Programa de Jornadas Escolares

Promoción del uso seguro y responsable de Internet entre los menores

---

Protección ante virus y fraudes

Charla sensibilización alumnado. Guía de preparación

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

Cofinanciado por la Unión Europea
Mecanismo «Conectar Europa»

Licencia de contenidos

CONTENIDO

1. Introducción 4
1.1. Objetivos didácticos 4
1.2. Metodología 5
2. Fundamentos teóricos sobre Protección ante virus y fraudes 5
TRANSPARENCIA 3: Definición 5
TRANSPARENCIA 4: Virus informáticos. Introducción 6
TRANSPARENCIA 5-7: Tipos de virus 6
TRANSPARENCIA 8: Reflexiona. ¿Qué sabes sobre los virus? ¿Cómo te enfrentas a ellos? 7
TRANSPARENCIA 9: Virus. Mecanismos y vías de infección 7
TRANSPARENCIA 10: Algunos ejemplos: Ransomware 8
TRANSPARENCIA 11: Redes zombies 8
TRANSPARENCIA 12: Definición de Ingeniería social 9
TRANSPARENCIA 13: Definición de Fraude electrónico 10
TRANSPARENCIA 14: Ejemplos de Fraude electrónico. Phishing 10
TRANSPARENCIA 15: Ejemplos de Fraude electrónico. Phishing 11
TRANSPARENCIA 16: Ejemplos de Fraude electrónico. Robo de información personal 11
TRANSPARENCIA 17: Ejemplos de Fraude electrónico. Robo de información personal 12
TRANSPARENCIA 18: Ejemplos de Fraude electrónico. Suscripción a servicios 'Premium' 12
TRANSPARENCIA 19: Fraude electrónico. Sección de 'Avisos' de OSI 13
TRANSPARENCIA 20: Virus y Fraudes. Medidas de prevención 13
TRANSPARENCIA 21: Virus y Fraudes. Medidas de prevención 13
TRANSPARENCIA 22-24: Virus y fraudes. Recomendaciones genéricas 13
TRANSPARENCIA 25: Virus y Fraudes. Entidades de soporte y referencia 15
TRANSPARENCIA 26: Dónde localizar más información 15
TRANSPARENCIA 27: Despedida 17

1. Introducción

El contenido de esta guía servirá como orientación al profesorado a la hora de desarrollar en el aula una charla de sensibilización sobre la **protección ante virus y fraudes,** apoyándose en la presentación **Protección ante virus y fraudes, charla de sensibilización al alumnado.**

Estos materiales tratarán de orientar el aprendizaje de los menores en la adquisición de pautas básicas de mantenimiento, actualización y seguridad en el uso de dispositivos electrónicos. Les enseñaremos a identificar los distintos tipos de virus y fraudes que circulan por Internet y se les capacitará para que sepan cómo aplicar las medidas preventivas para hacer frente a éstos. Haremos hincapié en la necesidad de **aplicar el sentido común y apelar a la responsabilidad personal de cada uno de nosotros a la hora de mantener protegidos (y actualizada esa protección) todos los dispositivos que utilizamos para conectarnos a Internet**.

Para ello, explicaremos los conceptos de ingeniería social, fraude y virus informáticos, sus características, medios y métodos de actuación, así como los riesgos que ambos – virus y fraudes – suponen para el usuario, analizando éstos mediante ejemplos y casos reales. Abordaremos también los mecanismos y pautas de prevención y actuación frente a virus y fraudes electrónicos, así como las entidades de referencia que pueden darnos soporte y ayuda ante éstos.

El docente encargado de la sesión con el alumnado desarrollará una estrategia metodológica de reflexión-participación, invitando a éste en la reflexión y el debate. Al mismo tiempo promoverá el análisis crítico de los contenidos que se tratan en ella, animando así a la exposición de los puntos de vista, reflexiones y sobre todo al planteamiento de las dudas de los participantes.

1.1. Objetivos didácticos

Esta guía, que acompaña a la presentación de la charla de sensibilización sobre la **Protección ante virus y fraudes**, responde al objetivo de informar y capacitar al alumnado para actuar de manera proactiva frente a los riesgos asociados a virus y fraudes informáticos extendidos a través de Internet, ofreciéndole recomendaciones, pautas y herramientas para su prevención y/o actuación en caso de verse afectados por ellos.

Los contenidos propuestos permitirán al alumnado:

- Conocer qué son y cómo funcionan los virus informáticos y los fraudes informáticos para poder prevenirse ante ellos.
- Aplicar medidas y pautas para la protección de ordenadores y dispositivos móviles ante la amenaza de éstos.
- Reconocer los recursos y entidades de referencia que facilitan soporte y la resolución de incidencias relacionadas con fraudes y virus informáticos.

