

**secureIT · Materiales del curso para el docente**

Autodefensa digital para estudiantes

13 lecciones · aprox. 90 minutos de clase · 26 actividades interactivas · Versión: 09/10/2026

Lo que tienes que saber sobre phishing, redes sociales, videojuegos y tus datos para moverte seguro por internet.

Cómo funciona el curso

Usted dirige el curso en la pizarra y decide cuándo trabajar cada lección; el curso no caduca. En la primera clase, el grupo se inscribe por código QR; basta con el nombre de pila para participar. Usted activa las actividades interactivas una a una, la clase responde en el móvil y, con «Resolver», la respuesta correcta aparece a la vez en la pizarra y en todos los móviles. La clave de respuestas de todas las preguntas está en su Cockpit; este PDF público no la incluye a propósito para que no llegue antes a la clase. Al final, usted cierra el curso y con ello inicia el entrenamiento de phishing: un escenario de prueba de phishing de secureIT con tres intentos de estafa por correo electrónico simulados y elaborados de forma profesional. Solo puede participar el alumnado que tenga el consentimiento de sus padres (modelo: carta a las familias) y haya indicado una dirección de correo. El certificado acredita la participación con éxito en este entrenamiento y solo se emite si se participa.

Qué necesita: un proyector o una pantalla con acceso a internet y la clase con smartphones. Quien no tenga móvil participa con su compañero de al lado.

Relación con el plan de estudios de Baden-Württemberg

De 8.º a 10.º curso (unos 13 a 16 años) · Duración: dos sesiones dobles o cuatro sencillas, lecciones utilizables por separado · Versión de 03.10.2026

Encaja en Informatik und Medienbildung (Informática y Educación Mediática), en horas de sustitución y de proyecto, y como pieza de la perspectiva transversal en Alemán, Ciencias Sociales, Economía y Orientación Profesional (WBS) y Ética. Ámbitos de acción





de la perspectiva rectora «Vivir y aprender en un mundo digitalizado»: Actuar con responsabilidad y protegerse, Comunicarse, cooperar y actuar en digital, Recopilar, comprender y evaluar información.

Ámbito	Competencia (guía de lectura de Informática y Educación Mediática 2026/27 o plan de estudios 2016)
Comunicación y seguridad	Explicar los motivos personales para proteger el propio acceso; describir y aplicar medidas para protegerlo Lecciones: Contraseñas y cuentas, Proteger tu smartphone
Comunicación y seguridad	Describir internet como red mallada y el recorrido de un mensaje; principio cliente-servidor; comparar lugares de almacenamiento (dispositivo, servidor, nube) según disponibilidad, seguridad y operador Lecciones: ¿Dónde está ahora mi mensaje? Cómo funciona internet
Comunicación y seguridad	Nombrar motivos y ejemplos cotidianos de cifrado; describir el cifrado de transporte y de extremo a extremo; aplicar el cifrado César y valorar su seguridad Lecciones: Cifrado: el candado del navegador y el truco de César
Digitalidad y participación	Nombrar situaciones en las que se recogen datos personales; explicar los intereses de los actores; reflexionar sobre el propio uso de los medios desde la autodeterminación informativa Lecciones: Qué sabe internet de ti, Redes sociales, Tus datos, tus derechos
Digitalidad y participación	Detectar indicios de desinformación; analizar fake news y deepfakes Lecciones: Perfiles falsos e ingeniería social, Deepfakes y voces falsas
Digitalidad y participación	Identificar modelos de monetización de los videojuegos; reflexionar sobre el propio uso Lecciones: Videojuegos: robo de cuentas, estafas y fraude dentro del juego
Perspectiva transversal de Educación Mediática	Autodeterminación informativa y protección de datos, protección de menores en los medios, comunicación y cooperación, fundamentos de informática



**Curso de
ampliación de
Informática,
3.1.3
Ordenadores y
redes / 3.1.4
Sociedad de la
información y
seguridad de los
datos**

Estructura de las redes informáticas; (1) motivos para cifrar, (2) cifrado César, (3) ataques de fuerza bruta, (4) aspectos de seguridad de los dispositivos móviles y medidas de protección, (6) generación de datos personales, beneficios y riesgos

Esta correspondencia es una valoración profesional del proveedor, no una aprobación oficial. Para los cursos 8.º a 10.º rige el plan de estudios de 2016 hasta la entrada en vigor del plan de Informática y Educación Mediática (2027/28).

