

SCAMS, ESTAFAS Y FRAUDE DIGITAL

El *Scamming*, es una industria en crecimiento. Los avances tecnológicos, así como la amplia disponibilidad de datos personales en línea, han creado una explosión de estafas y fraudes digitales. La palabra SCAM es un termino del inglés y se utiliza para describir las estafas por medios electrónicos. Sepa cómo detectar estas estafas y qué hacer si se convierte en víctima de ellas.



ALGUNOS TIPOS DE SCAMS



Scammers impostores.

- Realizan llamadas sobre reclamos de seguro falsos, garantías, problema de atención médica, soporte técnico, etc.
- El scammer quiere que usted crea que hay un problema que debe abordar de inmediato.
- Estas estafas tienen la intención de hacer que revele información personal (también conocido como "phishing").
- Algunos utilizan la clonación de voz de AI (Inteligencia artificial) para imitar la voz de un amigo o un ser querido en problemas.

Fraude de facturas, cuentas por pagar, crédito financiero y estafa por cobros anticipados.

- Estas estafas por correo electrónico quieren que piense que debe dinero y que está en peligro si no paga.
- Estos mensajes suelen tener algo raro: la dirección de correo electrónico es extraña, o el cuerpo del mensaje tiene errores tipográficos u otros errores, o parece copiado y pegado. (Algunos se ven muy reales, hay que mirar con atención)
- A menudo, los enlaces o archivos adjuntos son malware que puede infectar su computadora. El malware es un software malicioso diseñado para dañar su dispositivo acceder a su información ¡NO HAGA CLIC!

Filtración de datos.

- Si su información personal se ve comprometida en una filtración o violación de datos, los estafadores pueden aprovecharse de eso con correos electrónicos falsos de empresas afectadas por la filtración, o usar sus datos comprometidos para iniciar otra estafa.

Scareware - Estrategias de miedo

- Mensajes urgentes que aparecen como anuncios emergentes (pop-ups) en su pantalla.
- Esta información tiene la intención de hacerle creer que su computadora está infectada con malware o un virus.

SI TE ESTAFAN: ACCEDE A PROTECCIÓN DEL CONSUMIDOR POR LA FTC



- **Reportar un fraude:** reportefraude.ftc.gov
- **Reportar el robo de identidad:** robodeidentidad.gov
- **More resources:** consumidor.ftc.gov/estafas

COMO PROTEGERSE

Recuerde que los **estafadores utilizan las emociones como táctica.**

- Mantenga la calma.
- Cuelgue la llamada, retirese por un momento de la pantalla.
- Llame a alguien en quien confie.
 - Tal vez alguien que conozca que sea bueno con la tecnología.
 - Trate de comunicarse con su biblioteca local.

Utilice contraseñas difíciles y complejas.

- Almacene sus contraseñas en un administrador de contraseñas.
- Utilice la autenticación de 2 factores para mayor seguridad

Ejecute **actualizaciones de software** para la seguridad más reciente.

Utilice un bloqueador de anuncios (ad-blocker) para evitar el malware.

Asegúrese de que los sitios web que visite usen **HTTPS.**

Compruebe si su información se ha visto afectada en una filtración de datos en: **haveibeenpwned.com.**

Tenga cuidado al abrir enlaces o archivos adjuntos enviados por correo electrónico, o al responder llamadas de números desconocidos.

Use una frase de seguridad con familiares, amigos, proveedores de atención médica, etc.

- Si le llaman, pregunte por la frase de seguridad.