1.2. Metodología

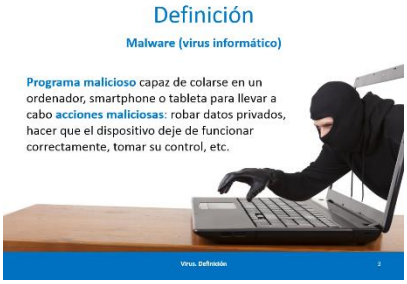
Durante la charla de sensibilización sobre **Protección ante virus y fraudes**, dirigido al alumnado, el docente realizará la exposición de contenido combinando el método **expositivo**[1] y el **interrogativo**[2].

Actuará también como facilitador de una sesión participativa con objeto de animar a compartir información, ideas, inquietudes, dudas, etc. Buscará en todo momento promover un entorno que favorezca la motivación del alumnado.

Esta metodología promoverá también la construcción del conocimiento a partir de la permanente reflexión del alumnado siempre orientada por aquél, asesorando y facilitando recursos e información. Procurará poner ejemplos vinculados a la realidad objetiva del perfil del alumnado destinatario. También utilizará un lenguaje acorde con el nivel de conocimientos previstos en el alumnado destinatario para facilitar la comprensión de los contenidos expuestos.

2. Fundamentos teóricos sobre Protección ante virus y fraudes

TRANSPARENCIA 3: Definición



A lo largo de las primeras transparencias de la presentación, el formador tratará de ofrecer al alumnado un breve resumen sobre **qué son los virus informáticos, cuál es su objetivo, sus métodos de infección y algunos ejemplos** (representados a través de fraudes, que la ingeniería social utiliza para infectar todo tipo de dispositivos y extender el daño y riesgo de los mismos), con el objeto de que esta información detallada, les ayude a comprender el riesgo que representan.

Entendiendo por "malware" o **virus informático**: "aquel programa malicioso capaz de colarse en un dispositivo con fines como robar datos privados, hacer que el dispositivo deje de funcionar correctamente o tomar su control, para llevar a cabo otras acciones maliciosas, el formador iniciará la charla de sensibilización al alumnado introduciendo esta definición.

Son muchos los ejemplos que los usuarios de dispositivos electrónicos encuentran cada día sobre alertas y casos reales de virus informáticos, que infectan éstos, causando la pérdida de información, el bloqueo del dispositivo, el robo de datos personales, etc.

La definición del concepto dará pie a la visualización de un vídeo sobre la temática, que de forma visual les acerque al concepto, permitiéndoles reflexionar sobre la información previa que tienen al respecto.

---

[1] ***METODOLOGÍA EXPOSITIVA:*** centrada en la transmisión de información, posibilita la transmisión de conocimientos ya estructurados, facilitando demostraciones de tipo verbal y la transmisión de información y conocimiento, de manera rápida y generalizada.

[2] **METODOLOGÍA INTERROGATIVA**: centrada en el proceso de aplicación del contenido a trabajar, basada en el proceso de comunicación que se establece entre docente y grupo, a través de **la pregunta**. Esta se convierte en elemento dinamizador, que desencadena el proceso de enseñanza aprendizaje.

TRANSPARENCIA 4: Virus informáticos. Introducción

Con la idea de acercar al alumnado a este concepto, proponemos la visualización del **vídeo 'Cómo proteger nuestros dispositivos de ataques de virus'** (1:01)**,** en el que se presenta una acción conjunta de Policía Nacional y empresas desarrolladoras de antivirus. Colaboran para concienciar a los usuarios sobre cómo prevenir todo tipo de virus, con los que los ciberdelincuentes nos pueden robar datos bancarios o información personal. Aunque en su titular el vídeo hace alusión a 'dispositivos móviles', la mayor parte de sus consejos y recomendaciones aplican a cualquiera de los dispositivos que utilizamos. En el vídeo se recogen recomendaciones y situaciones importantes sobre las que trabajaremos a lo largo de la sesión, como:

- Permanecer en alerta ante la presencia de **síntomas de un comportamiento anómalo** de nuestros dispositivos, como la aparición de anuncios que no esperas, la ralentización (enlentecimiento) del dispositivo, el cambio repentino de la "página de inicio" en nuestro navegador.
- La posibilidad de ser infectados o engañados a través de archivos adjuntos a un mensaje de correo, imágenes o enlaces enviados a través de SMS o mensajes en redes sociales, frente a los cuáles se pueden tomar medidas de prevención como:
  - Mantener nuestros dispositivos actualizados.
  - Navegar por páginas web seguras.
  - Tener precaución al facilitar datos personales y datos bancarios.
- La necesidad de estar atentos a las nuevas tendencias en fraudes y virus informáticos.
- No ceder a posibles chantajes y denunciando el caso ante la Policía.

