Castilla-La Mancha

CIBER SEGURIDAD

Castilla-La Mancha

Píldoras Formativas de Ciberseguridad

Casos de ingeniería social

Enero 2026

Agencia de Transformación Digital de Castilla-La Mancha. 2026

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

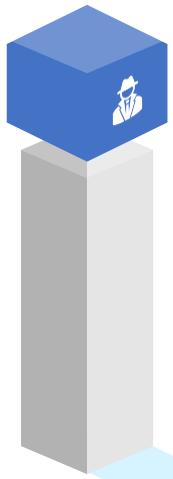
Castilla-La Mancha

Castilla-La Mancha

Casos de ingeniería social

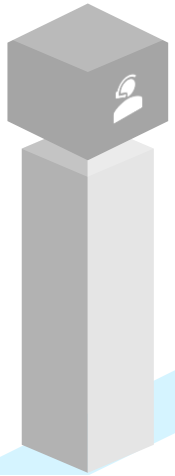
CIBER SEGURIDAD

Los ciberdelincuentes utilizan **técnicas de manipulación psicológica** para engañar tanto a particulares como a organizaciones, con el objetivo de obtener información sensible, lograr accesos no autorizados o cometer fraudes económicos. Estas prácticas se basan principalmente en crear una sensación de urgencia, abusar de la confianza y difundir información falsa, evolucionando de forma constante para aumentar su eficacia. Por ello, conocer los métodos más habituales resulta fundamental para identificar posibles intentos de fraude y evitar convertirse en víctima de estos ataques. A continuación, se describen los cinco casos más comunes, junto con las principales recomendaciones para su prevención.



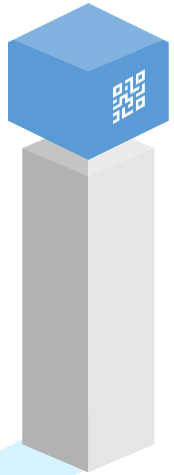
Spear-phishing dirigido

Correos personalizados que incluyen datos reales (nombres, cargos, proveedores) para parecer legítimos. Verifica siempre el remitente y desconfía de peticiones urgentes.



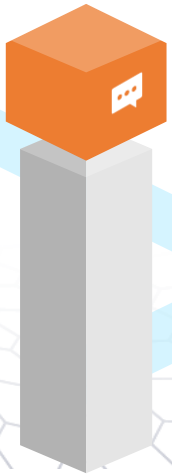
Vishing (llamadas telefónicas)

Suplantación de técnicos, bancos o proveedores por teléfono. Nunca facilites códigos, contraseñas ni datos personales a quien te llame.



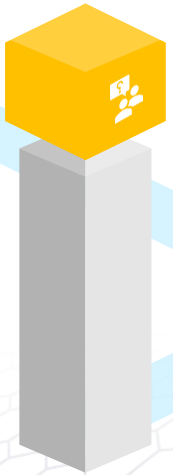
QR fraudulento (QRishing)

Pegatinas o códigos adulterados que redirigen a webs maliciosas. Revisa siempre el entorno y evita escanear QR desconocidos.



Smishing (SMS fraudulentos)

Mensajes que suplantan servicios de paquetería, bancos o administraciones. Evita pulsar enlaces y accede siempre desde apps oficiales.



Pretexting (historias fabricadas)

El atacante crea un contexto creíble para obtener información: “Soporte técnico”, “Proveedor con factura pendiente”, “Departamento de RR. HH.”. Verifica siempre por otro canal.

Agencia de Transformación Digital de Castilla-La Mancha. 2026

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Castilla-La Mancha