CREDIT SUISSE

La ciberseguridad y usted

Contenido

Ciberseguridad

En Credit Suisse, la seguridad de su información es siempre una prioridad. Estamos comprometidos a mantener la seguridad de nuestros sistemas, software, redes y otros activos tecnológicos contra los intentos no autorizado de acceder o destruir datos confidenciales, interrumpir nuestros servicios o causar otros daños.

Tenemos empleados en todo el mundo que se dedican a apoyar nuestros esfuerzos en materia de ciberseguridad, incluyendo la colaboración con nuestros reguladores, agencias de cumplimiento normativo y otras empresas para mantener al día nuestras defensas y mejorar la protección contra amenazas.

La tecnología evoluciona a grandes pasos en un mundo impulsado por las redes sociales, las operaciones online, uso de servicios en la nube y los procesos automatizados. Pero con la evolución tecnológica llega el avance de la **ciberdelincuencia**, que desarrolla continuamente nuevos tipos de ataques, herramientas y técnicas que permiten a este tipo de delincuentes penetrar en entornos más complejos o bien controlados y causar grandes daños incluso sin dejar rastro alguno.

Para usted, Internet es muy probablemente una parte integrante de todo lo que usted hace, y en consecuencia, el delito cibernético constituye una creciente y grave amenaza. Por ello, es **fundamental** para todos nosotros que integremos conscientemente la prevención del fraude informático en nuestras actividades diarias.

El objetivo de este folleto es recordarle cómo protegerse usted mismo, sus activos y su información personal de la ciberdelincuencia.

Su lista de control de ciberseguridad

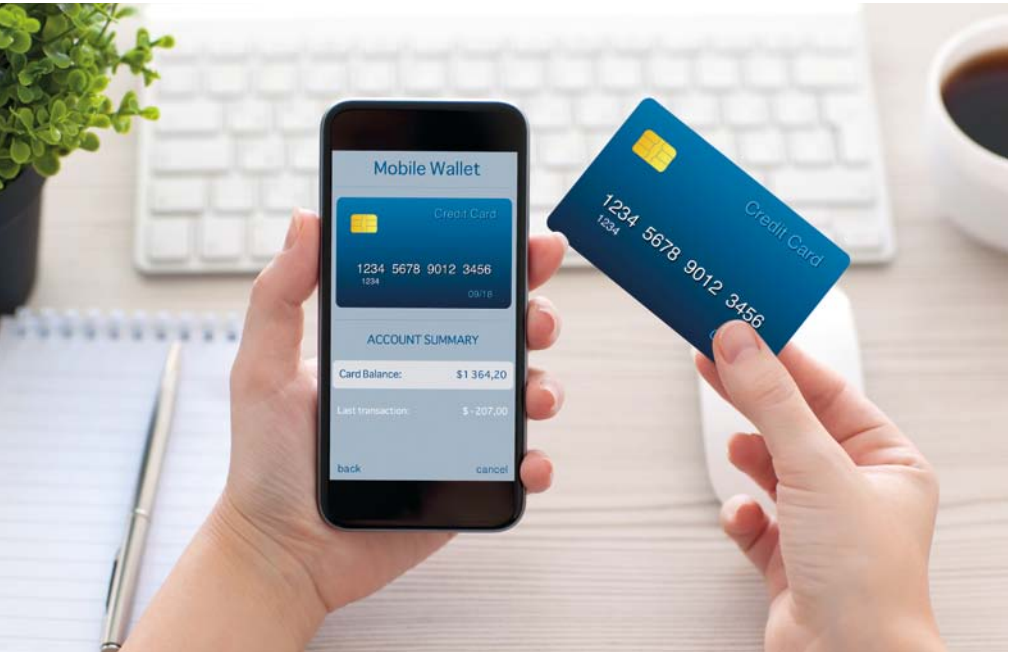
Algunos recordatorios para mantener sus ordenadores y su dinero a salvo de los ciberataques

1. Familiarícese con las funciones de seguridad estándar de Internet y Mantenga activos y actualice regularmente sus programas de seguridad informática para que puedan encontrar las últimas amenazas.

