

¡Cuidado con los falsos antivirus! O cómo prevenir el scareware

Si estás navegando por Internet y en la pantalla aparece un mensaje de alerta que parece legítimo diciendo que en tu ordenador se acaba de detectar un intento de infección con un virus y que debes descargar un programa para que tu equipo esté bien protegido: ¿pincharías en el botón de aceptar?

Pues resulta que hay que tener cuidado con estos avisos, ya que muchos cibercriminales utilizan este método, conocido como scareware (scare, significa “miedo” en inglés), para engañar a usuarios incautos, logrando que estos instalen programas maliciosos en su ordenador.

Estos avisos aparecen en forma de ventana emergente durante nuestras sesiones de navegación y nos advierten de supuestos (aunque realmente falsos) peligros en nuestro ordenador como virus o fallos del software.

En lugar de descargarse una solución antivirus, en realidad lo que se instala en el equipo es la pieza de malware, normalmente adware publicitario o incluso un troyano. Posteriormente, suelen pedir al usuario/cliente sus datos bancarios o su tarjeta de crédito para realizar el correspondiente cargo en concepto de pago por el producto.

Obviamente, a la vista está que estamos perdiendo nuestro dinero, pero además, en el trasfondo, si realizamos una transacción en línea con estos sujetos les estamos proporcionando detalles de nuestra tarjeta de crédito o débito y otros datos personales, por lo que con frecuencia la estafa no acaba ahí. Los cibercriminales pueden intentar acceder a esas cuentas ellos mismos o bien vender la información a otros que intentarán sacar partido de ella. También en ocasiones se producen “secuestros” del ordenador, haciendo que deje de funcionar o bloqueando con contraseñas parte de nuestra información, fotografías o documentos y pedir un rescate a cambio.

Las ventanas de alerta que utiliza el scareware suelen ser muy convincentes, por lo que un gran porcentaje de usuarios con bajos conocimientos informáticos suelen ser víctimas de este tipo de fraude.

Un informe de la empresa de seguridad Symantec realizado entre julio de 2008 y junio de 2009 afirmaba que más de 40 millones de usuarios habían sido víctimas de este engaño en esos 12 meses. La compañía de seguridad identificó 250 versiones de scareware, y se cree que los criminales habrían podido ganar más de 850.000 euros al año.

Recientemente en nuestra sección web de Actualidad Jurídica nos hacíamos eco de una noticia según la cual el FBI ponía de manifiesto el gran crecimiento en el último año de este tipo de estafa relacionada con falsos antivirus.

Algunos consejos para prevenir este tipo de fraude serían:

- Optar por software/servicios antimalware o antivirus disponibles directamente por proveedores de confianza.
- No aceptar promociones de software publicitados inesperadamente en las ventanas del navegador durante nuestra navegación por Internet.
- Evitar abrir mensajes de correo electrónico, archivos y links cuyas fuentes sean desconocidas o no inspiren confianza.
- Mantener el sistema operativo actualizado con las últimas versiones de software y actualizar diariamente las bases de datos de las herramientas antimalware y antivirus.

Y recuerde que, ante una sospecha de una práctica de scareware, deben dar aviso a las autoridades responsables para tratar los incidentes de esta naturaleza (Fuerzas y Cuerpos de Seguridad del Estado o el propio INTECO) para detener dicha práctica fraudulenta y a sus autores, advertir a posibles víctimas de los hechos y reparar los equipos infectados.

Fuente:

https://www.inteco.es/blog/Seguridad/Observatorio/BlogSeguridad/Articulo_y_comentarios/?postAction=getDetail&blogID=1000077536&articleID=1000646902