PROTECCIÓN AL CONSUMIDOR

La Semana Nacional **de Protección al Consumidor** (NCPW) es del 1 al 7 de marzo. Este evento anual **alienta a las personas y las empresas a conocer sus derechos** de consumidores y cómo mantenerse **seguros**. La Comisión Federal de Comercio (FTC) y sus socios de NCPW proporcionan recursos gratuitos para proteger a los consumidores contra el **fraude**, las **estafas** y el **robo de identidad**.

La Agencia de Ciberseguridad e Infraestructura (CISA) alienta a los consumidores a revisar la página de recursos NCPW de la FTC y revisar los siguientes consejos de **CISA**:

1. Protegiendo su privacidad

¿Cómo saber si su privacidad está siendo protegida?

POLITICA DE PRIVACIDAD: antes de enviar su nombre, dirección de correo electrónico u otra información personal en un sitio web, **busque la política de privacidad del sitio**. Ya que esta indica cómo se utilizará la información y si la información se distribuirá o no a otras organizaciones.

EVIDENCIA DE QUE SU INFORMACIÓN ESTÁ ENCRIPTADA: para evitar que los atacantes roben su información personal, las presentaciones en línea deben estar **encriptadas** para que solo el destinatario apropiado pueda leerlas. **Un icono de candado** en la esquina inferior derecha de la ventana indica que su información está encriptada.

¿Qué pasos adicionales puede tomar para proteger su privacidad?

1. Haga negocios con empresas **creíbles**.
2. **No use** su dirección de correo electrónico principal en envíos en línea.
3. **Evite** enviar información de tarjetas de crédito en línea.
4. **Dedique** una tarjeta de crédito a compras en línea.
5. **Evite** usar tarjetas de débito para compras en línea.
6. **Aproveche** las opciones para limitar la exposición de información privada.

2. Mantenerse a salvo en los sitios de redes sociales

¿Qué son los sitios de redes sociales?

Los sitios de redes sociales, a veces denominadas sitios de “amigo de un amigo”, se basan en el concepto de redes sociales tradicionales en las que estás conectado con personas nuevas a través de personas que ya conoces. El propósito de algunos sitios de redes puede ser **puramente social**, permitiendo a los usuarios establecer **amistades** o **relaciones románticas**, mientras que otros pueden centrarse en establecer **conexiones comerciales.**

¿Qué implicaciones de seguridad presentan estos sitios?

Las personas no saben cuanta información personal están **compartiendo** y es posible que las personas no ejerzan la misma **precaución** que tendrían al conocer a alguien en persona porque:

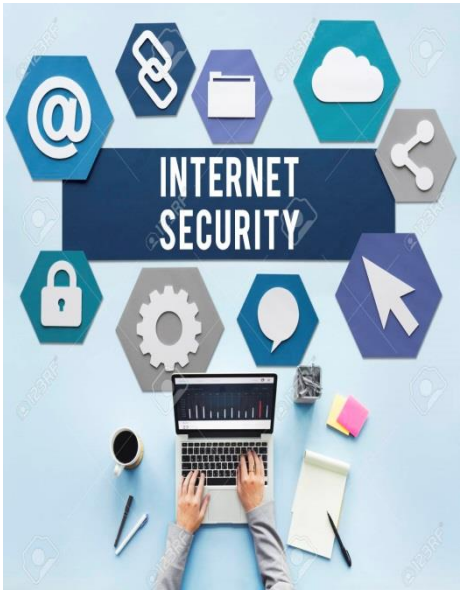
- Internet proporciona una **sensación de anonimato**
- La falta de interacción física proporciona **una falsa sensación de seguridad**
- Adaptan la información para que la lean sus amigos, **olvidando que otros pueden verla**
- Quieren ofrecer **ideas para impresionar** a posibles amigos o asociados

Si bien la mayoría de las personas que usan estos sitios no representan una amenaza, las personas maliciosas pueden sentirse atraídas por la accesibilidad y la cantidad de **información personal disponible**. Si usted proporciona sin ningún cuidado su **ubicación**, **pasatiempos**, **intereses** y **amigos**, una persona malintencionada podría **hacerse pasar por un amigo de confianza** o **convencerlo de que tiene autoridad para acceder a otros datos personales o financieros.**

Estos sitios pueden ser usados para **distribuir malware**. Las aplicaciones de terceros pueden ser desarrolladas por **atacantes**, personalizándolas para que parezcan inocentes mientras **infectan** su computadora/celular y **comparten su información sin su conocimiento.**

¿Cómo protegerse?