Resumen de las lecciones

Lección		Actividades interactivas
1.	Introducción: ¿qué sabe internet de ti? Curso 5/6 · Digitalidad y participación Por qué la autodefensa digital te afecta y qué pasa en este curso.	Nube de palabras, Quiz
2.	Redes sociales: lo que tus apps saben de verdad sobre ti Curso 5/6 · Digitalidad y participación Instagram, TikTok, Snapchat: cómo recopilan y usan tus datos las plataformas.	Quiz
3.	Tus datos, tus derechos: lo que dice la ley Curso 5/6 · Digitalidad y participación Qué tiene que ver la protección de datos contigo y qué derechos tienes.	Quiz
4.	Protección de datos en el trabajo: por qué los secretos valdrán dinero más adelante Complemento · Práctica de protección de datos (currículo de 2016, 3.1.4 (6)) El juego de la protección de datos. Encontrar pistas en un perfil y tender el puente a la vida laboral.	Juego: datenschutz, Juego: orion, Quiz, Quiz
5.	Perfiles falsos, catfishing e ingeniería social Curso 7 · Digitalidad y participación Cómo los estafadores se hacen pasar por otros e intentan manipularte.	Nube de palabras, Quiz





6.	Deepfakes y voces falsas: no te fíes de todo lo que ves y oyes Curso 7 · Digitalidad y participación Cómo la IA falsifica vídeos y voces que parecen auténticos, y cómo no dejarte engañar.	Quiz, Juego: faktencheck
7.	Videojuegos: robo de cuentas, estafas y cómo protegerte Complemento · Práctica: estafas cotidianas Por qué tu cuenta de juegos vale mucho y cómo intentan robarla los estafadores.	Quiz
8.	¿Dónde está ahora mi mensaje? Cómo funciona internet Curso 5/6 · Comunicación y seguridad Nodos, routers, servidores: qué camino sigue un mensaje, qué son un cliente y un servidor, y por qué el lugar de almacenamiento decide quién puede ver tus datos.	Quiz, Quiz, Nube de palabras
9.	Cifrado: el candado del navegador y el truco de César Curso 7 · Comunicación y seguridad Por qué WhatsApp y el candado del navegador te protegen, qué significa «de extremo a extremo» y cómo cifrar y descifrar tú mismo con el truco de César.	Quiz, Quiz, Nube de palabras
10.	Contraseñas y cuentas: lo que es tuyo y lo que nunca compartes Curso 5/6 · Comunicación y seguridad Por qué cada contraseña tiene que ser única y qué aporta la autenticación de dos factores.	Juego: password-knacker, Quiz
11.	Proteger tu smartphone: PIN, apps y permisos Curso 5/6 · Comunicación y seguridad Por qué tu móvil es tu dispositivo más importante y cómo protegerlo bien.	Juego: berechtigungen, Quiz
12.	Reconocer el phishing, aunque parezca tu juego favorito Complemento · Práctica: phishing Así reconoces mensajes y enlaces falsos antes de pulsar en ellos.	Juego: phishing-duell, Quiz
13.	Resumen: tu caja de herramientas digital Complemento · Resumen Todo lo importante de un vistazo y la preparación para la prueba práctica de phishing.	Nube de palabras

En las páginas siguientes aparece cada lección completa, con todas las preguntas y opciones de respuesta. Las soluciones marcadas solo están en su Cockpit.



1. Introducción: ¿qué sabe internet de ti?

Por qué la autodefensa digital te afecta y qué pasa en este curso.