Instale un software antivirus para protegerse contra el malware (software malicioso) que puede robar información como números de cuenta y contraseñas, y utilice un firewall para evitar el acceso no autorizado a su ordenador.

2. Tenga cuidado al decidir dónde y cómo se conecta a Internet para las comunicaciones bancarias u otras que incluyan información personal sensible.

Las redes Wi-Fi públicas y los ordenadores en lugares como bibliotecas o centros de negocios hoteleros pueden suponer un riesgo si no disponen de software de seguridad actualizado.



3. Ignore los correos electrónicos no solicitados que le pidan abrir un archivo adjunto o hacer clic en un enlace si no está seguro sobre quién se lo envió realmente y por qué.

Los ciberdelincuentes son hábiles en la creación de correos electrónicos falsos que parecen legítimos, pero que pueden instalar malware. Su mejor opción es ignorar las peticiones no solicitadas de abrir archivos u objetos adjuntos o verificar independientemente, contactando con una dirección de correo electrónico o un número de teléfono publicados, si la supuesta fuente le envió realmente el correo electrónico.

4. Sospeche si alguien le contacta online inesperadamente y le pide su información personal.

Una estrategia segura es ignorar las peticiones de información no solicitadas, sin importar cuán legítimas parezcan, especialmente si piden información como su DNI, números de cuenta bancaria y contraseñas.

5. Utilice el proceso más seguro que pueda al iniciar sesión en cuentas financieras.

Cree contraseñas complejas que sean difíciles de adivinar, cámbielas regularmente y trate de no usar las mismas contraseñas o PIN (números de identificación personal) para varias cuentas.

6. Sea discreto al usar la redes sociales.

Los delincuentes rastrean esos sitios buscando información como el lugar de nacimiento de una persona, el nombre de soltera de la madre o el nombre de una mascota por si esos detalles puedan ayudarles a adivinar o restablecer contraseñas para cuentas online.

7. Tenga cuidado al usar smartphones o tabletas.

No deje desatendido su dispositivo móvil y utilice una contraseña de dispositivo u otro método para controlar el acceso en caso de robo o pérdida.

Ciberseguridad personal de un vistazo

Proteja su ordenador. Instale software de protección contra malware o software malicioso, que puede acceder a un sistema informático sin su consentimiento para robar contraseñas o números de cuenta. Además, utilice un firewall para evitar el acceso no autorizado a su ordenador. Si bien hay distintas formas de protección, asegúrese de que los ajustes permitan actualizaciones automáticas.

Utilice el método más seguro posible para iniciar sesión en cuentas financieras. Utilice la autenticación más segura que se ofrece, especialmente para transacciones de alto riesgo. Utilice contraseñas difíciles de adivinar y manténgalas en secreto. Cree identificadores de usuario y contraseñas "fuertes" para sus equipos, dispositivos móviles y cuentas online utilizando combinaciones de letras mayúsculas y minúsculas, números y símbolos que son difíciles de adivinar y luego cámbielos a intervalos periódicos. Si bien puede ser tentador utilizar la misma contraseña o el mismo PIN para varias cuentas, hacerlo significa que, un delincuente que obtenga una contraseña o PIN pueda iniciar sesión en otras cuentas.

Entender las funciones de seguridad de Internet. Puede tener una mayor confianza en que un sitio web es auténtico y que encripta (codifica) su información durante la transmisión si la dirección web comienza con https://. Además, asegúrese de cerrar la sesión en las cuentas financieras cuando complete sus transacciones o se aparte del ordenador. Para conocer los pasos de seguridad adicionales, consulte las instrucciones de usuario de su navegador web.

