

Buenas prácticas en el uso del Correo

Índice

1. Introducción

2. Buenas prácticas generales

3. Buenas prácticas en la recepción de correo

4. Buenas prácticas en el envío de correo

5. Buenas prácticas en la realización de envíos masivos

1. Introducción

La práctica del **spam** constituye un verdadero problema que **afecta de forma negativa a todos los usuarios de Internet**. Esta práctica consiste en la realización de envíos masivos no solicitados, generalmente de comunicaciones de carácter comercial. **El medio a través del cual se realiza más frecuentemente es el correo electrónico**, aunque también tiene lugar a través de otros, como mensajes de texto a móviles, publicaciones en foros, etc.

Tanto la legislación vigente como nuestra política prohíben de forma expresa la realización de spam.

El objetivo de esta *Guía* es doble. Por un lado, pretende informar de las **medidas que puedes tomar para evitar ser víctima del spam**. Por otro lado, pretende dar una serie de **sencillas pautas para no incurrir en dicha práctica**.

Confiamos en que esta *Guía* de buenas prácticas pueda serte de utilidad y contribuya a evitar, en todo lo posible, el envío y recepción masiva de correos electrónicos no solicitados.

2. Buenas prácticas generales

1. **Mantén al día de parches y actualizaciones** el sistema operativo y aplicaciones instaladas en el ordenador (especialmente el antivirus). Muchos virus se aprovechan de esas vulnerabilidades para infectar los equipos.
2. El tamaño de tu buzón de correo es limitado. **Debes controlar asiduamente tu buzón de correo a fin de evitar que se quede sin espacio libre**. Este cuidado no sólo lo agradecerán quienes remiten los emails sino también el propio servidor de correo y tu propio equipo. En este sentido, conviene borrar periódicamente aquellos correos de poca importancia como acuses de recibo, o aquellos que proporcionaron la información, cumplieron su cometido y ya no son necesarios, así como emails no deseados (spam). Elimina mensajes (descarga los adjuntos e imprime el contenido del mensaje si lo necesitas) y vacía la papelera y la carpeta de correos enviados siempre que sea posible.
3. **Proteje las claves asociadas a los buzones de correo electrónico**, evitando su divulgación a terceras personas. En caso de pérdida o robo de tus claves de correo, cámbialas lo antes posible.
4. **Debes proporcionar la dirección de correo con moderación**. Utiliza, siempre que sea posible, una cuenta gratuita para el registro en páginas web, ya que podrían enviar publicidad no deseada.

4. Buenas prácticas en la recepción de correo

1. **No aceptes documentos ni archivos adjuntos provenientes de desconocidos o que tengan un origen poco fiable.** Debes prestar atención a correos electrónicos con datos adjuntos susceptibles de contener virus. Algunos mensajes pueden aparecer como provenientes de otra persona distinta del autor. Aplica tu sentido común antes de asumir que un mensaje es válido.
2. El spam o correo basura son los mensajes no deseados que **hacen referencia a publicidad, pudiendo además contener virus.** Estos mensajes deben eliminarse sin ser leídos para evitar el aumento de la cantidad de dicho correo basura en el buzón así como la posibilidad de intrusión de virus en el sistema.
3. **No abras o ejecutes directamente los documentos o ficheros adjuntos.** Es mucho más seguro extraerlos previamente a un directorio del ordenador y analizarlos con un buen antivirus.
4. **No confíes en regalos y promociones de fácil obtención.** En ocasiones la infección de tu equipo se puede producir al visitar una Web facilitada en un correo aparentemente inofensivo.
5. **Desconfía de los correos de supuestas entidades bancarias que te soliciten introducir o modificar tus claves de acceso.** No es la forma de proceder de las entidades legítimas y probablemente se trate de un intento de fraude. Ante cualquier duda ponte en contacto con tu entidad.
6. Es recomendable **desactivar la función de “vista previa”** en clientes de correo como Outlook Express para evitar la intrusión de virus.

