Ficha de formación

Título	Seguridad en línea: qué hacer y qué no
Palabras clave	Internet, seguridad, online, offline, contraseñas, privacidad
Proporcionado por	Internet Web Solutions
Idioma	Español

Área de formación	
	Alfabetización sobre información
	Comunicación y colaboración
X	Seguridad
	Resolución de problemas

Objetivos / Resultados de aprendizaje

Al finalizar este módulo, podrás:

- Comprender la importancia de tener un comportamiento responsable en Internet.
- Identificar riesgos comunes al estar en línea.
- Reconocer los beneficios de Internet.
- Aprender buenas prácticas en materia de seguridad online.
- Desarrollar habilidades de alfabetización digital.

Descripción

Este curso ofrece una completa visión de cómo permanecer seguro al utilizar Internet, proporcionando consejos prácticos sobre qué y qué no hacer, incluyendo consejos sobre conexiones seguras, gestión de contraseñas, ajustes de privacidad en redes sociales, prácticas para compras seguras por Internet, y reconocer y evitar fraudes y estafas. Al seguir estas directrices, serás capaz de navegar por el mundo en línea de manera segura, y de protegerte de las potenciales amenazas.

Índice de contenidos (3 niveles)

Módulo: Seguridad online: qué hacer y qué no
Unidad 1: Introducción a la seguridad en línea
1.1. ¿Qué significa estar seguro en línea?
1.2. ¿Cuáles son los riesgos de una navegación insegura por Internet?
1.3. ¿Por qué no deberías dejar de navegar por Internet a pesar de los riesgos?

Unidad 2: Qué hacer y qué no en línea
2.1. Conexiones seguras

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

2.2. Contraseñas
2.3. Privacidad y redes sociales
2.4. Compras online
2.5. Fraudes y estafas

Unidad 3: Extra: qué hacer y qué no fuera de Internet
3.1. Dispositivos digitales

Contenido desarrollado

Módulo: Seguridad online: qué hacer y qué no

Unidad 1: Introducción a la seguridad en línea

Sección 1.1: ¿Qué significa estar seguro en línea?
Estar seguro *online* (o en línea) significa tomar precauciones y adoptar comportamientos responsables al utilizar Internet. Implica comprender y gestionar los **riesgos y amenazas potenciales** asociados a las actividades en línea para proteger la información personal, los recursos financieros y el bienestar general.

El ciberespacio es como una autopista: hay que navegar por ella con seguridad para evitar accidentes. Al igual que abrocharse el cinturón de seguridad, algunas prácticas básicas de seguridad en Internet pueden ayudar a garantizar que tu experiencia en línea sea segura y agradable.

Estar seguro en Internet es importante por varias razones. Ayuda a **proteger tu información personal** para que no caiga en malas manos. Datos personales como tu nombre, dirección, número de teléfono e información financiera pueden ser utilizados para el robo de identidad, fraude u otras actividades maliciosas si los ciberdelincuentes acceden a ellos. Tu presencia en Internet contribuye a tu reputación, tanto personal como profesional.

Al estar seguro en Internet, puedes **prevenir la difusión de contenidos inapropiados o perjudiciales** que pueden afectar negativamente a tu imagen y a tus relaciones. Salvaguardar tu seguridad en línea garantiza la **protección de tu intimidad** y te **protege de fraudes y estafas financieras**.

Estar seguro en Internet también ayuda a **evitar casos de ciberacoso y hostigamiento**. Aplicando medidas de seguridad, se puede reducir el riesgo de encontrarse con personas o situaciones perjudiciales que pueden provocar angustia emocional o daños. La seguridad en línea también es crucial para **proteger a los niños** y garantizar su bienestar en el mundo digital.

Sección 1.2: ¿Cuáles son los riesgos de una navegación insegura por Internet?
La navegación insegura por Internet supone riesgos para las personas mayores, que

Co-funded by the European Union
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

pueden estar menos familiarizados con las plataformas y las amenazas en línea, por lo que es importante comprender los riesgos específicos a los que se enfrentan.