Recomendaciones y consejos sobre los que el formador seguirá trabajando a lo largo de la charla de sensibilización.

TRANSPARENCIA 5-7: Tipos de virus

Para entender mejor el concepto y los distintos **tipos de software malicioso** existentes, el formador presentará a lo largo de las 3 transparencias siguientes, la **infografía publicada en la web de OSI** en la que se detallan, en cada caso, sus riesgos, métodos de infección y principales medidas a tomar para actuar frente a éste.

El formador mostrará simplemente la ficha descriptiva de algunos de ellos (Ransomware, Spyware y Keylogger), resumiendo la información básica y deteniéndose en algunos ejemplos, como el **Ransomware,** un tipo de malware que "secuestra" el ordenador, smartphone o los ficheros que contiene, pidiendo un "rescate" para permitirnos usar de nuevo el dispositivo o que podamos recuperar los ficheros, sobre el que detallaremos más información a continuación, al hablar de ejemplos como el **virus de la Policía** o el de la **Falsa factura electrónica de Endesa,** en las siguientes transparencias.

TRANSPARENCIA 8: Reflexiona. ¿Qué sabes sobre los virus? ¿Cómo te enfrentas a ellos?

El análisis del contenido recogido en la **infografía anterior** puede dar pie a establecer un breve debate en el aula**,** que nos permita sondear el grado de familiarización del alumnado con estos términos y con las consecuencias y riesgos que los virus informáticos representan:

- ¿Qué tipos de virus conocéis?
- ¿Os habéis visto amenazados en alguna ocasión por alguno de ellos?
- ¿Cuál ha sido el 'detonante', la acción que ha activado y extendido ese virus?
- ¿Cuáles creéis que son los métodos más habituales de infección?
- ¿Qué crees que se podría haber hecho para evitarlos?
- ¿Afectan sólo a ordenadores? ¿Habéis detectado algún virus en vuestros dispositivos móviles?
- ¿Tenéis instalado y configurado un antivirus en vuestro Smartphone o Tableta?

TRANSPARENCIA 9: Virus. Mecanismos y vías de infección

Tras el debate, el formador repasará con el alumnado los **principales mecanismos y vías de infección:**

- **Correo electrónico.** Es una de las principales vías de entrada de virus, a través de ficheros adjuntos peligrosos o enlaces a páginas web maliciosas.
- **Dispositivos de almacenamiento externo** (USB, discos duros, tarjeta de memoria), al copiar archivos infectados de un USB a nuestro equipo. En ocasiones, simplemente por el hecho de conectar un USB a nuestro equipo podemos resultar infectados, ya que algunos virus tienen la capacidad de auto-ejecutarse.
- **Descarga de ficheros desde Internet**. Al abrir o ejecutar ficheros (programas, contenido multimedia, documentos, etc.) pueden traer camuflado/escondido algún tipo de malware. Hay que tener especial precaución con lo que descargamos mediante programas de compartición de ficheros (P2P) u obtenemos en las distintas páginas web de descarga de contenidos, ya que pueden ser más propensos a contener virus.
- **Páginas web maliciosas,** preparadas para infectar al usuario que las visita aprovechando **problemas de seguridad de un navegador no actualizado** o de los complementos instalados: Java, Flash, etc. También a través de páginas web legítimas, que han sido manipuladas por ciberdelincuentes, **redirigiéndonos a webs maliciosas o fraudulentas**. Una forma de llegar a éstas podría ser, por ejemplo, haciendo clic en **enlaces acortados** en Twitter (u otras redes sociales) o en enlaces facilitados en correos electrónicos fraudulentos.

- **Redes sociales,** utilizadas para infectar los dispositivos debido a la gran cantidad de usuarios que las frecuentan y el alto grado de propagación que facilitan. Hay que ser precavidos frente a publicaciones con enlaces a páginas web con mensajes o titulares llamativos que resulten "raros" o poco fiables, solicitudes para instalar programas para poder acceder o visualizar un contenido, o aplicaciones que solicitan autorización no justificada para el acceso a nuestra **información personal**.
- **Vulnerabilidades y fallos de seguridad** en los sistemas operativos, navegadores, aplicaciones, plugins o programas instalados en el dispositivo. Son aprovechadas por los ciberdelincuentes para infectar los equipos, a veces, sin que el usuario tenga que realizar una acción que le haga consciente de ello. El ejemplo comentado en este caso por el formador puede ser el **Fallo de seguridad de Abobe Flash Player**. A través de este fallo de seguridad, un atacante puede tomar el control remoto de un dispositivo y realizar cualquier acción, como por ejemplo instalar malware**.** Para evitarlos, es importante mantener actualizados nuestros dispositivos.

