Prevención de los Ciberdelitos

El ciberdelito es un problema grave y cada vez más preocupante para los usuarios de Internet. Aunque mantenerse conectado en línea es excelente, hay cosas que debe saber sobre el uso seguro de Internet. Los ciberdelincuentes dirigen sus ataques a personas que consideran vulnerables, como las personas con discapacidades intelectuales y/o del desarrollo. Todas las personas deben estar al tanto de los riesgos de la ciberdelincuencia y saber cómo usar Internet de forma segura.

¿Qué son los ciberdelitos?

Los ciberdelitos son delitos que se cometen en Internet mediante dispositivos móviles (como teléfonos celulares), computadoras y redes Wi-Fi públicas. Los ciberdelincuentes roban información sensible o personal para obtener un beneficio financiero.

Las personas son objeto de una variedad de estrategias para recopilar información personal de forma encubierta. Muchas personas son víctimas inconscientes de ciberdelitos que suelen traer aparejada una pérdida financiera (robo), violaciones de los datos personales y robo de la identidad para la víctima. Hoy en día, saber cómo prevenir y conseguir ayuda después de haber sido víctima de un ciberdelito es más importante que nunca.

Los ciberdelincuentes son oportunistas y acechan a las poblaciones vulnerables, como las personas que tienen una discapacidad intelectual o de desarrollo (IDD), con quienes procuran buscar un acercamiento o entablar una relación de confianza.

Tipos comunes de ciberdelitos

Phishing: uso del correo electrónico, mensajes de texto y llamadas telefónicas para obtener información personal o financiera, o bien credenciales de acceso.

Falta de entrega: uso de Internet para solicitar de forma ilegal el pago electrónico por la compra de bienes y servicios que nunca se reciben.

Extorsión: obtención de dinero o bienes mediante intimidación o amenazas por parte de una persona que pretende representar a una autoridad (como el IRS). Esto puede incluir amenazas de daño físico, procesamiento penal o exposición pública. También puede implicar el bloqueo del acceso a los datos de la víctima y la solicitud de un rescate para recuperarlos.

Violación de datos personales: robo y divulgación de la información y los datos personales y privados de una persona.

Robo de la identidad: robo y uso de la información personal de una persona para cometer fraude u otros delitos.

El Departamento de Servicios de Desarrollo elabora los boletines de bienestar y seguridad para alertar a los prestadores de servicios directos, a los centros regionales y a otras personas acerca de los riesgos específicos identificados en nuestra comunidad. Por medio de esta encuesta, le solicitamos que nos dé su opinión sobre este boletín y sobre lo que podemos mejorar: Encuesta del boletín

La ciberdelincuencia en EE. UU. en el año 2020

- Durante la pandemia de COVID-19, las personas con IDD fueron víctimas de ciberdelincuentes que desviaron los pagos de estímulo enviados a su nombre por el gobierno federal por medios electrónicos.
- California registró la mayor cantidad de reclamos por ciberdelitos de todo el país.
- El FBI recibió casi 800,000 reclamos por ciberdelitos, un **aumento del 69%** en relación con el año anterior.
- El ciberataque más común fue el phishing, con más de **241,000** denuncias por parte de víctimas.
- Se denunciaron pérdidas por más de **4,100 millones**.
- El grupo etario más afectado fueron las personas mayores de 60 años.

Ayude a proteger a las personas a quienes le brinda servicios contra la ciberdelincuencia

Internet es un espacio público

Recuerde a las personas que deben tener mucho cuidado antes de compartir información personal, como los números de Seguro Social, la información de la cuenta bancaria y la información médica en Internet.

- **Las redes Wi-Fi públicas siempre se deben usar con precaución.**
- Las redes Wi-Fi públicas están abiertas a cualquier persona que se encuentre dentro del rango de acceso y en general no solicitan que los usuarios acepten términos o condiciones de servicio para usarlas.
- Aunque estas redes resultan convenientes, en general no son seguras. Esto significa que existe la posibilidad de que otras personas puedan tener acceso por vía electrónica a información personal (como el nombre de usuario y la contraseña) sin conocimiento de la víctima.
- Las redes Wi-Fi seguras suelen pedir la contraseña del usuario y el pago de una tarifa para su uso.

Use contraseñas seguras para las cuentas en línea

Ayude a las personas a quienes brinda servicios a crear contraseñas seguras.

