

Taller formativo

Identificando riesgos en tiendas online, correos, SMS y llamadas fraudulentas

LICENCIA DE CONTENIDOS

La presente publicación pertenece a Instituto Nacional de Ciberseguridad (INCIBE) y está bajo licencia Reconocimiento-No Comercial-CompartirIgual 4.0 Internacional de Creative Commons. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- **Reconocimiento.** El contenido de esta publicación se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa a INCIBE y su sitio web: <https://www.incibe.es>. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- **Uso No Comercial.** El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.
- **Compartir Igual.** Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuirla bajo esta misma licencia.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.

Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE como titular de los derechos de autor.

Texto completo de la licencia:

https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es_ES



ÍNDICE

1. Objeto del documento.....	5
2. Organización y estructura	6
3. Objetivo	7
4. Metodología y recursos	8
5. Contenidos.....	9
5.1. Diapositiva 1. Presentación del taller	9
5.2. Diapositiva 2. Índice	9
5.3. Diapositiva 3. Introducción	9
5.4. Diapositiva 4. Tiendas legítimas vs tiendas ilegales	10
5.5. Diapositiva 5. Tiendas legítimas vs tiendas ilegales. Identificar la dirección web	10
5.6. Diapositiva 6. Tiendas legítimas vs tiendas ilegales. Buscar información sobre la tienda	11
5.7. Diapositiva 7. Tiendas legítimas vs tiendas ilegales. Revisar el aspecto visual de la tienda	12
5.8. Diapositiva 8. Tiendas legítimas vs tiendas ilegales. Comprobar los precios	12
5.9. Diapositiva 9. Tiendas legítimas vs tiendas ilegales. Revisar las condiciones de envío y devolución	13
5.10. Diapositiva 10. Tiendas legítimas vs tiendas ilegales. Comprobar las formas de pago	13
5.11. Diapositiva 11. Actividad 1	14
5.12. Diapositiva 12. Ejemplo tienda ilegal.....	14
5.13. Diapositiva 13. Identificando correos maliciosos.....	15
5.14. Diapositiva 14. Identificando correos maliciosos. Cómo reconocer un correo malicioso de <i>phishing</i>	15
5.15. Diapositiva 15. Identificando correos maliciosos. VIDEO.....	17
5.16. Diapositiva 16. Actividad 2	17
5.17. Diapositiva 17. Identificando correos maliciosos. Ejemplos de correos de <i>phishing</i>	17
5.18. Diapositiva 18. Identificando correos maliciosos. <i>Phishing</i> bancario	17
5.19. Diapositiva 19. Identificando correos maliciosos. <i>Phishing</i> a entidad pública.....	18
5.20. Diapositiva 20. Identificando correos maliciosos. <i>Phishing</i> a entidad privada	18
5.21. Diapositiva 21. Identificando correos maliciosos. Otros <i>phishing</i>	18
5.22. Diapositiva 22. Otro tipo de correos electrónicos fraudulentos	18
5.23. Diapositiva 23. Identificando correos maliciosos. Ejemplos de correos fraudulentos: Timo Nigeriano (lotería, viuda, enfermo terminal)	19
5.24. Diapositiva 24. Identificando correos maliciosos. Ejemplos de correos fraudulentos: Falsas ofertas de empleo	19
5.25. Diapositiva 25. Identificando correos maliciosos. Ejemplos de correos fraudulentos: Falsos prestamistas de dinero.....	19
5.26. Diapositiva 26. Identificando correos maliciosos. Ejemplos de correos fraudulentos: Novias rusas.....	20
5.27. Diapositiva 27. Identificando correos maliciosos. Ejemplos de correos fraudulentos: Correos de sextorsión	20

5.28. Diapositiva 28. Identificando correos maliciosos. Ejemplos de correos fraudulentos: Recomendaciones y consejos.....	21
5.29. Diapositiva 29. Identificando correos maliciosos. Ejemplos de correos fraudulentos: Recomendaciones y consejos.....	21
5.30. Diapositiva 30. Otras técnicas de engaño.....	22
5.31. Diapositiva 31. Ejemplos reales de <i>smishing</i>	22
5.32. Diapositiva 32. Ejemplos reales de <i>vishing</i>	23
5.33. Diapositiva 32. Cómo reportar fraudes.....	23
5.34. Diapositiva 33. Actividad 3	23
5.35. Diapositiva 34. En INCIBE te ayudamos.....	24
5.36. Diapositiva 35. Cuestionario de evaluación 1	24
5.37. Diapositiva 36. Cuestionario de evaluación 2	24
5.38. Diapositiva 37. Cuestionario de evaluación 3	24
5.39. Diapositiva 38. Cuestionario de evaluación 4	25
5.40. Diapositiva 39. Cuestionario de evaluación 5	25
5.41. Diapositiva 40. Cuestionario de evaluación 6	25
5.42. Diapositiva 41. Cuestionario de evaluación 7	25
5.43. Diapositiva 42. Cuestionario de evaluación 8	25
5.44. Diapositiva 43. Cuestionario de evaluación 9	25
5.45. Diapositiva 44. Cuestionario de evaluación 10.....	25
5.46. Diapositiva 45. Final del taller	26
6. Recursos de evaluación	27
6.1. Cuestionario de evaluación.....	28
ANEXO	30
Recursos para ampliar	30

1. OBJETO DEL DOCUMENTO

El presente documento constituye una herramienta didáctica que servirá de apoyo al docente para la planificación del **taller formativo “Identificando riesgos en tiendas online, correos, SMS y llamadas fraudulentas”**.

Esta herramienta supone un **instrumento específico de planificación, desarrollo y evaluación** de cada una de las áreas de las que se compone la acción formativa, y requiere de la labor docente para concretar los distintos elementos curriculares adaptándolos a las características del alumnado.

A lo largo de la guía docente, se profundizará en los **objetivos generales y específicos de la acción formativa, sus contenidos, criterios de evaluación y aquellos materiales y recursos adicionales** que se requieran para la impartición de las competencias recogidas en el taller.

2. ORGANIZACIÓN Y ESTRUCTURA

La estructura del taller estará compuesta por 5 temas que comprenderán los contenidos teóricos y actividades para el trabajo individual de cada alumno.

La estructura completa del taller es la siguiente:

1. Tiendas online legítimas vs tiendas ilegales.

- Identificar la dirección web.
- Buscar información sobre la tienda.
- Revisar el aspecto visual de la tienda.
- Comprobar los precios.
- Revisar las condiciones de envío y devolución.
- Comprobar las formas de pago.
- Comprobar las pasarelas y entidades de pago.

2. Identificando correos maliciosos:

- Como reconocer un correo malicioso o *phishing*
- Ejemplos de correos de *phishing*
 - *Phishing* bancario
 - *Phishing* de tarjetas de crédito
 - *Phishing* de cuentas de correo y redes sociales

3. Otros medios usados para propagar *phishing*

- Ejemplos de correos fraudulentos
 - Timo Nigeriano (lotería, viuda, enfermo terminal)
 - Falsas ofertas de empleo
 - Falsos prestamistas de dinero
 - Novias rusas
 - Correos de *sextorsión*
 - Recomendaciones y consejos
- Recomendaciones y consejos

4. Otras técnicas de engaño

- Ejemplos reales de *smishing*
- Ejemplos reales de *vishing*

5. Cómo reportar fraudes

3. OBJETIVO

Este taller tiene como objetivo principal **proporcionar a los alumnos las competencias necesarias para identificar los principales riesgos y amenazas al navegar por Internet**. Dado el enfoque teórico-práctico, así como el nivel de profundidad de sus contenidos, el taller va dirigido a un colectivo de usuarios con conocimientos muy básicos sobre tecnología y seguridad.