A lo largo de las próximas transparencias, el formador presentará diferentes ejemplos de algunos de estos medios de infección.

TRANSPARENCIA 10: Algunos ejemplos: Ransomware

A partir de esta transparencia, el formador presentará ejemplos destacados y documentados de diferentes virus y vías de infección, presentando en qué medida han afectado a las personas infectadas por los mismos y sus consecuencias.

Comenzará con el ejemplo del **virus de la Policía**, un tipo de malware clasificado como **Ransomware** que "secuestra" el ordenador, Smartphone o los ficheros que contiene, pidiendo un "rescate" para permitirnos usar de nuevo el dispositivo y recuperar los ficheros.

En este caso el virus bloquea o toma el control del ordenador infectado, y haciéndose pasar generalmente por una organización, empresa o entidad conocida con cierta reputación y prestigio solicita un ingreso económico para desbloquearlo.

TRANSPARENCIA 11: Redes zombies

Las **redes zombies** son otro mecanismo utilizado por los ciberdelincuentes para propagar malware y llevar a cabo distinto tipo de acciones maliciosas: atacar a páginas y servicios web legítimos para que dejen de estar disponibles, capturar contraseñas, enviar correos spam de forma masiva, reenviar y difundir dicho malware a otros usuarios...

Un ordenador se convierte en un zombi cuando se ha infectado con un tipo de virus capaz de controlar tu ordenador de forma remota. Esto quiere decir que alguien, sin estar físicamente delante de tu ordenador, y con los conocimientos técnicos suficientes, puede manejarlo a su antojo. Pero eso no es todo, si tu ordenador es un zombi, estará formando parte de una red zombi de

ordenadores, que no es más que un gran número de ordenadores zombi, infectados con el mismo tipo de virus, que están controlados por una misma persona u organización criminal.

Para mostrar con más detalle al alumnado la forma de actuar y posibles herramientas de lucha frente a este tipo de malware, el formador propondrá la visualización del vídeo (1:16'): **Servicio Antibotnet OSI**.

Además, indicará al alumnado la referencia de la página de la **Oficina de Seguridad del Internatua (OSI)** , desde la que el alumnado puede acceder gratuitamente al **Servicio Antibotnet**, que chequea la conexión a Internet del usuario para comprobar si está afectada por una botnet.

TRANSPARENCIA 12: Definición de Ingeniería social

A través del concepto de **Ingeniería social**, entendido como el conjunto de técnicas que utilizan los ciberdelincuentes para materializar, a través de engaños y manipulaciones sus ataques, el formador introducirá ejemplos que representan algunos de los fraudes más extendidos y sobre los que ya se tiene suficiente información recogida como para poder asesorar sobre las medidas a utilizar para prevenir al alumnado frente a éstos.

Sensibilizará al alumnado sobre los **medios más utilizados** para poner en práctica la ingeniería social, entre los que se encuentran el **correo electrónico, las aplicaciones de mensajería instantánea así como las redes sociales.** La característica esencial es que se trate un tema o situación que resulte atractivo o llamativo para el usuario, por ejemplo:

- **Desastres naturales/accidentes.** Este tipo de situaciones son utilizadas por los ciberdelincuentes para aprovecharse de la sensibilidad y vulnerabilidad que estos hechos provocan en las personas para, por ejemplo, difundir páginas fraudulentas de donaciones.
- **Celebración de olimpiadas, mundiales, festivales, congresos**... son una buena excusa para poner en circulación falsos sorteos, entradas, descuentos que todo el mundo querrá obtener. Para ello, solo tienen que introducir sus datos personales ¡Quién puede resistirse a conseguir algo gratis!
- **Noticias sobre famosos**: escándalos, controversias o muertes captan la atención de los usuarios. Los ciberdelincuentes, que de esto saben mucho, utilizan toda su imaginación para conseguir que hagamos clic en vídeos o links que nos darán detalles escabrosos de cómo el personaje conocido... El problema es que detrás de esa supuesta información se suele esconder algún virus.
- **Situaciones que generan alarma:** multas, denuncias, notificaciones, problemas de seguridad. En este grupo estarían clasificados los ya más que conocidos phishing, en los que a través de un email, se le alerta al usuario de que debe realizar una acción de forma inmediata. Principal objetivo de esto: robar datos personales y bancarios de los usuarios e infectar dispositivos para obtener un beneficio económico. Ejemplos típicos, típicos:
  - **Problemas de seguridad en cuenta bancaria**
  - **Multas de Policía**
  - **Notificaciones de la Agencia Tributaria**
  - **Envío de facturas electrónicas**

