Quiero proteger mi correo electrónico

"He recibido un mensaje de un amigo diciéndome que le he enviado un email con un fichero adjunto que es un virus y yo no he sido, ¿es posible que alguien haya accedido a mi buzón de correo? ¿qué ha podido pasar?"

Cuando alguien consigue nuestra dirección de correo electrónico -porque estaba publicada en algún blog, foro, etc.; por el reenvío de emails en cadena; participación en páginas con falsos concursos, promociones, premios en los que para participar era obligatorio introducir datos como el correo electrónico, acción de un virus, etc.- y, además, utilizamos una contraseña que no es segura para acceder al buzón, es relativamente sencillo que alguien acceda a nuestro buzón y pueda leer, modificar y borrar correos privados, enviar emails en nuestro nombre, cambiar las opciones de privacidad y seguridad asociadas al correo...

¿Qué puede pasar si alguien accede a tu correo electrónico?

Pérdida de privacidad

Tus conversaciones privadas quedarán expuestas.

Tendrán acceso a tus contactos y documentación importante enviada/recibida por email:

- *Facturas*
- *Nóminas*
- *DNI*
- *Fotografías*
- *Vídeos*
- *Etc.*

Problemas de seguridad

Puedes perder el acceso a la cuenta si cambian tu contraseña de acceso o los métodos de recuperación de cuenta alternativos:

- *Otra dirección de email, número de teléfono, etc.*

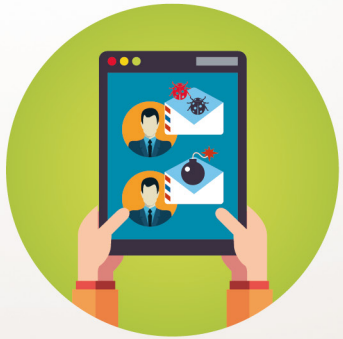
Si tienes otros servicios asociados a esa dirección de email también podrían verse afectados:

- *PayPal*
- *Facebook*
- *Amazon*
- *Dropbox*
- *Etc.*

Suplantación de identidad

Pueden enviar todo tipo de emails en tu nombre para:

- *Dañar tu reputación*
- *Ciberacosar a otras personas*
- *Enviar correos fraudulentos: phishing, malware, scam, etc.*
- *Poner en circulación bulos/hoax y spam/publicidad no deseada.*



Consejos y recomendaciones

El correo electrónico es una fantástica herramienta que te ofrece muchas posibilidades, tanto en el trabajo como en el ámbito privado, pero tienes que ser precavido cuando lo uses, por tanto, cúrate en salud y aplica las siguientes recomendaciones:

- *Asegúrate que utilizas una contraseña robusta y que no la estés utilizando para acceder a ningún otro servicio.*
- *Siempre que un servicio lo proporcione, activa la verificación en dos pasos para añadir una capa extra de seguridad en el proceso de autenticación.*
- *Evita facilitar información que pueda comprometer tu privacidad, en caso de que no tengas otra elección, cifra o comprime los ficheros con alguna contraseña que solo conozca el destinario del email y tú.*
- *No abras correos de usuarios desconocidos y elimínalos: podrían contener ficheros con malware, enlaces a páginas maliciosas o que suplantan la identidad de alguna entidad, etc.*
- *Aunque el remitente del correo sea conocido, si el mensaje te resulta sospechoso, consúlta directamente a esa persona para confirmar que no han falseado su dirección de email.*
- *No te olvides de realizar copias de seguridad para que no pierdas información de valor por si hubiera algún problema con el servidor de correo.*

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS
incibe_ 2006-2016 TRABAJANDO POR LA CONFIANZA DIGITAL
OSI Oficina de Seguridad del Internauta