DENUNCIAR DELITOS CIBERNÉTICOS

Desde el robo de identidad hasta las estafas de phishing y el acoso cibernético, el espectro de los delitos cibernéticos es amplio y la mayoría de nosotros, por desgracia, los encontraremos en nuestra vida digital. En honor al Mes de la Concientización sobre la Ciberseguridad, queríamos ayudarlo a comprender cómo enfrentar estos desafíos y protegerse.

General

Puede denunciar diversas formas de delitos cibernéticos a las siguientes agencias:

CISA: cisa.gov/report **FBI:** ic3.gov

Cuenta hackeada

Denuncie que su cuenta ha sido hackeada al equipo de soporte de la plataforma correspondiente. Encuentre enlaces directos a plataformas populares aquí: staysafeonline.org/online-safety-privacy-basics/hacked-accounts/

Ransomware

Comuníquese con las autoridades locales, incluidas las siguientes:

- **CISA:** cisa.gov/forms/report
- **FBI:** fbi.gov/contact-us/field-offices
- **Servicio Secreto de EE. UU.:** secretservice.gov/contact/field-offices

Robo de identidad

Denuncie el robo de identidad a:
FTC: identitytheft.gov

También puede informar al **Centro de recursos sobre robo de identidad:** idtheftcenter.org o llamar al 888.400.5530

Delitos cibernéticos relacionados con los impuestos

Denuncie mensajes o llamadas de phishing relacionados con impuestos al Servicio de Impuestos Internos (IRS, por sus siglas en inglés) por correo electrónico: phishing@irs.gov

Más información sobre el fraude fiscal: irs.gov/individuals/how-do-you-report-suspected-tax-fraud-activity

Fraude con tarjetas de crédito

Denuncie el fraude con tarjeta de crédito a su compañía de tarjeta de crédito o utilice la herramienta de denuncia de fraudes, estafas y malas prácticas comerciales de la Comisión Federal de Comercio (FTC, por sus siglas en inglés): reportfraud.ftc.gov

Fraude a personas mayores

Si usted o alguien que conoce ha sido víctima de un fraude a personas mayores, comuníquese con la Línea Directa Nacional contra el Fraude a Personas Mayores del Departamento de Justicia de los EE. UU. al 833.372.8311.

Fraude al Seguro Social

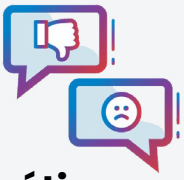
Notifique a la Administración del Seguro Social si sospecha alguna actividad fraudulenta relacionada con su número de seguro social: ssa.gov/fraud o llame al: 800.269.0271

Compromiso del correo electrónico empresarial

Denuncie correos electrónicos comerciales falsificados o estafas al departamento de TI de su organización y al FBI en: ic3.gov

Acoso en línea

Si cree que está siendo acosado o es víctima de stalkerware, llame, chatee o envíe un mensaje de texto a la Línea Directa Nacional de Ayuda contra la Violencia Doméstica:
Llamada: 800.799.7233
Chat: thehotline.org
Texto: "Start" a 88788



Acoso cibernético

Denuncie el acoso cibernético a la plataforma donde ocurrió el acoso o a la escuela de su hijo.

Denuncie ante la policía local si ha habido amenazas de violencia, acoso o delitos de odio a: stopbullying.gov/cyberbullying/how-to-report

Phishing

Denuncie los correos electrónicos sospechosos a su plataforma de correo electrónico y luego elimínelos. O también puede denunciarlos a:

- **FTC:** reportfraud.ftc.gov
- **Grupo de trabajo antiphishing:** reportphishing@apwg.org
- **Red de vigilancia contra el fraude de AARP:** 877.908.3360

Recuerde: recopile y conserve evidencias

Es posible que se le solicite que proporcione pruebas cuando denuncie ciertos tipos de delitos cibernéticos. Este material puede ayudar a las autoridades a detener y procesar a los hackers. Toda esta documentación podría considerarse evidencia, pero debe conservar todo lo que crea que podría estar relacionado con el incidente:

- Cheques cancelados
- Recibos de correo certificado o de otro tipo
- Texto de sala de chat o grupo de noticias
- Recibos de tarjetas de crédito
- Sobres (si recibió artículos a través de FedEx, UPS o correo de EE. UU)
- Archivos de registro, si están disponibles, con fecha, hora y zona horaria
- Mensajes en redes sociales
- Recibos de órdenes de pago
- Folletos o panfletos
- Facturas telefónicas
- Copias de correos electrónicos, preferiblemente copias electrónicas. Si imprime el correo electrónico, incluya la información completa del encabezado.
- Copias de páginas web, preferiblemente electrónicas
- Recibos de transferencia bancaria

Seguir estos pasos ayuda a **Secure Our World.**

Todos podemos ayudarnos unos a otros a mantenernos más seguros en línea, así que comparta estos consejos con un familiar o amigo.

cisa.gov/SecureOurWorld