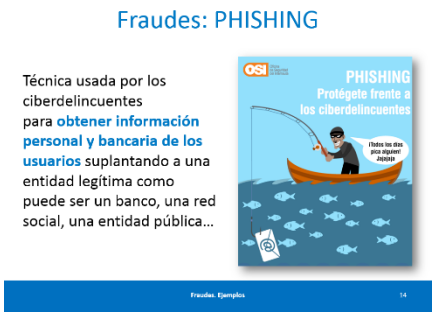
- **Lanzamiento de nuevos producto o servicios.** La presentación de un nuevo iPhone, actualizaciones en el sistema operativo de Bill Gates o cualquier otro producto o servicio de interés general, puede ayudar a propagar correos, mensajes, noticias, vídeos, imágenes con malware.
- **Situación política del país.** Difundir bulos sobre los políticos y sus partidos, es perfecto para recopilar direcciones de correo electrónico de usuarios así como otros posibles datos personales gracias al reenvío de los mensajes.

El formador podrá consultar más información sobre este concepto, a través del **enlace de la OSI: Conociendo lo que es la ingeniería social a fondo**.

TRANSPARENCIA 13: Definición de Fraude electrónico

Entendido como la actividad delictiva que se lleva a cabo a través de medios como Internet, ordenadores y dispositivos móviles, la definición del concepto de **fraude electrónico** dará pie al formador para presentar al alumnado ejemplos relativos a distintos tipos de fraude electrónico, propagados a través del correo electrónico, redes sociales (Facebook, Twitter, Instagram), juegos online y apps de mensajería (WhatsApp, Snapchat), como los enumerados el phising, el robo de datos personales a través de páginas web, fotografías y vídeos falsos, nuevas estafas a través de redes sociales o la suscripción a servicios Premium, que se analizan a continuación.

TRANSPARENCIA 14: Ejemplos de Fraude electrónico. Phishing

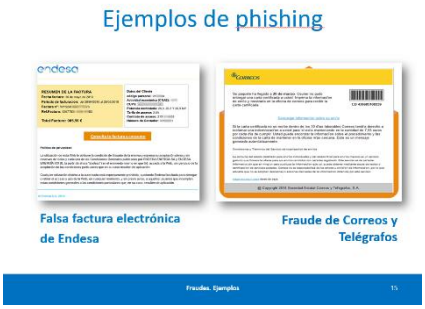


El **phishing** es una de las técnicas más usadas por los ciberdelincuentes, sobre la que puedes saber más a través de **este artículo**. Consiste básicamente en que los ciberdelincuentes, haciéndose pasar por una compañía o empresa conocida, intenta robar información privada de los usuarios como son, por ejemplo, las claves de acceso a los servicios online o datos bancarios.

Independientemente del medio utilizado, el objetivo final siempre es obtener información confidencial: nombres y apellidos, direcciones de correo electrónico, números de identificación personal, número de tarjeta de crédito, etc. Para obtener esta información, los ciberdelincuentes generalmente se valen de la ingeniería social y de un enlace que redirige al usuario a una página web fraudulenta que simula ser la web legítima, en algunas ocasiones pueden utilizar documentos adjuntos maliciosos para perpetrar el hurto de datos.

Para saber más sobre las estrategias que éstos usan para 'captar' a sus víctimas, veremos a continuación varios ejemplos.

TRANSPARENCIA 15: Ejemplos de Fraude electrónico. Phishing



- La **Falsa factura electrónica de Endesa**: ejemplo de una conocida campaña fraudulenta, de tipo phishing, que suplanta la identidad de la empresa Endesa y cuyo propósito es instalar malware (conocido como Ransomware) en el equipo de la víctima y cifrar los ficheros del equipo para impedir su acceso y posteriormente pedir un rescate (una cantidad de dinero) a cambio de la clave de descifrado que permita recuperar los datos.
- El **Fraude de Correos y Telégrafos:** una campaña masiva de correos fraudulentos que se propagó por email bajo el **falso aviso** de la imposibilidad de "Correos y Telégrafos" de entregar una carta certificada. En este caso, el objetivo del phishing fue infectar los equipos de los usuarios con el fin de poder controlarlos de forma remota para después llevar a cabo distintas actividades maliciosas.
- el **Virus de la Policía**, ya presentado anteriormente como ejemplo de 'Ransomware' y cuyo efecto provoca el bloqueo del ordenador del usuario, solicitando a éste un ingreso de dinero para desbloquearlo, con la excusa del pago de una multa.