A lo largo del taller, se ofrecerá a los alumnos recursos de ampliación en forma de enlaces de la OSI, con el fin de expandir sus competencias y satisfacer su curiosidad. Del mismo modo, servirán al docente para enriquecer los contenidos del taller.

4. METODOLOGÍA Y RECURSOS

La metodología empleada en el desarrollo de este taller es de **carácter teórico-práctico, visual y buscando la participación activa del alumnado** durante la impartición del taller:

- **Teórico-práctica:** Los contenidos teóricos vendrán acompañados en todo momento de ejemplos reales que aterricen la teoría. A través de casos reales y actividades, el alumnado pondrá en práctica la información transmitida a través del taller.
- **Visual:** Las imágenes técnicas y decorativas abundarán a lo largo de todo el taller. Además, para dinamizar aún más los talleres, se incluirán recursos audiovisuales relacionados con el contenido (al menos 1 vídeo por taller).
- **Participación activa:** El alumnado tendrá un papel fundamental en los talleres, pues no se limitarán a escuchar. Los contenidos están preparados para que se pongan en práctica desde el comienzo del taller en cada uno de los equipos del alumnado.
 - Además, se busca enriquecer la experiencia formativa a través de las dudas y comentarios que se expongan durante su desarrollo.

El taller cuenta con diferentes **actividades y recursos** al servicio del docente para la impartición:

- **Presentación en Power-Point.** Se trata de una presentación con comentarios en texto para apoyar al docente, y los contenidos a compartir con el alumnado.
- **Actividades.** Se trata de pequeñas actividades que permiten al alumnado poner en práctica los conocimientos recién adquiridos, y que acompañan a los apartados principales.
- **Vídeos y enlaces para ampliar.** Servirán para afianzar los contenidos desarrollados mediante ejemplos y contenidos para ampliar, con los que enriquecer la acción formativa.
- **Cuestionario de evaluación.** Cuestionario final del taller formado por 15 ítems con opción múltiple con el que realizar la evaluación final de los alumnos.

5. CONTENIDOS

A continuación, se muestra el contenido del taller ordenado en diapositivas para facilitar la tarea al docente.

5.1. Diapositiva 1. Presentación del taller

Presentación del taller “Identificando riesgos en tiendas online, correos, SMS y llamadas fraudulentas”. Debe mencionarse la labor de INCIBE y el teléfono de ayuda 017.

5.2. Diapositiva 2. Índice

Presentación del índice de contenidos del taller:

1. Tiendas online legítimas vs tiendas ilegales.
 - Identificar la dirección web.
 - Buscar información sobre la tienda.
 - Revisar el aspecto visual de la tienda.
 - Comprobar los precios.
 - Revisar las condiciones de envío y devolución.
 - Comprobar las formas de pago.
 - Comprobar las pasarelas y entidades de pago.
2. Identificando correos maliciosos:
 - Como reconocer un correo malicioso o *phishing*
 - Ejemplos de correos de *phishing*
 - *Phishing* bancario
 - *Phishing* de tarjetas de crédito
 - *Phishing* de cuentas de correo y redes sociales
3. Otros medios usados para propagar *phishing*
 - Ejemplos de correos fraudulentos
 - Timo Nigeriano (lotería, viuda, enfermo terminal)
 - Falsas ofertas de empleo
 - Falsos prestamistas de dinero
 - Novias rusas
 - Correos de sextorsión
 - Recomendaciones y consejos
 - Recomendaciones y consejos
4. Otras técnicas de engaño
 - Ejemplos reales de *smishing*
 - Ejemplos reales de *vishing*
5. Cómo reportar fraudes

5.3. Diapositiva 3. Introducción

Navegar por Internet nos permite tener al alcance de un clic una enorme variedad de servicios y comodidades que no estaban disponibles hace tan solo unos años.

Sin embargo, no hay duda de que **todas estas ventajas vienen acompañadas de todo tipo de riesgos y amenazas** en el momento que conectamos nuestros dispositivos a la

Red e ingresamos nuestros datos personales para hacer uso de muchos de los servicios de Internet.

Por suerte, podemos **aprender a detectarlas, prestando atención a los detalles y así, evitar estas amenazas.**

5.4. Diapositiva 4. Tiendas legítimas vs tiendas ilegales

Día a día, utilizamos Internet para un sin fin de gestiones, siendo una de las más populares, las compras online. Aunque las plataformas de [compra online](#) nos ofrecen numerosos descuentos, promociones y una mayor facilidad a la hora de realizar las transacciones, siempre existe la posibilidad de que se utilicen de forma fraudulenta.

Algunos de los principales **riesgos** son:

- **Sitios web falsos.** Plataformas falsas que copian el estilo de otras tiendas oficiales con el objetivo de atraernos a ellas para compartir nuestra información personal y/o caigamos en estafas con las que perder nuestro dinero.
- **Perfiles falsos de vendedor.** Los ciberdelincuentes también pueden registrarse en estas plataformas con el objetivo de vender productos falsos o que nunca llegarán a su destino.
- **Métodos de pago poco fiables.** Existen métodos más seguros que otros, y aquellas ofertas más llamativas pueden esconder formas de pago poco fiables.

A continuación, vamos a aprender a detectar aquellas **tiendas ilegítimas/ilegales**, donde es más probable que podamos acabar siendo estafados.

5.5. Diapositiva 5. Tiendas legítimas vs tiendas ilegales. Identificar la dirección web

Desde la propia *URL* podemos obtener información muy útil con la que identificar un sitio seguro, donde nuestras transacciones e intercambios de información van a estar protegidos, de uno que no. Para ello, deberemos fijarnos en lo siguiente:

- **HTTP / HTTPS:** Lo primero en lo que deberemos fijarnos es en el tipo de protocolo que aparece al comienzo de la *url*.

A diferencia del **http**, el **https** utiliza el **protocolo de cifrado SSL/TLS** que garantiza que la comunicación no se podrá leer ni manipular y que la información personal no caerá en las manos equivocadas, como nuestras credenciales, datos personales y/o bancarios.

- **Certificado de seguridad:** Podemos comprobar que una web tiene certificado de seguridad si dispone de un icono de un candado a la izquierda de la *URL*. Se trata de un certificado expedido por una empresa o autoridad de certificación, que certifica que la información intercambiada va a estar cifrada y que la web pertenece a quien dice ser, es decir, certifica su identidad y legitimidad.

Al hacer clic en el candado podremos acceder a los datos del certificado, como cuando se ha expedido, quién ha sido la empresa certificadora, la fecha de caducidad, etc.

- **Sello de confianza:** para [generar más confianza](#), las webs pueden ofrecer a los consumidores un sello en su página que acredita que sus procesos han sido validados y revisados por un tercero frente a un conjunto de buenas prácticas.

Normalmente, los sellos de confianza suelen colocarse en el pie de la página junto con otras cláusulas como el aviso legal, la política de cookies, las condiciones de contratación y los términos y condiciones.

