Decálogo de buenas prácticas

Cryptolocker (ransomware)

Dentro de estas amenazas cibernéticas están desarrollándose con mucha rapidez e impacto, las denominadas genéricamente como *ransomware*. La palabra se forma al juntar ransom (secuestro, en inglés) y el sufijo ware utilizado habitualmente para referirnos a un componente informático (como el hardware, software, etc.) es decir, es un software (o aplicación informática) diseñado con fines maliciosos, que bloquea el acceso a equipos informáticos o a los datos, hasta que se recibe un pago que se solicita como rescate.

¿Qué puede pasar?

Si somos infectados por un *ransomware* (cryptolocker) los principales riesgos a los que nos exponemos son:

Acceso a tu información privada

Pérdida de información

¿Cómo me protejo?

- Ser desconfiados. No abras ficheros adjuntos de correos que desconoces o pinches en links desconocidos.
- Haz copias de seguridad de forma periódica de tus datos importantes.
- Si las copias de seguridad las haces en un dispositivo externo, desconéctalo del PC una vez haya finalizado el proceso de copia.
- Usar software antivirus o antimalware en tus equipos y actualízalo.
- Tratar de mantener actualizado el sistema operativo de tu equipo y los programas que uses en la medida de lo posible.
- Evitar el pago del rescate, acude a un especialista en caso de infección dado que existen técnicas para recuperar la información.
- En caso de infección denunciar el caso a las Fuerzas y Cuerpos de Seguridad.

AUDITORES
Instituto de Censores Jurados de Cuentas de España