MOBILE MONEY

Módulo 2

Seguridad y prevención

Cofinanciado por la Unión Europea

Financiado por la Unión Europea. No obstante, los puntos de vista y opiniones expresados son exclusivamente los del autor o autores y no reflejan necesariamente los de la Unión Europea ni los de la Agencia Ejecutiva en el Ámbito Educativo y Cultural Europeo (EACEA). Ni la Unión Europea ni la EACEA pueden ser consideradas responsables de las mismas. Número de proyecto: 2023-1-RO01-KA220-ADU-000157797

Socios

Asociatia Four Change, Rumanía

Zavod IZRIIS, Eslovenia

E-SENIORS: INITIATION DES SENIORS AUXNTIC ASSOCIATION, Francia

GUnet, Grecia

Asociatia Niciodata Singur - Prietenii Varstnicilor, Rumanía

Fundació Gesmed Fundació de la Comunitat Valenciana,

MOBILE MONEY

Módulos

1. Competencias digitales básicas
2. **Seguridad y prevención**
3. Gestionar una cuenta bancaria online
4. Soluciones online para recibir y enviar dinero
5. Utilizar una tarjeta de crédito para comprar bienes y servicios online
6. Pagos online de impuestos y facturas

Unidad 1

Introducción

Objetivos

Al finalizar esta unidad, tendrás conocimiento sobre:

✓Los objetivos de aprendizaje y el contenido formativo de este módulo

✓La metodología de formación utilizada y la duración de este módulo

Imagen de vectorjuice en Freepik

Cofinanciado por la Unión Europea

MOBILE MONEY

Competencias

Este modulo te ayuda a:

- Adquirir los conocimientos necesarios para utilizar las soluciones de dinero digital con seguridad y confianza:
  - ✓ Entender qué es la seguridad online.
  - ✓ Entender qué es un dato personal y qué es un dato sensible.
  - ✓ Comprender los conceptos de privacidad y seguridad.
  - ✓ Saber qué son el spam y el phishing y cómo responder a ellos
  - ✓ Conocer los criterios para decidir qué enlaces son seguros de visitar
  - ✓ Conocer tus derechos en Internet
  - ✓ Entender qué es el GDPR y por qué lo necesitamos
  - ✓ Saber aplicar medidas de seguridad y prevención

Cofinanciado por la Unión Europea

MOBILE MONEY

Contenido de la formación

1. Introducción de la sesión: duración, objetivos, contenido y metodología
2. Seguridad online, datos personales, datos sensibles, privacidad y seguridad
3. Reconocer spam y el phishing y saber qué hacer al respecto
4. Conocer tus derechos online, el ejemplo del GDPR
5. Protegerse en Internet
6. Test: comprueba tus conocimientos

Cofinanciado por la Unión Europea

Metodología y duración de la formación

Duración: 4 horas

- Formación presencial: 2 horas
- Formación online: 2 horas

Metodología

- Activo y participativo
- Formación presencial:
  - ✓Diálogo ✓ Juegos de Rol ✓ Trabajo en equipo
- Formación online:
  - ✓Vídeos seleccionados o de producción propia
  - ✓Aplicación práctica de algunos consejos acordados en el aula
  - ✓Algunos trabajos en colaboración
  - ✓Simulación

Cofinanciado por la Unión Europea

Unidad 2

Seguridad online y datos personales

Objetivos

Al finalizar esta unidad, sabrás:

✓Qué es la seguridad online

✓Qué son los datos personales y ejemplos de ellos

Imagen de vectorjuice en Freepik

Cofinanciado por la Unión Europea

Seguridad online

Estar en línea expone a los usuarios de Internet a **amenazas de seguridad online**. Una vez que un usuario envía datos por Internet (paquetes de llamadas de vídeo o voz, chat, correo electrónico o números de tarjetas de crédito, sitios web) **no** tiene **control sobre quién puede acceder a ellos**. Los datos pasan por muchos servidores, routers y dispositivos a los que cualquier hacker, proveedor de servicios o agente gubernamental puede acceder y leer.

