Guía Didáctica

PREVENCIÓN DE FRAUDES Y ESTAFAS DIGITALES

Educación Secundaria de Personas Adultas (ESPA)

PROGRAMA EDUCATIVO

Autoría:

Nerea Garrido Toscano, Adriana Pinilla Roa, Laura Hernández Aldama

Web: https://foronativosdigitales.educarex.es

Contacto: foronativosdigitales@educarex.es

JUNTA DE EXTREMADURA

Consejería de Educación y Formación Profesional

CC BY SA

Apoyo conceptual

Unidad Didáctica: **Prevención de fraudes y estafas digitales**

Phishing

El phishing es el modelo base de engaño. Se define como un intento de engañar a las personas a través de mensajes de correo electrónico para que divulguen información confidencial, como contraseñas, números de tarjetas de crédito o datos bancarios.

• Mecánica: El atacante se hace pasar por una entidad de confianza (un banco, una red social o un jefe) para "pescar" a la víctima usando un cebo, como una urgencia o un problema en la cuenta.

• Variantes comunes:

◦ Desactivación de cuenta: Alertan de que la cuenta será cerrada si no se ingresan las credenciales inmediatamente.

◦ Falsificación de sitios web: Crean páginas idénticas a las originales para capturar datos en el momento del inicio de sesión.

◦ Phishing de clonación: Copian un correo legítimo previo, pero cambian el enlace o el archivo adjunto por uno malicioso.

Smishing

El smishing es una variante del phishing que utiliza los mensajes de texto (SMS) o aplicaciones de mensajería instantánea para atacar directamente los dispositivos móviles personales.

• ¿Por qué es efectivo? A diferencia del correo electrónico, el SMS se percibe como un canal más personal e íntimo, lo que genera una falsa sensación de confianza.

Vishing

El vishing (Voice Phishing) utiliza la voz y las llamadas telefónicas para manipular a las víctimas.

• Técnicas avanzadas: Actualmente, los atacantes utilizan inteligencia artificial para la clonación de voz y el *deepfake*, logrando que la llamada parezca provenir de un familiar o un cargo directivo de una empresa.

• El factor psicológico: Las llamadas telefónicas permiten una interacción en tiempo real donde el estafador presiona psicológicamente a la víctima (por ejemplo, simulando una

emergencia de un proveedor o un problema técnico urgente) para que tome decisiones impulsivas.

• Suplantación de identidad (Spoofing): Pueden manipular el identificador de llamadas para que en la pantalla del móvil aparezca un número oficial de una entidad gubernamental o bancaria.

Comparativa: Diferencias críticas

Características	Phishing	Smishing	Vishing
Canal Primario	Correo electrónico.	SMS o mensajería.	Llamadas de voz.
Dispositivo	PC y portátiles de trabajo.	Smartphones.	Teléfonos fijos o móviles.
Disparador emocional	Temor a perder acceso.	Curiosidad o entusiasmo (premios).	Ansiedad por la presión en tiempo real.

Actividades

Unidad Didáctica: **Prevención de fraudes y estafas digitales**

ACTIVIDAD 1: ¿Me están engañando? (diapositivas 2 a 6)

Objetivo: Desarrollar en el alumnado la capacidad de identificar y prevenir intentos de fraude digital (phishing, smishing y vishing), fomentando una actitud crítica y responsable ante comunicaciones sospechosas.

Tiempo previsto: 1 hora aprox.

Diapositiva 2: ¿Me están engañando?

A través de la comparación entre el queso de una trampa para ratones y los enlaces engañosos en la web, reflexionamos sobre cómo las personas pueden ser engañadas en internet.

Para ello el docente lanza preguntas abiertas como: ¿Alguna vez has recibido un SMS raro del banco? ¿Te han llamado diciendo que había un problema con tu cuenta? ¿Has recibido un correo diciendo que un paquete no pudo entregarse?

El alumnado comparte experiencias reales o cercanas (propias o de familiares).

