1. Ciberseguridad

El objetivo de este capítulo es informarte sobre la aplicación de buenas prácticas que debes emplear para mantener segura tu información en el mundo cibernético, creado y regulado mediante computadora.

2. *Phishing*

Contenido ya desarrollado y publicado en el Programa de Educación Financiera, capítulo Nº 16 “Seguridad en medios electrónicos I”.

3. *Malware* o programa malicioso

Contenido ya desarrollado y publicado en el Programa de Educación Financiera, capítulo Nº 17 “Seguridad en medios electrónicos II”.

4. Aplicaciones seguras

Las aplicaciones se han convertido en parte de nuestras vidas. Recuerdas ese eslogan que dice: ¿"Hay una aplicación para todo"? Hoy en día parece que realmente hay una aplicación para todo: juegos, ejercicio físico, belleza, pasatiempos y más. No es de extrañar que casi el 50% de todos los usuarios de teléfonos móviles descarguen al menos una aplicación nueva al mes.

Sin embargo, al igual que con cualquier dispositivo o programa, es importante que elijas y uses tus aplicaciones con cuidado. Algunas aplicaciones pueden ser estafas o contener virus.

Al momento de instalar una aplicación en tu dispositivo móvil, toma en cuenta lo siguiente:

Primero, busca los permisos. Cada vez que instales una aplicación, te pedirá tu consentimiento para acceder a las funciones de tu dispositivo móvil, por ejemplo: la cámara, los mensajes de texto y la lista de contactos. Pero, ¿una aplicación de ejercicio físico necesita usar tu cámara o una aplicación de juego, necesita saber a quién llamas? Puedes hacer clic en "Denegar" para evitar que una aplicación obtenga ciertos permisos.

Segundo, obtén tus aplicaciones de las fuentes oficiales. Apple App Store y Google Play tienen estándares para las aplicaciones que publican, y es menos probable que algo de la tienda oficial te cause problemas.

Recomendaciones

- Cuidado con los permisos: Cuando instalas una aplicación, ¿qué permisos solicita? Una aplicación de seguimiento puede querer saber tu ubicación, pero una aplicación de belleza no necesita esa información.
- Siempre que sea posible, instala aplicaciones de un autor acreditado y descárgalas sólo de la tienda de aplicaciones oficial.
- Identifica la estafa: Hay varias señales de que una aplicación podría ser una estafa o un ataque encubierto. Si la aplicación tiene muchas clasificaciones de cinco estrellas pero no tiene críticas, podría ser una estafa. Si el autor está sospechosamente silencioso o no promociona su aplicación, entonces debes tener cuidado.
- Vacuna tu dispositivo: Todos los dispositivos necesitan un antivirus, incluso si terminas descargando una aplicación peligrosa, o una aplicación previamente segura se infecta, un antivirus te ayudará a proteger tu dispositivo.

5. Contraseñas seguras

¡Contraseñas! Qué dolor de cabeza, especialmente cuando te preocupas por tener una contraseña segura. A veces parece que para estar seguro, tu contraseña debe contener letras, números, signos de puntuación, emojis, colores y al menos un jeroglífico egipcio.

Pero la verdad es que es más fácil crear una contraseña larga, fuerte y segura de lo que la mayoría de la gente piensa. Echemos un vistazo rápido a algunos consejos para crear una contraseña que mantenga segura tu cuenta.

Primero, intenta usar una “frase contraseña” en lugar de una contraseña. Las “frases contraseña” u oraciones siempre serán más largas que una sola palabra y se te quedarán mejor en la mente porque tendrán un significado sólo para ti.

Segundo, asegúrate de que sea algo que puedas recordar sin anotar. Si tienes que escribir tu contraseña, asegúrate de proteger ese papel con mucho cuidado, guardarlo bajo llave en un cajón del escritorio o en una caja fuerte.

Tercero, verifica la seguridad de tu contraseña. Muchas empresas de ciberseguridad tienen disponibles verificadores de seguridad de contraseña gratuitos en sus sitios web.

Recomendaciones

- Las contraseñas más cortas son más fáciles de romper para los hackers. NIST, el Instituto Nacional de Estándares y Tecnología de los Estados Unidos, recomienda que las contraseñas tengan entre 8 y 64 caracteres.
- ¿Te gusta mezclar idiomas o inventar tus propias palabras? Si es así, entonces te será fácil crear una contraseña. Si sólo tiene sentido para ti, es menos probable que aparezca en las listas de contraseñas rotas y publicadas que usan los hackers.
- ¿Cómo recuerdas una contraseña de 64 caracteres? Piensa en oraciones, no en palabras. Una frase o una oración es más fácil de recordar que una combinación sin sentido de letras y números, y proporciona esa longitud tan importante para que sea más difícil de descifrar.
- Si bien las reglas de tu empresa obliga a los usuarios a incluir muchos símbolos y números no necesariamente aumenta la seguridad de la contraseña. Enfócate en la longitud y la forma de memorizarla.
- No reutilices las contraseñas. Las contraseñas se descifran todo el tiempo, y cada contraseña rota se agrega a la base de datos de contraseñas de un hacker para usar en el futuro. Siempre usa contraseñas únicas.

6. Doble factor de autenticación

La “autenticación multifactor” es un término de la industria tecnológica para usar diferentes tipos de verificación para ingresar a una cuenta. La idea es que uses varias cosas al mismo tiempo para demostrar que realmente eres tú. Una contraseña es un ejemplo de un factor, una huella digital es otra.

La autenticación multifactor hace que sea mucho más difícil para los hackers entrar en las cuentas de las personas. Si tienen una contraseña pero no el otro factor o ninguno de los dos, no podrán acceder a tu cuenta.

Veamos algunos consejos para la autenticación:

Primero, verifica si puedes configurar el segundo factor de autenticación en cualquiera de tus cuentas. La mayoría de las cuentas que deseas proteger lo ofrecen. En una configuración como esta, la cuenta te pedirá algo además de una contraseña, generalmente, enviando un mensaje de texto a tu teléfono móvil.

Segundo, usa diferentes tipos de autenticación. Hay diferentes tipos de factores: algo que sabes, algo que tienes y, algo que eres. Usa una combinación de estos para mayor protección.

Recomendaciones

- Dos cerrojos son mejores que uno: Tener dos o más pasos de autenticación hace que sea más difícil para los atacantes violar una cuenta. La mayoría de las aplicaciones, dispositivos y servicios tienen la opción de habilitar la autenticación multifactor, y siempre es recomendable usarla.
- Existen tres tipos diferentes de autenticación: lo que sabes, lo que tienes y, lo que eres. La combinación de estos tipos de autenticación te brindará una mayor protección. Si alguien ha robado tu contraseña pero no tu teléfono celular, ¡no tiene suerte!
- La autenticación biométrica, el factor “algo que eres”, puede ser cualquier cosa, desde una firma hasta una huella digital, una palma o incluso un escaneo de iris. Considera implementar biometría para proporcionar una capa adicional de seguridad.

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

43

Aprendiendo con el BNB

Programa de Educación Financiera

Protección y Prevención Financiera

Ciberseguridad I