

CONSEJOS PRÁCTICOS PARA FAMILIAS

Consejo 10. ¿Cómo deberíamos actuar respecto del correo electrónico?

1. No debes abrir correos electrónicos de remitentes desconocidos, y menos si se encuentran en otros idiomas. Con frecuencia se trata de spam (correo basura) y pueden contener archivos o documentos adjuntos con virus que dañarían tu dispositivo o enlaces a páginas falsas. Nunca deberías hacer clic en los enlaces incluidos en los correos electrónicos, sino que deberías entrar a la web tecleando su dirección en la barra del explorador.
2. Cuando llegan formularios por correo electrónico, en especial aquellos que piden datos personales, no deberíamos rellenarlos. Por otro lado, al rellenar formularios de nuestro interés debiéramos saber que los campos con asteriscos hay que rellenarlos obligatoriamente, mientras que el resto de campos son opcionales.
3. Cuidado con los correos de entidades bancarias pidiéndote que confirmes una cuenta o un pago bancario; siempre son falsos y podríamos ser víctimas de phishing¹. Las entidades bancarias nunca nos pedirán información personal a través de un correo electrónico. Si recibimos un mensaje de este tipo deberíamos comunicárselo a nuestra entidad bancaria.
4. Es útil tener dos cuentas de correo electrónico, una para asuntos formales y otra para asuntos informales, de este modo seleccionas la información que compartes en cada cuenta y das una dirección u otra en función del destinatario.
5. En la cuenta de correo que utilices habitualmente no incluyas tu nombre y apellidos, edad o fecha de nacimiento. A veces es más interesante utilizar apodos, nombres inventados o neutros.
6. La contraseña de tu correo electrónico es muy importante. No la compartas con nadie, y utiliza combinaciones de letras y números, utilizando alguna mayúscula si puede ser. Por seguridad, no utilices siempre la misma contraseña para todo.
7. El tratamiento de los datos personales es responsabilidad de todas las personas. No debemos seguir y reenviar las cadenas que se envían a través del correo electrónico. Ahora bien, si se desea reenviar el mensaje a muchos destinatarios, se recomienda usar el campo CCO (con copia oculta) para insertar allí las direcciones que de esta manera no podrán ser visualizadas por las personas destinatarias.
8. Si recibimos correos amenazantes, de coacción, insultos o amenazas, es importante conservarlos como prueba para un posible litigio.
9. Es importante no compartir datos ni imágenes personales con gente desconocida a través del correo electrónico.
10. Como medida de seguridad, puedes bloquear la visualización de imágenes en el cuerpo de los mensajes que recibes. De esta manera es posible descargar o hacer visibles las imágenes solo cuando estemos seguros de que el correo es de confianza.

¹ El phishing consiste en el robo de datos personales por medio de fuentes aparentemente fiables, pero que realmente son páginas webs falsificadas donde la persona usuaria introduce sus datos.