Sospeche de los correos electrónicos no solicitados que le piden hacer clic en un enlace, descargar un archivo adjunto o facilitar información de la cuenta. Para los ciberdelincuentes es fácil copiar el logotipo de una empresa u organización de buena reputación a un correo electrónico de phishing. Al responder a una simple petición, es posible que esté instalando malware. Su estrategia más segura es ignorar las peticiones no solicitadas, sin importar cuán legítimas o atractivas parezcan.

Tenga cuidado dónde y cómo se conecta a Internet. Cuando acceda a Internet para realizar actividades bancarias u otras actividades que impliquen información personal, utilice su propio ordenador portátil o dispositivo móvil a través de una conexión conocida, fiable y segura. Un ordenador público como en un centro de negocios hotelero o una biblioteca pública y las redes Wi-Fi gratuitas no son necesariamente seguros. Para los ciberdelincuentes, puede resultar relativamente fácil interceptar el tráfico de Internet en estos lugares.

Tenga cuidado al usar la redes sociales. Los ciberdelincuentes utilizan las redes sociales para recopilar información sobre las personas, como su lugar o fecha de nacimiento, el nombre de una mascota, el apellido de soltera de su madre y otra información que puede ayudarles a averiguar las contraseñas o a restablecerlas. No comparta su "página" o acceso a su información con una persona que no conozca y en la que no confíe. Los ciberdelincuentes pueden simular ser su "amigo" para convencerle de que envíe dinero o divulgue información personal.

Tome precauciones con su tableta o smartphone. Considere la posibilidad de activar las actualizaciones automáticas para el sistema operativo de su dispositivo y sus "apps" (aplicaciones) cuando estén disponibles para ayudar a reducir su vulnerabilidad. Nunca deje su dispositivo móvil desatendido y utilice una contraseña u otra función de seguridad para limitar el acceso en caso de que pierda o le roben su dispositivo. Asegúrese de habilitar la función de "tiempo de espera " o "bloqueo automático" que protege su dispositivo móvil cuando no se utiliza durante un periodo determinado. Examine cualquier aplicación antes de descargarla.

Ciberseguridad comercial de un vistazo

Proteja los ordenadores y las redes. Instale software de seguridad y antivirus que proteja contra el malware o software malicioso, que puede acceder a un sistema informático sin el consentimiento del propietario para diferentes fines, incluido el robo de información. Además, utilice un firewall para evitar el acceso no autorizado. Existen diferentes opciones de protección, por lo que debería buscar una solución que se ajuste al tamaño y a la complejidad de su negocio. Actualice el software, según corresponda, para mantenerlo al día. Por ejemplo, configure el antivirus para que ejecute un escaneo después de cada actualización. Si utiliza una red inalámbrica (Wi-Fi), asegúrese de que es segura y está cifrada. Proteja el acceso al router mediante el uso de contraseñas seguras.

Exija una autenticación segura. Asegúrese de que los empleados y otros usuarios que se conecten a su red utilicen identificadores de usuario y contraseñas seguras para ordenadores, dispositivos móviles y cuentas online utilizando combinaciones de letras mayúsculas y minúsculas, números y símbolos difíciles de averiguar y los cambien regularmente. Considere la posibilidad de implementar una autenticación multifactorial que, además de una contraseña para obtener acceso, requiera información adicional.

Consulte con los proveedores que manejan datos confidenciales para ver si ofrecen una autenticación multifactorial para acceder a sistemas o cuentas.

Controle el acceso a los datos y ordenadores y cree cuentas de usuario para cada empleado. Tome medidas para limitar el acceso o uso de ordenadores de la empresa a las personas autorizadas. Bloquee los ordenadores portátiles cuando no estén en uso, ya que pueden ser fácilmente robados o perdidos. Exija de cada empleado que tenga una cuenta de usuario separada y prohíba a los empleados que compartan cuentas y contraseñas. Sólo dé acceso a los sistemas de datos específicos a los empleados que los necesitan para hacer su trabajo, y no les permita instalar software sin previa autorización. Además, asegúrese de que los derechos de administradores estén reservados a los empleados que los necesiten, como el personal de TI y el personal clave, y revise periódicamente su necesidad de acceso.