En otras ocasiones, las páginas mencionan en su aviso legal que disponen de dicho certificado y enlazan al mismo.

No obstante, cuidado con todas las evidencias anteriores, que una web disponga de certificado digital o protocolo HTTPS no implica necesariamente que sea fiable o legítima. Hoy en día es bastante habitual encontrar sitios web fraudulentos con certificados, precisamente para dotar de mayor credibilidad al fraude. Por este motivo, habrá que seguir analizando más aspectos de la web.

5.6. Diapositiva 6. Tiendas legítimas vs tiendas ilegales. Buscar información sobre la tienda

Cuando compramos por Internet, puede resultar de utilidad saber qué opinan otros usuarios sobre la tienda ya que en muchas ocasiones nos ayudan a saber si estamos ante una web legítima o un fraude. Para valorar la [reputación de una tienda](#), podemos apoyarnos en:

1. **Valoraciones de los usuarios:** en todas las tiendas online existe un sistema de valoraciones donde los usuarios pueden evaluar la experiencia y se nos indica la puntuación que los compradores han obtenido en sus intercambios. Debemos fijarnos en las notas que les han dado los usuarios y los comentarios que han hecho, ya que será una pista de si la tienda o vendedor puede ser más o menos fiable.
2. **Búsqueda en Internet:** esta opción es tan simple como buscar información sobre la tienda en nuestro buscador favorito. Podremos obtener información interesante, como alguna plataforma de denuncia o foro donde se reflejen posibles casos de fraude.
3. **Búsqueda de información legal.** Si la empresa está creada en España, ha de cumplir una serie de requisitos legales para vender. Esos requisitos están recogidos en varias leyes, como la Ley de Ordenación del Comercio Minorista, Ley de Servicios de la Sociedad de la Información LSSI, Ley de Protección de Datos LOPD, Ley de Condiciones de Uso, Ley de Consumidores y Comercio Electrónico, etc.

Además, es obligatorio que el comercio proporcione los siguientes datos:

1. Titular de la web (persona o empresa).
2. NIF/CIF.
3. Domicilio social.
4. Email de contacto.
5. Condiciones de venta, devoluciones, reclamaciones.
6. Propiedad intelectual de uso de cookies.

7. Inscripción del fichero de datos en la AGPD

Todo esto debería estar redactado de una forma correcta y coherente en una tienda online. En las webs fraudulentas se omite esta información de forma muy deficiente y, aunque la información aparezca, no es coherente y suele estar copiada de otras tiendas online.

5.7. Diapositiva 7. Tiendas legítimas vs tiendas ilegales. Revisar el aspecto visual de la tienda

Un vistazo al diseño y elementos gráficos o visuales de la web nos ayudará a identificar si se trata de una tienda falsa:

- **Homogeneidad en el diseño:** si se utilizan varios tipos de tipografía, imágenes de tamaños diferentes o existen errores en el diseño es muy probable que se trate de una web falsa.
- **Legitimidad de las imágenes:** si hacemos una búsqueda en Google imágenes de las imágenes o fotografías utilizadas por la web, podremos comprobar si se trata de un plagio y reutilizan imágenes de otra web o sustraídas de un banco de imágenes de Internet.
- **Calidad de las imágenes:** con las prisas, los ciberdelincuentes no suelen editar y asegurar la buena calidad de las imágenes utilizadas en las webs falsas. Aunque pueden copiar el estilo de una web legítima, se les escapan detalles como logotipos de otras webs, marcas o productos ajenos a esa tienda online, etc.
- **Secciones de la página:** las webs legítimas suelen contar con secciones correctamente detalladas como: quiénes somos, aviso legal, política de privacidad, contacto, etc. Una web fraudulenta, aun incluyendo los anteriores apartados, los tendrá incompletos, mal redactados o con traducciones a medias.
- **Información de contacto:** lo normal sería que, si se ofrece una dirección de correo electrónico, esta coincidiera con el dominio de la web. Es decir, un correo electrónico para una tienda llamada Ropa de marca, debería incluir el dominio @ropademarca.

5.8. Diapositiva 8. Tiendas legítimas vs tiendas ilegales. Comprobar los precios

Todos los productos en venta tienen un precio determinado en el mercado. Si en una tienda física vemos un producto muy rebajado, podemos entrar y constatar calidad, pero en una tienda online eso no es posible.

Por lo tanto, **¿qué aspectos referentes al precio nos deben hacer sospechar?**

- **Precios anormalmente bajos:** que un artículo tenga un precio excesivamente bajo en comparación con el mismo producto en otra tienda online, debe hacernos sospechar. Es una estrategia muy utilizada para engañar a los usuarios.

- **Todos los productos al mismo precio:** normalmente distintos productos tienen distintos precios, si se hacen descuentos, aunque estos sean importantes, los precios quedan rebajados, pero no iguales.

Otra táctica muy habitual de los ciberdelincuentes es crear tiendas online suplantando a marcas muy conocidas cuyos productos estén muy rebajados y todos al mismo precio. Ejemplos: páginas de zapatillas, gafas de sol, cazadoras de cuero, vaqueros, etc.

- **Otro tipo de gastos:** es importante que verifiquemos los gastos “añadidos”, y que no son los gastos asociados al IVA ni al envío del paquete sino a conceptos como: seguros, gastos de manipulación, costes de aduanas y/o bajo cualquier otra excusa que, por supuesto, no están detallados durante el proceso de compra.

5.9. Diapositiva 9. Tiendas legítimas vs tiendas ilegales. Revisar las condiciones de envío y devolución

La tienda debe informar de forma clara cuál es su política de envío y devolución, además de indicar en caso de querer efectuar una devolución quién será el encargado de asumir los costes del envío.

- **En caso de que la web sea española,** debemos saber que los consumidores tenemos el derecho al desistimiento de una transacción online. Es decir, disponemos de 14 días en los que disponemos de la opción de devolver el producto.
- **Si hacemos una compra online a una tienda fuera de España,** debemos tener muy claro que estas políticas pueden cambiar. Por lo tanto, es muy importante que tengamos claras cuáles son y revisar su apartado de condiciones para el envío y devolución, así como otros aspectos legales que puedan afectarnos.

Esta información suele venir junto a los avisos legales, datos de la empresa o los métodos de pago.

5.10. Diapositiva 10. Tiendas legítimas vs tiendas ilegales. Comprobar las formas de pago

Este punto es fundamental, ya que en toda transacción online estamos enviando información bancaria y si se lleva a cabo en una tienda online fraudulenta, podríamos acabar siendo víctimas de un robo. Para prevenirlo, es recomendable comprobar que la tienda cuente con varias opciones o formas de pago.

El hecho de que una tienda facilite pagar por medio de tarjeta de crédito, un intermediario como por ejemplo *PayPal* o a contra reembolso es un síntoma de que la tienda es legítima.

- **Tarjeta de crédito o débito.** Usar las tarjetas para el pago es cómodo, rápido y puede ser muy seguro. Sin embargo, no es el mejor método si tenemos alguna duda sobre la fiabilidad de la web, ya que estamos proporcionando toda la información necesaria para realizar compras.