Por lo tanto, es de suma importancia que los usuarios de Internet tomen medidas para:

- Protección de tus **datos personales sensibles;**
- Utilizar herramientas y servicios online, como el cifrado de datos, que **garanticen la privacidad y seguridad de** la información de sus clientes cuando se comuniquen con ellos online.

¿Qué son los datos personales?

Los **datos personales** son toda información relativa a una **persona viva, identificada o identificable**.

También son datos personales los diversos elementos de información que, en conjunto, pueden utilizarse para **identificar a una persona concreta**.

Imagen de storyset en Freepik

Ejemplos de datos personales

Algunos ejemplos de datos personales son los siguientes:

- Nombre y apellidos;
- Domicilio;
- Dirección de correo electrónico como

  name.surname@company.com;
- Datos de localización, como la función de datos de localización de un teléfono móvil);
- Número de tarjeta de identificación;
- Dirección de Protocolo de Internet (IP);
- Un ID de cookie;
- El identificador de publicidad de tu teléfono;
- Datos en poder de un hospital o un médico, que pueden ser un símbolo que identifique a una persona de forma inequívoca.

Unidad 3

Datos sensibles, privacidad y seguridad

Objetivos

Al terminar esta unidad, sabrás:

- ✓ Qué datos personales se consideran sensibles.
- ✓ Qué son los datos personales y financieros sensibles.
- ✓ Comprender los conceptos de privacidad y seguridad
- ✓ Qué es la privacidad en Internet y cómo estar seguro en la red

Cofinanciado por la Unión Europea

¿Qué datos personales se consideran sensibles?

Datos personales sensibles

Los siguientes datos personales se consideran "**sensibles**" y están sujetos a condiciones específicas de tratamiento:

- Datos personales que revelen el origen racial o étnico, las opiniones políticas o las creencias religiosas o filosóficas;
- Fotos, vídeos;
- Afiliación sindical;
- Datos genéticos, datos biométricos tratados únicamente con fines de identificación de un ser humano;
- Datos relativos a la salud;
- Datos relativos a la vida sexual o la orientación sexual de una persona.

Datos financieros sensibles

- Cuenta y contraseña para un sistema de banca electrónica
- El CCV, fecha de caducidad de una tarjeta de crédito o débito
- El código PIN de tu teléfono móvil

➔ Ejemplos y ejercicios

Imagen de redgreystock en Freepik

¿Qué es la privacidad?

Se trata de la **intimidad**:

- Cómo **controlamos nuestros datos personales**, y
- cómo **son utilizados** por los terceros que los han recibido, de forma segura.

⟹ Piensa en las **políticas de privacidad** que te piden que leas y aceptes cuando visitas un sitio web o descargas una nueva aplicación para smartphone.

Imagen de storyset en Freepik

¿Qué es la seguridad?

La seguridad consiste en **asegurar y proteger tus datos personales** frente a **accesos no autorizados,** ya sea en tu dispositivo, en el servidor web remoto o durante la comunicación a través de Internet.

Utilizamos **controles de seguridad** a nivel técnico para limitar quién puede acceder a la información. Estos controles están en vigor:

- En nuestros dispositivos (PC, tableta, teléfono móvil), es decir, aplicando actualizaciones del sistema operativo y del software, utilizando contraseñas seguras;
- En el servidor web remoto mediante contraseñas seguras;
- Cuando se envia información a través de Internet, se usa el protocolo seguro **https**.

Imagen de vectorjuice en Freepik

Seguridad y privacidad

- La seguridad consiste en **proteger los datos**, mientras que la privacidad consiste en **proteger la identidad de los usuarios**.

  Por ejemplo, el personal de hospitales y clínicas utiliza sistemas seguros para comunicarse con los pacientes sobre su salud, en lugar de enviar información a través de cuentas personales de correo electrónico. Este tipo de comunicación es un ejemplo de seguridad.

- Por otro lado, la política y las disposiciones de privacidad pueden limitar el acceso a los historiales médicos de los pacientes a **determinados miembros del personal del hospital**, como médicos, enfermeras y auxiliares médicos.

