CONSEJOS DE SEGURIDAD CIBERNÉTICA

PARA LOS MAYORES

México Ciberseguro®

Una iniciativa de ESET®

MÁS SEGURIDAD ONLINE

México Ciberseguro ofrece las siguientes prácticas destacadas sobre conductas no tecnológicas y conductas online para que aprendas a protegerte mejor a ti mismo y a tus seres queridos mientras exploran Internet y los maravillosos recursos e información que ofrece.

Definiciones

APP: aplicaciones móviles, típicamente utilizadas en teléfonos celulares o inteligentes.

ROBO DE IDENTIDAD: una forma de robar la identidad de una persona mediante la cual un individuo se hace pasar por otra persona y asume su identidad, normalmente como método para obtener acceso a recursos, créditos y otros beneficios en nombre de dicha persona.

PHISHING: el intento de obtener información financiera u otros datos confidenciales de los usuarios de Internet, típicamente mediante el envío de un correo electrónico que dice pertenecer a una organización legítima, en general una institución financiera, pero que en realidad contiene un vínculo a un sitio Web falso que imita el real.

SMS: servicio de mensajes cortos (por sus siglas en inglés), es un componente para el servicio de mensajería de texto utilizado por el teléfono, la Web o los sistemas de comunicación móviles.

ENVÍO DE MENSAJES: el acto de enviar mensajes cortos de texto en forma electrónica, en particular cuando es de un teléfono celular a otro.

URL: localizador de recursos uniforme (por sus siglas en inglés), también conocido como dirección Web, en especial cuando se usa con HTTP.

Vulnerabilidades no tecnológicas y acciones correctivas

Los ladrones de identidad usan los documentos robados, preferentemente los documentos financieros, para obtener crédito, servicios y bienes en nombre de la víctima.

Los tachos de basura, los buzones de correo y los vehículos son algunos de los lugares comunes donde los ladrones suelen buscar este tipo de información.

1. Lleva el correo que necesitas enviar al buzón que se encuentra dentro de la Oficina de Correos, en especial si contiene cheques o instrumentos financieros.

2. No escribas tu número de cuenta de la tarjeta de crédito en los cheques cuando pagues las facturas de la tarjeta de crédito.

3. No imprimas tu número de seguro social en tus cheques.

4. Instala un buzón de correo con llave para el correo entrante y no dejes mucho tiempo el correo entrante en el buzón.

5. Destruye los documentos financieros y los cheques cancelados antes de tirarlos a la basura.

6. Saca los libros de cheques, los documentos viejos sobre préstamos para la compra de automóviles y otros documentos financieros similares de la guantera de tu auto.

7. Fotocopia el contenido de tu billetera y mantén las copias en un lugar seguro en caso de que la billetera se te pierda o te la roben. De esta forma, sabrás los números de tarjetas de crédito y los teléfonos de las instituciones financieras cuando necesites llamar para informar que los extraviaste.

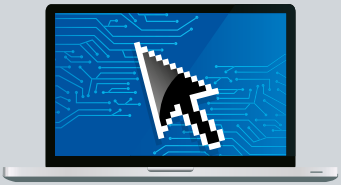
8. Sé diligente en cuanto a la verificación de los estados de cuenta y busca irregularidades y actividades sospechosas.

9. Pide un informe de crédito anual gratuito y verifica que las cuentas listadas sean legítimas.

Vulnerabilidades tecnológicas y acciones correctivas

Los ladrones de identidad que se basan en la tecnología se aprovechan de las medidas de seguridad laxas que suelen tener los usuarios casuales de dispositivos tecnológicos e intentan obtener información de las cuentas y credenciales para el inicio de sesión.

Las contraseñas débiles, las medidas limitadas de seguridad, la confianza en los vínculos integrados y las respuestas a los mensajes de phishing les dan a los ladrones la oportunidad que necesitan para lograr su cometido.



Siempre recuerda

DETENTE. PIENSA. CONÉCTATE©

1. Debes utilizar contraseñas fuertes, que incluyan letras en mayúscula y minúscula, así como números y caracteres especiales, y cada cuenta debe tener su propia contraseña.

2. Mantén actualizados los parches del sistema operativo y del software antivirus, y protege las redes inalámbricas domésticas con contraseña y cifrado.

3. No hagas clic en cada vínculo que te llegue por correo electrónico, muchos archivos adjuntos de los correos que te dicen "Tienes que ver esto" incluyen cargas maliciosas. Además, nadie necesita mirar otro vídeo de gatos en YouTube.

4. Nunca respondas a un mensaje de SMS o a un mensaje de correo electrónico que diga ser de una institución financiera y te pida tu nombre de usuario para iniciar la sesión y tu contraseña. Infórmale a la institución financiera sobre el mensaje para que sus investigadores de fraudes estén al tanto del intento de phishing.

5. No realices transacciones financieras en redes inalámbricas sin protección: uno nunca sabe quién las puede estar interceptando.

6. Piénsalo dos veces antes de descargar aplicaciones gratuitas para teléfonos inteligentes: algunas tienen incorporados códigos maliciosos capaces de atacar tu teléfono o tu computadora cuando la sincronizas con el teléfono. Al igual que gran parte del software gratuito online puede dañar tu PC, muchas de las aplicaciones móviles pueden atacar tu smartphone.

7. Sé cauteloso con las llamadas telefónicas no solicitadas que te exigen hacer un pago por teléfono usando tarjetas prepagas Green Dot o Western Union. Existen muchísimas estafas donde los que realizan la llamada se hacen pasar por una empresa de servicios públicos, la corte e incluso miembros de la familia y te piden que hagas un pago online. No lo hagas. Si lo haces, pueden pasar cosas terribles.

México Ciberseguro está ayudando a crear un entorno digital seguro donde podamos vivir, trabajar y jugar mediante la conciencia, educación y preparación en seguridad informática.

www.mexicociberseguro.org | info@mexicociberseguro.org