STOP | THINK | CONNECT™

RANSOMWARE: INFORMACIÓN Y CONSEJOS

El *ransomware* es in tipo de virus informático cuyo uso está creciendo tanto entre consumidores como en empresas. Es importante que la gente esté bien informada sobre este tema porque vivimos en una sociedad cada vez más conectada.

¿QUÉ ES EL RANSOMWARE?

Es un tipo de malware que obtiene acceso a los archivos de su víctima, y los codifica para después demandar un precio de rescate de la víctima para poder recuperarlos. Estos ataques comienzan intentando convencer a la víctima de que seleccione un enlace o abra unos archivos que parecen legítimos pero que en realidad contienen el programa de robo y captura. Ransomware es un secuestro virtual de datos valiosos –desde fotos personales y memorias a información sobre clientes, datos financieros personales, o propiedad intelectual-. Todos somos víctimas potenciales, desde individuos a empresas.

¿QUÉ HAGO AL RESPECTO?

Todos podemos protegernos –y nuestras empresas- siguiendo los pasos de PARAR.PENSAR.CONECTAR.:

- **Mantenga su equipo limpio:** Todos los dispositivos que se conectan a la red –incluyendo PCs, teléfonos y tabletas- se pueden proteger de virus y malware teniendo siempre actualizadas todas las versiones de antivirus, programas y apps.
- **Esté dos pasos por delante:** habilite el uso de autentificación bifactorial en aquellas cuentas que lo permiten. Esto le da una capa adicional de protección, más allá del nombre de usuario con contraseña de siempre.
- **Haga archivos de respaldo**: Proteja lo que le es valioso -el trabajo, las fotos y cualquier otra información digital- realizando archivos de respaldo electrónicos periódicos y guardando esas copias en un lugar seguro.
- **Use mejores contraseñas:** si tiene claves débiles, mejórelas usando frases (sí, frases) con mayúsculas, minúsculas, cifras y símbolos; además, utilice contraseñas distintas para cada cuenta.
- **Si duda, tírelo:** Los enlaces por correo electrónico, tuits, los artículos y publicidad en línea a menudo contienen la llave de acceso a su computadora para cíber criminales.
- **Enchufar y escanear:** los archivos USB y otros dispositivos externos pueden ser infectados con virus y malware. Use su programa antivirus para escanearlos antes de abrirlos.

Traducido del original por Terry Inskip para OAS FCU.