Pequeño Negocio, Gran Amenaza

Consejos Rápidos para estar seguro en línea

Existen pocas cosas que puede hacer para protegerse y proteger a sus empleados.

Etiqueta de Contraseñas
Contraseñas han estado con nosotros por un largo tiempo y todavía son nuestra primera línea de defensa. Cuando necesite usar una contraseña, es importante que **NO**:

- Use información personal como parte de su contraseña
- Guarde su contraseña en una nota adhesiva cerca de su computadora
- Use la misma contraseña para cuentas múltiples
- Comparta su contraseña con **NADIE.**

Por favor **SIGA** estas mejores prácticas cuando cree contraseñas:

- Use una frase larga en lugar de una contraseña compleja:
    a. EJEMPLO: TheDetroitLionsRock123 en lugar de d3tr0it
- Use diferentes contraseñas para diferentes cuentas
- Utilice un gestor de contraseñas para manejar contraseñas múltiples.

Encuentre la "S" en HTTPS
Todas las páginas de web seguras y de servicios como banca en línea usan sesiones de navegación seguras, usando protocolos HTTPS. Y Usted puede verificar cuando navega mirando en la barra de dirección por HTTPS al inicio del URL. Esto asegura que cualquier información enviada sobre esta conexión está protegida por encripción SSL. Por ejemplo: **https**://www.google.com/

Esté alerta con remitentes desconocidos de correos electrónicos
Es recomendado que a menos que usted conozca el remitente o está esperando un correo específico que no abra el correo electrónico. Muchos virus encuentran la manera de llegar a los PCs a través de mensajes de correos electrónicos bien elaborados. Mientras filtro de correos no deseados (spam) es una opción, no existe una manera de detener el 100% de correos no deseados (spam), entrenamiento del usuario y conocimiento es de extrema ayuda en este tipo de situaciones.

Si algo no se siente correcto, probablemente no es
Sentido común va de la mano cuando está tratando de protegerse en línea. Si algo se ve muy bueno como para ser verdad o algo no se ve correcto, simplemente no se arriesgue. Si encuentra algo que necesita tener acceso pero no sabe si es seguro, contacte su proveedor de servicios de IT para más asistencia evaluando amenazas potenciales.

No busque información sensible en Wi-Fi público
Wi-Fi público es tan solo eso, PUBLICO. Cualquiera puede acceder y usar la red. Esto significa también potenciales hackers. Es muy común para hackers estar "olfateando" información en estas redes públicas para ver si pueden reunir información personal. Por lo tanto es altamente recomendable que no se tenga acceso a cualquier información personal o laboral a través de estas redes.

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.