Consejos para evitar el robo de identidad a los estudiantes

El uso del Internet y el intercambio de información por el Internet se ha convertido en parte de nuestra vida cotidiana. La tecnología está cambiando la forma en que interactuamos y, si bien hace que la comunicación sea más eficiente, también aumenta el riesgo de robo de identidad. A continuación, se ofrecen algunos consejos para minimizar las amenazas de robo de identidad por medio del Internet.

No responda a mensajes de texto, correos electrónicos o ventanas emergentes que soliciten información personal o financiera.

1. **Tenga cuidado con la información que comparte en las redes sociales**. Ya sea que use *Instagram*, *Snapchat, Twitter* o *Facebook*, tenga cuidado con la información que comparte. Limite la información personal que publique, por ejemplo: nombre completo, edad, fotografías, dirección particular y de correo electrónico, número de teléfono o nombre de la escuela. Una vez que haga las publicaciones, no podrá retirarlas. Suponga que todo lo que pone en un sitio de redes sociales es permanente. Considere lo que revela una publicación, quién podría verla y cómo podría percibirse ahora y en el futuro. Elija su sitio de redes sociales con cuidado y comprenda la política de privacidad. La mayoría de los sitios de redes sociales tienen configuraciones de privacidad. Descubra cómo activar estas configuraciones y utilizarlas.
2. **Piense antes de hacer clic.** No haga clic en enlaces de remitentes desconocidos. No abra archivos adjuntos a mensajes inesperados o cuestionables de fotos, canciones o videos, aunque el mensaje haya sido enviado por sus amigos. Consulte con el remitente para asegurarse de que el mensaje provenga de una fuente confiable. Tenga cuidado al descargar software, juegos, música o cualquier otro contenido, ya que los virus destructivos pueden ocultarse en sitios web, en las aplicaciones que descargamos o en los archivos adjuntos de correo electrónico. Si algo parece sospechoso, lo mejor es eliminarlo.
3. **Utilice redes seguras para compartir archivos**. El intercambio de archivos entre compañeros le permite compartir fácilmente música y juegos con amigos, pero estas redes informales son propensas al malware. En el momento de instalar el software, verifique la configuración de seguridad para compartir archivos, de manera que no comparta nada privado y pueda proteger su información personal. Haga un análisis de seguridad en todos los archivos que le sean compartidos. Hable con sus padres sobre los riesgos de seguridad que implica compartir archivos.
4. **Cuidado con los impostores.** Los piratas informáticos pueden ingresar a cuentas para acceder a su información personal y enviar mensajes que, aunque parezcan ser de sus amigos, o de una empresa o su escuela, no lo son. Si sospecha que un mensaje es fraudulento, utilice un método alternativo para comunicarse con su amigo y averiguar si realmente lo envió. Pregúntese: ¿conoce y confía en con quién está comunicándose? Limite su grupo de amigos en Internet, para que solo tenga entre sus amigos a personas que realmente conoce, de manera que evite compartir información con extraños que posteriormente podrían usarla en su contra.

5. **No se deje engañar por las estafas de phishing.** Tenga cuidado con los estafadores que le lanzan cebos engañosos para ver si usted muerde y revela su información personal. No responda a mensajes de texto, correos electrónicos o ventanas emergentes que soliciten información personal o financiera, y no haga clic en ningún enlace en el mensaje. Tenga cuidado al abrir cualquier archivo adjunto o descargar archivos de los correos electrónicos que reciba, independientemente de quién los envió. Los archivos inesperados pueden contener malware.

6. **Sea inteligente con los teléfonos inteligentes.** Bloquee su teléfono con una contraseña y no la comparta con nadie. La mayoría de los teléfonos inteligentes tienen tecnología GPS que le permite saber dónde están sus amigos y les permite encontrarse. Ajuste la configuración de su ubicación para que solo las personas que conoce puedan ver su ubicación y apáguela cuando no esté en uso. No responda mensajes de texto de remitentes desconocidos que soliciten información personal. Comuníquese con su proveedor de servicios móviles para bloquear los mensajes de texto no deseados. Es probable que cuando descargue algunas aplicaciones, comparta más información de la que desearía compartir con los creadores de la aplicación. Verifique su configuración de privacidad antes de descargar una nueva aplicación y verifique la información que recopila la aplicación.

7. **Utilice redes wifi seguras.** Cuando utilice una red doméstica, active su programa informático de seguridad, mantenga su navegador y sus sistemas operativos al dìa y preste atención a las advertencias de seguridad. Utilice su propia red 4G cuando navegue la web desde su teléfono inteligente. Se recomienda que use una red protegida con contraseña si va a navega la web en una red pública de wifi, y absténgase de acceder a sitios web que tengan su información personal. Limítese a usar sitios web cifrados: sitios web que comiencen con “https” (la “s” significa seguro).

8. **Cree contraseñas seguras**. Las contraseñas son la primera línea de defensa para protegerse de los delincuentes cibernéticos. Elija contraseñas seguras para todas sus cuentas. Las mejores combinaciones suelen ser las que combinan letras mayúsculas con minúsculas, con números y símbolos. Asegúrese de cambiar sus contraseñas con regularidad y nunca las comparta con nadie. Utilice la autenticación de dos pasos si se le ofrece y cierre siempre la sesión de sus cuentas antes de apagar su computadora.

9. **Coloque un congelamiento de seguridad en su informe crediticio**. Los padres y tutores legales pueden congelar el informe crediticio de un menor u otra persona protegida. Un congelamiento de seguridad prohibirá la divulgación de cualquier información del informe crediticio sin una autorización expresa de la persona. El congelamiento de seguridad está diseñado para evitar que se apruebe una extensión de crédito sin su consentimiento, lo que dificulta que los ladrones de identidad abran nuevas cuentas a su nombre.

10. **Pregúntale a alguien**. Antes de proporcionar su información personal, hacer clic en un enlace o visitar un nuevo sitio web, consulte con alguien que conozca y en quien confíe. Hable con sus padres sobre los sitios que visita y revise las políticas de privacidad juntos con ellos.

Para obtener más información o poner una queja, visite nuestro sitio web o contáctenos:

Wisconsin Department of Agriculture,
Trade and Consumer Protection
Bureau of Consumer Protection
2811 Agriculture Drive, PO Box 8911
Madison, WI 53708-8911

Correo electrónico: DATCPHotline@wi.gov
Sitio Web: datcp.wi.gov
Teléfono: (800) 422-7128 TTY: (608) 224-5058

StudentTipsPreventIDTheftSPANISH980 (rev 1/24)