PRINCIPALES ESTAFAS INFORMÁTICAS Y CÓMO PROTEGERTE

Compras, banca, redes sociales, trámites... Conoce las estafas informáticas más habituales y aprende a defenderte.

Escuela de Consumo
Ayuntamiento de Salamanca

Ayuntamiento de Salamanca

ESTAFAS INFORMÁTICAS QUE SE PRODUCEN A TRAVÉS DEL TELÉFONO

- **Smishing:** SMS o mensajes que simulan ser un banco, empresa de paquetería o administración pública. Solicitan pulsar un enlace, llamar a un número o facilitar datos bancarios.
- **SIM Swapping:** Duplicación fraudulenta de la tarjeta SIM de una persona para recibir sus códigos de verificación bancaria y acceder a sus cuentas.
- **Spyware**: Software malicioso que se instala en el móvil sin que lo adviertas para recopilar información, registrar actividad y robar credenciales.
- **Vishing**: Llamada telefónica que suplanta la identidad de un banco, una empresa de suministros o una administración pública para obtener datos, claves o autorizaciones de pago.

Escuela de Consumo
Ayuntamiento de Salamanca

Ayuntamiento de Salamanca

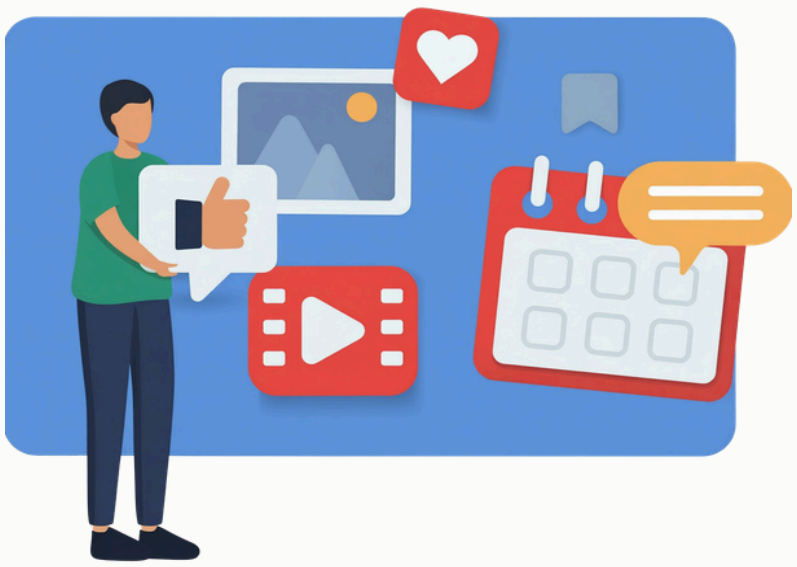
ESTAFAS INFORMÁTICAS QUE SE PRODUCEN A TRAVÉS DEL CORREO ELECTRÓNICO

- **Phishing:** Correos que suplantan a empresas, bancos o administraciones para que pulses un enlace, descargues un archivo o introduzcas tus datos en una web falsa.
- **Ransomware**: Malware que bloquea o cifra tus archivos y exige un rescate económico para recuperarlos. El pago del rescate no garantiza la recuperación de la información ni la eliminación de la amenaza.
- **Spoofing**: Falsificación de la identidad del remitente para que el mensaje parezca proceder de una persona o entidad conocida. El remitente visible puede no ser el real.
- **Spam malicioso:** Correos masivos no deseados que pueden incluir enlaces fraudulentos, archivos maliciosos o intentos de phishing camuflados como publicidad.

Escuela de Consumo
Ayuntamiento de Salamanca

Ayuntamiento de Salamanca

ESTAFAS INFORMÁTICAS QUE SE PRODUCEN A TRAVÉS DE LAS REDES SOCIALES



- **Suplantación de identidad:** creación de perfiles falsos o acceso a cuentas reales para pedir dinero, vender productos inexistentes o difundir enlaces fraudulentos.
- **Gusanos y troyanos:** malware que se difunde por mensajes privados, archivos, falsas promociones o aplicaciones no oficiales. Desconfía también de mensajes extraños enviados desde cuentas de personas conocidas: pueden estar comprometidas.
- **Noticias falsas y bulos:** contenidos falsos o llamativos usados para redirigir a páginas fraudulentas, obtener datos o instalar malware. Verifica siempre la fuente y la URL antes de compartir o introducir datos.
- **Phishing en redes:** sorteos falsos, mensajes de premios, supuestas verificaciones de cuenta o avisos urgentes que buscan que pulses un enlace o facilites tus claves bancarias.

