Ciberseguridad

UNA GUÍA RÁPIDA PARA PADRES Y ADOLESCENTES

ConnectSafely

(Cybersecurity: A Quick-Guide for Parents)

¿Por qué debe importarnos la seguridad?

Los dispositivos y prácticas inseguras pueden poner en peligro su privacidad, su bienestar financiero e incluso su seguridad personal. También puede afectar a otros, porque los dispositivos inseguros pueden propagar programas maliciosos a los dispositivos de otras personas a través de Internet.

¿Cuáles son los pasos más importantes que puede tomar mi familia?

Cree contraseñas seguras (y no las comparta), tenga cuidado dónde hace clic, utilice programas de seguridad, mantenga sus aplicaciones y sistemas operativos actualizados, tenga cuidado con las aplicaciones que instala y no sea víctima de estafas.

¿Están en alto riesgo los adolescentes y los niños?

Sí. Los jóvenes son muy vulnerables a las estafas y pirateos informáticos. No solo están mucho tiempo en línea, sino que tienden a ser curiosos y aventureros -buenas cualidades que pueden llevarlos a lugares problemáticos-. Los jóvenes son especialmente vulnerables al robo de identidad porque, por lo general, tienen un historial de crédito limpio y es más difícil de detectar una identidad falsa.

¿Qué es una autentificación de dos factores y por qué usarla?

Como una tarjeta de cajero automático, la autentificación requiere que usted sepa algo y tenga algo. Lo que "sabe" es su contraseña y lo que "tiene" por lo general es un teléfono celular. Si intenta iniciar sesión en un sitio o aplicación desde un dispositivo desconocido, recibirá un código enviado a su teléfono, que usted debe teclear para obtener acceso. Esto reduce en gran medida las posibilidades de que alguien acceda a sus cuentas de manera remota.

*Para obtener más información, visite ConnectSafely.org/cybersecurity. Para obtener un PDF para imprimir, visite ConnectSafely.org/quickguides.

Cree una contraseña segura y potente que pueda recordar.

Invente una frase única como “Conocí a Susie Jones en la Escuela Lincoln High en el 2012”, y utilice la primera letra de cada palabra y números y un símbolo. Su contraseña podría ser "ImSJaLHSi#12, pero cámbiela para cada sitio agregándole una letra o dos. También considere utilizar un administrador de contraseñas que recordará sus contraseñas. Más en ConnectSafely.org/passwords.

No quede atrapado en el “phishing”.

Phishing es cuando usted obtiene un enlace en un correo electrónico que parece ser de un sitio legítimo como su escuela o su banco. Tal vez dice que su seguridad está en riesgo y que debe iniciar sesión para cambiar su contraseña. No obstante, el enlace lo envía a un sitio clandestino cuyo propósito es obtener sus credenciales de usuario o engañarlo para que suministre una tarjeta de crédito u otra información personal. Es una de las principales maneras que usan los piratas informáticos para comprometer las cuentas.

Tenga cuidado dónde hace clic.

Los sitios web falsos o maliciosos (o los legítimos que han sido pirateados por criminales) pueden poner en peligro su dispositivo y los datos que se encuentran en el mismo. Estos sitios, a través de las a veces denominadas “descargas ocultas”, pueden instalar programas maliciosos en su dispositivo si los visita o tal vez hace clic en los enlaces de los sitios. A menudo parecen legítimos, ofrecen algo que es demasiado bueno para ser verdad o contienen algún tipo de contenido “prohibido” como material sexual explícito, apuestas, películas o música gratis. Luego existe el “clickjacking” –enlaces falsos en páginas de redes sociales que han sido pirateados–. Parecen enlazar a algo tentador, pero, en lugar de eso, lo redireccionan a un sitio que contiene propaganda no solicitada, planta programas maliciosos en su dispositivo o publica enlaces malos en su propio perfil.

Mantenga actualizados los programas informáticos y las aplicaciones.

Más allá de si usted está usando una computadora o un dispositivo móvil, es realmente importante mantener actualizados su sistema operativo y programas informáticos (o aplicaciones), porque es bastante común que los desarrolladores descubran fallas de seguridad y vulnerabilidades que arreglan con actualizaciones. Esto es importante en especial para los sistemas operativos y los navegadores web, que pueden ser más vulnerables a los ataques si no están actualizados (verifique si su sistema operativo y su navegador se actualizan a sí mismos de manera automática). Y si usted actualiza una aplicación o un programa, revise su configuración de privacidad nuevamente para asegurarse de que no hayan regresado a la configuración predeterminada.

Tenga cuidado con las estafas.

Las grandes noticias sobre personas famosas o catástrofes naturales y otros eventos importantes despiertan la curiosidad y el tráfico en la web, lo que hace salir a los expertos estafadores. Cuando ocurren catástrofes, las personas de buen corazón, tanto jóvenes como ancianas, pueden ser vulnerables a los pedidos falsos de ayuda. Si usted recibe un pedido de ayuda de caridad, teclee el nombre de la causa u organización en un buscador y a menudo encontrará un sitio oficial junto con varios otros que parecen estar relacionados. Los sitios oficiales por lo general aparecen primeros en los resultados de las búsquedas. No hay problema con ellos, así como con los sitios de organizaciones de noticias legítimas que cubren el evento. No obstante, aborde los otros sitios con precaución y haga un poco de investigación en la web sobre ayuda para catástrofes y otras organizaciones benéficas. Y recuerde: si una oferta es “demasiado buena para ser real”, probablemente no sea verdadera.

Tenga precaución antes de descargar.

Una manera común de plantar un programa informático malicioso en su dispositivo es hacer que usted descargue una aplicación, una pieza de programa informático o un documento (como un PDF) que puede contener código malicioso. Solo descargue aplicaciones de tiendas de aplicaciones legítimas como la Tienda de aplicaciones de Apple o Google Play. Lea los comentarios o al menos las clasificaciones de los usuarios. Lo mismo en el caso de los programas informáticos. Evite sitios desconocidos de descarga de programas que pueda encontrar en un motor de búsqueda y, en lugar de eso, utilice los sitios legítimos como Download.com o los sitios asociados con empresas conocidas de programas informáticos.