

3.º ESO · CFG · UNIDADE 10

Fraudes e ciberseguridade

Fraudes e estafas: sinais de alarma, datos, contrasinais e que facer se caíches

10

PARA COMEZAR

Nesta unidade aprenderás a...



Recoñecer as mensaxes e as chamadas que suplantan un banco, unha empresa de paquetaría ou un organismo.



Detectar os sinais dunha estafa: urxencia, ligazóns raras, peticións de contrasinais e ofertas demasiado boas.



Explicar outras estafas habituais entre mozos, como as compras falsas, os perfís falsos e as «mulas» de diñeiro.



Describir que datos teus teñen valor e que dereitos tes sobre eles.



Comparar contrasinais segundo a súa lonxitude e activar a autenticación de dous factores (ou verificación en dous pasos).



Seguir os pasos adecuados segundo o ocorrido cando xa caíches nun fraude.

SITUACIÓN DE PARTIDA · CASO FICTICIO

Unha situación de partida



É abril en 3.º B do IES Ribera Norte. Martina agarda unhas zapatillas de balonmán e recibe un SMS que di que o seu paquete está retido. Dani xa abriu a ligazón no portátil «para ver». Hugo asoma á pantalla. Inés Varela escribiu unha pregunta no encerado: esa mensaxe é de verdade?

❓ Se che chega unha mensaxe do teu banco que che pide un contrasinal, que farías antes de contestar?

❓ Por que cres que os estafadores piden pouco diñeiro ou poñen prazos moi curtos?

❓ Cal destes contrasinais é máis difícil de adiviñar: a data do teu aniversario ou unha frase longa que só ti lembras? Por que?

MAPA DA UNIDADE

O que imos ver

- **10.1** Phishing, smishing e vishing
- **10.2** Outras estafas
- **10.3** Os teus datos valen diñeiro
- **10.4** Contrasinais e dobre factor
- **10.5** Se che pasou: que facer

Phishing, smishing e vishing



Phishing

O engano chega por correo electrónico.



Smishing

O engano chega por SMS.



Vishing

O engano chega por unha chamada de voz.

CLAVE

A regra de ouro: **non actúes desde a propia mensaxe.** Comproba por outro canal.

Seis sinais nun SMS

SINAL	QUE SE VE NO SMS
Remitente	Un número de móbil sen nome
Urxencia	«antes de 24 h»
Importe pequeno	1,99 €
Ligazón raro	envios-lana-entrega.info
Datos de tarxeta	Páganse «taxas» na ligazón
Mensaxe xenérica	«O seu paquete», sen nome nin pedido

CLAVE

Cun só sinal xa habería que parar. Con seis, non se preme nada.

O que custa unha mensaxe



Quen envía os SMS

10.000 mensaxes; pica o 2 %.

1. **Persoas.** 10.000 × 0,02 = 200 persoas.
2. **Taxas.** 200 × 1,99 = 398,00 €.
3. **Datos de tarxeta.** Con 450 € de perda media: 200 × 450 = 90.000,00 €.

✔ **A «taxa» é a isca; o negocio son os datos da tarxeta.**

Outras estafas



Compras falsas

Piden pagar antes «para reservar», ou unha ligazón «para cobrar».



«Fillo en apuros»

Unha mensaxe dun familiar con outro número; hoxe ata se imita a voz.



Mulas de diñeiro

Ofrécente diñeiro por reenviar transferencias: 300 × 5 = 1.500 €, pero é un risco.

CLAVE

Fala cunha persoa de confianza **antes** de facelo.

Canto tarda en romperse

CONTRASINAL	COMBINACIÓNS	TEMPO
6 díxitos	10^6 = 1.000.000	menos de 1 segundo
8 minúsculas	26^8 ≈ 2,1 × 10^11	uns 3 minutos
8 con maiúsculas, minúsculas e cifras	62^8 ≈ 2,2 × 10^14	uns 3 días
12 con maiúsculas, minúsculas e cifras	62^12 ≈ 3,2 × 10^21	uns 102.000 anos

CLAVE

A lonxitude pesa máis ca calquera truco. Suposto: mil millóns de intentos por segundo.

Se pasou, cinco pasos

1. **Bloquea**
   Bloquea a tarxeta ou a conta.
2. **Avisa**
   Cóntalle ao banco o ocorrido, coa hora.
3. **Cambia os contrasinais**
   Do correo, das redes e do banco, e activa o dobre factor.
4. **Garda probas**
   Capturas, enderezo, hora e xustificantes.
5. **Denuncia**
   Ante a Policía ou a Garda Civil.

CLAVE

A liña gratuíta e confidencial **017** de INCIBE atende cada día do ano, de 8 a 23 horas.

REPASO

Ideas clave

- **Suplantación.** Phishing, smishing e vishing, urxencia, ligazóns e contrasinais, comprobar por outro canal, un banco non pide o contrasinal por mensaxe.
- **Outras estafas.** Compras falsas e perfís falsos, «fillo en apuros» e sorteos, mulas de diñeiro, présa e premios imposibles.
- **Os teus datos.** Datos persoais e financeiros, dereitos: acceso, rectificación, supresión, oposición..., consentimento desde os 14, os datos financeiros tamén son persoais se identifican a alguén.
- **Contrasinais.** Longos e únicos, xestor e dobre factor, actualizacións e redes abertas, unha frase longa multiplica combinacións.
- **Se caíches.** Bloquear, avisar, cambiar contrasinais, gardar probas e denunciar, liña 017 e aepd, contalo a un adulto.

PARA REMATAR

Para pensar

1. Que sinais de alarma ten un SMS fraudulento?
2. Que é o dobre factor?
3. Que é o primeiro que fas se caíches nun fraude?



Agora tócache a ti!

Repasa, practica e comproba o que aprendiches.

📝 **Resumo**

✅ **Test**

👆 **Interactivos**

Libro, presentacións, resumos e tests gratuítos en **josesande.com**