Ciberseguridad II

En el capítulo anterior se presentaron aspectos relativos a las aplicaciones seguras, las contraseñas seguras y el doble factor de autenticación. En este capítulo veremos otros temas complementarios a la ciberseguridad.

1 Uso responsable de redes sociales

Existen más de tres billones de personas en Internet y muchas de ellas usan las redes sociales para comunicarse. Pero si bien las redes sociales pueden ser divertidas y una excelente manera de chatear con amigos, también pueden ser riesgosas. Cuando las personas comparten información personal sobre sí mismas, pueden convertirse en blanco de estafadores y ladrones de identidad.

Sin embargo, puedes tomar algunas simples precauciones para que tú, tus amigos y familiares se mantengan seguros en las redes sociales. Veamos cómo:

Primero, usa siempre la configuración de privacidad más sólida que puedas. Consulta la sección Configuración de tu perfil de redes sociales y asegúrate de que solo tus amigos puedan ver lo que estás publicando.

Segundo, piensa en lo que publicas antes de hacerlo. Es fácil que las personas mal entiendan una broma o un meme divertido, especialmente con miles de millones de personas que podrían verlo. Sin embargo, es fácil evitar esto. Piensa en tus redes sociales como tu atuendo: hay algunas cosas que no usarías en público porque la gente se reiría o pensaría que no era una buena opción.

Recomendaciones

- Hay más de tres billones de personas en Internet, y no todas son quienes dicen ser. Mantén tu lista de amigos pequeña y nunca te hagas amigo de alguien que no conozcas en la vida real.
- Los atacantes a menudo incitan a las personas a tomar decisiones rápidas, con la esperanza de aprovechar sus errores. Piensa rápido, pero escribe despacio y no podrán tocarte.
- Es tentador compartir todo sobre tu vida, pero lo que compartes puede ser utilizado por otra persona. Con esa información, un atacante puede hacerse pasar por ti o entrar en tus cuentas en diferentes sitios.

2 Configuraciones de privacidad

Tu privacidad vale mucho: no sólo para ti, sino también para las personas que te importan. Si comprometen tus cuentas e información privada, también podrían comprometer la información de otras personas. Por eso, es importante que tomes buenas decisiones en tus configuraciones de privacidad para mantenerlas seguras.

Hay varias acciones inteligentes y simples que puedes hacer para asegurarte de que tu configuración de privacidad sea tan buena como sea posible. Mantén y restringe tus listas de amigos y contactos en redes sociales a personas que conozcas en la vida real. Asegúrate de que cuando compartas algo en Facebook, la publicación sea privada y no pública.

La configuración de privacidad no se aplica sólo a los sitios en Internet y redes sociales. Algo tan simple como usar una pantalla de bloqueo en tu teléfono móvil inteligente, hará que sea más difícil para otros entrar en él, protegiéndote a ti y a cualquier otra persona que se haya contactado contigo a través de ese teléfono.

Recomendaciones

- Pocos pero buenos amigos: La mejor manera de protegerte y proteger tu información es limitar tu lista de amigos y restringir lo que publicas sólo para tus amigos.
- No compartas tus datos: Cuando inicias la sesión de tu cuenta con una aplicación o servicio de terceros, la información se comparte entre ese servicio y tu cuenta. Controla tus datos utilizando el inicio de sesión individual y no instalando extensiones.
- Sincronización de datos: Deshabilita la sincronización automática de tu dispositivo, ya que obligará al que ha robado tu cuenta o dispositivo a ingresar tu contraseña, lo que detendrá al atacante porque desconoce ese dato.
- Bloqueo: La pantalla de bloqueo ahorra muchos problemas a largo plazo, si tu dispositivo es robado el atacante probablemente no sabrá tu contraseña. Habilita el cifrado para que, incluso si el atacante logra eludir la pantalla de bloqueo, los datos sean inaccesibles.

3 Mantén tu software actualizado

Las actualizaciones de software son como las vitaminas: no todos piensan en ellas pero todos las necesitamos y pueden marcar una gran diferencia para mantener un sistema saludable. Dediquemos un momento para hablar sobre las actualizaciones.

Las actualizaciones ayudan a mantener actualizado un software o un sistema. Debido a que se están desarrollando nuevas amenazas todo el tiempo, los fabricantes envían correcciones y actualizaciones para ayudar a proteger a sus usuarios de las nuevas amenazas, o simplemente de problemas que no encontraron cuando se creó el software por primera vez. Si alguien descubre un problema de seguridad en un programa y el usuario no descarga la actualización para solucionar el problema, está dejando una puerta abierta.