1. **Limite** la cantidad de información personal que publica
2. Recuerde que internet es un **recurso público**
3. Tenga cuidado con los **extraños**
4. Sea **escéptico**
5. Evalúe **su configuración**
6. Tenga cuidado con las **aplicaciones de terceros**
7. Utilice contraseñas **seguras**
8. Consulte **las políticas de privacidad**
9. Mantenga **actualizado el software**, particularmente su navegador web
10. **Instale y actualice** periódicamente sus herramientas de **antivirus, anti-spam, anti-spyware.**



3. Prevención y respuesta al robo de identidad

¿El robo de identidad es solo un problema para las personas que envían información en línea?

Puede ser víctima de robo de identidad **incluso si nunca usa una computadora**. La información personal (como números de tarjetas de crédito, números de teléfono, números de cuenta y direcciones) **puede sustraerse** si pierde o roban su billetera, escuchando una conversación telefónica, hurgando en su basura o recogiendo un recibo en un restaurante que tenga su número de cuenta. Con esta información pueden hacerse **pasar por usted** para comprar artículos, abrir nuevas cuentas o solicitar préstamos.

Internet facilita que los ciberdelincuentes obtengan estos datos personales, ya que la mayoría de las empresas almacenan está información de sus clientes en bases de datos.

¿Cómo se eligen las víctimas del robo de identidad en línea?

El robo de identidad suele ser un delito de **oportunidad**, por lo que puede ser víctima simplemente porque su información está disponible. Los ladrones pueden elegir a una víctima por el tipo de **compañía para la que trabaja**, el sitio **donde vive** o porque su información es de fácil acceso.

¿Hay formas de evitar ser una víctima?

Desafortunadamente **NO** existe una garantía, pero **existen formas de minimizar** su riesgo:

1. Haga negocios con compañías **de buena reputación.**
2. Aproveche las **características de seguridad** (doble factor, contraseñas fuertes y robustas).
3. Verifique **las políticas de privacidad**.
4. Tenga cuidado con **la información que publica**.
5. Utilice y mantenga un **software antivirus y un firewall**.
6. Tenga en cuenta la actividad de su **cuenta.**

7. Utilice servicio de SMS en su móvil que **notifique actividades de sus cuentas**.

¿Cómo saber si su identidad ha sido robada?

Las empresas tienen diferentes políticas para notificar a los clientes cuando descubren que alguien ha accedido a una base de datos. **Sin embargo, debe tener en cuenta los cambios en la actividad normal de su cuenta**. Los siguientes son ejemplos de cambios que **podrían indicar** que alguien ha accedido a su información:

- **Cargos** inusuales o inexplicables en sus facturas
- Llamadas telefónicas o facturas de cuentas, **productos o servicios que no tiene**
- **No recibir** facturas o correos regulares
- **Cuentas** nuevas y extrañas que aparecen en su informe de crédito
- **Denegación** inesperada de su tarjeta de crédito

¿Qué hacer si sospecha o sabe que su identidad ha sido robada?

Recuperarse del robo de identidad puede ser un proceso **largo**, **estresante** y potencialmente **costoso**. Muchas compañías de tarjetas de crédito han adoptado políticas que **intentan minimizar la cantidad de dinero de la que usted es responsable**, pero las implicaciones pueden extenderse más allá de sus cuentas existentes. Para minimizar la extensión del daño, tome medidas lo antes posible:

- Comience por **reportar** esto a su banco emisor para que efectúen un bloqueo inmediato de sus tarjetas
- **Cambie las contraseñas** de sus cuentas y establezca controles de doble factor y contraseñas más robustas
- **Reporte** a las autoridades competentes
- **Continúe con los procesos hasta finalizarlos y tener una respuesta satisfactoria.**