- **Tarjetas prepago.** Permiten realizar pagos sin que estos estén asociados a alguna cuenta bancaria. Nosotros decidimos el dinero que vamos a ingresar en la tarjeta y, una vez se ha agotado el dinero, podemos recargarla de nuevo.
- **Transferencia bancaria.** En este tipo de pago se envía el dinero desde nuestra cuenta bancaria directamente a la del vendedor. Aunque previene del robo de datos personales por la web, si la cuenta del vendedor está en el extranjero, o si se trata de un vendedor fraudulento, podemos acabar siendo víctimas de un fraude.
- **Plataformas de pago.** Estos son servicios independientes que actúan como intermediarios entre nosotros y el vendedor. La más famosa es *PayPal* y su principal ventaja es que no compartimos los datos de nuestra tarjeta de crédito, además estas entidades regulan los cobros y pagos, actuando como mediadores en errores y posibles fraudes.
- **Transferencia instantánea.** Servicios como *Western Union* o *MoneyGram* están diseñados para enviar dinero, no para gestionar compras y una vez se haya enviado el dinero, la cancelación o el reembolso no son posibles.
- **Pago contra reembolso.** Esta opción asegura que no se hace el pago hasta que se recibe y verifica el artículo comprado. El inconveniente es que no está siempre aceptada por los vendedores y puede implicar un coste adicional.
- **Pago con el teléfono móvil.** Este sistema utiliza la tecnología [NFC](#), que nos permite utilizar nuestro dispositivo como si de una tarjeta de crédito se tratara. Más información en: [Pagos con el móvil. Lo que necesitas saber](#) y [Pagar a través del móvil. ¿Cómo lo hago?](#)

5.11. Diapositiva 11. Actividad 1

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3 y 5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

Actividad 1:

Seguro que has comprado alguna vez por Internet. ¿Recuerdas cuál fue el último sitio donde compraste? Accede de nuevo y comprueba que todos los elementos que se han descrito en el contenido coinciden con la plataforma de compra online que utilizaste. ¡Esperemos que no te lleses una mala sorpresa!

5.12. Diapositiva 12. Ejemplo tienda ilegal

Diapositiva que recoge capturas de pantalla obtenidas de una web de venta online que muestra los aspectos más relevantes de la misma que delatan que estamos ante un fraude.

- Home: banner navideño cuando ya no estamos en esa época del año.

- Módulo de divisas: permite cambiar el precio a monedas de muchos países del mundo. Muy utilizado en tiendas online fraudulentas.
- Información del certificado: está utilizando un certificado gratuito, muy habitual en webs fraudulentas.
- Módulo de redes sociales: no tienen hipervínculo a ningún perfil de ninguna red social, se muestran solo para dotar de mayor credibilidad al fraude.
- Sección de “Contacto”: únicamente se facilita un formulario, no se facilita teléfono ni ninguna otra vía de contacto.
- Sección “Sobre nosotros”: no están traducidas, aparecen en otro idioma.
- Sección “Envío y devoluciones”: textos mal traducidos, expresiones en un español incorrecto.
- Características del producto: precios muy rebajados, condiciones de envío muy ventajosas (en 24h) y políticas de devolución poco habituales (hasta 365 días), que no estaban además recogidas en la sección de “Envío de devoluciones”.
- Carrito: aplicación de descuentos no mencionados anteriormente así como aplicación de una tasa en concepto de “seguro” y “envío” no informado anteriormente.
- Identificación en la página web: no hay confirmación de registro de la cuenta.
- No hay verificación de datos: da igual los datos que se introduzcan, aunque sean falsos, la web no hace ninguna verificación.
- No hay pasarela de pagos segura: los datos de la tarjeta de crédito se envían directamente al servidor de la web, no interviene ninguna pasarela de pago segura de ningún banco, ni PayPal ni cualquier otro servicio de estas características que garanticen un proceso de pago seguro.

5.13. Diapositiva 13. Identificando correos maliciosos

El correo electrónico es uno de los canales más utilizados por los ciberdelincuentes para llevar a cabo sus ataques. Especialmente, aquellos **relacionados con la [ingeniería social](#)**, es decir, al conjunto de técnicas que los ciberdelincuentes emplean para ganarse la confianza de los usuarios y que hagamos algo bajo su manipulación y engaño, como puede ser ejecutar un [malware](#), compartir nuestras credenciales o acceder a un sitio web malicioso.

En los siguientes apartados veremos pautas con las que aprender a reconocer este tipo de emails maliciosos o [phishing](#), así como varios ejemplos y formas de fraude comunes.

5.14. Diapositiva 14. Identificando correos maliciosos. Cómo reconocer un correo malicioso de *phishing*

El *phishing* es una técnica utilizada por ciberdelincuentes para obtener información personal y bancaria de nosotros, los usuarios. A raíz de un mensaje donde al atacante se hace pasar por una entidad legítima, como puede ser un banco, una red social, o una entidad pública, intenta engañarnos y manipularnos para que llevemos a cabo alguna acción que ponga en peligro nuestros datos.

Por suerte, su *modus operandi* suele ser siempre el mismo y hay una serie de aspectos en los que fijarnos para [identificar si se trata de un correo malicioso](#):

- **Contenido del mensaje:** el primer paso es analizar el contenido del correo electrónico. Como hemos mencionado anteriormente, el intento de suplantación

puede ser a un banco, una plataforma de pago, una red social, un servicio público, etc.

El objetivo puede ser asustarnos con un mensaje urgente y tratar de convencernos de que accedamos a un enlace debido a un inicio de sesión sospechoso, o una alerta de nuestro banco sobre una transacción fuera de lugar. En otros contextos, pueden recurrir a promociones u ofertas demasiado atractivas, que ninguno de nosotros dejaría escapar si fuesen reales.

Acompañando al mensaje suele ir un enlace a una web fraudulenta y/o un archivo adjunto con *malware*. Además, es muy habitual que soliciten nombre de usuario, claves y otros datos de acceso a las cuentas, práctica que las entidades legítimas nunca llevarían a cabo.

- **Errores ortográficos y gramaticales:** si nos fijamos detenidamente, podremos encontrar diversos errores en la escritura del mensaje. La mayoría de estos correos maliciosos se lanzan a muchos usuarios a la vez y de forma muy rápida o utilizando traductores gratuitos, por lo que los errores en la redacción son muy habituales.
- **Mensaje anonimizado:** cuando no son ataques dirigidos a un usuario en concreto, la mayoría de los correos maliciosos utilizan fórmulas genéricas, como: “Estimado cliente”, “Hola”, “Hola amigo”, etc. para evitar decir un nombre. Cuando una entidad tiene que dirigirse a nosotros, siempre lo hará enviando correos electrónicos personalizados.
- **Remitente del correo:** un paso fundamental es comprobar el remitente del correo. Una entidad legítima utilizará un dominio relacionado con el nombre de la misma, por ejemplo, *Microsoft* utilizará *@microsoft.com*. Sin embargo, no es una comprobación 100% eficaz, ya que los atacantes pueden haber suplantado una dirección de correo legítima.
- **Enlaces:** cuando el mensaje malicioso viene acompañado de un enlace, este suele redireccionarnos a un sitio web fraudulento. Para comprobar a dónde nos lleva realmente la url, es tan sencillo como situar el cursor sobre el enlace y comprobar la dirección real que se muestra en la parte inferior izquierda del navegador. Sin embargo, es posible que la url fraudulenta sea muy parecida a la original y nos cueste distinguirla. En ocasiones, son tan parecidas que solo cambian o añaden una letra para diferenciarlas.

