Pequeño Negocio, Gran Amenaza

Mejores prácticas de Seguridad en Línea

Antecedentes e Introducción

El propósito del siguiente documento es para ayudar a su negocio a tomar las medidas necesarias para utilizar las mejores prácticas de seguridad para los dispositivos de sus empleados y para ayudarlos a proteger la información del negocio y la información personal mientras navega en internet.

Este documento discute las prácticas de seguridad más básicas que **TODOS** deberían seguir como punto de partida. Si usted siente que pertenece a una categoría más compleja, es altamente recomendable que contacte a su proveedor de IT para futura dirección y asistencia.

Esta no es una lista comprensiva de todos los posibles procedimientos de seguridad, como muchas de las necesidades más avanzadas de IT dependen de la naturaleza del negocio y si el negocio tiene que cumplir con requerimientos de conformidad con su industria

Contraseñas

- Habilite Contraseñas/PINs/Cierre de posiciones en computadoras, teléfonos y tabletas. Si no los tiene, cualquiera que tome sus dispositivos tiene acceso a toda a su información y también las cuentas. Recuerde bloquear sus dispositivos si los deja solos.
- Contraseñas deberán incluir una mezcla de letras mayúsculas y minúsculas, números, y caracteres especiales.
- Contraseñas largas son mejores que contraseñas complejas y es la única defensa en contra de la "fuerza bruta" de los hackers (adivine su contraseña intentando sistemáticamente toda posible combinación).
- Para crear fácilmente una contraseña el doble de larga, muy complicada, pero todavía fácil de recordar, considere ingresar cada carácter doblemente. Por ejemplo: cat = ccaatt.
- Las contraseñas deben ser únicas; NUNCA use la misma contraseña para múltiples sitios y servicios. De otra manera si un sitio con baja seguridad es hackeado, el hacker tendrá acceso a todos sus sitios y servicios.
- Si las contraseñas necesitan ser escritas, deberán ser guardadas en un sitio físicamente seguro y bajo llave (no escondidas cerca del computador de escritorio). Si las contraseñas necesitan ser guardadas en su computadora, no deberán ser guardadas en un documento

en la computadora, en su lugar deberán ser guardadas con una herramienta de "gestor de contraseñas, entonces todas las contraseñas estarán encriptadas con una contraseña maestra.

- "2-Factores de Autenticación" es mejor si solo una contraseña protege su cuenta. Por ejemplo: Factor 1, es algo conocido (su contraseña); Factor 2, es algo que tiene (como un mensaje de texto enviado a un teléfono). Si tiene "2-Factores de Autenticación" habilitados, un hacker con su contraseña no tiene ningún poder sin el mensaje de texto especial del teléfono.

Copias de Seguridad de Datos

- Si los datos existen tan solo en un lugar no es una "copia de seguridad apropiada". Las Computadoras se averían. Las memorias externas también se averían o pueden ser robadas.
- Pruebe y verifique sus "copias de seguridad" restaurando un archivo de prueba por los menos una vez al año, preferiblemente una vez cada trimestre.
- Las copias de Seguridad son necesarias; existen virus y malware que encriptan toda la información en las computadoras con una contraseña desconocida y esta información es retenida hasta que una suma de dinero es pagada.
- Las copias de seguridad en la nube digital son una buena solución, pero primero lea los detalles de servicio para mirar si la información es confidencial cuando se necesita, debido a que no todas las copias de seguridad encriptan la información.

Tarjetas de Crédito

- Si su tarjeta de crédito es robada: 1) inmediatamente contacte a la compañía de la tarjeta de crédito y reporte el robo, 2) solicite una nueva Tarjeta de Crédito 3) y monitoree cobros falsos en sus estados de cuenta mensualmente. Si reporta el robo inmediatamente la Compañía de Tarjeta de Crédito revertirá cualquier cobro fraudulento.
- Si su compañía acepta pagos con tarjeta de crédito, establezca Políticas Laborales para entrenar a sus empleados en el manejo adecuado de tarjetas de crédito.
- Si tiene que escribir números de tarjetas de crédito, estos deben ser escritos en un papel de color específico, el papel necesita estar guardado en un lugar seguro y cerrado, y todos los papeles deberán ser destruidos y cortados en pedazos antes de ser desechados.
- Los números de tarjetas de crédito NUNCA deben ser almacenados como textos en la

computadora o servidores que no estén encriptados y protegidos con una contraseña compleja.

- Los números de tarjetas de crédito nunca deben ser enviados por correo electrónico, ya que los correos electrónicos no están encriptados.