Algunos de los riesgos más comunes son:

- **Phishing (suplantación de identidad) y estafas**: Las personas mayores son más susceptibles a los correos electrónicos de phishing, los sitios web fraudulentos y las estafas telefónicas, en las que los estafadores les engañan para que revelen información sensible.
- **Robo de identidad**: La navegación insegura por Internet aumenta el riesgo de robo de información personal y de identidad, lo que provoca pérdidas económicas y trastornos en sus vidas.
- **Fraude financiero**: Las personas mayores son objeto de falsos planes de inversión, estafas de lotería o compras fraudulentas, explotando su confianza y vulnerabilidad.
- **Malware y virus**: La navegación insegura por Internet puede dar lugar a descargas involuntarias de programas dañinos que ponen en peligro la seguridad del dispositivo y la información personal.
- **Hostigamiento y ciberacoso**: Las personas mayores pueden sufrir angustia emocional y problemas de bienestar mental debido al acoso en línea.
- **Vulneración de la intimidad**: Las prácticas inadecuadas de protección de la intimidad y privacidad pueden poner al descubierto información personal y provocar robos de identidad o solicitudes no deseadas.
- **Estafas de servicio técnico**: Las personas mayores son más susceptibles de sufrir estafas en las que los estafadores se hacen pasar por representantes del servicio técnica.
- **Falta de conocimientos digitales**: La inseguridad de la navegación por Internet se ve agravada por la falta de conocimientos digitales de las personas mayores, que las hace más vulnerables a amenazas y estafas.

Las personas mayores deben ser conscientes de estos riesgos y tomar medidas proactivas para prevenirlos, por ejemplo buscando ayuda y apoyo de personas de confianza o comunicando sus preocupaciones a las autoridades o plataformas pertinentes.

Sección 1.3: ¿Por qué no deberías dejar de navegar por Internet a pesar de los riesgos?

La seguridad en Internet es importante, pero no tiene por qué ser estresante. La concienciación es un primer paso poderoso para protegerse junto con un software antivirus de confianza (¡muchos de ellos son gratuitos!).

No deberías dejar por completo de navegar por internet a pesar de los riesgos en línea, ya que la red puede tener enormes ventajas para tu bienestar e inclusión social. Internet ofrece una gran cantidad de **información y recursos** que pueden

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

beneficiarte enormemente. Permite acceder a noticias, material educativo, recursos sanitarios, herramientas de comunicación y diversos servicios online.

En términos de **conexión social**, Internet permite mantenerse en contacto con la familia, los amigos y las comunidades, especialmente cuando la movilidad física o la distancia suponen una barrera. Las plataformas de redes sociales, las videollamadas y los foros en línea permiten mantener relaciones, compartir experiencias y combatir el aislamiento o la soledad. Las plataformas en línea ofrecen comodidad e **independencia** a todas las personas en diversos aspectos de la vida cotidiana. Se puede **comprar online, acceder a servicios bancarios en línea, concertar citas y pedir medicamentos**, lo que proporciona una mayor comodidad y red**uce la necesidad de desplazamientos físicos** o de **asistencia**.

Navegar por Internet es también una fuente de **estimulación cognitiva y compromiso mental**, ya que ofrece oportunidades para aprender, jugar, participar en aficiones o comunidades virtuales y mantenerse mentalmente activo, lo que puede contribuir al bienestar general.

Navegando por Internet y adoptando prácticas seguras en línea, puedes **desarrollar habilidades de alfabetización digital**, aumentar tu confianza y mantener un sentido de **autonomía**. Internet ofrece una gran cantidad de **recursos de aprendizaje**, como cursos en línea, tutoriales y plataformas educativas. Puedes explorar nuevos intereses, aprender nuevas habilidades y participar en oportunidades de aprendizaje permanente, fomentando el crecimiento personal y la estimulación intelectual.

Aunque es importante ser consciente de los riesgos en línea y tomar precauciones, **evitar Internet por completo puede provocar aislamiento, acceso limitado a recursos y pérdida de oportunidades**.

Unidad 2: Qué hacer y qué no en línea

Sección 2.1: Conexiones seguras
Qué SÍ hacer:

Utiliza redes Wi-Fi seguras: Siempre que sea posible, conéctate a redes Wi-Fi seguras y de confianza. Estas redes suelen requerir contraseña y cifrado, lo que proporciona un entorno de navegación más seguro. Evita acceder a cuentas confidenciales o realizar transacciones financieras en redes Wi-Fi públicas.