- **Es posible tener seguridad sin privacidad**.

  De hecho, por ejemplo, los datos personales pueden transmitirse y almacenarse de forma segura en un sitio web, pero éste puede seguir vendiéndolos.

- **No es posible tener privacidad sin seguridad.**

  En efecto, por ejemplo, un pirata informático podría acceder sin autorización a su dispositivo, servidor web o datos transmitidos y robar sus datos personales.

Unidad 4

Spam y phishing

Objetivos

Al terminar esta unidad, sabrás:

- ✓ ¿Qué es el spam y el phishing?
- ✓ Cómo identificar el spam
- ✓ Cuando es seguro visitar un enlace

Imagen de vectorjuice en Freepik

Cofinanciado por la Unión Europea

¿Qué es el spam y el phishing?

Es posible que hayas recibido correos electrónicos molestos de un **remitente desconocido**, normalmente de carácter comercial.

Además, **los correos electrónicos pueden ser peligrosos porque** pueden contener enlaces que lleven a sitios web de phishing o sitios web que alojen programas maliciosos o que contengan programas maliciosos como archivos adjuntos.

Por tanto, **no abras ningún archivo adjunto ni hagas clic en ningún enlace**. Y nunca facilites tus datos personales, los detalles de tu cuenta de banca electrónica (cualquier nombre de usuario, contraseña) o los detalles de tu tarjeta de crédito/débito, como la fecha de caducidad y los 3 dígitos del CCV.

Es lo que se denomina **phishing:** los delincuentes envían correos electrónicos con apariencia oficial para engañarte y que reveles datos que pueden utilizarse para robar tu identidad.

Imagen de vectorjuice en Freepik

¿Cómo identifico el spam?

Un correo electrónico es sospechoso si contiene uno o varios de los siguientes elementos

- Errores gramaticales y ortográficos
- Correos en lengua extranjera
- Falta el nombre del remitente
- Necesidad urgente de actuar, especialmente en combinación con una amenaza

- Solicitud de introducción de datos personales (por ejemplo, PIN o TAN)
- Solicitud de apertura de un expediente
- Nunca recibí ningún correo electrónico del banco o de un cliente

Imagen de freepik

¿Qué hacer o no hacer?

- ✓ Evita abrir archivos adjuntos que no hayan sido analizados por un programa antivirus.
- ✓ Recuerda cerrar la sesión, especialmente si utilizas un ordenador público compartido.
- ✓ Elimina todos los correos electrónicos de desconocidos.
- ✓ No respondas nunca al spam.
- ✓ No hagas clic en los enlaces de los mensajes de spam.

Actividad: ¿Es seguro visitar el enlace?

Decida si es seguro visitar el enlace:

Supongamos que recibes un correo electrónico de un banco en el que se te pide que hagas clic en un enlace como el que aparece a continuación y que envíes datos personales, como el nombre de usuario, las contraseñas y los datos de la tarjeta de crédito.

http://url5423.eka.de/ls/click?upn=V1OaWNMSPs2Lb0JqHpnyTLRlk2703ToIFpo2vd2MKt5gB6dYAUvw1B-2FnC6T5iVsCdbcug7l6pkTad-2FBfACSlC-2BKw-3D-3DhmuAs-OaWNMSPs2Lb0JqHpn-asDvdva

1. *No te apresures, piénsalo dos veces y decide si es seguro visitar este enlace.*
2. *Piensa en las razones.*

Imagen de pch.vector en Freepik

Imagen de freepik

Actividad: ¿Es seguro visitar el enlace? (2)

La respuesta. *Este enlace* **no** es **seguro** por varias razones:

- Utiliza http en lugar de https.
- El nombre de dominio no está relacionado con el nombre oficial del banco.
- El enlace es sospechosamente largo.
- El nombre de dominio del enlace es diferente del nombre de dominio de la dirección de correo electrónico del remitente.
- Un banco de verdad nunca te pedirá nombres de usuario, contraseñas ni datos de tarjetas de crédito.

Unidad 5

¿Cuáles son tus derechos online?