4. Buenas prácticas en el envío de correo

1. **Incluye un "Asunto" en el mensaje** e indica en dicho campo una breve frase descriptiva del mismo. Esto facilita la lectura, clasificación y posterior recuperación al destinatario y constituye una norma de cortesía.
2. **Utiliza las mayúsculas y minúsculas correctamente.** No se debe escribir todo el texto del mensaje en mayúsculas, ya que implica GRITAR. En la medida de lo posible, limita el uso de letras mayúsculas en el texto del correo. Si deseas enfatizar un término, puedes usar comillas, negrita, otros colores, etc. Si estimas que la letra es muy pequeña, puedes agrandar la letra hasta un tamaño que resulte más conveniente, pero no extravagante. El uso de mayúsculas en Internet sugiere emociones fuertes.
3. **No utilices estilos con fondos de mensaje** ya que aumentan el tamaño del mismo y pueden provocar problemas de recepción en el destinatario (filtrado por el sistema antivirus-antispam).
4. **Debes tener cuidado con el tamaño de los mensajes.** Incluir documentos de gran tamaño, imágenes o programas pueden hacer tu mensaje tan pesado que tenga problemas de recepción, así como un consumo de recursos innecesarios al receptor del mensaje. Cuando envíes un adjunto debes indicar en el mensaje cuál es su contenido y propósito para evitar que el destinatario sospeche que se trata de un virus. Asimismo es recomendable comprimirlos siempre que sea posible. Hay que conocer las aplicaciones Internet y usar cada una para la finalidad con la que fueron diseñadas. El correo electrónico debe ser usado con tamaños de mensajes moderados pues para tamaños grandes es más útil usar otros medios (cuentas FTP, por ejemplo). El correo electrónico no es el mecanismo adecuado ni eficiente para transferir ficheros.
5. **Las firmas automáticas deben ser lo más esquemáticas posible**, tratando de evitar imágenes o información innecesaria.
6. **No facilites datos personales o financieros a personas desconocidas.**
7. **No debes responder al correo no solicitado** (spam). Responder al correo comercial no solicitado es una forma de aumentar la cantidad de correo basura ya que indica al remitente que la cuenta es leída.
8. **No debes enviar publicidad**, a no ser que el receptor esté de acuerdo en recibirla.
9. **Debe evitarse el participar en el reenvío de correo no solicitado** (cadenas de mensajes, rumores, publicidad, etc.) o hoax (<http://es.wikipedia.org/wiki/Bulo>). Las casas comerciales y centros de alerta legítimos tienen como norma redirigir a servidores web donde dan información de forma fiable y detallan las acciones a tomar.
10. **Se debe respetar la privacidad de los mensajes y el destinatario.** No reenvíes mensajes sin el permiso del remitente, sobre todo aquellos con contenido conflictivo o confidencial.
11. **No debe abusarse de funcionalidades como el "aviso de lectura"**, su eficacia es escasa cuando lo utilizamos de manera indiscriminada o continuada, llegando a molestar al remitente. Se debe activar sólo en los casos en los que realmente sea necesario.

5. Buenas prácticas en la realización de envíos masivos

1. Si necesitas realizar envíos masivos **haz uso de las herramientas diseñadas para ello** (listas de distribución) **o realiza un diseño a medida de tu aplicación** de forma que se cumplan las recomendaciones que citamos en los apartados siguientes.
2. **Divide los destinatarios en varios grupos o listas de distribución** de forma que el volumen de correo quede repartido de forma equitativa. Mejor cuantos más grupos y menor número de destinatarios por grupo. Recuerda que hay proveedores de correo con sistemas de monitorización que chequean el número de correos que reciben desde una determinada IP o remitente.
3. **Realiza los envíos en horas valle** y espaciando los envíos entre grupos.
4. **Realiza un mantenimiento periódico de los usuarios suscritos a tus listas**, tratando de evitar suscripciones no deseadas, direcciones de correo sospechosas, y direcciones de correo que rebotan constantemente los correos que les envías.
5. Asegúrate de que el proceso de suscripción a tus listas de distribución cuenta con el **mecanismo de confirmación necesario** para verificar el deseo expreso del destinatario por pertenecer a ellas.
6. **Revisa los posibles correos de abuso relacionados con envíos que hayas realizado, así como los emails devueltos** y estudia las posibles causas.
7. Incluye en cada uno de tus envíos masivos las **instrucciones necesarias para que un destinatario pueda darse de baja de tu lista de distribución**.
8. **Realiza tus envíos con la periodicidad necesaria** o permite a tus usuarios elegir cada cuánto tiempo desean recibirlos.
9. Asegúrate que para tus usuarios es **fácil ponerse en contacto contigo**.
10. **Nunca pongas tu lista completa de destinatarios en el campo “Para” o “CC”** por dos razones fundamentales:
 - Todas las personas en el campo “Para” o “CC” pueden ver las direcciones de email en esos campos y podrán usarlas en la forma que ellos deseen.
 - Si alguien decide “Responder a todos”, todas las direcciones en los campos “Para” o “CC” recibirán la respuesta.
11. Asegúrate de que tus **emails son compatibles con RFC**.