DECÁLOGO DE SEGURIDAD PARA LA ABOGACÍA EN EL USO DEL CORREO ELECTRÓNICO

1 - Siempre tener cuidado al abrir correos electrónicos con documentos adjuntos.

En el caso de remitentes desconocidos, es muy extraño que una persona que contacta por primera vez te envíe un documento adjunto para tu consulta. Hay que desconfiar de estas situaciones. Piensa siempre que ese documento adjunto podría esconder algún tipo de *programa dañino (malware)* que puede infectar tu ordenador.

En todo caso, asegúrate de que el archivo realmente procede del remitente del que parece provenir. En ocasiones los correos infectados provienen de personas aparentemente conocidas y en las que confiamos. Si no estamos seguros de su verdadero origen, confirmemos con el emisor la veracidad del envío.

Es necesario conocer el riesgo que supone abrir los adjuntos que se reciben a través del correo electrónico y la necesidad de pasar el antivirus antes de abrirlos.

2 - Siempre tener cuidado al hacer clic en enlaces incluidos en correos electrónicos de remitentes desconocidos

Quienes nos envían correo basura con malas intenciones, saben que los antivirus cada vez son más eficaces en la detección y bloqueo de correos que incluyen adjuntos con virus. Pero también saben que es más fácil convencer al destinatario a que haga clic en un link. Por eso suelen utilizar también una segunda técnica consistente en el envío de enlaces al malware en el propio cuerpo del correo.

Es necesario ser cauteloso ante estas situaciones, sobre todo si el correo procede de remitentes desconocidos o poco confiables. Si hacemos clic podríamos encontrarnos en la situación anterior y los dispositivos de nuestro despacho podrían verse comprometidos.

3 - Instalar aplicaciones antimalware y activar los filtros antispam

Es necesario que tengas implantada una solución antimalware/antivirus empresarial que, entre otras tareas, escanee los correos electrónicos que recibáis en el despacho para confirmar que no ocultan virus.

En tu cuenta de Correo Abogacía ya cuentas con un filtro antiSPAM. Recuerda activarlo también en tus otras cuentas para filtrar correo basura o spam.

4 - Usar siempre contraseñas seguras

Para garantizar la seguridad de una contraseña, ésta debe tener más de 8 caracteres e incluir mayúsculas, minúsculas y letras o caracteres. En caso contrario nos arriesgamos a que cualquier persona, utilizando alguna de las herramientas existentes para este fin, nos descubra la contraseña y acceda a nuestros correos.

Utiliza siempre contraseñas robustas y cámbialas periódicamente.

5 - Evitar utilizar el correo electrónico desde conexiones públicas

Cuando nos conectamos a una red pública, como puede ser la wifi de una cafetería, el ordenador de un hotel, etc, hay que tener presente que el tráfico de red que envía o recibe nuestro ordenador puede ser interceptado por cualquiera de los usuarios conectados a esta red.

Para evitar ese acceso no consentido a la información confidencial que tratamos de salvaguardar, podemos implementar medidas como las de cifrar el correo, establecer una *red privada virtual* con nuestra empresa (VPN) de manera que todo el tráfico viaje cifrado; o, como última opción (pero sin duda la más adecuada) utilizar redes de telefonía móvil, como el 3G o el 4G.

6 - Cifra el correo electrónico al enviar información confidencial

El correo electrónico, si no va cifrado, viaja «en claro» a través de internet, esto quiere decir que cualquiera, a través de técnicas no muy complejas, podría leer el contenido de nuestros mails.

Por esta razón, si tenemos que enviar información de naturaleza profesional y/o confidencial deberemos cifrar nuestro correo electrónico o bien enviar un documento comprimido y cifrado. De esta forma, en caso de que sea interceptado, el tercero no podrá acceder al documento confidencial. Además, este tipo de buenas prácticas nos ayuda a tener una mejor imagen en cuanto al cuidado que damos a la información de nuestros clientes.

7 - No publicar direcciones de correo electrónico en la web ni en redes sociales

Una de las técnicas más comunes usadas por los ciberdelincuentes para obtener direcciones de correos electrónicos a los que enviar correo basura consiste en utilizar aplicaciones que rastrean direcciones de correo electrónico publicadas en páginas web y en redes sociales.

Para quienes desean ofrecer una cuenta de correo de contacto en la web o para la resolución de incidencias, es preferible la publicación de un formulario web que, a través de código, reenvíe el texto introducido en el formulario a una cuenta de correo electrónico.

8 - Nunca responder al correo basura

Los spammers (individuos o empresas que envían spam - correo basura) solicitan a menudo respuestas respecto al contenido de sus mensajes, o incluso llegan a pedir el envío de un correo electrónico para evitar recibir más spam. Nunca se debe caer en estas trampas, porque con ellas estamos confirmando al spammer que la cuenta de correo está activa y que hay alguien leyendo el correo.

9 - Desactivar el HTML en las cuentas de correo críticas

Muchos de los correos electrónicos se envían en formato HTML, lo que permite utilizar colores, negritas, enlaces, etc. Sin embargo este formato también permite incluir un lenguaje de programación denominado JavaScript, muy utilizado para funcionalidades que nos ofrece el correo electrónico. Esta funcionalidad, también permite a los spammers verificar que la dirección de correo electrónico es válida o, incluso, redirigir el navegador web del usuario a una página web maliciosa que acabe infectando nuestro ordenador.

Es recomendable la desactivación del formato HTML en el correo electrónico, al menos en las cuentas de correo críticas o que se encuentren a disposición del público. De esta manera no sería posible la visualización de correos electrónicos atractivos, pero este sería mucho más seguro.

10 - Utilizar la copia oculta (BCC o CCO) cuando se envíen direcciones a múltiples destinatarios

Cuando se envíen direcciones a múltiples destinatarios debe usarse siempre copia oculta (BCC o CCO). No hay que olvidar que en los correos electrónicos puede incluirse información de carácter personal de nuestros clientes que debe ser protegida y tratada con respeto a la privacidad. Todo ello sin perjuicio de las obligaciones deontológicas que puedan resultar aplicables.