Como recomendación, si queremos acceder a la web legítima, deberemos escribir directamente la url en la barra de direcciones de nuestro navegador, sin pasar por el enlace del correo electrónico.

- **Archivos adjuntos:** en el caso de los archivos adjuntos, los atacantes siempre tratarán de utilizar archivos o ejecutables que puedan infectarnos por *malware*. Una vez los descargamos y se ejecutan, el *malware* se instala en nuestro sistema y comienza a funcionar. Aunque la mejor recomendación es no descargar ningún archivo de un email sospechoso, también es recomendable mantener actualizado nuestro antivirus.

5.15. Diapositiva 15. Identificando correos maliciosos. VIDEO

En esta diapositiva se compartirá con los usuarios un vídeo que representará los pasos necesarios para identificar un correo malicioso o *phishing*, haciendo hincapié en los aspectos descritos en apartados anteriores. La duración será de 1 min. aproximadamente.

5.16. Diapositiva 16. Actividad 2

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3 y 5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

Actividad 2:

¿Alguna vez has recibido algún correo malicioso? Si no, es probable que encuentres alguno en tu bandeja de *spam*. Da un vistazo rápido, a ver si eres capaz de identificar algún correo que cumpla con las características típicas de un *phishing*.

5.17. Diapositiva 17. Identificando correos maliciosos. Ejemplos de correos de *phishing*

Veamos ahora varios **ejemplos de *phishing*** donde podemos identificar los aspectos mencionados anteriormente.

5.18. Diapositiva 18. Identificando correos maliciosos. *Phishing* bancario

El contenido del correo nos informa de que **nuestra cuenta bancaria ha sido suspendida por motivos de seguridad**. Si queremos recuperar nuestra cuenta, deberemos hacer clic en el enlace adjunto en el mensaje.

- Lo primero que podemos observar es que el remitente del correo no coincide con el dominio habitual de la entidad bancaria. Además, el **asunto es escueto y busca alarmarnos**.
- Por otro lado, en el cuerpo del mensaje podemos encontrar varios **errores ortográficos**, como si el mensaje estuviese escrito con prisas.
- Finalmente, si accediésemos al **enlace**, seríamos redirigidos a una web que simula ser la del banco, aunque, una vez hayamos introducido nuestras credenciales de acceso, estas serán compartidas con el atacante y se nos redirigirá a la web legítima.

Se muestran dos ejemplos concretos de *phishing* que suplantán a entidades bancarias. Las particularidades concretas de cada caso pueden consultarse en los siguientes enlaces:

- [Correos electrónicos suplantán a Bankia, Banco Santander y otras entidades bancarias](#)

- [Campaña de correos fraudulentos que suplantan a CaixaBank](#)

5.19. Diapositiva 19. Identificando correos maliciosos. *Phishing* a entidad pública

Se muestran dos ejemplos concretos de *phishing* que suplantan a entidades públicas, en concreto a la Agencia Tributaria y a la Dirección General de Tráfico (DGT). Las particularidades concretas de cada caso pueden consultarse en los siguientes enlaces:

- [Suplantan a la Administración para intentar instalarte un *malware* bajo el asunto “Comprobante Fiscal”](#)
- [Fraudes que suplantan a organismos oficiales y a empresas para descargar *malware*](#)

5.20. Diapositiva 20. Identificando correos maliciosos. *Phishing* a entidad privada

Se muestran dos ejemplos concretos de *phishing* que suplantan a entidades privadas, en concreto a la Agencia Tributaria y a la Dirección General de Tráfico (DGT). Las particularidades concretas de cada caso pueden consultarse en los siguientes enlaces:

- [Nuevo *phishing* a Endesa con facturas falsas](#)
- [Detectada nueva campaña de *phishing* que intenta suplantar a Carrefour](#)

5.21. Diapositiva 21. Identificando correos maliciosos. Otros *phishing*

Facilitamos otros ejemplos de correo de tipo *phishing* que podemos recibir:

[Detectada campaña de correos electrónicos que suplantan a Netflix](#)

[Nuevo *phishing* a Apple. Quieren robarte datos personales y bancarios](#)

[Nueva campaña de *phishing* que suplanta la identidad de PayPal](#)

5.22. Diapositiva 22. Otro tipo de correos electrónicos fraudulentos

Los atacantes pueden emplear otros medios, como redes sociales o aplicaciones de mensajería instantánea. Aprovechándose de la popularidad y el volumen de usuarios de estos servicios, han encontrado en ellos un canal por el que **maximizar el éxito de sus ataques y fraudes**. Por cualquiera de estas vías es muy sencillo enviar un mensaje que contenga un enlace que nos redirija a un sitio fraudulento.

Nuestra mejor defensa es **configurar debidamente las opciones de seguridad y privacidad** para evitar que contactos desconocidos puedan tratar de llegar a nosotros con algún mensaje fraudulento que pueda hacernos caer en la trampa.

Identificar este tipo de ataques e **ignorarlos o denunciarlos sí es posible**.

A continuación, vamos a analizar varios ejemplos de correos electrónicos fraudulentos que, a través de distintas tácticas, buscan ganarse nuestra confianza para engañarnos y conseguir algo a nuestra costa, principalmente un beneficio económico.

Algunos son “viejos conocidos”, que, al seguir teniendo éxito entre los usuarios menos concienciados, continúan en circulación.

5.23. Diapositiva 23. Identificando correos maliciosos. Ejemplos de correos fraudulentos: Timo Nigeriano (lotería, viuda, enfermo terminal)

Este tipo de fraude tiene muchas formas y variantes, pero es comúnmente conocido como el “Timo nigeriano”.

Su *modus operandi* es muy simple, se muestra una oportunidad única en la vida del usuario, por ejemplo, un familiar lejano que tras su muerte nos ha dejado una herencia multimillonaria, o un rico príncipe de Nigeria que necesita una pequeña ayuda económica para traspasar sus fondos, tras lo cual nos recompensará con una suma mucho mayor.

Otras veces, se informa al usuario de que ha ganado algún premio, concurso o lotería en el que probablemente no recuerde haber participado, y para obtener el premio debe introducir una serie de datos personales o hacer un ingreso en forma de gastos de gestión.

Enlaces de interés:

- [Una herencia demasiado cuantiosa para ser real.](#)

5.24. Diapositiva 24. Identificando correos maliciosos. Ejemplos de correos fraudulentos: Falsas ofertas de empleo

El paro sigue siendo uno de los principales problemas en muchos países del mundo. Los ciberdelincuentes lo saben, y se aprovechan de la necesidad de los trabajadores por encontrar un trabajo para llevar a cabo este tipo de engaños.

- Suelen ser habituales en **plataformas de empleo con menos protecciones a la hora de identificar y eliminar posibles fraudes**, pero también pueden llegar a nosotros a través del correo electrónico.
- A partir de unas **condiciones muy atractivas**, se ganan nuestro interés. Luego, ya sea a través de un enlace o una llamada telefónica (de pago) consiguen **sustraernos alguna cantidad de dinero** por medio de llamadas de tarificación especial, en concepto de gastos administrativos, como adelanto de compra de material para el trabajo, etc.
- En otras ocasiones, **el objetivo de los atacantes pueden ser nuestros datos personales**, para lo cual nos harán rellenar formularios muy invasivos, o pedirnos el envío de documentos de identidad, por ejemplo.