Transmita los conocimientos básicos a los empleados. Establezca prácticas y políticas de seguridad para los empleados, tales como directrices sobre el uso apropiado de Internet, y establezca expectativas y consecuencias correspondientes en caso de violación de las políticas. Establezca una cultura corporativa "de arriba hacia abajo" que haga hincapié en la importancia de una ciberseguridad sólida, especialmente a la hora de manejar y proteger la información de los clientes y otros datos fundamentales. Asegúrese de que todos los empleados sepan cómo identificar y notificar posibles incidentes de seguridad. Instruya a los empleados para que tengan cuidado dónde y cómo se conectan a Internet. Los empleados y terceros sólo deberían conectarse a su red utilizando una conexión segura y de confianza. Los ordenadores públicos, como los que se encuentran en un cibercafé, un centro de negocios hotelero o una biblioteca pública, pueden no ser seguros. Además, sus empleados no deben conectarse a la

red de su empresa si no están seguros de la conexión inalámbrica que están utilizando, como es el caso de muchas redes Wi-Fi gratuitas en zonas públicas, ya que en estos lugares puede ser relativamente fácil para los ciberdelincuentes interceptar el tráfico de Internet.

Instruya a los empleados sobre los peligros de los correos electrónicos sospechosos. Los empleados deben desconfiar de los correos electrónicos no solicitados que les pidan hacer clic en un enlace, abrir un archivo adjunto o proporcionar información de cuenta. Para los ciberdelincuentes, es fácil copiar el logotipo de una empresa u organización de buena reputación a un correo electrónico falso. Al atender lo que parece ser una simple petición, sus empleados pueden estar instalando malware en su red. La estrategia más segura es ignorar las peticiones no solicitadas, sin importar cuán legítimas parezcan. Los proveedores de software proporcionan regularmente parches o actualizaciones a sus productos para corregir los fallos de seguridad y mejorar la funcionalidad. Una buena práctica es descargar e instalar estas actualizaciones de software tan pronto como estén disponibles. Puede ser más eficiente configurar el software para que tales actualizaciones se instalen automáticamente.

Haga copias de seguridad de los sistemas y datos importantes y haga copias periódicas de los datos de los equipos que utiliza su empresa. Recuerde aplicar las mismas medidas de seguridad, como el cifrado, a los datos de las copias de seguridad que aplicaría al original. Además de las copias de seguridad automatizadas, haga copias periódicas de los datos empresariales confidenciales en un dispositivo de almacenamiento en una ubicación distinta y segura.

Preste mucha atención a sus cuentas bancarias y vigile si se han realizado disposiciones no autorizadas. Establezca controles adicionales, tales como llamadas de confirmación antes de que se autoricen las transferencias en la institución financiera. En los últimos años se ha producido un aumento de transferencias electrónicas no autorizadas realizadas desde cuentas bancarias de empresas. Una estafa común es la toma de control de cuentas en la que los ciberdelincuentes utilizan software malicioso, como los que registran pulsaciones de teclas, para obtener los identificadores y contraseñas de las cuentas bancarias online y, a continuación, realizar disposiciones. Otra estafa llamada “Business Email Compromise” (BEC) consiste en enviar a empresas solicitudes de pago falsificadas para proveedores legítimos y dirigir los fondos a la cuenta del ciberdelincuente cibernético. Las empresas generalmente no están cubiertas por las normas de protec-

ción del consumidor contra transferencias electrónicas de fondos no autorizadas.

No se olvide de las tabletas y los smartphones. Los dispositivos móviles pueden ser una fuente de problemas de seguridad, especialmente si contienen información confidencial o pueden acceder a la red de su empresa. Si sus empleados conectan sus dispositivos a la red de la empresa, exíjales que protejan sus dispositivos con contraseña, cifren sus datos e instalen aplicaciones de seguridad para evitar que los delincuentes accedan al dispositivo mientras está conectado a una red pública. Asegúrese de elaborar y aplicar procedimientos de notificación para la equipos perdidos o robados.