Diapositiva 3: Phishing, smishing y vishing

Presentación de un vídeo explicando qué es el phishing (correos electrónicos fraudulentos); smishing (mensajes SMS engañosos); y vishing (llamadas telefónicas fraudulentas).

Diapositiva 4: Análisis de casos reales

Se pone en práctica la teoría vista en la diapositiva anterior a través de un análisis de casos reales. Para ello se divide al alumnado en pequeños grupos y cada grupo se le entrega un caso:

- Un SMS falso de un banco.

- Un correo que simula ser de Correos.

- El inicio de una llamada de "soporte técnico".

Cada grupo analiza: ¿Quién envía el mensaje? ¿Qué pide? ¿Qué intenta provocar (miedo, urgencia, confianza)? ¿Qué harías tú si lo recibes?

Una vez que lo han pensado en pequeños grupos, se realiza una puesta en común en la que cada grupo comparte sus conclusiones con el resto de la clase.

Diapositiva 5: Conviértete en detective

A partir de los casos analizados, el docente guía una reflexión conjunta sobre las señales de alarma, como: mensajes urgentes o amenazantes; errores ortográficos o de redacción; enlaces sospechosos; petición de contraseñas o datos personales; remitentes desconocidos o direcciones extrañas. Se comentan las diferentes señales de alarma a través de la

infografía “no piques el anzuelo” y se refuerza la idea de no actuar impulsivamente.

Diapositiva 6: Identificación de señales de alarma

En gran grupo, se elabora un listado de señales de alerta usando la plantilla descargable que aparece enlazada en la diapositiva.

Opcional: Se puede hacer un cartel con un decálogo de seguridad digital para colocarlo en un lugar visible del aula o del centro y de esa forma tenerlo siempre presente.

Tipo de agrupamiento del alumnado:
Individual, pequeños grupos y gran grupo.

Finalidad de la actividad: Proteger y empoderar a las personas frente a los fraudes digitales, promoviendo un uso seguro, crítico y responsable de las tecnologías de la comunicación en su vida cotidiana.

ACTIVIDAD 2: “Antes de hacer click…” (diapositivas 7 a 10)

Objetivo: Desarrollar en el alumnado habilidades prácticas de verificación y prevención frente a fraudes digitales, capacitándolo para analizar enlaces, mensajes y configuraciones de seguridad antes de interactuar con ellos.

Tiempo previsto: 1 hora aprox.

Diapositiva 7: Antes de hacer click

El docente muestra, de forma guiada y práctica, cómo comprobar una URL (dominio real, errores, enlaces acortados), qué significa https y el icono del candado, y cómo realizar una búsqueda inversa de números de teléfono o mensajes sospechosos.
Después, se analizan los ejemplos que aparecen en la diapositiva para ver si son reales o fake sin necesidad de tener que hacer click en ellos.

Diapositiva 8: ¿Fraude o real?

El alumnado trabaja por parejas. Se les presentan 8 situaciones (SMS, correos, anuncios publicados en redes sociales) y deben decidir conjuntamente si cada caso es fraude o legítimo, justificando su respuesta. Posteriormente, se realiza una puesta en común con explicación guiada.

Diapositiva 9: Protegiendo nuestro móvil

Actividad práctica en la que cada uno usará su propio móvil. Se les irán explicando los conceptos y a la vez se activará en sus dispositivos o se revisará que tengan activado el doble factor de autenticación (2FA); que usen apps de autenticación; se revisarán los permisos de las aplicaciones; y se identificarán posibles apps falsas o peligrosas que pueden tener en sus dispositivos.

Diapositiva 13: Guía de buenas prácticas

En gran grupo se elabora una guía de buenas prácticas en ciberseguridad, para ello se usará la plantilla enlazada a la diapositiva. El objetivo es recopilar los consejos clave aprendidos durante la actividad.

Opcional: Se puede colocar la guía de buenas prácticas en algún lugar visible del aula o centro para que siempre que lo necesiten lo puedan consultar.

Tipo de agrupamiento del alumnado: individual, parejas y gran grupo.

