"Recibí un email, supuestamente de mi tienda online favorita, que detallaba que estaban regalando varios productos por tiempo limitado. Solo tenía que entrar en el enlace y completar varios campos.

Me interesó, así que los rellené, incluyendo mi nombre, dirección y datos de mi tarjeta de crédito. Días más tarde me di cuenta de que faltaban 600€ en mi cuenta."

¿Cómo nos afectaría?

Suplantando la identidad de personas, entidades y servicios conocidos, **el ciberdelincuente es capaz de engañarnos para que le facilitemos información personal.** Para ello, crean correos electrónicos y mensajes que utilizan como reclamo para que finalmente accedamos a una web fraudulenta.

Comprobar la ortografía y redacción

Muchos de los correos de phishing contienen errores ortográficos y de redacción, no son propios de entidades debido al uso de traductores automatizados.

Verificar que la cuenta es original

Debemos comprobar que el email coincide con la empresa que nos envía el correo. Generalmente utilizan dominios públicos o que se parecen al que sería el correo oficial.

Por ejemplo: gooogle.com en vez de **google.com**

Recomendaciones "Buenas prácticas del cibernauta"

Revisar la URL

Los enlaces del correo deben ser comprobados. Antes de hacer clic, podemos colocar el cursor del ratón sobre el hipertexto para ver la URL a la que nos redirige.

No descargar archivos adjuntos

Bajo ningún concepto descargaremos archivos adjuntos del email si no podemos confirmar que se trata de un mensaje legítimo.

Enlaces relacionados

- Conoce a fondo qué es el phishing
- No hagas clic en todo lo que lees
- Phishing. No muerdas el anzuelo

OSI Oficina de Seguridad del Internauta