Enlaces de interés:

- [Buscaba un trabajo y me encontré con una estafa en toda regla](#)
- [Recibí un e-mail con la oferta de trabajo ideal, ¡pero tenía truco!](#)
- [Falso puesto de trabajo en empresa del sector petrolero](#)

5.25. Diapositiva 25. Identificando correos maliciosos. Ejemplos de correos fraudulentos: Falsos prestamistas de dinero

Los apuros económicos que pasamos los usuarios son a menudo aprovechados por los ciberdelincuentes.

- Este tipo de fraude consiste en que una persona, aparentemente desinteresada, **nos puede prestar una gran cantidad de dinero, a un interés muy bajo** (desde el 1.5% al 3%), y **sin pedir apenas documentación ni justificante** alguno.
- Sin embargo, el prestamista **nos pedirá una cantidad de dinero relativamente pequeña en concepto de gastos de gestión**.
- El proceso del préstamo se irá alargando hasta que el prestamista desaparezca o las exigencias de pequeñas cantidades vaya en aumento y nos demos cuenta de la estafa.

Enlaces de interés:

- [Necesitaba dinero y caí en la trampa de un prestamista online.](#)
- [Préstamos de dinero a particulares.](#)

5.26. Diapositiva 26. Identificando correos maliciosos. Ejemplos de correos fraudulentos: Novias rusas

El amor a través de Internet puede ser más engañoso de lo que nos gustaría. Un tipo de fraude muy común es el conocido como “Novias rusas”, aunque tiene sus variantes. Este tipo de estafas se aprovechan de nosotros y nuestro interés en encontrar una media naranja.

- En el mensaje, se nos informa de que **una chica está interesada en entablar una conversación con nosotros** y solo deberemos acceder a una **web de contactos gratuita**.
- El fraude llega cuando, tras hablar un poco con la chica, esta **comience a pedirnos dinero para pagarse regalos, un viaje para vernos o por un asunto personal**.

La realidad es que la chica no existe, y todo es una trampa para que cientos de usuarios convencidos de que han encontrado a su alma gemela envíen dinero a los atacantes.

Enlaces de interés:

- [Encontrar el amor por Internet me salió caro](#)
- [¿Chicas rusas por Internet? ¡No es lo que parece!](#)

5.27. Diapositiva 27. Identificando correos maliciosos. Ejemplos de correos fraudulentos: Correos de sextorsión

Este tipo de fraudes consiste en un **chantaje donde el atacante afirma tener en su poder material íntimo sobre la víctima**, generalmente de índole sexual. A cambio de un pago, no compartirá dicho material con el resto de sus contactos.

- En la mayoría de los casos, **dicho material no existe y es una invención del atacante**.
- Para darle mayor peso a sus argumentos, el mensaje suele venir acompañado de algún **correo o contraseña antigua que ha podido obtener por medio de otro tipo de ataque**, por ejemplo, a raíz de un ataque aprovechando la brecha de seguridad de algún servicio, como una red social o un servicio de nube, o un ataque de forma masiva, como un ataque DDoS o una *Botnet*.
De este modo, nos asustará y creemos que está en posesión del material que dice tener.

- El pago exigido suele ser en forma de **criptomonedas** o en forma de **material íntimo de la víctima**.
- En ocasiones, este tipo de fraude se da tras practicar [sexting](#) con un usuario que aprovechará el intercambio de contenido íntimo para llevar a cabo la extorsión.

Enlaces de interés:

- [¿Buscas pareja por Internet? ¡Ten cuidado!](#)
- [Mi nueva amiga de Facebook no era lo que parecía](#)
- [¿Se puede practicar sexting sin correr riesgos?](#)

5.28. Diapositiva 28. Identificando correos maliciosos. Ejemplos de correos fraudulentos: Recomendaciones y consejos

Este tipo de fraudes son fácilmente reconocibles. Las claves en las que debemos fijarnos para detectar uno de ellos son:

- Una **oportunidad demasiado atractiva para ser verdad**, con dinero fácil o una cantidad muy sustancial.
- La redacción de los mensajes suele estar llena de **faltas de ortografía, errores gramaticales o una mala traducción del texto**.
- Generalmente **se referirán a nosotros de forma genérica** o, en su defecto, con alguna prueba como un correo o contraseña nuestra con la que probar su mensaje, como es el caso de la sextorsión.
- En algún momento **se nos pedirá dinero por adelantado** o que **compartamos con ellos información personal**.

5.29. Diapositiva 29. Identificando correos maliciosos. Ejemplos de correos fraudulentos: Recomendaciones y consejos

Tanto si creemos estar ante uno de estos fraudes, como si hemos sido víctima de uno de ellos, deberemos seguir las siguientes [recomendaciones](#):

- **Nunca responder al correo**: si lo hacemos, es más probable que traten de llevar la extorsión al siguiente nivel. Y, por supuesto, no debemos hacer nada de lo que nos pida, como compartir información personal, hacer clic, descargar un adjunto o llamar a un número de teléfono.
- **Nunca compartir información**: en caso de que nos pidan datos personales, jamás deberemos compartirlos con ellos.
- **Actualizar el antivirus**: aunque sea por prevención, conviene que tengamos activo y actualizado a la última versión todas las herramientas de protección de nuestro dispositivo.
- **Actualizar las contraseñas**: utilizando [contraseñas distintas para servicios diferentes](#) y actualizándolas cada cierto tiempo, nos aseguraremos de minimizar el impacto de este tipo de amenazas.
- **Nunca descargar ningún archivo adjunto**: casi con total seguridad, se tratará de un archivo malicioso con el que tomar control de nuestro equipo, robar nuestros datos o hacerse con nuestras cuentas.
- **Nunca hacer clic en enlaces de correos sospechosos**: en caso de incluir un enlace, lo más probable es que nos redirija a una web fraudulenta que suplante la de una entidad legítima o que ejecute código malicioso desde el momento en que

accedemos a la misma. Una buena práctica es que pasemos el cursor por encima y confirmar que el enlace nos lleva a donde dice llevarnos.

En caso de haber respondido al chantaje, deberemos recopilar todas las pruebas de las que dispongamos y contactar con las [Fuerzas y Cuerpos de Seguridad del Estado \(FCSE\)](#) para presentar una denuncia. Para la recopilación de evidencias, puedes apoyarte en alguna herramienta específica para ello ([testigo online](#)).

5.30. Diapositiva 30. Otras técnicas de engaño

- **Pretexting:** Base de cualquier ataque de ingeniería social. Consiste en elaborar un escenario/historia ficticia, donde el atacante tratará de que la víctima comparta información que, en circunstancias normales, no revelaría.
- **Phishing:** Busca “pescar” víctimas. Generalmente se emplean correos electrónicos con archivos adjuntos infectados o links a páginas fraudulentas con el objetivo de tomar el control de sus equipos y robarles información confidencial.
- **Sextorsión:** Chantaje donde amenazarán a la víctima con distribuir supuestamente contenido comprometido de ella a sus contactos (aunque no exista dicho contenido), si no accede a las peticiones del ciberdelincuente, generalmente a realizar un pago.
- **Smishing:** Se trata de una variante del *phishing* pero que se difunde a través de SMS. Se pide al usuario que llame a un número de tarificación especial o que acceda a un enlace de una web falsa.
- **Baiting:** Emplea un cebo con *software* malicioso a la vista de sus víctimas para que ellos mismos infecten sus dispositivos.
- **Vishing:** Llamadas telefónicas donde el atacante se hace pasar por una organización/persona de confianza para que revele información privada.
- **Shoulder Surfing:** Consiste en mirar por “encima del hombro”. Al atacante le basta con observar lo que escribe o tiene en pantalla otro usuario para obtener información muy útil.
- **Dumpster diving:** Se refiere al acto de “husmear en la basura”, para obtener documentos con información personal o financiera.
- **Quid pro quo:** Prometen un beneficio a cambio de información personal y suelen ser compensaciones en formato regalo (merchandising, dinero o acceso gratuito a programas de pago).
- **Redes Sociales:** Las técnicas de engaño más comunes a través de las redes sociales son mediante cupones descuento, juegos y concursos, donde crees que puedes ganar algo.