Objetivos

Al terminar esta unidad, sabrás:

✓ ¿Cuáles son tus derechos y obligaciones digitales?

✓ Qué es el GDPR y por qué lo necesitamos

Imagen de vectorjuice en Freepik

Cofinanciado por la Unión Europea

Somos ciudadanos digitales

Ahora todos estamos conectados por Internet, como neuronas en un cerebro gigante.

Stephen Hawking

Los ciudadanos digitales pueden disfrutar de derechos de privacidad, seguridad, acceso e inclusión, libertad de expresión y mucho más. Sin embargo, esos derechos conllevan ciertas responsabilidades, como la ética, la empatía y otras responsabilidades para garantizar un entorno digital seguro y responsable para todos.

Imagen de storyset en Freepik

¿Qué es el GDPR y quién debe cumplirlo?

¿Qué es el GDPR?

- **El Reglamento General de Protección de Datos** es una ley de la Unión Europea que entró en vigor el 25 de mayo de 2018 y obliga a las organizaciones a salvaguardar los datos personales y defender los derechos de privacidad de cualquier persona en territorio de la UE.

¿Quién debe cumplir el GDPR?

- Cualquier organización que procese datos personales de individuos en la UE debe cumplir el RGPD.
- "**Tratamiento**" es un término amplio que abarca prácticamente todo lo que se puede hacer con los datos: recogida, almacenamiento, transmisión, análisis, etc.
- "**Datos personales**" es cualquier información relativa a una persona, como nombres, direcciones de correo electrónico, direcciones IP, color de ojos, creencias políticas, etc.

¿Quién debe cumplirla?

Incluso si una organización no tiene ninguna conexión con la UE en sí, pero procesa datos personales de personas en la UE (por ejemplo, a través del seguimiento en su sitio web), todavía tiene que cumplir con el GDPR.

El RGPD no se limita a las empresas con ánimo de lucro.

¿Es el GDPR algo positivo?

- El GDPR está ahí para proteger sus derechos como usuario.
- Es bueno saber qué está consintiendo y qué significan las cookies.
- Gestionar bien a los clientes vulnerables no es sólo algo que espera la ley, sino también lo correcto desde el punto de vista social y una decisión empresarial inteligente.

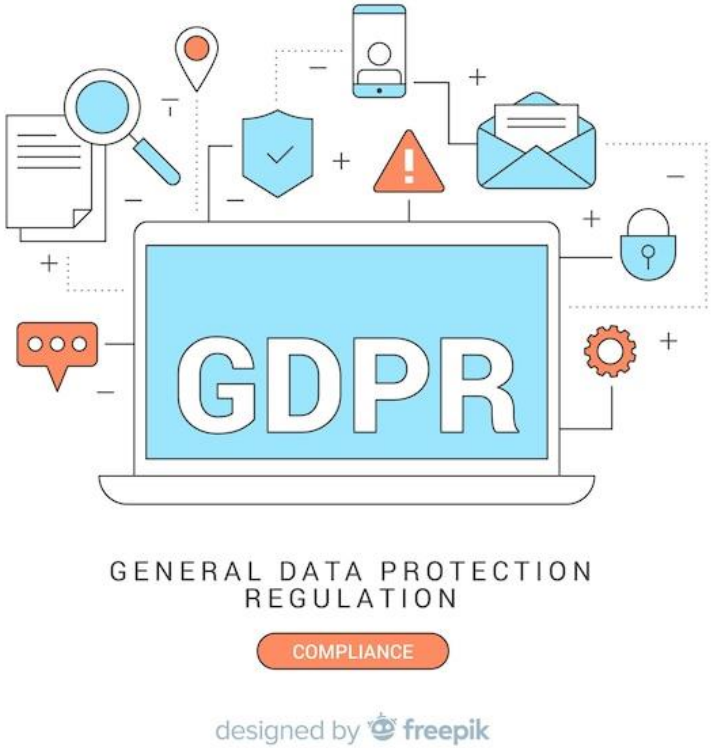


Imagen en Freepik

Unidad 6

Cómo protegerse de antemano

Objetivos

Al terminar esta unidad, sabrás:

✓ Cómo puedes protegerte identificando sitios seguros, enlaces, cookies, consentimientos

Cofinanciado por la Unión Europea

Algunos ejemplos para que estés seguro (1/3)

- Evita pagar a alguien mediante transferencia bancaria, giro postal o tarjetas regalo. Los estafadores suelen solicitar este tipo de pagos, ya que no dejan rastro en papel.
- Nunca compartas tus contraseñas con nadie en Internet. Sólo con la persona de confianza.
- Se escéptico ante cualquier cosa urgente. Los estafadores suelen querer que actúes antes de que tengas tiempo de pensar críticamente sobre la situación. Recuerda hacer una pausa y quizás alejarte del ordenador en lugar de dejarte llevar por el pánico si crees que algo es sospechoso y no estás seguro de cómo proceder.
- Haz clic inmediatamente en la X o en No para cerrar cualquier sitio web o ventana emergente sobre virus o sorteos.

Algunos ejemplos para que estés seguro (2/3)

- Llama a un ser querido o busca consejo en Internet (por ejemplo, escribiendo "Necesitamos apoyo urgentemente.."
- Comprueba en Google si otras personas han denunciado este tipo de estafas.
- Asegúrate de que los sitios web llevan la indicación **https://** delante. La "**s**" indica que el sitio es seguro. El nombre también debe tener un pequeño candado al lado.
- Desconfía de todo lo que parezca demasiado bueno para ser verdad.
- Considera la posibilidad de activar la autenticación multifactor. Esto requiere que introduzcas un código (enviado por mensaje de texto o correo electrónico) o que utilices una aplicación para acceder a algunas de tus cuentas, incluidas las redes sociales o los portales bancarios. Esto puede impedir que los piratas informáticos inicien sesión.

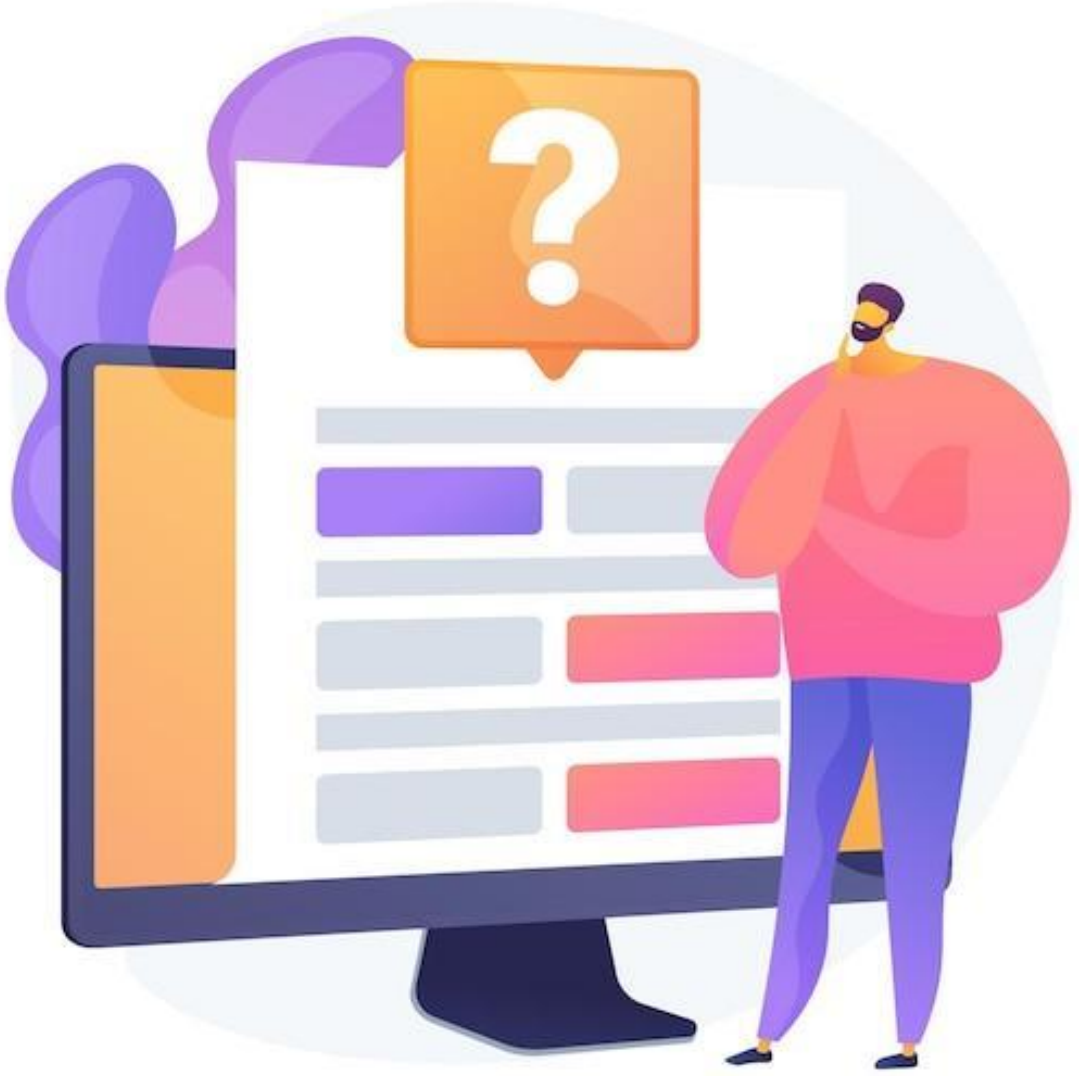
Algunos ejemplos para que estés seguro (3/3)

