Castilla-La Mancha

Que hacer si caes en una trampa de phishing

CIBER SEGURIDAD

El phishing es una técnica de engaño usada por ciberdelincuentes para obtener información confidencial, como contraseñas o datos bancarios. Si crees que has caído en una trampa de este tipo, es importante actuar con rapidez para minimizar los daños.

Algunos consejos

Contacta a tu banco o entidad financiera si has proporcionado datos bancarios, para que puedan bloquear o monitorear movimientos sospechosos

Informa a tus contactos de confianza si crees que el atacante podría usar tu identidad para engañarlos. Así evitarás que otras personas caigan en la misma trampa.

Cambia tus contraseñas inmediatamente, especialmente las de correos electrónicos, cuentas bancarias y redes sociales.

Activa la verificación en dos pasos en todas tus cuentas importantes para añadir una capa extra de seguridad.

Escanea tu dispositivo con un antivirus actualizado para detectar posibles malware o programas espía.

Posibles señales

Ten cuidado si detectas:

- Correos o mensajes con urgencia o amenazas (“Tu cuenta será suspendida si no respondes en 24 horas”).
- **Errores ortográficos o gramaticales** inusuales.
- Solicitudes de **datos personales o bancarios** a través de enlaces sospechosos.
- Mensajes de remitentes desconocidos o **dominios extraños** que imitan a empresas reales.

Algunos enlaces maliciosos tienen esta forma:

- https.//micuenta-banco123.com (en lugar de https://banco123.com)
- http://secure-paypal-login.ru (en lugar de https://www.paypal.com)
- https://go0gle-support.net (parecido a Goodle, pero con un Cero en lugar de una “o”

Agencia de Transformación Digital de Castilla-La Mancha. 2025

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