5.31. Diapositiva 31. Ejemplos reales de *smishing*

Smishing es una palabra compuesta que hace referencia a SMS y *phishing*, debido a su similitud con este ataque tan popular. Mientras que este último lleva a cabo ataques de ingeniería social utilizando el correo electrónico como medio, en el *smishing* se utilizan mensajes de texto en forma de SMS o a través de las distintas aplicaciones de mensajería instantánea.

El *modus operandi* sigue siendo muy similar a otros ataques donde el ciberdelincuente suplanta la identidad de alguna persona o entidad de confianza para su víctima, con el objetivo de engañarla y conseguir que comparta información personal, realice un pago, haga clic en un enlace malicioso o se descargue un archivo adjunto.

El mayor riesgo de este tipo de ciberataque es el desconocimiento de los usuarios, ya que no esperan ser engañados a través de un mensaje de texto. Mientras que la mayoría de nosotros estamos concienciados sobre los riesgos de navegar por Internet, el spam y los correos electrónicos maliciosos, no percibimos el mismo nivel de amenaza cuando se trata de un mensaje de texto que nos notifica una actividad sospechosa. Nos propone una promoción única en la vida o nos informa sobre algún tema importante, todo ello simplemente accediendo a un enlace.

El detalle de los casos concretos incluidos en la diapositiva pueden consultarse en:

- [Campaña de SMS suplantando a Correos para descargar una app maliciosa con malware y robar datos bancarios](#)
- [Identificados SMS fraudulentos con enlace a una web para solicitar una supuesta ayuda económica de entre 350 y 700 euros](#)

5.32. Diapositiva 32. Ejemplos reales de *vishing*

El *vishing*, como otros muchos ataques de ingeniería social, se basa en una serie de técnicas con las que ganarse la confianza del usuario, generalmente, haciéndose pasar por una persona o entidad reconocida por los usuarios. Pero a diferencia del *smishing* y *phishing*, se lleva a cabo mediante llamadas de teléfono.

Más información sobre este fraude en: [Vishing, la llamada del fraude](#).

Los casos de *vishing* que más incidencia están teniendo entre los usuarios son los relacionados con el falso soporte técnico de Microsoft, todos los detalles de cómo funciona este fraude están disponibles en: [¿Microsoft te ha llamado sin haberlo solicitado?](#)

5.33. Diapositiva 32. Cómo reportar fraudes

Se pueden reportar fraudes del siguiente modo:

- A través del buzón del servicio de gestión de incidentes de INCIBE-CERT: incidentes@incibe-cert.es
 - Facilitando el mayor detalle posible del fraude que se quiere reportar.
 - Enviando todas las evidencias de las que se dispongan: correo electrónico, URL, etc.
- A través de la Línea de Ayuda de Ciberseguridad de INCIBE: el teléfono gratuito y confidencia 017 disponible los 365 días del año en horario de 9.00 a 21.00 horas.

5.34. Diapositiva 33. Actividad 3

Diapositiva para introducir a los usuarios la actividad. El tiempo aproximado de duración será de entre 3 y 5 minutos. Los pasos habrán sido descritos en las diapositivas anteriores.

La labor del docente será la de acompañar a los usuarios y ayudar en caso necesario. Se debe valorar la iniciativa, la resolución de la actividad y la proactividad.

Actividad 3:

En ocasiones, este tipo de fraudes llegan a través de las redes sociales. ¿Alguna vez te ha intentado agregar algún contacto o te ha llegado un mensaje con pinta de fraude? Trata de aplicar las pautas que hemos visto para identificar alguno, o busca en Internet algún fraude reciente que se haya popularizado y compártelo.

5.35. Diapositiva 34. En INCIBE te ayudamos

Mostramos la información de INCIBE prestando especial atención a la Línea de Ayuda en Ciberseguridad de INCIBE a través de la cual cualquier menor o adulto puede contactar de manera gratuita y confidencial cuando tengan una duda o un problema en Internet, llamando al número de teléfono 017 o enviando un mensaje a través de la página web <https://www.incibe.es/linea-de-ayuda-en-ciberseguridad>.

Animamos a los participantes a visitar las diferentes webs de INCIBE en función del público (Ciudadanos, Menores o Empresas) y a seguirnos en redes sociales.

Además, explicamos que en la web pueden encontrar mucha información y actividades para trabajar cualquier tema de ciberseguridad, juegos y recursos pedagógicos.

5.36. Diapositiva 35. Cuestionario de evaluación 1

Para identificar una tienda online legítima debemos fijarnos en:

- A. La url.
- B. Las valoraciones de usuarios.
- C. El tipo de producto.

5.37. Diapositiva 36. Cuestionario de evaluación 2

Un candado cerrado en la url quiere decir que:

- A. La web cifra la información.
- B. La web está cerrada.
- C. La web requiere contraseña para acceder.

5.38. Diapositiva 37. Cuestionario de evaluación 3

¿Cómo podemos saber si nos encontramos ante una web falsa mirando solo el precio de los productos?

- A. Los precios son muy bajos.
- B. Los productos tienen el mismo precio.
- C. Ambas opciones.

5.39. Diapositiva 38. Cuestionario de evaluación 4

De las siguientes opciones, ¿cuál es la opción de pago menos segura?

- A. Tarjeta prepago.
- B. Transferencia bancaria.
- C. Plataforma de pago.

5.40. Diapositiva 39. Cuestionario de evaluación 5

¿Cómo podemos saber si un enlace adjunto en un correo es fraudulento?

- A. Haciendo clic y comprobando la url.
- B. Poniendo el cursor encima para ver la url real.
- C. Copiando la url en un navegador distinto al habitual.

5.41. Diapositiva 40. Cuestionario de evaluación 6

La mayoría de los correos de phishing suelen:

- A. Utilizar un mensaje urgente o atractivo.
- B. Estar llenos de errores ortográficos y gramaticales.
- C. Ambas opciones.

5.42. Diapositiva 41. Cuestionario de evaluación 7

Una entidad bancaria jamás te pedirá tus credenciales o tus datos personales en un correo:

- A. Correcto.
- B. Falso.
- C. Solo en caso de suplantación.

5.43. Diapositiva 42. Cuestionario de evaluación 8

¿Cómo se conoce al fraude que utiliza la supuesta posesión de material íntimo del usuario para extorsionarlo?

- A. *Sexting*.
- B. *Sextorsión*.
- C. *Baiting*.

5.44. Diapositiva 43. Cuestionario de evaluación 9

¿Qué caracteriza a los fraudes por falsos prestamistas?