- Se pueden tomar más precauciones para evitar estafas.
- Nadie tiene por qué tener miedo de seguir utilizando Internet, siempre que esté equipado con los conocimientos necesarios para usarla con seguridad.
- Busca un espacio seguro en tu comunidad o círculo social donde puedas sentirte cómodo hablando de estos temas sin miedo a ser juzgado.

Si ya se ha producido una estafa, aquí tienes algunas medidas que puedes tomar:

- Llama a tu banco. Pueden congelar tu cuenta para que nadie pueda acceder a tus fondos y también emitirte una nueva tarjeta de débito. Si ya te han robado dinero, puedes ver si el banco puede anular esas transacciones y devolverte los fondos.
- Considera la posibilidad de presentar una denuncia policial.

¡Comprueba lo aprendido!



Co-funded by the European Union

1. ¿Cuál de las siguientes contraseñas es más segura?

Sólo hay una respuesta correcta.

A. John1234

B. John1990

C. John051190

D. J0Hn!2nO

2. ¿Cuál de los siguientes es un dato personal

Sólo hay una respuesta correcta.

A. Dirección IP

B. Dirección de correo electrónico

C. Todas

D. Cookies IDs en el navegador

3. Cuando aparece el símbolo del candado en el navegador significa que éste ha bloqueado la página porque no es segura.

Sí, la afirmación es correcta.

No, la afirmación es errónea.

4. ¿Cuál de los siguientes NO es un dato personal sensible

Sólo hay una respuesta correcta.

A. Fotos

B. Domicilio

C. Datos relacionados con la salud

D. Opiniones políticas

5. ¿Puede el remitente ser un indicador de si un correo electrónico es spam?

Sí

No

6. ¿Qué no debes hacer nunca si recibes un supuesto correo basura?

Sólo hay una respuesta correcta.

A. Borrar el correo electrónico

B. Comprobar el remitente

C. Comprobar online de referencia

D. Responder y preguntar si se trata de un correo basura

MOBILE MONEY

¡Enhorabuena!

Has completado este módulo.

Cofinanciado por la Unión Europea

Financiado por la Unión Europea. No obstante, los puntos de vista y opiniones expresados son exclusivamente los del autor o autores y no refl necesariamente los de la Unión Europea ni los de la Agencia Ejecutiva en el Ámbito Educativo y Cultural Europeo (EACEA). Ni la Unión Europea EACEA pueden ser consideradas responsables de las mismas. Número de proyecto: 2023-1-RO01-KA220-ADU-000157797