

La caza del fraude: ¿es de verdad mi banco quien me escribe?

Caso práctico en parejas sobre cinco mensajes reales (SMS, correos y notificaciones de Bizum) para distinguir cuáles son intentos de phishing y cuáles son legítimos, marcando las señales de alarma y decidiendo qué hacer en cada caso.

DURACIÓN

50 min · 1 sesión

AGRUPACIÓN

parejas con puesta en común en grupo clase

UNIDAD 4

El dinero y los medios de pago

MATERIALES

- Ficha con los cinco mensajes anonimizados (uno por pareja, incluidos en esta actividad)
- Tabla de respuestas: ¿fraude o legítimo? / señales / qué hago
- Pizarra para el recuento final

ENCAJE CURRICULAR · Saberes B.1 · Comp. específicas CE4 · Comp. clave CD, CPSAA, CC

Planteamiento

El dinero ya casi no se toca: viaja por el móvil en tarjetas, Bizum y apps del banco. Eso es muy cómodo, pero ha abierto la puerta a un montón de engaños que buscan robaros el dinero o las claves. La unidad ha explicado qué es el phishing y cómo protegerse; esta actividad os pone delante **cinco mensajes reales** del estilo de los que recibe cualquiera, para que practiquéis lo más útil: pararse un segundo y decidir si pinchar o no.

El objetivo no es asustarse, sino entrenar el ojo. Quien sabe reconocer las cinco señales de alarma del fraude digital no va a caer en él, por muy bien hecho que esté el engaño.

Objetivos didácticos

- Reconocer las señales típicas del fraude digital (urgencia, errores de redacción, enlaces raros, petición de claves, remitente sospechoso).
- Distinguir un mensaje legítimo de un intento de phishing con ejemplos cercanos.
- Decidir la acción correcta ante un mensaje sospechoso (no pinchar, no dar claves, verificar por el canal oficial).
- Aplicar las normas básicas de seguridad con medios de pago digitales.

El caso: cinco mensajes en tu móvil

Los mensajes son **realistas pero inventados** para la actividad. Ninguna entidad real ha enviado estos textos.

1. **SMS:** “BANCO: Hemos detectado un acceso no autorizado. Confirma tus datos en las próximas 2h o tu cuenta será bloqueada: <http://seguridad-banco-cliente.info>”
2. **Notificación Bizum:** “Has recibido un Bizum de 15 € de Laura Pérez. Concepto: entradas concierto.”
3. **Correo:** “Estimado clietne, su tarjeta a sido suspendida. Pinche aqui para reactivarla y introduzca su PIN completo y CVV.”

4. **SMS:** “Tu pedido de Correos no se ha podido entregar. Paga 1,79 € de aduana aquí: bit.ly/corr-eos-pago”
5. **App del banco:** “Tienes un cargo de 42,90 € en tu tarjeta terminada en 4417. Si no lo reconoces, ábrelo desde la app.”

Pasos

1. **(5 min) Encuadre.** El profesor recuerda las cinco señales de alarma del fraude vistas en la unidad y reparte la ficha.
2. **(20 min) Investigación en parejas.** Para cada uno de los cinco mensajes, la pareja completa la tabla:

MENSAJE	¿FRAUDE O LEGÍTIMO?	SEÑALES QUE LO DELATAN	¿QUÉ HAGO?
1			
2			
3			
4			
5			

Regla de oro: ante la duda, **nunca se pincha el enlace ni se dan claves**; se verifica entrando uno mismo en la app oficial o llamando al teléfono que viene en la tarjeta.

3. **(15 min) Puesta en común.** Cada mensaje se comenta en clase. Se vota a mano alzada “fraude” o “legítimo” antes de revelar la respuesta. El profesor destaca las pistas: la urgencia del 1, las faltas de ortografía del 3 (“clietne”, “a sido”), el enlace acortado del 4, y por qué el 2 y el 5 son legítimos (no piden claves ni meten prisa).
4. **(10 min) Cierre.** Cada estudiante escribe su propia **regla personal anti-fraude** en una frase para pegarla en la funda del móvil. Ejemplos reales que salen en clase: “*Ningún banco me va a pedir nunca el PIN por un enlace*” o “*Si tengo prisa, es trampa: respiro y entro yo a la app*”.

Para el profesorado

Solución orientativa: **1, 3 y 4 son fraude** (phishing y smishing); **2 y 5 son legítimos** (no piden claves ni datos, solo informan). El mensaje 5 es el más interesante para debatir, porque parece alarmante pero es justo lo que hace un banco de verdad: avisar sin pedir nada. Insiste en que la señal definitiva es **¿me piden claves o que pinche con urgencia?** Si la respuesta es sí, es trampa.

Evaluación

CRITERIO	DESCRIPCIÓN	PESO
Clasificación correcta	Acierta fraude/legítimo en al menos 4 de los 5 mensajes	30 %
Señales detectadas	Identifica las pistas concretas que delatan cada engaño	35 %
Acción correcta	Propone la respuesta segura (no pinchar, verificar por canal oficial)	25 %
Regla personal	Formula una norma anti-fraude clara y aplicable	10 %