos. Desconfíe de sitios web o plataformas desconocidos que pueden no tener supervisión editorial o procesos de verificación de hechos.

2. **Verifique con varias fuentes:** Contraste la información con fuentes confiables antes de aceptarla como verdadera. Las noticias falsas a menudo existen en un vacío, mientras que las historias creíbles suelen ser publicadas por varios medios de comunicación confiables.

3. **Evalúe las pruebas:** Busque evidencia que respalde las afirmaciones presentadas en el artículo. El buen periodismo incluye citas de expertos, datos y otros hechos verificables. Desconfíe de artículos que carecen de pruebas o se basan en gran medida en fuentes anónimas o atribuciones vagas como "los expertos dicen" o "algunas personas afirman".

TRUCO PROFESIONAL:

Verifique antes de reenviar

Las noticias falsas a menudo son sensacionalistas, diseñadas para captar su atención y aprovechar su impulso natural de compartir información actual, sorprendente o que refuerza sus prejuicios. Contribuya a detener la difusión de información falsa. Verifique rápidamente los hechos antes de compartirlos.

**Por supuesto, Abraham Lincoln nunca dijo esto, ya que falleció más de un siglo antes de que se inventara el internet.*

CONFÍE EN SÍ MISMO:

Evite estafas y desinformación usando su pensamiento crítico

- **Siga su intuición:** Si algo parece incorrecto o demasiado bueno para ser verdad, probablemente lo sea.
- **Opte porla precaución:** Frente a los mensajes sospechosos, decida no responder.
- **Haga preguntas:** Nunca dude en pedir más detalles si algo no está claro.
- **Verifique los hechos:** Siempre confirme la información usando fuentes confiables o sitios de web autorizados.
- **Consulte con personas de confianza:** Discútalo con amigos o familiares — dos cabezas (o más) a menudo piensan mejor que una.
- **Cuidado con la presión:** Desconfíe de quien lo presiona para tomar decisiones rápidas o le impide obtener una segunda opinión. Las oportunidades genuinas no necesitan una respuesta inmediata.

Cultive hábitos como hacer preguntas, mantener un sano escepticismo, ser precavido y mantenerse conectado con su círculo de confianza. Esto le ayudará a evitar estafas y desinformación.

Acerca de Brightspeed

Lanzada en 2022, Brightspeed está construyendo un futuro donde un mayor número de comunidades puede beneficiarse de una vida más conectada. Creemos que el lugar donde una persona elige vivir no debería estar limitado por sus opciones de conexión, y por ello estamos construyendo la infraestructura necesaria para ofrecer Fibra Óptica rápida y confiable, y así llegar a millones de hogares y empresas. Brightspeed Fiber Internet, brinda una experiencia ininterrumpida para ver videos, estudiar, jugar en línea o trabajar. Si desea conocer más información ingrese a: **www.brightspeed.com**.

In collaboration with ciena