Verifica la seguridad del sitio web: Antes de introducir información confidencial o realizar transacciones en línea, verifica que el sitio web tenga una conexión segura. Busca "https://" en la dirección del sitio web y el símbolo de un candado en la barra de direcciones del navegador.

Mantén actualizado el software: Actualiza regularmente el sistema operativo, los

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

navegadores web y el software de seguridad de tu dispositivo. Las actualizaciones de software suelen incluir parches de seguridad que ayudan a protegerse frente a vulnerabilidades conocidas.

Utiliza protección de Firewall, o cortafuegos: Activa y mantén un cortafuegos en tu ordenador o router para que actúe como barrera contra accesos no autorizados y posibles amenazas procedentes de Internet.

Qué NO hacer:

No compartas información sensible: Evita introducir información confidencial, como contraseñas, datos de tarjetas de crédito o números de la Seguridad Social.

Evita los sitios web sospechosos: Evita visitar sitios web sospechosos o desconocidos. Para realizar actividades en línea, limítate a sitios web fiables y de buena reputación.

No ignores las advertencias del navegador: Presta atención a las advertencias y alertas del navegador sobre posibles riesgos de seguridad o sitios web no fiables.

No te conectes automáticamente a las redes: Desactiva la función de conexión automática de tus dispositivos, ya que podrían conectarse automáticamente a redes no seguras sin tu conocimiento.

Sección 2.2: Contraseñas
Qué SÍ hacer:

Crea contraseñas fuertes y únicas: Utiliza contraseñas fuertes y únicas para cada cuenta online. Debe incluir una combinación de letras mayúsculas y minúsculas, números y caracteres especiales. Evita utilizar información que pueda adivinarse, como cumpleaños o nombres.

Contraseñas largas: Opta por contraseñas más largas, ya que suelen ser más seguras. Intenta que tengan un mínimo de 12 caracteres. Considera el uso de frases como contraseña: series de palabras o una frase que sea más fácil de recordar pero difícil de adivinar para los demás. Por ejemplo, "MiColorFavoritoEsAzul!".

Activa la autenticación de dos factores (2FA): Siempre que sea posible, activa la autenticación de doble factor para tus cuentas online. Esto añade una capa adicional de seguridad al requerir un segundo paso de verificación, como un código único enviado a tu teléfono móvil.

Actualiza las contraseñas regularmente: Cambia tus contraseñas periódicamente, preferiblemente cada pocos meses.

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Qué NO hacer:

No reutilices contraseñas: Nunca reutilices la misma contraseña en varias cuentas. Si una cuenta se ve comprometida, podría dar acceso a otras cuentas. Utiliza contraseñas únicas para cada servicio o plataforma en línea.

Evita contraseñas demasiado comunes: Evite contraseñas comunes o fáciles, como "123456", "contraseña" o "qwerty". Estas contraseñas suelen estar en el punto de mira de los piratas informáticos y pueden descifrarse fácilmente.

No compartas ni anotes contraseñas: Evita compartir tus contraseñas con otras personas, incluidos familiares o amigos. Además, evita anotar las contraseñas en notas físicas o almacenarlas en archivos digitales de fácil acceso.

No guardes contraseñas en los navegadores: No guardes contraseñas en los navegadores ni utilices la función "Recuérdame". Aunque puede resultar cómodo, supone un riesgo para la seguridad si alguien accede sin autorización a tu dispositivo.

Sección 2.3: Privacidad y redes sociales
Qué SÍ hacer:

Revisa la configuración de privacidad: Familiarízate con la configuración de privacidad de las plataformas de redes sociales que utilizas. Ajusta la configuración para controlar quién puede ver tu perfil, tus publicaciones y tu información personal. Considera limitar el acceso a amigos y familiares de confianza.

Sé selectivo con las solicitudes de amistad: Ten cuidado al aceptar solicitudes de amistad o de conexión de desconocidos. Verifica la identidad de la persona antes de aceptar su solicitud.

Piensa antes de compartir: Ten cuidado al compartir información personal, fotos o actualizaciones en las redes sociales. Evita compartir públicamente datos sensibles como tu dirección completa, número de teléfono o información financiera.

Revisa y actualiza periódicamente la lista de amigos: Revisa periódicamente tu lista de amigos o contactos en las redes sociales. Elimina de tu lista de amigos a las personas en las que ya no confíes o que no reconozcas.