Das un gran paso para proteger tu sistema cuando tomas conciencia de las actualizaciones. Te brindamos algunos consejos.

Primero, siempre actualiza el software de seguridad (ej. antivirus), el navegador web y el sistema operativo. ¡Estos son los tres más importantes para mantenerte a ti y tu información a salvo!

En segundo lugar, puedes habilitar la actualización automática. Verifica la configuración de tus programas, como la opción para descargar automáticamente nuevas actualizaciones, siempre que estén disponibles.

Recomendaciones

- Actualízate siempre: Las actualizaciones corrigen errores, inseguridades y mantienen tus programas y dispositivos funcionando sin problemas. Recuerda, los delincuentes están actualizando sus métodos de ataque.
- Ataques al hacer clic: Una advertencia falsa te pedirá que descargues un archivo o completes un formulario, pero una advertencia real del navegador sólo te pedirá que no continúes con la acción.
- Licencia para fallar: Nunca uses versiones de software, un sistema operativo pirateado o sin licencia, estos a menudo contienen malware y causan más problemas de los que resuelven.
- La fuente importa: Sólo descarga actualizaciones de software de fuentes oficiales. Si no tienes la opción de actualizar automáticamente, consulta el sitio del fabricante para obtener actualizaciones y parches; no confíes en las advertencias del navegador que te piden que descargues cosas.
- Protege tu sistema con actualizaciones automáticas: Los programas legítimos a menudo te darán la opción de habilitar la actualización automática. Con esto, el software descargará automáticamente las actualizaciones y parches cuando éstos estén disponibles, eliminando el estrés de la actualización y asegurándose de que estés ejecutando las últimas versiones.

4 WiFi seguro

El WiFi es genial. ¿Qué tan genial es poder acceder a Internet desde cualquier lugar? Actualmente, muchas empresas ofrecen WiFi a sus clientes, para que puedan mantenerse conectados.

Sin embargo, eso no significa que sea perfecto. Usar WiFi público es algo así como hacer cualquier cosa en público: deseas estar seguro y no meterte en problemas accidentalmente. Hablemos sobre lo que puedes hacer para protegerte en un WiFi público.

Primero, cuando estés conectado a una red WiFi pública, nunca accedas a información privada. ¿Ver resultados deportivos? Bien. ¿Acceder a tu cuenta bancaria? No tan bien —no cuando el propietario del WiFi podría estar mirando la información a la que accedes—.

En segundo lugar, si utilizas el WiFi de una empresa, asegúrate de pedirle al propietario el nombre y la contraseña exactos de la red. De esa manera evitarás conectarte por error a la red de un imitador.

Recomendaciones

- Lo público no tiene privacidad: Usar redes públicas siempre es un riesgo. Cuando utilices una red pública, como en una cafetería o en un aeropuerto, nunca accedas a información privada como la de tu banco o correo electrónico.
- No es correcto conectarse automáticamente: Tener un dispositivo que se conecta automáticamente a redes conocidas y recordarlas es una puerta abierta para los programas maliciosos (malware). Deshabilita la conexión automática y elije cuidadosamente la red que deseas usar.
- Identifica al imitador: Los hackers a veces crean redes de imitación con los mismos nombres o nombres similares a las redes legítimas existentes. Estas redes de imitación no tendrán contraseña de protección para atraer a las personas. Al conectarte a una red administrada por una persona o una empresa, siempre confirma exactamente qué red es la suya y si está protegida por alguna contraseña.
- Contraseña preferida: Las redes públicas no protegidas tienen más probabilidades de ser ejecutadas por piratas informáticos que buscan un objetivo fácil. Cuando trabajes de forma remota, usa siempre las redes protegidas con contraseñas controladas y monitoreadas por el propietario del negocio.

Aprendiendo con el BNB

Acerca del Programa

En el marco de la Responsabilidad Social Empresarial y en virtud al fuerte compromiso con sus clientes y la comunidad en general, el Banco Nacional de Bolivia S.A. ha estructurado el programa "Aprendiendo con el BNB", con el objetivo de mejorar la cultura financiera de los bolivianos, dotándoles de los conocimientos básicos y las herramientas necesarias para que administren sus finanzas de forma responsable e informada, promoviendo de esta manera el uso efectivo y provechoso de todos los productos bancarios que se ofrecen en el sistema financiero.

Datos de contacto

Para más información acerca del programa ingresa a www.bnb.com.bo o escribe a bnbrse@bnb.com.bo.

BNB Banco Nacional de Bolivia

44

Aprendiendo con el BNB

Programa de Educación Financiera

Protección y Prevención Financiera

Ciberseguridad II