

Detecta estafas, phishing y fraudes

GUÍA INTRODUCTORIA · MATERIAL EDUCATIVO



Aprende a identificar mensajes engañosos, enlaces sospechosos y fraudes antes de actuar.

Nivel: Principiante · Duración estimada del curso: 2.5–3.5 horas · Precio de catálogo: \$12 USD

Esta guía es una introducción escrita a los temas del catálogo. No equivale a un curso completo ni incluye videos. No otorga certificación oficial ni garantiza empleo.

Tus primeras herramientas

1. Cómo identificar correos fraudulentos

El phishing busca que entregues datos o realices acciones mediante mensajes que suplantán a una entidad. Puede llegar por correo, SMS, redes sociales o llamadas. Un mensaje bien escrito o con logotipos reales no demuestra que sea auténtico.

2. Reconocimiento de enlaces sospechosos

Revisa el dominio completo antes de abrir un enlace. En un computador puedes situar el cursor para ver su destino; en el celular, una pulsación prolongada puede mostrarlo según la aplicación. No abras el enlace solo para comprobarlo: entra escribiendo la dirección oficial o usando la app habitual.

3. Suplantación de identidad

La urgencia, los premios inesperados y las amenazas de cierre son señales de alerta. Si alguien pide un pago, confirma por un canal independiente que ya conocías. Nunca uses el número de teléfono incluido en el mensaje sospechoso como única verificación.

De la teoría a tus hábitos

4. Estafas en redes sociales

Un perfil conocido puede haber sido clonado o comprometido. Desconfía de inversiones con ganancias garantizadas, pagos previos para cobrar premios y solicitudes de códigos. Verifica con la persona por otro canal antes de transferir dinero o compartir información.

5. Prevención de fraudes digitales

Si recibes un mensaje sospechoso, no respondas ni descargues archivos. Repórtalo con las herramientas del servicio. Si ya entregaste credenciales, cambia la contraseña desde el sitio oficial, cierra sesiones y revisa MFA. Si pagaste, contacta cuanto antes con tu entidad financiera.

Ejercicio seguro

Redacta un mensaje ficticio de premio inesperado y marca tres señales de alerta. Anota cómo verificarías su legitimidad sin abrir enlaces ni contactar al supuesto remitente.

Antes de continuar

Realiza actividades únicamente en tus propias cuentas, equipos o entornos expresamente autorizados. No compartas contraseñas, códigos ni información privada. Los ajustes pueden variar según tu dispositivo o proveedor; consulta siempre su documentación oficial.