Cherokee County School District

PAUTAS DE SEGURIDAD EN INTERNET

Dr. Brian V. Hightower
Superintendente de Escuelas

Bobby Blount
Director de Informática

- No publiques información personal en sitios web, en perfiles de salas de chat, en perfiles de mensajes de texto o en mensajes de correo electrónico. La información personal incluye tu nombre y apellido legal, dirección, números de teléfono, estado civil, fecha de nacimiento, género, información financiera, información de seguro, número de seguro social, claves secretas, información de ingreso a sistemas y otros nombres de usuario.

- Una estrategia básica para evitar el robo de identidad y el fraude en línea es que mantengas en secreto tu información personal siempre que estés en línea. Sé igualmente cuidadoso al compartir información fuera de la Internet y asegúrate de saber cómo las organizaciones usarán tu información antes de que se las des.

- Elige un nombre de pantalla que no te identifique.

- No compartas tus claves secretas con nadie.

- Usa claves secretas "seguras" que puedas recordar y no las escribas en un lugar donde puedan verse o llevarse. La seguridad de la contraseña tiene que ver con la cantidad de caracteres, complejidad e imprevisibilidad. Una clave secreta segura generalmente tiene más de ocho caracteres y contiene al menos una letra mayúscula, un número y un símbolo (p. ej., Pa$sW0rd).

- Si el servicio lo permite, crea tus propias preguntas de seguridad para tu clave secreta. Elige esta opción en lugar de usar las preguntas de seguridad predefinidas.

- No respondas mensajes de correo electrónico o de texto donde te pidan información personal.

- No abras mensajes de correo electrónico enviados por desconocidos.

- Sé precavido al confiar en un mensaje que parece haber sido enviado por alguien conocido. Los hackers se pueden infiltrar en las cuentas y enviar mensajes que parecen venir de amigos o colegas. Si sospechas que un mensaje es fraudulento, usa un método alternativo para comunicarte con tu amigo y averiguarlo. Esto incluye invitaciones a participar en redes sociales.

- Piensa que todo lo que pongas en formato electrónico es permanente. Aun si borras el contenido o tu cuenta, cualquiera en la Internet puede guardar, imprimir o reenviar fácilmente fotos, textos o videos a una computadora, o la información puede almacenarse en otro servidor.

- Antes de publicar o enviar contenido, piensa que todos podrán verlo. Todo lo que se envíe en un texto, incluso las imágenes sexualmente explicitas o provocativas, puede ser reenviado fácilmente y hacerse público.

- Respeta la privacidad de los otros. Publicar una foto vergonzosa o reenviar un texto privado sin pedir permiso pueden causar un daño involuntario o lastimar a otras personas.

- Usa las configuraciones de seguridad. La mayoría de los sitios de las redes sociales y de los sitios que comparten fotografías te permiten decidir quién puede tener acceso y responder tus comentarios.

- Si encuentras información acerca de ti en línea que es poco atractiva, vergonzosa o falsa, comunícate con el dueño del sitio web o su administrador y pídeles que la retiren, o busca una opción para notificar infracciones. La mayoría de los sitios tienen políticas para responder a estos pedidos.

- Cuéntale a un adulto de confianza si pasa alguna cosa en línea o si recibes un mensaje de texto que te moleste o cause temor.

- No hagas planes para encontrarte con alguien que hayas conocido en la Internet sin habérselo dicho a un adulto de confianza.

- Cuando realices una videoconferencia, no aceptes invitaciones de usuarios que no conozcas en las que te pidan que los agregues a tus contactos.

- No aceptes archivos de sean sospechosos o de usuarios que no conozcas cuando estés participando en una videoconferencia.

- Ten presente que muchas soluciones de videoconferencia permiten la grabación. No digas ni hagas nada en la conferencia que no desees que se haga público.

- Las descargas ilegales, hacer trampa por medios digitales y copiar el contenido de otras personas podría ser fácil, pero no significa que sea correcto. Tú tienes la responsabilidad de respetar el trabajo creativo de los demás, y el derecho a que se respete tu propio trabajo.

- Crea, comparte, etiqueta, comenta y contribuye en el mundo en línea de una forma que sea positiva.

- Los dispositivos móviles deben protegerse contra el robo de identidad. Esto es especialmente cierto si el dispositivo móvil tiene aplicaciones ("apps") con acceso a las redes sociales y a otros sitios que contenga información personal.

- Los dispositivos móviles no son inmunes a los virus y a los códigos malintencionados. Ten cuidado cuando descargues archivos o navegues en los sitios web.