Bienvenido a la autodefensa digital

Antes de empezar, una pregunta sincera: ¿cuánto sabe internet de ti en realidad? Probablemente más de lo que crees y, sobre todo, más de lo que nunca has puesto ahí conscientemente.

Nube de palabras

¿Qué tiene que quedar privado sí o sí para ti?

De qué trata este curso

En las próximas sesiones no se trata de tecnología, sino de ti: cómo consiguen desconocidos tus datos, qué hacen con ellos y cómo lo evitas. Vamos a ver las redes sociales, los videojuegos, tu smartphone, tus contraseñas y, al final del todo, recibirás sin aviso algunos correos falsos, para ver si lo has aprendido.

Importante

Todo lo que subes a internet lo pueden encontrar desconocidos. Aunque creas que solo lo ven tus amigos.

Por qué esto ya es importante ahora

Imagina que alguien conoce tu nombre completo, tu centro escolar, tu juego favorito y el nombre de tu mascota. ¿Parece inofensivo? Con esa información, alguien puede:



- **Adivinar tu contraseña** (muchas personas usan el nombre de su mascota)
- Escribirte un **mensaje falso** que encaja exactamente con tus intereses
- **Hacerse pasar por tu amigo** y engañar a otras personas

No es teoría, pasa todos los días, miles de veces. Y justo por eso estás aquí.

Pregunta de quiz

¿Cuáles de estos datos no deberías publicar nunca en abierto?

Opciones de respuesta
Tu canción favorita
Tu número de móvil
Tu fecha de nacimiento con el año
Tu película favorita
Tu dirección
El nombre de tu centro escolar y tu clase

Consejo

Regla práctica: todo lo que permita a alguien encontrarte, contactarte o hacerse pasar por ti no debe estar en un perfil público.



2. Redes sociales: lo que tus apps saben de verdad sobre ti

Instagram, TikTok, Snapchat: cómo recopilan y usan tus datos las plataformas.

Tu perfil es solo la superficie

Publicas una foto, das like a un reel, haces scroll en TikTok. Parece inofensivo. Pero detrás de cada deslizamiento, las plataformas recopilan datos sobre ti, muchos más de los que crees.

Lo que Instagram, TikTok y compañía guardan sobre ti

Lo que haces	Lo que guarda la app
Ver un reel	Cuánto tiempo lo ves, si pasas al siguiente o lo vuelves a ver
Publicar una foto	Ubicación, hora, tipo de dispositivo, quién la ve
Seguir a alguien	Tu red social, quién conoce a quién
Escribir en la app	Incluso los textos que no envías se registran en parte
Llevar el móvil encima	Perfil de movimientos a partir de los datos de ubicación

Importante

TikTok, por ejemplo, recoge según su propia política de privacidad: ID del dispositivo, dirección IP, pulsaciones de teclado, historial de navegación dentro de la app, datos biométricos (rasgos de la cara y de la voz) y ubicación. Y eso es solo lo que reconocen oficialmente.

¿Por qué es un problema?



1. El producto eres tú. Las apps son gratis porque pagas con tus datos. Cuanto más saben de ti, más dirigida es la publicidad que te pueden mostrar y más dinero ganan.

2. Los datos se pueden robar. Cuando hackean una plataforma, tus datos acaban en la dark web. Eso ya ha pasado con TikTok, Facebook, Instagram y Snapchat, varias veces, con millones de cuentas.

3. Tu huella digital se queda. Lo que publicas hoy puede aparecer dentro de diez años, en una solicitud de empleo, de una beca o en una discusión.

Lo que puedes hacer

- **Poner tu perfil en privado:** se puede en Instagram, TikTok y Snapchat
- **Desactivar la ubicación:** la mayoría de las apps no necesitan de verdad tu ubicación
- **Revisar los permisos:** ¿de verdad necesita TikTok acceder a tus contactos?
- **Limpiar las publicaciones antiguas con regularidad:** lo que tenía gracia hace dos años no tiene por qué estar en internet para siempre

Consejo

Ve ahora a los ajustes de tu móvil → Aplicaciones → Permisos. Mira qué app puede acceder a qué. Te vas a sorprender.