Tenga cuidado con las transacciones y facturas fraudulentas. Las estafas pueden abarcar desde pagos con un cheque sin valor o una tarjeta de crédito o débito falsa hasta devoluciones fraudulentas de productos. Compruebe que dispone de un seguro para protegerse contra los riesgos. Además, asegúrese de comunicar inmediatamente cualquier irregularidad.

Correo electrónico

Su proveedor de correo electrónico no puede garantizar su ciberseguridad, y los piratas informáticos atacan a los proveedores para obtener acceso a las cuentas de usuario, o atacan directamente a las cuentas de correo electrónico individuales utilizando el phishing, la ingeniería social, el malware u otras estafas.

Limite su exposición al riesgo manteniendo cuentas de correo electrónico separadas para:

- negocios;
- amigos y familiares;
- avisos importantes;
- sitios que exigen una dirección de correo electrónico como ID de usuario.

Además, para proteger su información:

- Habilite la autenticación de dos factores en su servicio de correo electrónico, si está disponible, para recibir un texto cuando haya un inicio de sesión desde un nuevo dispositivo.
- Utilice el cifrado de datos para transmitir información personal. El cifrado de la información hace imposible que puedan leerla los que no tengan las claves de cifrado.
- Emplee filtros de spam para reducir el riesgo de software malicioso y estafas de phishing (el spam representa el 65% del tráfico total de correo electrónico).
- Si debe enviar a una persona un documento protegido con contraseña, envíe el documento por correo electrónico y la contraseña por separado.

Ingeniería social

La ingeniería social puede exponerle al fraude. Las redes sociales como Facebook o LinkedIn pueden proporcionar a los hackers una gran cantidad de información sobre usted, que puede ser utilizada para robar sus activos o su información.

- Limite la información que proporciona en línea. Los delincuentes buscarán información sobre usted en Facebook, Twitter y otros medios sociales y la utilizarán para cometer un fraude contra usted, su familia y/o sus amigos.
- No ponga información personal/financiera en correos electrónicos (y no siga los enlaces que se le envían en los correos electrónicos, incluso si provienen de fuentes fiables).
- Póngase en contacto por teléfono con el remitente del correo electrónico o abra una nueva ventana de correo electrónico (no pulse “responder” para preguntarle al remitente si el correo electrónico recibido es válido).
- Preste atención a la URL. Los sitios web malignos parecen idénticos a los reales, pero la URL puede utilizar una variación ortográfica o un dominio diferente (p. ej. ¿dice ‘.net’ cuando debería decir ‘.com’?).
- No introduzca información confidencial en sitios web a menos que usted compruebe que existe una seguridad apropiada (la URL debería comenzar por: https://).

Por teléfono

Confirme la identidad de una persona desconocida que llama: pida la ortografía completa y correcta de su nombre, un número de devolución de llamada y una explicación de por qué se necesita la información.

Tenga cuidado con los suplantadores: valide la fuente a través de canales públicos oficiales.

No proporcione información sobre terceras personas: pida a solicitante que se ponga en contacto directamente con la persona cuyos datos está solicitandoapropiada.

En persona

Manténgase precavido en lugares públicos con las personas que nos observan por encima del hombro ("shoulder surfers") al teclear nuestra información personal (como los PIN o las contraseñas) con el fin de robarla y obtener acceso a sus cuentas.

- Tenga cuidado con las personas que intentan acceder junto a usted en un área segura sin usar su propia autorización, como una tarjeta de acceso o una clave.
- No inserte en su ordenador unidades de almacenamiento extraíbles desconocidas, como pendrives USB, que haya encontrado o que le hayan sido entregadas, ya que pueden contener malware.

Internet

Los hackers recrean sitios web muy conocidos para captar sus credenciales de usuario, como por ejemplo contraseñas, DNI o información de tarjetas de crédito. Después utilizan esta Información robada para acceder a sus cuentas bancarias y otras cuentas.