Otros ejemplos reales de este tipo de fraude son:

- Phishing al **servicio de iCloud de Apple**
- Phishing a **PayPal**
- Phishing a **Dropbox**
- Phishing a **Iberia**

TRANSPARENCIA 16: Ejemplos de Fraude electrónico. Robo de información personal

El **robo de información** de forma engañosa (ingeniería social) o sin nuestro consentimiento (malware), es otra excusa para poner en circulación fraudes. El formador mostrará, a modo de ejemplo, dos referencias reales de fraude que intentan obtener información personal del usuario:

- **Falsa página de Mercadona**. El robo de datos se realizaba a través de una preparada específicamente para robar datos personales a los usuarios que introdujesen su información personal en ella bajo la excusa de que dichos datos eran necesarios para obtener un supuesto premio.
- **Webcam controlada desde otro ordenador**: a consecuencia de un virus, que toma el control del ordenador accediendo a la información captada desde ella sin nuestro consentimiento. El formador puede utilizar como referencia, para preparar el resumen sobre la noticia a presentar al alumnado, el **siguiente artículo**.

TRANSPARENCIA 17: Ejemplos de Fraude electrónico. Robo de información personal

El **robo de información personal** es también el fin buscado por los casos de fraude como los siguientes:

- El **Falso vídeo viral en Facebook:** se trata de un vídeo que se propaga a través de los muros de los usuarios de Facebook, infectando el dispositivo afectado con un virus de tipo "troyano". Éste permite el robo de información y la instalación de una extensión en el navegador, para publicar en Facebook de forma automática y seguir propagando el contenido entre más usuarios.

- O las **nuevas estafas en redes sociales**, recogidas en este **vídeo**, en el que la Policía Nacional alerta de nuevos fraudes, estafas, timos y bulos que se propagan, con especial rapidez, a través de redes sociales y aplicaciones de comunicación, como *WhatsApp*, y que pretenden lograr beneficio económico al margen de la ley. El formador, podrá visualizar el vídeo junto con el alumnado como herramienta de apoyo a esta breve introducción sobre las últimas tendencias en la infección de virus y fraudes electrónicos.

TRANSPARENCIA 18: Ejemplos de Fraude electrónico. Suscripción a servicios 'Premium'

Por último, en cuanto a los ejemplos de Fraude electrónico que el formador utilizará para explicar con más detalle este contenido, hablará de 2 extendidos casos reales, como:

- **Videollamadas de WhatsApp.** Los mensajes de esta nueva campaña ofrecen a los usuarios activar las videollamadas para el sistema de mensajería instantánea WhatsApp (a día de hoy esta funcionalidad no la ofrece la app). La promoción fraudulenta se propaga a través de redes sociales en teléfonos móviles, con mensajes que contienen un enlace que dirige a una web, que trata de suplantar la identidad de WhatsApp, desde la que le anima a "Descargar Videollamadas", remitiéndole a una web desde la que se intentará subscribir al usuario a un servicio SMS Premium.

- **Vales descuento de Lidl** (y de otras muchas empresas similares): nueva campaña de correo electrónico, que ofrece supuestos vales descuento de la cadena de supermercados Lidl. El objetivo es obtener datos personales y suscribir a un servicio de recepción de ofertas con un coste de 24.9€ mensuales.

TRANSPARENCIA 19: Fraude electrónico. Sección de 'Avisos' de OSI

Para finalizar esta serie de ejemplos y dada la proliferación de los mismos, que mañana pueden ser sustituidos por otros con el mismo fin pero distinta forma (haciendo más fácil que podamos ser engañados), el formador presentará la **sección de AVISOS de la OSI**, que de forma permanente nos mantiene informados sobre nuevo software malicioso y fraudes informáticos, facilitando consejos y recomendaciones, tanto para prevenir la infección como para atajarla, una vez infectado nuestro sistema o dispositivo.

TRANSPARENCIA 20: Virus y Fraudes. Medidas de prevención

A través del vídeo: **'Usa un escudo e impide el avance de los virus'**, el formador introducirá algunas de las características y ventajas que ofrece utilizar medidas básicas de protección, como la instalación y actualización adecuada de un antivirus, antispyware y antispam.

