Consejos para la seguridad de sus comunicaciones

Les ofrecemos las siguientes mejores prácticas solamente como referencia general y recomendamos a los lectores consultar con sus departamentos de IS (Seguridad de la Información) para instrucciones específicas.

Las amenazas de seguridad cibernética afectan regularmente a las personas en sus dispositivos corporativos y personales y es necesario un nivel superior de seguridad y conciencia tanto en los dispositivos personales como los de la empresa. Como cada vez es más común que los empleados participen en programas corporativos de Bring Your Own Device (Traiga su Propio Dispositivo), la línea entre comunicaciones personales y corporativas cada vez es más difusa, ya que se accede frecuentemente a la información de la empresa a través de dispositivos personales. La siguiente lista de mejores prácticas de la industria no es una lista exhaustiva, pero puede ayudarle a reducir el riesgo de infección.

En Dispositivos Personales:

- **Asegúrese de acceder a la información de la empresa utilizando herramientas de seguridad implementadas por su organización.** No evite estas herramientas utilizando webmail o conectándose a la red corporativa por fuera de una conexión segura. No almacene información corporativa sensible en dispositivos personales. Cada vez que sea posible, priorice la separación entre recursos utilizados para el trabajo y para asuntos personales.
- **Evite el uso de conexiones Wi-Fi gratuitas y públicas.** Si esto es inevitable considere el uso de una solución VPN comercialmente disponible en su computadora personal y en su teléfono móvil personal para impedir la captura de su flujo de datos.
- **Aplique una vigilancia extrema al presionar sobre cualquier hipervínculo o al abrir archivos adjuntos.** Si cualquiera de los siguientes elementos no son los comunes, no haga clic en el hipervínculo o no abra el adjunto – horario de envío, variaciones mínimas en la dirección del correo electrónico, nombre del archivo, o la dirección misma de la red del hipervínculo incluida en el correo electrónico. En el caso que Usted llegase a presionar en el hipervínculo o en el archivo adjunto sospechoso, no utilice su dispositivo hasta ejecutar un detector de virus y llevar a cabo cualquier recomendación de limpieza necesaria.
- **Averigüe y verifique la legitimidad de cualquier aplicación que autorice para ser instalada en su dispositivo personal.** Las aplicaciones maliciosas circulan ampliamente y pueden capturar todas sus pulsaciones de teclado y aún la información almacenada en su dispositivo.

- **Siga periódicamente estos pasos para garantizar que sus dispositivos personales sean seguros:**
  - Actualice el sistema operativo de su dispositivo portátil/laptop cuando le sea indicado por los mensajes de actualización del sistema.
  - Asegúrese que esté utilizando un buscador de Internet que esté actualizado.
  - Preste atención a los alertas pop-up cuando esté navegando y no otorgue excepciones de seguridad, especialmente para certificados vencidos, o para sobrepasar notificaciones o advertencias de seguridad.
  - Las laptops deben incluir una solución anti-virus disponible comercialmente que se actualice periódicamente.
  - Asegúrese que se utilice el cifrado (HTTPS en la barra de la dirección) cuando ingrese cualquier nombre de usuario y contraseñas; si Usted no está seguro que el cifrado esté implementado en la aplicación, utilice un servidor de VPN comercialmente disponible y acreditado.
- **Todos los dispositivos deben ser protegidos por una contraseña, utilizando una contraseña compleja y única.** Mientras esté de viaje, trate de mantener sus dispositivos portátiles personales o laptops en su poder o al resguardo de un colega. Evite dejar dispositivos sin supervisión en habitaciones de hoteles o cajas de seguridad, aun estando cerradas. Mientras esté de viaje en el exterior, evite autorizar actualizaciones del sistema ya que éstas pueden ser alertas fraudulentas enviadas cuando se conecta a un servicio de Wi-Fi del hotel.

Acerca de los Social Networking Sites (SNS – Sitios de Redes Sociales):

- Cambie periódicamente las contraseñas y asegúrese que las mismas no estén duplicadas en varios SNS o en otras plataformas sensibles tales como cuentas corporativas, cuentas bancarias, cuentas de correo electrónico personales.
- Habilite la autenticación multifactor, si es que está disponible. Esta prestación se ofrece a menudo en los SNS más conocidos; sin embargo, el usuario debe optar por activar la misma. Esta se puede hallar en la solapa de ayuda de SNS o en la barra de búsqueda.
- Esté atento a las solicitudes de conexión de parte de usuarios, aún aquellos con conexiones ya establecidas con familiares y amigos dentro de su red. Los impostores son activos online, haciéndose pasar como contactos legítimos.
- Manténgase familiarizado con los filtros y reglas de privacidad para estar consciente de cómo se comparten sus contenidos. Frecuentemente los SNS realizan cambios, solicitando atención periódica, por parte del usuario, en cuanto a las configuraciones. Establezca sus filtros de privacidad en los niveles más altos.
- Sea cauteloso cuando hace clic en un hipervínculo enviado por correo electrónico, especialmente las URL abreviadas, cuando esté conectado a un SNS. Este es el principal mecanismo para infectar un dispositivo con malware. Para acceder al sitio, diríjase a una nueva solapa y escriba el nombre del sitio en la barra de direcciones; no corte y pegue el URL.
- La calidad de los sitios SNS falsos es difícil de discernir respecto de los sitios SNS reales, lo cual engaña a los usuarios y los induce a brindar información personal después de hacer clic en un hipervínculo para conectarse con el sitio SNS. Evite presionar sobre cualquier hipervínculo dentro de correos electrónicos o abrir archivos adjuntos que Usted no esté esperando, especialmente cuando los correos electrónicos estén marcados con el logo del SNS. Por el contrario, regístrese al SNS directamente a través del URL.

1454847 07/16