Abogacía Española CONSEJO GENERAL

Aviso Seguridad: recepción de correos falsos con el mismo remitente que el destinatario

Estimados amigos:

En los últimos días, se ha detectado una nueva campaña de correos falsos "**phising**" que llevan como remitente la misma dirección que el destinatario y que tiene un texto como la muestra siguiente:

"¡Hola! Como te habrás dado cuenta, te envié un correo electrónico desde tu cuenta. Esto significa que tengo acceso completo a su cuenta.Te he estado observando desde hace unos meses. El hecho es que usted fue infectado con malware..."

Estos correos forman parte del "spam" habitual, que se ha convertido en una verdadera "lacra" de nuestros días. En este caso particular, **no supone riesgo** al tratarse de un correo sin contenido ejecutable y sin enlace que dirija a una web fraudulenta en la que nos pudieran incluir algún malware. Y por supuesto, **no efectuar ningún pago.**

Para más información sobre este tipo de mensaje puede consultarse este enlace de la Oficina de Seguridad del Internauta: https://www.osi.es/es/actualidad/avisos/2020/10/tu-dispositivo-no-ha-sido-hackeado

Aunque el servicio de Correo Abogacía incorpora un buen sistema antiSPAM, hay algunos tipos de correo que son difíciles de detectar. Póngase por caso este ejemplo, al tener la apariencia de que son enviados desde nuestro remitente dificulta tal detección. Una acción que se puede realizar de forma particular, es informar al servicio del Correo de que este correo en concreto es "phising", se adjunta, en el enlace de más abajo, una guía explicativa de cómo proceder.

Adicionalmente, y como ayuda general, adjuntamos este enlace de Microsoft con indicaciones de cómo detectar si un correo es fraudulento: https://support.microsoft.com/es-es/help/4033787/windows-protect-yourself-from-phishing

De forma general, recordamos estas recomendaciones de seguridad:

- No abrir correos de usuarios desconocidos.

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

- Utilizar contraseñas robustas y no compartirlas.

- Realizar copias de seguridad con frecuencia.

- Utilizar sistemas antivirus.

Atentamente,
RedAbogacía - Consejo General de la Abogacía Española

Outlook-Indicaciones para informar de correo de phising-v2.pdf