TRANSPARENCIA 21: Virus y Fraudes. Medidas de prevención

El formador complementará la información sobre medidas básicas de prevención y protección, con una visita guiada a la **página de OSI**, donde el alumnado puede acceder a información sobre **herramientas gratuitas para proteger los dispositivos**, haciendo más segura su navegación por Internet.

TRANSPARENCIA 22-24: Virus y fraudes. Recomendaciones genéricas

Como hemos visto, tanto en el vídeo como en la web de OSI, los consejos y recomendaciones genéricas, para prevenir y protegernos ante virus y fraudes, aplican el **sentido común**, fomentando el uso responsable de la tecnología a través de sencillas pautas entre las que el formador destacará:

Recomendaciones genéricas

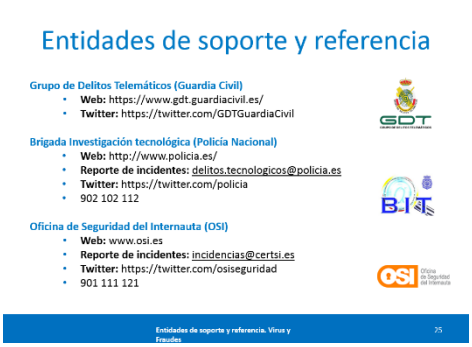
- Llevar a cabo instalaciones seguras, que no comprometan nuestros dispositivos, a través de sitios oficiales de descarga. Descargar programas y aplicaciones sólo desde páginas oficiales.
- Instalación y correcta actualización de programas antivirus, tanto en ordenadores como en tabletas y smartphones, descargándolos desde la web oficial del fabricante.
- Instalación de cortafuegos (integrado por el sistema operativo) que bloquea el acceso no autorizado a nuestros dispositivos, permitiendo las comunicaciones autorizadas.
- Actualizaciones: sistema operativo, navegadores, plugins y programas.
- Realización de copias de seguridad: para impedir que la acción de algún virus nos haga perderla.
- Cifrado de la información como medida de protección de ésta, para que solo pueda acceder a ésta las personas autorizadas que dispongan de la clave de descifrado.
- Gestionar el acceso a dispositivos compartidos con cuentas de usuario limitadas, que permiten la instalación de aplicaciones o modificaciones en la configuración, sólo a través del perfil “administrador”.
- Llevar a cabo una buena gestión de contraseñas (secretas, robustas y no repetidas).
- Cambiar periódicamente la contraseña de la clave wifi del router.
- Tomar precauciones al utilizar dispositivos públicos y conectarse a redes wifi públicas.
- Tener precaución con los enlaces cortos (tipo bit.ly; goo.gl;) antes de acceder a ellos – sobre todo desde pantallas móviles, Twitter y otras redes sociales, donde se usan para ahorrar caracteres -, que pueden dirigirnos a páginas web fraudulentas, que contienen malware.
- Evitar la navegación por páginas web sospechosas (programas y juegos gratuitos, fotos de famosos, etc.).
- Configurar adecuadamente los ajustes de privacidad en las redes sociales.
- Evitar introducir en nuestros dispositivos, medios de almacenamiento extraíbles (USB) de dudosa procedencia, que pueden ser una puerta de entrada para los virus.

Todas ellas recogidas y presentadas por el formador, a lo largo de estas 3 transparencias.

TRANSPARENCIA 25: Virus y Fraudes. Entidades de soporte y referencia

Comprender que la tecnología evoluciona constantemente y con ella, la elaboración de nuevas formas de infectar dispositivos electrónicos y engañar a sus usuarios, nos obliga a permanecer en alerta e informados a través de entidades y servicios de referencia.

Además, debemos saber que ante la sospecha de estar siendo víctima de software malicioso o fraude electrónico, podemos contactar con **entidades de soporte y ayuda.**



Grupo de Delitos Telemáticos (Guardia Civil):

- Web sección **Colabora**
- **Formulario web de denuncia**
- Canal **Twitter**

Brigada Investigación tecnológica (Policía Nacional):

- **Web**
- **delitos.tecnologicos@policia.es**
- 902.102.112
- Canal **Twitter**

Oficina de Seguridad del Internauta (OSI):

- **Web OSI**
- Formulario alta incidentes: **incidencias@certsi.es**
- 901.111.121
- Canal **Twitter**

TRANSPARENCIA 26: Dónde localizar más información

Recomendaremos dos páginas imprescindibles para saber más y estar perfectamente actualizado:

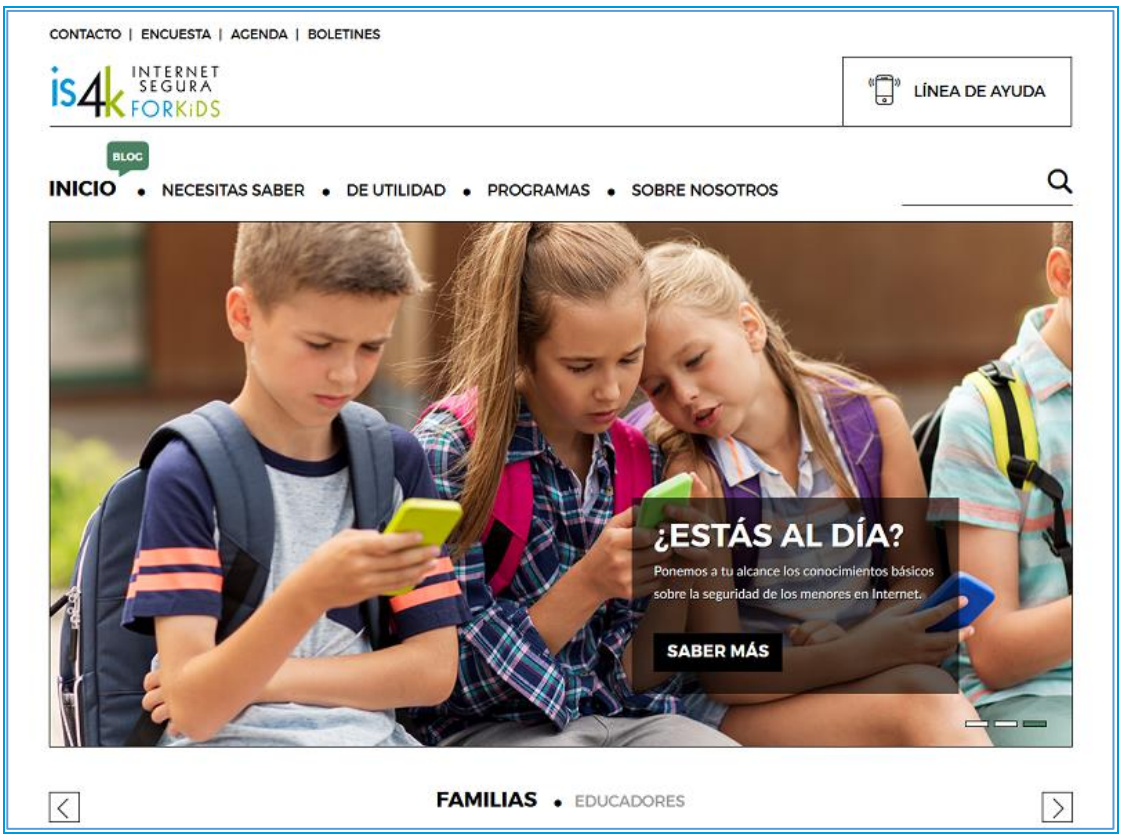
La página de OSI Oficina de Seguridad del Internauta **https://www.osi.es** Destacar las siguientes secciones con información de interés:

- **Ponte al día (sección de actualidad):**
  - **Avisos de seguridad**
  - **Blog**
  - **Historias reales**
- **¿Qué deberías saber?**
  - Sobre tus dispositivos

- Sobre tu información
- Sobre el fraude
- Sobre tus conexiones
- Sobre tu actividad online

Y la página Internet Segura for Kids **http://www.is4k.es** con:

- La información que "**necesitas saber**" sobre privacidad, ciberacoso escolar, sexting, contenido inapropiado, uso y configuración segura, mediación parental.
- Artículos de interés y actualidad en el "**blog**".
- Guías, juegos, herramientas de control parental y otros recursos "**de utilidad**".
- Información de "**programas**" de sensibilización para un uso seguro y responsable de Internet por los menores.
- Una "**línea de ayuda**" con una serie de preguntas frecuentes y un contacto para resolver dudas.



TRANSPARENCIA 27: Despedida

Siempre podéis poneros en contacto con nosotros a través de la web:

- **https://www.is4k.es**

Internet Segura for Kids (IS4K), es el nuevo Centro de Seguridad en Internet para menores en España. Allí podéis encontrar información, guías, juegos y otros recursos de utilidad sobre los principales riesgos de Internet, cómo prevenirlos y afrontarlos. Además disponéis de una línea de ayuda con una serie de preguntas frecuentes y un contacto para resolver vuestras dudas.

Recordad que podéis seguir nuestros perfiles públicos de redes sociales:

- **Facebook**, buscando “Internet Segura for Kids”
- **Twitter**, usuario @is4k