RedAbogacía ABOGACÍA ESPAÑOLA

Aviso Seguridad: correos de suplantación de identidad (phising) y forma de proceder

Estimados amigos y amigas,

Ponemos en vuestro conocimiento que recientemente se viene observando un incremento en la recepción de correos maliciosos (que incluyen técnicas de "phising" y de suplantación del remitente).

Es frecuente, que nuestros destinatarios o incluso nosotros mismos recibamos algún correo electrónico con nuestro propio nombre o dirección de correo electrónico en el remitente. La gran mayoría de estos mensajes son interceptados por el filtro antiSPAM del servicio del CORREO ABOGACIA. Pero de vez en cuando puede recibirse algún correo, como sucedió el pasado 2 de octubre con correos que supuestamente provenían de miembros de la Subcomisión de Blanqueo de Capitales y que adjuntaban un archivo malicioso en forma de virus.

Para protegernos de esta lamentable lacra que sufrimos hoy en día, es fundamental estar informados. Existen actualmente estas estrategias en los correos maliciosos:

- Correos que llevan como adjunto algún tipo de archivo que contiene virus. Incluso pueden ser archivos de tipo documento, como el Word, con el propósito de que hagamos clic en el mismo para que se produzca la infección de nuestro equipo.

- Correos que simulen ser de entidades u organismos que incorporan algún enlace para que hagamos clic y pongamos nuestras credenciales. Un ejemplo de ellos, son los correos que se hacen pasar por entidades bancarias o incluso por Microsoft, se adjunta un ejemplo de ello.

- Correos que solo tienen un texto amenazador por el cual nos indican que hagamos algún tipo de ingreso a través de monedas virtuales. Se adjunta otro caso para facilitar su identificación.

La mejor forma de proceder para todos estos casos de "phising" es utilizar la herramienta que nos pone a disposición el programa de Outlook on-line (OWA) para informar de que el mensaje es de este tipo. De esta manera, haremos que el sistema sea capaz de reconocer este mensaje y evitar que se distribuya entre el resto de compañeros. Se adjunta un archivo con las instrucciones de cómo realizarlo.

Aprovechamos esta comunicación para recordar algunas pautas de seguridad que son de utilidad:

- No abrir correos de usuarios desconocidos. Si llevan un remitente falso seguir los pasos del documento para marcarlos como "phising".

- No pinchar en enlaces ni abrir adjuntos de mensajes de correo que puedan resultar sospechosos (aunque parezcan provenir de usuarios conocidos).

- Utilizar contraseñas robustas y no compartirlas.

- Tener nuestro sistema operativo actualizado con los últimos parches que remita el fabricante (Microsoft, Apple, etc.).

- Realizar copias de seguridad con frecuencia.

- Utilizar sistemas antivirus que se encuentre actualizado.

- Firmar digitalmente nuestros mensajes que enviamos a clientes y colaboradores.

Os recomendamos seguir el servicio de alertas que proporciona el Instituto Nacional de Ciberseguridad para estar al día de las posibles amenazas:

https://www.incibe.es/protege-tu-empresa/avisos-seguridad

Sería de interés que hicierais llegar esta información a todos los colegiados y colegiadas.

Atentamente,
RedAbogacía - Consejo General de la Abogacía Española

20190801-Ejemplo correo phising con enlaces.pdf
20191013-Ejemplo correo phising solo texto.pdf
Outlook-Indicaciones para informar de correo de phising.pdf