PARA | PIENSA | CONÉCTATE® | ARGENTINA

Ministerio de Seguridad
Argentina

RANSOMWARE: DATOS Y CONSEJOS

A medida que la tecnología evoluciona, la cantidad de los ataques de ransomware crece de manera exponencial entre las empresas y los consumidores por igual. Por ello, es importante que los ciudadanos estén atentos a la higiene digital básica en un mundo cada vez más conectado.

¿QUÉ ES EL RANSOMWARE?

El ransomware es un tipo de programa malicioso que accede a los archivos de la víctima, los bloquea y luego exige que la víctima pague un rescate para recuperarlos. Los ciberdelincuentes utilizan estos ataques para intentar que los usuarios hagan click en archivos adjuntos o enlaces que parecen legítimos pero que en realidad contienen código malicioso.

El ransomware es como el "secuestro digital" de datos valiosos, tales como los registros financieros. Cualquier individuo u organización podría ser un objetivo potencial de un ataque de ransomware.

¿QUÉ PODÉS HACER?

Todos podemos ayudar a protegernos a nosotros mismos y a nuestras organizaciones contra el ransomware, siguiendo estos consejos:

MANTENÉ TUS DISPOSITIVOS LIMPIOS: Procurá mantener actualizado el software en todos los dispositivos conectados a Internet. Todo el software crítico, incluidos los sistemas operativos de computadoras y dispositivos móviles, el software de seguridad y otros programas y aplicaciones de uso frecuente, deben ejecutarse en sus versiones más recientes.

ACTIVÁ LA AUTENTICACIÓN EN DOS PASOS: La autenticación de dos factores puede usar cualquier medio, desde un mensaje de texto a su teléfono hasta un token o un biométrico, como tu huella digital, para brindar una mayor seguridad de la cuenta.

REALIZÁ UNA COPIA DE SEGURIDAD: Protegé tu trabajo, música, fotografías y otra información digital realizando periódicamente una copia de respaldo y almacenándola de forma segura. Tene en cuenta que esta copia puede ser hecha en frío (Cuando se detiene la operatoria del sistema para realizar la copia de respaldo) o en caliente (Continua la operatoria del sistema al realizarse la copia de respaldo).

MEJORÁ TUS CONTRASEÑAS: Si tus contraseñas son débiles, fortalecelas añadiendo mayúsculas, números y símbolos, y utilizando contraseñas diferentes para cada cuenta.

SI TENÉS DUDAS, NO LO ABRAS: Los enlaces enviados a través de correos electrónicos y mensajes son, a menudo, la forma en que los ciberdelincuentes intentan robar tu información o infectar tus dispositivos. Incluso si conoces la fuente, si algo parece sospechoso, no lo abras.

CONECTÁ Y ANALIZÁ: Los dispositivos USB y otros dispositivos externos pueden infectarse con facilidad. Por ello, usá tu software de seguridad para realizar un escaneo cuando conectes un dispositivo externo a tus equipos.