



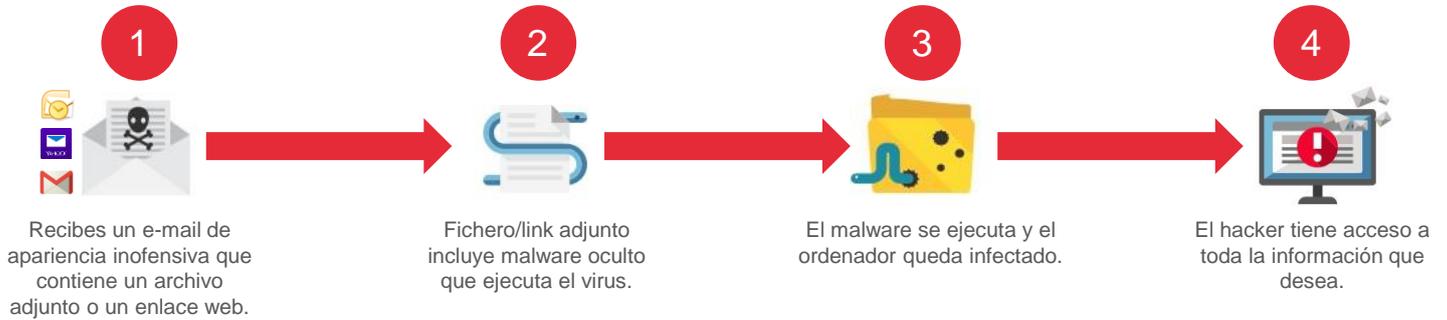
Decálogo de buenas prácticas

Phishing/Spam – e-mails maliciosos



▶ **¿QUÉ ES EL PHISHING?:** Es una técnica que utilizan los hackers para **acceder a información de tu ordenador o infectarlo a través del envío de correos electrónicos maliciosos** (con archivos adjuntos que incluyen programas maliciosos o enlaces que redirigen a páginas web no fiables).

¿Cómo funciona?



¿Qué puede pasar?

Abrir los ficheros adjuntos o acceder a enlaces web incluidos en correos electrónicos no deseados puede ocasionar consecuencias muy graves. Las más frecuentes son:



Fuga de información



Robo de identidad a través del uso de credenciales robadas.



Eliminación de ficheros almacenados en el equipo o en la red.



Propagación de malware a otros usuarios y sistemas de la red.

¿Cómo me protejo?

Evitar ser víctima de malware originado por campañas de *phishing* o *spam* es una tarea fácil si se adoptan ciertos **hábitos en situaciones cotidianas**. Podemos evitar infecciones de nuestros dispositivos o de terceros, fugas de información o reducir riesgos innecesarios.

- ▶ Si no esperas un e-mail, **evita abrirlo** especialmente si el origen es desconocido.
- ▶ **Analiza con detalle el e-mail** para identificar cualquier aspecto sospechoso.
- ▶ **Nunca pulses en el enlace o abras el fichero adjunto** de correos sospechosos.
- ▶ **Nunca proporciones tu usuario y contraseña** como contestación a un e-mail. Los administradores de sistemas nunca te lo solicitarán por esta vía.
- ▶ **Si sospechas** del e-mail o detectas un comportamiento extraño de tu equipo, **comunícalo** inmediatamente para su revisión.

Aspectos comunes del phishing

Aprende a identificar posibles correos maliciosos – 10 consideraciones básicas



- ✓ Correo electrónico no esperado y aparentemente dudosa legitimidad.
- ✓ Cuenta de correo o dominio del correo (@xxxxyz.com) sospechoso.
- ✓ Saludos genéricos.
- ✓ Redacción extraña o con faltas de ortografía.
- ✓ Temática u otros aspectos sospechosos si comparamos con correos previos intercambiados el pasado con el remitente original, al que se está suplantando.
- ✓ Carácter urgente.
- ✓ Enlaces a otras páginas web.
- ✓ Archivos adjuntos no esperados.
- ✓ Solicitud de información confidencial.
- ✓ Diseño extraño o que no cumple el estilo de compañía a la que intenta suplantar.