Finalidad de la actividad: Capacitar al alumnado para actuar de forma segura, crítica y responsable en entornos digitales, reduciendo el riesgo de fraude mediante la adquisición de conocimientos prácticos y hábitos de prevención aplicables en su vida cotidiana.

ACTIVIDAD 3: El familiar en apuros (diapositivas 11 y 12)

Objetivo: Desarrollar en el alumnado una actitud crítica ante posibles estafas digitales, especialmente aquellas que utilizan la suplantación de identidad de familiares, fomentando habilidades de verificación de la información, toma de decisiones seguras y establecimiento de planes personales de protección digital.

Tiempo previsto: 20 minutos

Desarrollo: Diapositiva 12.

Se proyecta el video sobre cómo funciona la estafa. En gran grupo, el alumnado analiza los elementos que hacen que el mensaje resulte creíble (tono urgente, apelación emocional, uso de un familiar cercano, presión para actuar rápidamente, etc.).

En pequeños grupos, el alumnado reflexiona y responde a la pregunta:

¿Qué pasos seguiría antes de enviar dinero o datos personales?

Se trabajan estrategias como comprobar la identidad, no responder de inmediato, contrastar la información por otra vía, buscar señales de alerta, etc.

Plan personal de seguridad: De forma individual, cada alumno/a elabora un pequeño plan de actuación respondiendo a:- ¿Qué haré la próxima vez que reciba un mensaje extraño? ¿Con quién puedo contrastar la información (familia, profesorado, personas de confianza)?

Se comparten en gran grupo las conclusiones y planes elaborados, reforzando las buenas prácticas y aclarando dudas.

Tipo de agrupamiento del alumnado: Gran grupo (presentación del caso y puesta en común). Pequeños grupos (taller de verificación). Trabajo individual (plan personal de seguridad).

Finalidad de la actividad: Concienciar al alumnado sobre los riesgos de las estafas digitales, dotarlo de herramientas prácticas para detectar mensajes fraudulentos y promover conductas responsables y seguras en el uso de la tecnología y la comunicación digital.

Ficha técnica

Unidad Didáctica: **Prevención de fraudes y estafas digitales**

Objetivos

1. Identificar las señales más comunes del phishing, smishing, vishing y estafas híbridas.
2. Analizar casos reales de engaños que simulan familiares en apuros o urgencias.
3. Reconocer enlaces, adjuntos y aplicaciones potencialmente peligrosas.
4. Aplicar estrategias de verificación y contraste antes de actuar.
5. Conocer medidas básicas de autoprotección digital (contraseñas, 2FA, antivirus, webs seguras).
6. Practicar la toma de decisiones ante situaciones simuladas de fraude.
7. Fomentar la comunicación con familia y profesorado para detectar riesgos.

Contenidos

- Tipos de fraude digital:
  - Phishing: correos electrónicos que suplantan a entidades legítimas para robar datos personales o bancarios mediante enlaces o archivos.
  - Smishing: mensajes SMS o de mensajería instantánea con enlaces fraudulentos que buscan el mismo objetivo.
  - Vishing: llamadas telefónicas en las que el estafador se hace pasar por bancos o servicios oficiales para obtener información confidencial.
  - Apps falsas: aplicaciones que imitan a las oficiales y capturan credenciales o datos del dispositivo.

- La estafa del "familiar en apuros". Un fraude basado en la suplantación de un familiar que solicita dinero urgente alegando una emergencia.
  - Por qué funciona: uso de la urgencia y la carga emocional.
  - Señales: cambio de número, petición de transferencias inmediatas, mensajes insistentes y poco habituales.

- Señales de alerta
  - Mensajes o llamadas con tono urgente o amenazante
  - Errores ortográficos o remitentes desconocidos
  - Enlaces sospechosos o acortados
  - Solicitud de claves, códigos o datos sensibles

CC BY SA

- Webs falsas
    - Cómo se construyen: copian la imagen de webs reales y usan dominios muy similares.
    - Cómo detectarlas: revisar la URL, evitar enlaces recibidos por mensajes y comprobar la autenticidad del sitio.