- A. No prestan grandes cantidades de dinero.
- B. Suelen dirigirse solo a empresas.
- C. Apenas piden condiciones e información.

5.45. Diapositiva 44. Cuestionario de evaluación 10

Por norma general, los fraudes se refieren a nosotros:

- A. Utilizando nuestro nombre.
- B. De forma genérica exclusivamente.
- C. De forma genérica o aportando una prueba, como una contraseña.

5.46. Diapositiva 45. Final del taller

¡Gracias por vuestra atención!

6. RECURSOS DE EVALUACIÓN

Las herramientas de evaluación del alumnado permitirán controlar la calidad del aprendizaje recibido, gracias a una serie de **criterios de evaluación**:

1. **Participación durante el taller.** La participación del alumnado mediante dudas u otro tipo de aportaciones resulta de un gran valor evaluativo (10% de la evaluación final).
2. **Actividades.** Estas actividades situadas al final de la mayoría de los apartados son uno de los medios de mayor potencial para la asimilación de las competencias recogidas en el taller. Además, permitirá al docente recibir u *feedback* directo sobre la evolución del alumnado (25% de la evaluación final).

1	Seguro que has comprado alguna vez por Internet. ¿Recuerdas cuál fue el último sitio donde compraste? Accede de nuevo y comprueba que todos los elementos que se han descrito en el contenido coinciden con la plataforma de compra online que utilizaste. ¡Esperemos que no te lleses una mala sorpresa!
2	¿Alguna vez has recibido algún correo malicioso? Si no, es probable que encuentres alguno en tu bandeja de <i>spam</i> . Da un vistazo rápido, a ver si eres capaz de identificar algún correo que cumpla con las características típicas de un <i>phishing</i> .
3	En ocasiones, este tipo de fraudes llegan a través de las redes sociales. ¿Alguna vez te ha intentado agregar algún contacto o te ha llegado un mensaje con pinta de fraude? Trata de aplicar las pautas que hemos visto para identificar alguno, o busca en Internet algún fraude reciente que se haya popularizado y compártelo.

3. **Cuestionario de evaluación.** Este instrumento de evaluación proporcionará gran parte de la puntuación final del alumnado y pondrá a prueba a los alumnos al finalizar un taller (65% de la evaluación final).

EVALUACIÓN FINAL = Participación + Actividades aprendizaje + Cuestionario de evaluación

6.1. Cuestionario de evaluación

El cuestionario de evaluación está compuesto por 10 preguntas de tipo test “opción múltiple” (3 opciones). La respuesta correcta está destacada en color verde.

1	Para identificar una tienda online legítima debemos fijarnos en:	La url.
		Las valoraciones de usuarios.
		El tipo de producto.
Feedback: La url nos dará información sobre el tipo de protocolo de cifrado de la información, mientras que el resto de las opciones pueden ser trampeadas fácilmente.		
2	Un candado cerrado en la url quiere decir que:	La web cifra la información.
		La web está cerrada.
		La web requiere contraseña para acceder.
Feedback: El candado es el certificado de seguridad y asegura que la información intercambiada con la web va a estar cifrada y protegida contra terceros.		
3	¿Cómo podemos saber si nos encontramos ante una web falsa mirando solo el precio de los productos?	Ambas opciones.
		Los precios son muy bajos.
		Los productos tienen el mismo precio.
Feedback: Una web falsa utilizará precios muy bajos para atraer a los usuarios. Además, todos los productos de la web suelen tener precios muy similares.		
4	De las siguientes opciones, ¿cuál es la opción de pago menos segura?	Transferencia instantánea.
		Tarjeta prepago.
		Plataforma de pago.
Feedback: Los servicios de transferencia instantánea no se hacen cargo en caso de fraude, por eso son tan utilizados por los ciberdelincuentes.		
5	¿Cómo podemos saber si un enlace adjunto en un correo es fraudulento?	Poniendo el cursor encima para ver la url real.
		Haciendo clic y comprobando la url.
		Copiando la url en un navegador distinto al habitual.
Feedback: Al poner el curso encima podremos comprobar la url real a la que nos redirige el enlace. Podremos comprobar si es la misma o si se trata de una web segura que comienza con 'https' en su url.		
6	La mayoría de los correos de <i>phishing</i> suelen:	Ambas opciones.
		Utilizar un mensaje urgente o atractivo.
		Estar llenos de errores ortográficos y gramaticales.

	Feedback: Los correos maliciosos emplean un asunto urgente para impedir que utilicemos el sentido común. También suelen recurrir a promociones u ofertas demasiado atractivas como para dejarlas pasar. Por otro lado, el mensaje suele estar lleno de errores, malas traducciones, etc.	
7	Una entidad bancaria jamás te pedirá tus credenciales o tus datos personales en un correo:	Correcto.
		Falso.
		Solo en caso de suplantación.
	Feedback: Una entidad bancaria, o de cualquier otro tipo, que se dirija a nosotros por correo electrónico jamás nos pedirá nuestras credenciales, da igual la situación.	
8	¿Cómo se conoce al fraude que utiliza la supuesta posesión de material íntimo del usuario para extorsionarlo?	Sextorsión.
		Sexting.
		Baiting.
	Feedback: Este tipo de fraude se conoce como sextorsión y busca engañarnos para sacar un beneficio, pero en la mayoría de los casos no disponen del material que el atacante afirma tener.	
9	¿Qué caracteriza a los fraudes por falsos prestamistas?	Apenas piden condiciones e información.
		No prestan grandes cantidades de dinero.
		Suelen dirigirse solo a empresas.
	Feedback: En este tipo de fraudes, buscan atraer nuestra atención poniendo unos requisitos muy bajos para atraer a la mayor cantidad de víctimas posibles.	
10	Por norma general, los fraudes se refieren a nosotros:	De forma genérica o aportando una prueba como una contraseña.
		Utilizando nuestro nombre.
		De forma genérica exclusivamente.
	Feedback: Dado que buscan engañar al máximo número de usuarios posibles, los fraudes no suelen dirigirse a nosotros con nuestro nombre. Sin embargo, en ocasiones como la sextorsión, sí utilizan alguna prueba adicional, como una contraseña, que han podido obtener a raíz de un ataque anterior o aprovechándose de la vulnerabilidad de algún servicio que hayamos utilizado.	

ANEXO

RECURSOS PARA AMPLIAR

Se recomienda la lectura de la siguiente selección de recursos complementarios, por parte del docente:

- [Conoce a fondo qué es el phishing](#)
- [Guía para aprender a identificar fraudes online](#)
- [Prueba de detección de ingeniería social](#)
- [Ponle freno a los fraudes y bulos con buenas prácticas](#)
- [¿Hacemos buen uso de las redes sociales?](#)
- [Un doble en la Red.](#)
- [Detectando fraudes “¿Me suena esta foto!”](#)
- [Falsas ofertas de empleo](#)
- [Muévete seguro por las redes sociales.](#)
- [Spoofing o el robo de identidades, ¿qué no te engañen!](#)
- [El fraude del email con supuestos vídeos extorsionadores circula de nuevo](#)
- [Cómo identificar un correo electrónico malicioso.](#)
- [¡A quién le van a interesar mis datos! \(Día Europeo de Protección de Datos\).](#)
- [Campaña ¡Contraseñas seguras!](#)
- [Campaña ¿Es seguro dónde guardas y cómo envías la información?](#)