Internet Inalámbrico

- Tenga mucho cuidado cuando se conecte a lugares de internet inalámbrico desconocidos. Si necesita usar uno, asegúrese de que es una conexión inalámbrica legítima (y no un falso WiFi usado por un hacker), confirme que el tráfico de internet está encriptado, examinando los certificados de seguridad de todas las páginas web, para asegurarse que el tráfico no ha sido manipulado.
- Cuando configure su red inalámbrica, cambie el nombre de su red (SSID) por algo único (y no dé ninguna información personal), habilite encriptación inalámbrica (WPA2), y use una contraseña: larga, compleja y única (asegúrese de seguir las “Mejores Prácticas de Contraseñas, señaladas en la parte superior).
- Cuando configure su propio equipo de red inalámbrica, cambie todos las contraseñas de inicio de sesiones única (asegúrese de seguir las “Mejores Prácticas de Contraseñas, señaladas en la parte superior).
- Cuando configure su propio equipo de red inalámbrica, revise periódicamente las actualizaciones proveídas por el fabricante de los dispositivos, ya que los equipos de redes, usualmente tienen fallas (similar a las computadoras).

Mantenimiento General de Dispositivos y Seguridad

- Toda computadora, teléfono inteligente y tableta tienen fallas de software y requieren actualizaciones regulares.
- Nunca retrase actualizaciones de las aplicaciones y del sistema; esto a menudo causa problemas o permite que los sistemas sean comprometidos.
- Reinicie la mayora de dispositivos semanalmente para aplicar actualizaciones, refresque sus aplicaciones y revise por nuevas actualizaciones.
- Aplique únicamente software de seguridad aprobado; investigue todos los sistemas de seguridad antes de que sean instalados; hackers han lanzado software de seguridad falso en el pasado.
- Su software de seguridad debe incluir (como mínimo) detección de malware/virus y filtro de contenido en las páginas web.

Pequeño Negocio, Gran Amenaza

- El filtro de contenidos en las páginas web es importante ya que muchos de los virus ahora son propagados engañando con la visita a páginas de web comprometidas que explotan fallas en los buscadores e instalan software malicioso en los dispositivos. Tenga mucho cuidado con las páginas web que haga click!
- Cuando ejecuta software de seguridad no significa que está protegido en contra de nuevos virus; software de anti-virus tan solo ayuda a detector virus "conocidos". Existen un sin número de virus desconocidos que han sido creados para capturar a todos. Tenga mucho cuidado con los archivos que ejecuta y con las aplicaciones que instala!
- Investigue todas las aplicaciones para teléfonos inteligentes/tabletas antes de instalarlos; hackers son conocidos por lanzar falsas aplicaciones parecidas a las originales con el objetivo de comprometer los dispositivos.

Percepción de Seguridad

- Hackers son conocidos por llamar y pretender que son "Soporte Técnico" engañan y ganan acceso a los dispositivos, cuando se abren archivos adjuntos en extraños correos electrónicos, solicitan que se visite páginas web comprometidas o entregando las contraseñas. Una sana sospecha de este tipo de comportamiento le ayudará a identificar atentados maliciosos.
- Si recibe una llamada telefónica no solicitada, pregunte por el nombre, la organización y número telefónicos para que se los vuelva a llamar una vez que se les investigue. Si no le entregan esta información sea muy desconfiado. Investigue la compañía para asegurarse que el número entregado es legítimo. Tenga mucho cuidado con la información que entrega sin confirmar la identidad de la llamada.
- Tenga mucho cuidado con la información que tiene en su página web y en las redes sociales; un hacker puede usar esta información para comprometer sus redes o engañar a sus empleados.
- La seguridad es un "proceso"; no un "producto". No existe una sola pieza de software o hardware que le brinde "seguridad".
- Incluso si no considera su información sensitiva y confidencial, sus dispositivos e información personal pueden ser usados por hackers para lanzar un ataque o cometer fraude.
- La "Seguridad" tecnológica puede lograrse teniendo conciencia de los riesgos, siguiendo mejores prácticas como sugieren los expertos de seguridad y tomando buenas decisiones tecnológicas.

Pequeño Negocio, Gran Amenaza

Seguridad Avanzada para negocios

- Si tiene servidores en el lugar de su compañía, los servidores deben estar configurados en un segmento dedicado de su red, protegido con un dispositivo interno firewall, ya que los dispositivos al navegar en internet son los primeros en ser comprometidos, y muy fácilmente los servidores pueden ser comprometidos si se puede tener acceso directamente a ellos.

- Si los dispositivos viajan con información sensible, el almacenaje total del dispositivo deber ser encriptado y protegido con una contraseña larga y compleja.
- La seguridad física de sus equipos es crítica. Si un atacante puede tener acceso físico a su computadora o servidor, estos serán comprometidos eventualmente.

Desarrollado por el SBDC de Michigan con apoyo de la Administración de Pequeños Negocios de los U.S. y la Corporación de Desarrollo Económico de Michigan.