- Seguridad básica en banca online y plataformas de pago.
    - Contraseñas seguras y únicas
    - Doble factor de autenticación
    - Uso exclusivo de apps y webs oficiales
    - Revisión periódica de movimientos

- ¿Qué hacer si ya he caído en un fraude? Pasos iniciales.
    - Contactar de inmediato con la entidad bancaria
    - Bloquear accesos y cambiar contraseñas
    - Conservar pruebas del fraude
    - Presentar denuncia ante las autoridades

Destinatarios

Alumnado de Educación Secundaria para Personas Adultas (ESPA), como formación transversal aplicable a cualquier grupo y contexto educativo.

Metodología

Metodología **activa**, **participativa y práctica**, centrada en el reconocimiento de fraudes digitales y la toma de decisiones seguras en contextos reales.

- **Aprendizaje basado en casos**: análisis de ejemplos reales de phishing, smishing, vishing y estafas de suplantación.

- **Identificación guiada de señales de alerta**: detección colectiva de indicios de fraude en mensajes, llamadas, enlaces y webs.

- **Simulación de situaciones cotidianas**: resolución de escenarios como compras online, uso de banca digital o mensajes de "familiar en apuros".

- **Dinámica de preguntas rápidas**: desmontaje de mitos y falsas creencias ("¿el banco puede pedirme un código?").

- **Enfoque preventivo**: recomendaciones claras y accionables para la vida diaria.

Recursos

- Casos reales impresos o proyectados
- Capturas de mensajes fraudulentos
- Pizarra digital
- Móviles del alumnado para análisis real
- Fichas de verificación (en anexo)
- Guía de seguridad básica (que puedo crear también)
- Herramientas:
    - Comprobación de URL
    - Búsqueda inversa de imágenes
    - Listas públicas de estafas activas (INCIBE)

Temporalización

3 sesiones de 1 hora.

Evaluación

Evaluación formativa, continua y flexible, concebida como un proceso integrado en el desarrollo de las sesiones y orientado a la obtención de **feedback inmediato**. Esta información permitirá ajustar de manera constante los contenidos, las explicaciones y el ritmo de trabajo a las necesidades reales del grupo.

La evaluación se apoyará en la **observación sistemática** de la participación y las intervenciones del alumnado, así como en **preguntas de comprobación y la resolución de casos prácticos en tiempo real**. Este enfoque facilitará la detección temprana de dificultades, la verificación de la comprensión y la asimilación progresiva de los contenidos, y la toma de decisiones pedagógicas para adaptar las actividades y garantizar un aprendizaje significativo.

Material consultado

Unidad Didáctica: **Prevención de fraudes y estafas digitales**

• **Bank of America (BofA Securities).** (s.f.). *Smishing: What Is It, How It Works & Tips on How to Prevent It*. Sección de Fraude y Ciberseguridad..

• **Keepnet Labs.** (2025). *10 Real-Life Smishing Examples to Strengthen Cybersecurity Awareness*. Blog de Ciberseguridad. Actualizado el 12 de septiembre de 2025..

• **SentinelOne.** (2025). *Phishing Vs. Smishing Vs. Vishing: 6 Critical Differences*.

Cybersecurity 101 / Threat Intelligence. Actualizado el 9 de julio de 2025..

• **Tertiary Education Commission (TEC).** (2024-2025). *Phishing Response Guidance: How to prepare and respond*. Guía de respuesta ante incidentes. Publicado en junio de 2024 y actualizado en octubre de 2025..

• **Trest, J. (VIPRE / Inspired eLearning).** (s.f.). *SMiShing Red Flags: How to Spot Fake Text Messages*. Blog de Inspired eLearning..

Anexos

Unidad Didáctica: **Prevención de fraudes y estafas digitales**

- Check list señales de alarma
- Ejercicio ¿Fraude o real?
- Guía de buenas prácticas en ciberseguridad