Sugerencias para Adolescentes: Seguridad de contraseñas

Mantener tu identidad e información segura

Sameer Hinduja, Ph.D. y Justin W. Patchin, Ph.D.

1. Protégelas. Nunca le des a nadie tu contraseña (de Instagram, Snapchat, Xbox Live, Fortnite, email o cualquier servicio similar) o tu código de celular – ni siquiera a un amigo. A veces las amistades no duran, y esa contraseña puede ser usada en tu contra.

2. RECUERDA TU RESPUESTA SECRETA. Cuando creas una cuenta en línea, y te pide dar una respuesta que sólo tú conoces – no lo tomes a la ligera ni como broma. Asegúrate de que sea algo de la que te acordarás años después, en caso de que ocurra un problema.

3. NO DIVULGUES INFORMACIÓN DE TI. No uses contraseñas basadas en información personal (tu nombre de usuario, fecha de nacimiento, dirección, número telefónico, segundo nombre, nombre de tu mascota, etc.).

4. MÉZCLALO. Si es posible usa una mezcla de mayúsculas y minúsculas, números y símbolos.

5. SÉ CREATIVO. Cuando creas una contraseña, inventa tu propio acrónimo de una frase que signifique algo para ti, y agrupa las primeras letras de cada palabra. Cuando puedas usa números y símbolos. Asegúrate que el acrónimo que creaste tenga al menos siete dígitos.
Estos son algunos ejemplos:
"La semana pasada corrí treinta minutos" (Lspctm30$)
"Kiki, do you love me? Are you riding?" (Kdylm@yr)
"Que la fuerza esté con usted" (Qlfecu!!!)

6. Cámbiale. Cambia tu contraseña frecuentemente. Gasta tiempo y es algo latoso, pero aun así hazlo. Gasta más tiempo y es más latoso tratar de recuperar una cuenta hackeada o el robo de identidad.

7. NO LA ENVÍES A NADIE. Nunca envíes tu contraseña por texto, mensaje directo, captura de pantalla, ni respondiendo a que te la hayan pedido. Podrías enviarla accidentalmente a la persona equivocada o esa persona la podría mostrar a alguien más, o podría ser una estafa.

8. NO LA PUBLIQUES. No escribas tu contraseña en un papel y no la pegues a tu monitor, computadora portátil, ni en las notas de tu celular, etc. Busca un lugar seguro para guardar las contraseñas que escribes – o si es posible – nunca escribas en papel tus contraseñas: es mejor memorizarlas, o usar aplicaciones o programas que te ayudan a crearlas.

9. EVITA INGRESAR EN APARATOS NO CONFIABLES. No pongas tus contraseñas en aparatos de los no eres dueño, no controlas, o no son confiables. Solo debes usar las computadoras y tabletas en los salones de computación, bibliotecas, oficinas, u otros lugares públicos para las búsquedas anónimas en línea, y no para acceder a tus cuentas en internet.

10. USA DIFERENTES CONTRASEÑAS. No uses la misma contraseña en todas las cuentas que tengas en línea. Trata de usar diferentes contraseñas en distintos sitios web, para que una cuenta hackeada no conduzca a que todas tus cuentas sean hackeadas.

CIBERACOSO
Centro de investigaciones

© 2018 Centro de investigaciones de ciberacoso | cyberbullying.org
La reproducción es permitida para propósitos educativos sin fines de lucro.
Deben pedir autorización por escrito del autor para cualquier otro uso.