

3.º ESO · CFG · UNIDAD 10

Fraudes y ciberseguridad

Fraudes y estafas: señales de alarma, datos, contraseñas y qué hacer si has caído

PARA EMPEZAR

En esta unidad aprenderás a...

- Reconocer los mensajes y las llamadas que suplantan a un banco, a una empresa de paquetería o a un organismo.
- Detectar las señales de una estafa: urgencia, enlaces raros, peticiones de claves y ofertas demasiado buenas.
- Explicar otras estafas habituales entre jóvenes, como las compras falsas, los perfiles falsos y las «mulas» de dinero.
- Describir qué datos tuyos tienen valor y qué derechos tienes sobre ellos.
- Comparar contraseñas según su longitud y activar la autenticación de dos factores (o verificación en dos pasos).
- Seguir los pasos adecuados según lo ocurrido cuando ya has caído en un fraude.

SITUACIÓN DE PARTIDA · CASO FICTICIO

Una situación de partida



Es abril en 3.º B del IES Ribera Norte. Martina espera unas zapatillas de balonmano y recibe un SMS que dice que su paquete está retenido. Dani ya ha abierto el enlace en el portátil «para ver». Hugo se asoma a la pantalla. Inés Varela ha escrito una pregunta en la pizarra: ¿ese mensaje es de verdad?

❓ Si te llega un mensaje de tu banco que te pide una clave, ¿qué harías antes de contestar?

❓ ¿Por qué crees que los estafadores piden poco dinero o ponen plazos muy cortos?

❓ ¿Cuál de estas contraseñas es más difícil de adivinar: la fecha de tu cumpleaños o una frase larga que solo tú recuerdas? ¿Por qué?

MAPA DE LA UNIDAD

Lo que vamos a ver

- **10.1** Phishing, smishing y vishing
- **10.2** Otras estafas
- **10.3** Tus datos valen dinero
- **10.4** Contraseñas y doble factor
- **10.5** Si te ha pasado: qué hacer

Phishing, smishing y vishing



Phishing

El engaño llega por correo electrónico.



Smishing

El engaño llega por SMS.



Vishing

El engaño llega por una llamada de voz.

CLAVE

La regla de oro: **no actúes desde el propio mensaje.** Comprueba por otro canal.

Seis señales en un SMS

SEÑAL	QUÉ SE VE EN EL SMS
Remitente	Un número de móvil sin nombre
Urgencia	«antes de 24 h»
Importe pequeño	1,99 €
Enlace raro	envios-lana-entrega.info
Datos de tarjeta	Se pagan «tasas» en el enlace
Mensaje genérico	«Su paquete», sin nombre ni pedido

CLAVE

Con una sola señal ya habría que parar. Con seis, no se pulsa nada.

Lo que cuesta un mensaje



Quien envía los SMS

10.000 mensajes; pica el 2 %.

1. **Personas.** 10.000 × 0,02 = 200 personas.
2. **Tasas.** 200 × 1,99 = 398,00 €.
3. **Datos de tarjeta.** Con 450 € de pérdida media: 200 × 450 = 90.000,00 €.

✔ **La «tasa» es el cebo; el negocio son los datos de la tarjeta.**

Otras estafas



Compras falsas

Piden pagar antes «para reservar», o un enlace «para cobrar».



«Hijo en apuros»

Un mensaje de un familiar con otro número; hoy hasta se imita la voz.



Mulas de dinero

Te ofrecen dinero por reenviar transferencias: 300 × 5 = 1.500 €, pero es un riesgo.

CLAVE

Habla con una persona de confianza **antes** de hacerlo.

Cuánto tarda en romperse

CONTRASEÑA	COMBINACIONES	TIEMPO
6 dígitos	10^6 = 1.000.000	menos de 1 segundo
8 minúsculas	26^8 ≈ 2,1 × 10^11	unos 3 minutos
8 con mayúsculas, minúsculas y cifras	62^8 ≈ 2,2 × 10^14	unos 3 días
12 con mayúsculas, minúsculas y cifras	62^12 ≈ 3,2 × 10^21	unos 102.000 años

CLAVE

La longitud pesa más que cualquier truco. Supuesto: mil millones de intentos por segundo.

Si ha pasado, cinco pasos

1. **Bloquea**
   Bloquea la tarjeta o la cuenta.
2. **Avisa**
   Cuéntale al banco lo ocurrido, con la hora.
3. **Cambia las claves**
   Del correo, las redes y el banco, y activa el doble factor.
4. **Guarda pruebas**
   Capturas, dirección, hora y justificantes.
5. **Denuncia**
   Ante la Policía o la Guardia Civil.

CLAVE

La línea gratuita y confidencial **017** de INCIBE atiende cada día del año, de 8 a 23 horas.

REPASO

Ideas clave

- **Suplantación.** Phishing, smishing y vishing, urgencia, enlaces y claves, comprobar por otro canal, un banco no pide la clave por mensaje.
- **Otras estafas.** Compras falsas y perfiles falsos, «hijo en apuros» y sorteos, mulas de dinero, prisa y premios imposibles.
- **Tus datos.** Datos personales y financieros, derechos: acceso, rectificación, supresión, oposición..., consentimiento desde los 14, los datos financieros también son personales si identifican a alguien.
- **Contraseñas.** Largas y únicas, gestor y doble factor, actualizaciones y redes abiertas, una frase larga multiplica combinaciones.
- **Si has caído.** Bloquear, avisar, cambiar claves, guardar pruebas y denunciar, línea 017 y aepd, contarlo a un adulto.

PARA TERMINAR

Para pensar

1. ¿Qué señales de alarma tiene un SMS fraudulento?
2. ¿Qué es el doble factor?
3. ¿Qué es lo primero que haces si has caído en un fraude?



¡Ahora te toca a ti!

Repasa, practica y comprueba lo que has aprendido.

📝 **Resumen**

✅ **Test**

👆 **Interactivos**

Libro, presentaciones, resúmenes y tests gratis en **josesande.com**