Qué NO hacer:

No hagas clic en enlaces sospechosos: Desconfía de hacer clic en enlaces compartidos en las redes sociales, especialmente si proceden de fuentes desconocidas o sospechosas. Estos enlaces pueden conducir a sitios web de phishing o a descargas de programas maliciosos. Verifica la fuente antes de hacer clic.

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Ten cuidado con las aplicaciones de terceros: Sé selectivo a la hora de conceder permisos a aplicaciones de terceros que soliciten acceso a tus cuentas de redes sociales. Revisa los permisos solicitados y considera la credibilidad de la aplicación antes de conceder el acceso.

Evita dar publicidad a acontecimientos personales: Evita anunciar tus próximas vacaciones o periodos prolongados fuera de casa en las redes sociales. Esto puede alertar a posibles ladrones o delincuentes de que tu casa está desocupada.

Sección 2.4: Compras online

Qué SÍ hacer:

Compra en sitios web de confianza: A la hora de comprar, limítate a tiendas online conocidas y de buena reputación. Busca sitios web que tengan opiniones positivas de los clientes y opciones de pago seguras, como tarjetas de crédito o plataformas de pago acreditadas.

Verifica la seguridad del sitio web: Antes de introducir datos personales o de pago, asegúrate de que el sitio web tiene una conexión segura. Busca "https://" en la dirección del sitio web y el símbolo de un candado en la barra de direcciones del navegador.

Haz seguimiento de las transacciones: Mantén un registro de tus transacciones de compra en línea, incluidas las confirmaciones de pedido, los recibos y los números de seguimiento. Esto te permitirá hacer un seguimiento de las entregas y resolver cualquier problema que pueda surgir.

Qué NO hacer:

No compartas información innecesaria: Ten cuidado al compartir información personal innecesaria durante el proceso de pago. Los comercios suelen pedir datos básicos como la dirección de envío y la información de pago.

Cuidado con los correos electrónicos o enlaces de phishing: Desconfía de correos electrónicos o mensajes que afirmen proceder de comercios online, especialmente si te piden información personal o te incitan a hacer clic en enlaces sospechosos.

Evita las redes Wi-Fi no seguras para realizar transacciones: Cuando hagas compras por Internet, evita utilizar redes Wi-Fi públicas o no seguras. Estas redes pueden ser vulnerables a piratas informáticos que podrían interceptar tu información personal y financiera.

No caigas en las estafas de suplantación de identidad: Ten cuidado con los vendedores en línea que se hacen pasar por marcas de renombre o utilizan tácticas engañosas para obtener tu información personal o financiera. Verifica la

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

autenticidad del vendedor y de su sitio web antes de realizar una compra.

Sección 2.5: Fraudes y estafas
Qué SÍ hacer:

Ser escéptico y vigilante: Mantén un sano escepticismo cuando te encuentres con correos electrónicos, llamadas telefónicas o mensajes no solicitados en los que te pidan información personal o te ofrezcan gangas extrañas. Verifique la legitimidad de la fuente antes de facilitar información o asumir compromisos financieros.

Infórmate: Mantente informado sobre las estafas habituales en Internet y las tácticas de fraude dirigidas a personas mayores. Familiarízate con las señales de las estafas, como las solicitudes de pago a través de métodos poco convencionales o la presión para actuar con rapidez.

Verifica la identidad del contacto: Si una persona afirma representar a una organización, pídele información de contacto oficial y confirma su autenticidad poniéndote en contacto directamente con la organización utilizando datos de contacto verificados.

Consulta con personas de confianza: Si recibes una solicitud sospechosa o te encuentras con una situación desconocida en Internet, pide consejo a un familiar, amigo o profesional de confianza.

Ignora las llamadas telefónicas no solicitadas y las "llamadas robóticas". Trata con escepticismo cualquier llamada telefónica no solicitada. Una persona en directo o una voz grabada te da información falsa que parece importante y urgente. Puede que digan ser un pariente en apuros, que la garantía de tu coche está a punto de caducar y que hay que pagar, puede que se presenten como "servicio técnico" y te digan que tienes que reparar tu ordenador a cambio de una cantidad de dinero…

Qué NO hacer:

No te precipites ni te sientas presionado: Los estafadores suelen utilizar tácticas para crear una sensación de urgencia o presión, coaccionando a las víctimas para que tomen decisiones rápidas sin la debida consideración. Tómate tu tiempo, investiga y sé prudente antes de asumir compromisos financieros.