Escuela de Consumo
Ayuntamiento de Salamanca

Ayuntamiento de Salamanca

ESTAFAS INFORMÁTICAS QUE SE PRODUCEN A TRAVÉS DE ELEMENTOS EXTERNOS

- **Man in the middle:** Interceptación de las comunicaciones entre un dispositivo y el servicio al que se conecta con el fin de obtener información o manipular los datos transmitidos. Es especialmente frecuente en redes wifi públicas inseguras.
- **Malware en soportes externos:** Software malicioso incrustado en pendrives, discos externos, descargas, archivos comprimidos o aplicaciones no oficiales. Se presentan con técnicas atractivas para captar la curiosidad del usuario.
- **Quishing (fraude con códigos QR):** Códigos QR manipulados o falsos que redirigen a páginas fraudulentas de pago o falsas webs de inicio de sesión. Especialmente frecuente en pegatinas sobre parquímetros, cartas de restaurante o carteles.

Escuela de Consumo
Ayuntamiento de Salamanca

Ayuntamiento de Salamanca

MEDIDAS PARA PROTEGERTE DE LAS ESTAFAS INFORMÁTICAS

1. **No pulses enlaces** en SMS, correos o mensajes que pidan datos urgentes. Accede siempre directamente a la web oficial.
2. **No facilites contraseñas ni códigos** de verificación por teléfono, SMS o correo. Ninguna entidad legítima te los pedirá así.
3. **Ante llamadas sospechosas**, cuelga y llama tú al número oficial. No uses el número facilitado por quien llama.
4. **Contraseñas únicas y robustas** para cada servicio. Usa un gestor de contraseñas y no reutilices claves.
5. **Activa la verificación en dos pasos** siempre que sea posible, preferiblemente con una app autenticadora.

Escuela de Consumo
Ayuntamiento de Salamanca

Ayuntamiento de Salamanca

MEDIDAS PARA PROTEGERTE DE LAS ESTAFAS INFORMÁTICAS

6. **Mantén actualizados** el sistema operativo, navegador, aplicaciones y antivirus.
7. **Evita operaciones sensibles** desde redes wifi públicas.
8. **Haz copias de seguridad** periódicas. En caso de ransomware, puede ser la única forma de recuperar tus archivos sin pagar.
9. **Verifica los QR** antes de escanear y comprueba la URL antes de introducir datos o pagar.
10. **Desconfía de archivos inesperados**, ejecutables o comprimidos, aunque procedan de contactos conocidos.
11. **Nunca accedas a tu banco desde un enlace del correo.** Escribe siempre la dirección manualmente en el navegador.

Escuela de Consumo
Ayuntamiento de Salamanca

Ayuntamiento de Salamanca

¿QUÉ HACER SI HAS SUFRIDO UN CIBERDELITO?

1. **Conserva todas las pruebas** antes de borrar nada: capturas, SMS, correos, URLs, números de teléfono, justificantes de pago y movimientos bancarios.

2. **Cambia inmediatamente las contraseñas** de las cuentas afectadas y de cualquier otra donde usaras la misma clave. Activa la verificación en dos pasos.

3. **Contacta con tu banco** si has facilitado datos bancarios o detectas cargos no reconocidos. El Banco de España recomienda comunicarlo cuanto antes.

4. **Avisa a tu operadora** si sospechas de SIM Swapping o te quedas sin cobertura sin causa aparente.

5. **Denuncia ante Policía Nacional o Guardia Civil,** especialmente si hay cargos económicos, suplantación, extorsión o acceso a cuentas.

6. **Contacta con INCIBE 017** para orientación inicial. Servicio gratuito y confidencial: teléfono 017

7. **Acude a la AEPD si el problema afecta al uso indebido de tus datos personales, difusión de imágenes o perfiles falsos.**

Escuela de Consumo
Ayuntamiento de Salamanca

Ayuntamiento de Salamanca

BASE LEGISLATIVA

- **Real Decreto Legislativo 1/2007, de 16 de noviembre,** por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.

- **Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.**
  - Arts. 197 a 201 (delitos contra la intimidad).
  - Arts. 248 a 251 bis (estafa informática).
  - Art. 264 (daños informáticos y ransomware).

- **Reglamento EU 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016** relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

- **Ley Orgánica 3/2018, de 5 de diciembre,** de Protección de Datos Personales y garantía de los derechos digitales.

- **Ley 34/2002, de 11 de julio**, de servicios de la sociedad de la información y de comercio electrónico.

PARA MÁS INFORMACIÓN

Para consultarnos dudas puedes encontrarnos, de lunes a viernes, de 8:30 a 14:00 h en:

CMI Victoria Adrados (Avd. Villamayor 71)

923282306

omic@aytosalamanca.es

@omic_salamanca

OMIC Ayto Salamanca

Escuela de Consumo
Ayuntamiento de Salamanca

Ayuntamiento de Salamanca