Precauciones que debe tomar en línea

- Asegúrese de mantener actualizado el software de su navegador.
- Mantenga un nivel de seguridad medio o alto en la configuración de su navegador.
- Asegúrese de que la dirección de cualquier sitio web que visite comience por https://. Algunos navegadores muestran un icono de un candado junto a https:// para indicar que tiene una conexión segura.
- Recuerde: http:// no es seguro.
- Desconéctese después de utilizar un servicio de banca por Internet o comercio electrónico para asegurarse de que ha cerrado la sesión.
- Mantenga limpios el caché y sus cookies del navegador para que los hackers no puedan acceder a su historial de navegación y obtener información.
- Recuerde que los hackers se dirigen cada vez más a niños en redes sociales y sitios web de juegos.
- Tenga precaución con las páginas web que accede: no visite sitios que ofrecen descargas ilegales o contenido ilegal (p. ej., uso compartido de archivos): incluso si no descarga ningún archivo, está expuesto a virus que pueden infectar su equipo.
- Mantenga las ventanas emergentes y los anuncios bloqueados, y no responda nunca a las ventanas emergentes que le pidan enviar o volver a enviar su información de inicio de sesión.

Buenas prácticas

- Revise regularmente los historiales de transacciones bancarias y de tarjetas de crédito y sus estados de cuenta para detectar transacciones sospechosas.
- Utilice la autenticación de dos pasos cuando esté disponible -confirma su ID en dos pasos cada vez que utiliza un cajero automático-, con una tarjeta de débito y PIN. Haga lo mismo para accesos online: utilice una contraseña y un código que se le enviará a través de texto, correo

electrónico o llamada para acceder a su cuenta. Recibirá una alerta si alguien inicia sesión desde un nuevo equipo.

- Evite hacer clic en el botón “cerrar” de un anuncio o en cualquier parte de la ventana para cerrarlo.
- Habilite la navegación privada siempre que sea posible: evite que las cookies y el historial de navegación se almacenen en su dispositivo.
- Utilice marcadores de confianza para sitios importantes, no para enlaces de correo electrónico o ventanas emergentes.
- Cierre las ventanas que contengan anuncios emergentes o advertencias inesperadas utilizando la X en la esquina superior derecha.
- No compre nada promocionado en un mensaje de spam, incluso si es una empresa legítima, su compra fomenta el envío de spam.

Recuerde: cada dispositivo implica un riesgo

Los ordenadores portátiles, tabletas y teléfonos móviles son susceptibles a las brechas de seguridad inalámbrica. No se conecte a sitios que no conoce o no reconoce. No suponga que un enlace Wi-Fi es legítimo; los hackers crean puntos de acceso fraudulentos que parecen idénticos a uno legítimo. En su lugar, utilice una red privada virtual (VPN), que sólo permite acceder a la red a los usuarios autorizados, para que los datos no puedan ser interceptados. No se conecte a sitios que no conoce o no reconoce.

Seguridad para móviles

Dependemos cada vez más de nuestros smartphone y nuestras tabletas para banca online, compras y redes sociales, por lo que es esencial proteger sus dispositivos móviles. Todos deberíamos tomar precauciones para asegurarnos de que estos dispositivos están protegidos.

