BOLETÍN SEGURIDAD: VIRUS CRYPTOLOCKER

Como se avisó en el reciente comunicado sobre el virus CryptoLocker, se han estado recibiendo correos electrónicos falseando la identidad de Endesa o de la Sociedad Estatal de Correos, con el objeto de engañar al receptor para que visite la web de estas empresas informando de una factura desorbitada o alegando que tienen un paquete que no ha podido ser entregado. El fin es secuestrar los ficheros y pedir un rescate[1].

La mayoría de los correos electrónicos recibidos, de naturaleza similar, son bloqueados por los sistemas de seguridad y los usuarios nunca llegan a recibirlos. Pero la previsión es que los métodos de ingeniería social empleados por los atacantes será cada vez mayor y, por tanto, se hace necesario seguir unas pautas y hábitos en el uso de las nuevas tecnologías.

En este caso concreto, se evitaría con preguntarse: ¿cómo es que Endesa conoce mi cuenta corporativa?

A continuación se recopilan algunas pautas alineadas con la vigente Normativa de Seguridad y buen uso de la Información, para una utilización preventiva y responsable, de los recursos informáticos.

- Mantener el sistema, los programas y el antivirus actualizados.
- Utilizar, para el trabajo diario, un usuario que no tenga privilegios de administrador.
- Tener siempre, usuarios con contraseña.
- Habilitar la opción del explorador de archivos para que se vean las extensiones de archivos conocidos[2].
- La utilización de Internet debe limitarse a la obtención de información relacionada con el trabajo que se desempeña como personal de la UNED o que pudiera conducir a una mejora, en la calidad del trabajo desarrollado.
- Ser precavidos al recibir mensajes no esperados, o de remitentes desconocidos, y nunca abrir ficheros anexos de mensajes, ni visitar páginas web que vengan en ellos.
- Si recibe un correo electrónico sospechoso comuníquelo al CAU o al administrador de correo.
- Marque los correos no deseados como SPAM y nunca pulse los enlaces para darse de baja.
- Bloquear la sesión del usuario en el supuesto de ausentarse temporalmente, a fin de evitar accesos de otras personas al equipo informático. Los sistemas operativos Windows pulsando simultáneamente la tecla “Windows” y “L” de LOCK.
- Mantener la configuración software de los equipos, no desinstalando o instalando programas o cualquier otro tipo de software distinto al necesario para su trabajo.
- Guardar todos los ficheros importantes en las carpetas compartidas habilitadas en la red informática, a fin de facilitar la realización de las copias de seguridad o respaldo. O en su defecto, guarde periódicamente una copia en algún dispositivo de almacenamiento USB.

1. Si ha recibido este correo electrónico y cree poder estar infectado porque ha visitado la web o ha descargado algún fichero, además de pedir ayuda al CAU, puede buscar en su disco duro los archivos encriptados, poniendo en el buscador del Explorador de Archivos: *.encrypted.
2. Desde el **Explorador de Archivos** > **Organizar** > **Opciones de Carpeta y búsqueda** > Pestaña **‘VER’** > Desmarcar **‘Ocultar las extensiones de archivos conocidos’**.