No envíes dinero a desconocidos: Desconfía de las solicitudes de dinero o transferencias bancarias de personas que no conozcas personalmente. Verifica la identidad y legitimidad de la persona antes de realizar cualquier transacción financiera.

No hagas clic en enlaces de correos electrónicos de remitentes desconocidos. Desconfía de los mensajes extraños o inesperados, aunque sean de personas

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

conocidas. Podrían contener enlaces maliciosos o de suplantación de identidad. Si un mensaje te parece sospechoso pero procede de alguien que conoces y en quien confías, consúltale antes de hacer clic.

No abras ningún archivo adjunto. No abras ningún archivo adjunto que no esperes o que proceda de un contacto desconocido, sobre todo si tiene la extensión .exe o .zip. Si el archivo o archivos parecen proceder de un amigo o familiar, pídele que te asegure que te ha enviado algo. Esta norma de seguridad también se aplica a los archivos adjuntos enviados a través de mensajes de texto y redes sociales.

No hagas clic en las ventanas emergentes de tu teléfono u ordenador. Una estratagema habitual es el *scareware*, que utiliza alertas de seguridad emergentes para asustarte y que descargues o pagues por software falso disfrazado de protección real de ciberseguridad. Por ejemplo, aparecerá una alerta diciendo que tu dispositivo está en peligro y necesita reparación. Cuando llames al servicio de asistencia, es posible que los estafadores te pidan acceso remoto a tu ordenador y te soliciten una tarifa. Otra técnica de malware consiste en utilizar botones engañosos como "Cerrar" o "X", que instalan automáticamente un virus al hacer clic en ellos.

Unidad 3: Extra: qué hacer y qué no fuera de Internet

Sección 3.1: Dispositivos digitales
Qué hacer:

Bloquea tus dispositivos. Asegúrate de que los dispositivos con acceso a información sensible se bloquean automáticamente y requieren una contraseña para reactivarse. Asegúrate de configurar el router Wi-Fi doméstico y los puntos de acceso con nombres de usuario y contraseñas únicos que no sean los predeterminados.

Mantén tus dispositivos a salvo: Asegúrate de que tus dispositivos digitales, como smartphones, tablets u ordenadores portátiles, están físicamente seguros. Guárdalos en un lugar seguro y protegido cuando no los utilices.

Actualiza regularmente el software: Mantén actualizados el sistema operativo y las aplicaciones de tus dispositivos. Las actualizaciones de software suelen incluir importantes parches de seguridad que ayudan a proteger frente a vulnerabilidades y garantizan un rendimiento óptimo.

Activa el seguimiento y bloqueo a distancia: Activa las funciones de seguimiento y bloqueo remoto de tus dispositivos, si están disponibles. Esto te permite localizar tu dispositivo o bloquearlo a distancia en caso de pérdida o robo.

Desecha con seguridad los dispositivos viejos: Cuando te deshagas de dispositivos

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

digitales antiguos, asegúrate de que todos los datos personales se borran completamente del dispositivo. Realiza un restablecimiento de fábrica o utiliza software especializado para borrar tus datos de forma segura.

Qué NO hacer:

No dejes los dispositivos desatendidos: Evita dejar tus dispositivos digitales desatendidos en lugares públicos, como cafeterías o transportes públicos. Mantenlos siempre a la vista o guardados de forma segura.

No instales aplicaciones no autorizadas: Evita descargar e instalar aplicaciones de fuentes no fiables. Limítate a las tiendas de aplicaciones oficiales, como Google Play Store o Apple App Store, para reducir el riesgo de descargar aplicaciones maliciosas o falsificadas.