- Aliente a las personas a que no usen contraseñas comunes o fáciles de descifrar.
- Una contraseña segura tiene al menos 8 caracteres e incluye una combinación de letras mayúsculas y minúsculas, símbolos y números. Cuanto más larga sea la contraseña, más segura será.
  - **Contraseñas débiles**: “contraseña”, su nombre o fecha de nacimiento, 12345
  - **Contraseñas seguras**: 8blu3Car$dr1vinG, 1&n%00Xb#, Y3!!oWfL0w3rs

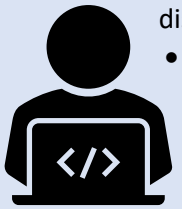
Verifique la configuración de privacidad regularmente

Ayude a las personas a quienes brinda servicios a verificar los ajustes de privacidad en sus dispositivos móviles y computadoras. Explique cómo configurar la autenticación de doble factor al cambiar los ajustes de privacidad en las cuentas en Internet. Con la autenticación de doble factor, el usuario recibe un mensaje de texto o un correo electrónico con un código especial cada vez que inicia sesión en su cuenta en línea.

El Departamento de Servicios de Desarrollo elabora los boletines de bienestar y seguridad para alertar a los prestadores de servicios directos, a los centros regionales y a otras personas acerca de los riesgos específicos identificados en nuestra comunidad. Por medio de esta encuesta, le solicitamos que nos dé su opinión sobre este boletín y sobre lo que podemos mejorar: Encuesta del boletín

Virus y software malicioso

- El ***software malicioso*** es un tipo de software diseñado para causar daños a su dispositivo móvil o su computadora.



- Los ***virus*** son códigos informáticos que ingresan a una computadora sin su permiso y la "infectan". Se ocultan en archivos o aplicaciones enviados por correo electrónico o mensajes de texto e infectan la computadora cuando se abren. Los virus son un tipo de software malicioso.
- Los virus pueden robar la información del usuario, ralentizar y destruir la computadora, o tomar el control absoluto de una computadora o un dispositivo.
- Los virus no se pueden propagar por sí solos. Se propagan cuando las personas los comparten sin saberlo. Esto ocurre comúnmente al compartir archivos o correos electrónicos infectados.

Qué hacer después de ser víctima de un ciberdelito

Explique la importancia de llamar al banco y cancelar las tarjetas de débito o crédito afectadas por el ciberdelito. Brinde ayuda para cambiar la información de acceso a las cuentas en línea. Alerte a la institución de la cuenta que sufrió el ataque y consulte sobre cualquier cargo fraudulento que se haya acreditado.

El Kit de herramientas para el bienestar del Departamento de Servicios de Desarrollo tiene información adicional sobre la forma de apoyar y ayudar a proteger a las personas a quienes brinda servicios.

Recursos útiles

Departamento de policía local

Centro de Denuncias de Delitos por Internet (IC3)

Comisión Federal de Comercio (FTC)

- Denuncie un fraude en ReportFraud.ftc.gov
- Llame a la línea directa de la FTC al 1-877-IDTHEFT (1-877-438-4338)
- Denuncie el robo de identidad y solicite información adicional a identitytheft.gov

Piense antes de hacer clic

- Desaliente a las personas a las que le brinda servicios de abrir archivos adjuntos no solicitados o hacer clic en enlaces que no reconocen, ya que pueden contener virus o software malicioso que causen daños a las computadoras.
- Advierta a las personas que tengan cuidado antes de hacer clic en enlaces que parecen juegos o que prometen obtener algo “gratuito” al ingresar en ellos.
- Aliente a las personas a verificar las direcciones de los correos electrónicos que reciben para confirmar la legitimidad del remitente. Si reciben un correo electrónico inesperado con enlaces o archivos adjuntos, sugiérales que se comuniquen con el remitente por teléfono o mensaje de texto para confirmar que ellos de hecho lo han enviado.
- El phishing es una estafa común por Internet que utiliza mensajes falsos que parecen reales para engañar a las personas para que compartan su información personal.
    - Antes de responder mensajes, preste atención a signos reveladores de este tipo de estafa: remitente desconocido, errores ortográficos o gramaticales, enlaces sospechosos que no coinciden con el contenido del mensaje, adjuntos aleatorios, contenido del correo con un sentido de urgencia.

Antes de responder o hacer clic en un correo electrónico

Aliente a los clientes a verificar quién envía el correo.

- Pase el cursor sobre el enlace o el nombre del remitente para comprobar la dirección de correo electrónico y asegurarse de que su información va a ser recibida por la empresa que corresponde.

El Departamento de Servicios de Desarrollo elabora los boletines de bienestar y seguridad para alertar a los prestadores de servicios directos, a los centros regionales y a otras personas acerca de los riesgos específicos identificados en nuestra comunidad. Por medio de esta encuesta, le solicitamos que nos dé su opinión sobre este boletín y sobre lo que podemos mejorar: Encuesta del boletín