

Los reflejos de seguridad en línea

5 reflejos diarios + 3 preguntas antes de hacer clic, para evitar las estafas más comunes.

LOS 5 REFLEJOS

1

Leer la dirección antes de introducir cualquier dato

Un solo carácter de diferencia = un sitio falso. El candado no demuestra legitimidad: solo indica una conexión cifrada.

2

Nunca a través del enlace recibido

¿Mensaje inesperado? Abre una pestaña nueva y escribe tú mismo la dirección oficial. Ante la duda: llama gratis al 017 (INCIBE).

3

Una contraseña única por cuenta

Gestor de contraseñas (ej. Bitwarden, gratuito). Mínimo 12 caracteres; una frase larga vale más que una palabra complicada.

4

Actualizaciones automáticas activadas

En todos tus dispositivos y aplicaciones. Cada actualización aplazada es un fallo que sigue abierto.

5

Verificación en dos pasos (2FA) siempre que sea posible

Primero el correo, luego banco y redes sociales. Prefiere una aplicación de autenticación al SMS.

Ante la duda — las 3 preguntas antes de hacer clic

1. ¿Esperaba este mensaje?
2. ¿Me presionan para actuar rápido (urgencia, amenaza, oferta limitada)?
3. ¿Puedo verificar por otro canal seguro (aplicación oficial, número al dorso de la tarjeta)?

Una sola respuesta inquietante → no se hace clic, primero se verifica.

¿Víctima o intento de estafa?

Datos bancarios comunicados: llama a tu banco inmediatamente (bloqueo de tarjeta).

Contraseña introducida en un sitio falso: cámbiala en todas partes donde la usabas.

Ayuda oficial y gratuita: línea 017 · incibe.es