Guía de buenas prácticas para sus dispositivos personales

- Ajuste su configuración de seguridad para limitar el acceso de terceros a sus datos a través de conexiones inalámbricas y Bluetooth.
- Evite hacer clic en los anuncios de Internet: existen aplicaciones de bloqueo de anuncios tanto para dispositivos Android como Apple, y la configuración del navegador puede ajustarse para limitar el seguimiento de anuncios.
- Actualice las aplicaciones del dispositivo cuando haya nuevas versiones disponibles, ya que a menudo incluyen parches de seguridad.
- Si cree que su dispositivo ha sido infectado con un virus: póngase en contacto con el fabricante del dispositivo o con su operador de telefonía móvil para obtener ayuda.
- Instale una aplicación de seguridad para escanear y eliminar aplicaciones infectadas.
- No intente eludir los controles de seguridad del sistema operativo del dispositivo (es decir, no haga un 'jailbreak' ni 'root' de su teléfono).
- Mantenga bloqueado su teléfono u ordenador: asegúrese de que está protegido en todo momento con contraseña/PIN.
- Mantenga actualizado el software del sistema operativo del dispositivo y asegúrese de que dispone de los parches de seguridad más recientes.
- Cifrar información confidencial: si su dispositivo móvil o portátil tiene funciones de cifrado de datos, utilícelas.
- Controle cómo se comportan las aplicaciones en tu teléfono: haga un seguimiento de los permisos de acceso/solicitudes de las aplicaciones instaladas en su dispositivo.
- Utilice un programa anti-malware/antivirus de confianza y actualícelo regularmente. Los dispositivos móviles son susceptibles a los mismos riesgos que los ordenadores de su casa u oficina.
- Apague Bluetooth cuando no necesite la conexión: su dispositivo será menos vulnerable a los ataques cibernéticos y la batería no se agotará tan rápido.
- Elija un smartphone con funciones de seguridad antirrobo. Si pierde o le roban su teléfono, tener un acceso remoto al mismo le permitirá bloquearlo, borrar los datos almacenados e localizar su ubicación.
- Haga copias de seguridad periódicas de sus dispositivos en el equipo doméstico o en la red en la nube para tener acceso a la información en caso de pérdida, robo o daño del dispositivo.
- Los delincuentes utilizan software malicioso para robar o destruir sus datos, y durante el proceso, comprometen la seguridad e integridad de los equipos y/o sistemas que utiliza. No ignore las advertencias. Instale un software antivirus y preste atención a las advertencias que reciba, como por ejemplo cuando intente acceder a un sitio no seguro en Internet.
- Tenga cuidado donde hace clic y con lo que descarga. Al hacer clic en vínculos desconocidos puede exponerse a programas de software maliciosos que exploran el equipo o rastrean pulsaciones de teclas, incluidas contraseñas y números de cuenta.
- Algunos programas incluyen intencionalmente malware. Durante la instalación, preste atención a los cuadros de mensa-

jes y a la letra pequeña. Cancele cualquier instalación si cree que puede ser dañina.

- Tenga cuidado con el correo electrónico de aspecto sospechoso. Incluso un correo electrónico de personas que usted conoce puede contener vínculos o archivos adjuntos de malware si su cuenta ha sido corrompida.
- Tenga cuidado al seguir los vínculos en el correo electrónico entrante. Cuando sea posible, visite los sitios web introduciendo directamente la dirección deseada en su navegador.
- Escanee los archivos con software de seguridad antes de abrirlos. No asuma que los archivos enviados por correo electrónico o los que se le dan en un disco o pendrive son seguros.

Malware

No confíe en las ventanas emergentes que le piden que descargue software. Su objetivo es convencerle de que su equipo ha sido infectado y que la descarga del software solucionará el problema. Cierre esta ventana inmediatamente, asegurándose de no hacer clic en nada dentro de la ventana emergente.

- La mayoría de los sitios de intercambio de archivos son ilegales y deben evitarse. Hay muy poco control de vigilancia para el malware en este tipo de servicios. El malware se puede disfrazar como una película, álbum o programa popular.
- Si su equipo está infectado con un virus de ransomware, en el que aparece una ventana emergente que le informa de que sus archivos han sido cifrados a cambio de un rescate, no se asuste. Desconecte inmediatamente el dispositivo de la red e intente restaurar los archivos desde una anterior copia de seguridad limpia. No pague el rescate.

Apuntes

CREDIT SUISSE AG, SUCURSAL EN ESPAÑA
Registro Mercantil de Madrid, Tomo 12.929,
Folio 12, sección 8, Hoja M-208189, Inscripción 1.ª
C.I.F. A-81956856
credit-suisse.com

MCIZ 1 12.2017