5 entradas de glosario

Contraseña. Una contraseña es una combinación secreta de caracteres que se utiliza para autenticar y obtener acceso a un dispositivo o una cuenta. Se recomienda establecer una contraseña segura para proteger la información sensible.
Redes sociales. Las redes sociales son plataformas y tecnologías en línea que permiten a los usuarios crear, compartir e intercambiar información, ideas y contenidos con otras personas. Estas plataformas suelen incluir contenidos generados por los usuarios y facilitan la comunicación, la creación de redes y la interacción entre individuos o grupos.
Seguridad online. La seguridad online o en línea se refiere a las medidas y precauciones adoptadas para proteger a las personas y su información personal cuando utilizan Internet y participan en actividades en Internet. Abarca prácticas y directrices destinadas a prevenir diversos riesgos en línea, como el ciberacoso, el robo de identidad, el fraude, la piratería informática y la exposición a contenidos inapropiados. La seguridad en línea implica comprender y aplicar estrategias para salvaguardar la privacidad, la seguridad y el bienestar en el uso de plataformas digitales.
Apps maliciosas. Las apps maliciosas son aplicaciones diseñadas para dañar o comprometer la seguridad de un dispositivo o los datos de un usuario. Instalar apps de fuentes no fiables aumenta el riesgo de descargar apps maliciosas que pueden robar información personal o realizar acciones no autorizadas.
Información sensible. Por información sensible se entiende cualquier dato o detalle que, de ser revelado o accedido por personas no autorizadas, podría suponer un riesgo para la privacidad, la seguridad o el bienestar de una persona. Incluye información personal identificable (IPI) como nombres completos, direcciones, números de teléfono, números de la seguridad social, información financiera, credenciales de acceso e historiales médicos. La información sensible requiere una protección y un tratamiento especiales para evitar su uso indebido, el robo de identidad, el fraude u otras consecuencias perjudiciales.

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

5 preguntas y respuestas de elección múltiple

Pregunta 1. ¿Qué necesita una conexión Wi-Fi para ser segura?
Opción a: Requiere que sea privada, con uso de contraseña y cifrado.
Opción b: Requiere un uso ilimitado de datos.
Opción c: Requiere alta velocidad de Internet.
Opción d: Requiere que la conexión Wi-Fi sea pública.
Opción correcta: a

Pregunta 2. ¿Por qué es importante actualizar regularmente el software de tu dispositivo?
Opción a: Porque aumenta el espacio de almacenamiento del dispositivo.
Opción b: Porque hace que la interfaz del dispositivo parezca bonita.
Opción c: Porque te protege frente a vulnerabilidades y amenazas de seguridad conocidas.
Opción d: Porque aumenta la duración de la batería del dispositivo.
Opción correcta: c

Pregunta 3. ¿Cómo puedes identificar posibles fraudes o estafas?
Opción a: Ignorando las alertas de seguridad.
Opción b: Compartiendo información personal y financiera en cualquier lugar.
Opción c: Apresurándote a contraer compromisos financieros rápidamente.
Opción d: Conociendo las estafas habituales en Internet y manteniéndote alerta.
Opción correcta: d

Pregunta 4. ¿Cómo puedes crear una contraseña segura?
Opción a: Utilizar una sola palabra en minúsculas, sin números ni caracteres especiales.
Opción b: Incluyendo letras mayúsculas y minúsculas, números y caracteres especiales.
Opción c: Reutilizando la misma contraseña para varias cuentas.
Opción d: Escogiendo una contraseña fácil de adivinar y compartiéndola con amigos para no perderla.
Opción correcta: b

Pregunta 5: Cuando compras en Internet, ¿qué debes hacer si un sitio web no tiene una conexión segura?
Opción a: Proceder a la compra de todos modos.
Opción b: Lo mejor es evitar introducir datos personales o de pago en ese sitio web, y realizar la compra en un sitio web más fiable con una conexión segura.
Opción c: Debería pedirle a otra persona que utilice sus datos y realice la compra por mí en ese sitio web.
Opción d: Si realizo la compra utilizando una red Wi-Fi pública, no habrá ningún problema en compartir mis datos con ese sitio web.

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Opción correcta: b	
Bibliografía y referencias	
https://www.enisa.europa.eu/ http://www.eun.org/ https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 https://www.microfocus.com/en-us/what-is/cyber-security https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20210410.html https://openwebinars.net/blog/origen-e-importancia-de-la-ciberseguridad/ https://www.europol.europa.eu/wannacry-ransomware	
Material relacionado	BOOMER_OnlineSafety_IWS_ES
Enlace de referencia	
Vídeo en formato Powtoon	https://www.youtube.com/watch?v=D3nJSePaVYk

Co-funded by the European Union

This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.