Acertijo: detective de datos

Alguien publica en Instagram:

- Un selfi delante del instituto (el nombre del centro se ve en el cartel)
- Una historia con «¡Por fin 16! 🎉» el 15 de marzo
- Bio: «Gaming 🎮 | Maguncia | @max_gamer en Discord»





¿Qué información podría juntar un desconocido a partir de esto?

Pregunta de quiz

¿Qué recopilaba normalmente una app de redes sociales sobre ti?

Opciones de respuesta

Tu ubicación

Cuánto tiempo ves cada vídeo

Tu agenda de contactos, si lo permites

Solo lo que publicas tú

3. Tus datos, tus derechos: lo que dice la ley

Qué tiene que ver la protección de datos contigo y qué derechos tienes.

La protección de datos no es aburrida, te protege

Si alguien te hace una foto y la publica sin tu permiso, no solo es de mala educación: en la mayoría de los casos es **ilegal**. El Reglamento General de Protección de Datos (RGPD) y el derecho a la propia imagen (en Alemania, *Recht am eigenen Bild*) te dan derechos de verdad.

Tus derechos más importantes

- 1. Derecho de acceso:** puedes saber qué datos guarda un servicio sobre ti. En Instagram, TikTok y compañía puedes pedir una copia de tus datos, y te sorprenderá todo lo que hay.
- 2. Derecho de supresión:** puedes exigir que se borren tus datos. Eso vale también para fotos y vídeos tuyos que hayan publicado otras personas.
- 3. Derecho a la propia imagen:** nadie puede publicar fotos o vídeos tuyos sin tu consentimiento. Eso vale también en el centro, en las fiestas y en el club deportivo.
- 4. Derecho al olvido:** los buscadores tienen que retirar, si lo pides, los enlaces a información tuya desfasada o irrelevante.

Lo que los demás no pueden hacer

Situación	¿Está permitido?
Un compañero publica una foto tuya sin preguntar	☐
Alguien reenvía tu chat privado	☐
Una app pasa tus datos a redes publicitarias sin informarte	☐



Situación	¿Está permitido?
Tus padres miran tu móvil (eres menor de 18)	☐ Zona gris, depende de la edad y del contexto

Importante

«No tengo nada que esconder» no es un argumento. Protección de datos no significa que escondas algo. Significa que **decides tú** quién sabe qué de ti.

Lo que puedes hacer si se vulneran tus derechos

1. **Hablar directamente con la persona:** «Por favor, quita la foto».
2. **Denunciarlo en la plataforma:** todos los grandes servicios tienen funciones para denunciar
3. **Implicar a tus padres o a un docente:** sobre todo si se trata de acoso
4. **Presentar una reclamación oficial:** ante la autoridad de protección de datos (en Alemania, la de tu estado federado; es gratis)

Consejo

Haz capturas de pantalla como prueba **antes** de pedir que lo borren. Una vez borrado, ya no se puede demostrar nada.

Cuestionario: tus derechos

¿Es verdad? Debatidlo en clase.

1. «Si tengo menos de 16 años, las redes sociales necesitan el consentimiento de mis padres».
2. «Lo que he publicado una vez en internet no lo puedo borrar nunca».





3. «Mi profesor puede grabarme en clase sin permiso».
4. «Si un amigo conoce mi contraseña e inicia sesión, eso no es hackear».

Pregunta de quiz

¿Qué derechos tienes frente a un proveedor que ha guardado datos sobre ti?

Opciones de respuesta

Puedes saber qué está guardado

Puedes exigir que se borre

Puedes hacer que se corrijan datos erróneos

Tienes que ser mayor de edad para ello



4. Protección de datos en el trabajo: por qué los secretos valdrán dinero más adelante

El juego de la protección de datos. Encontrar pistas en un perfil y tender el puente a la vida laboral.

De tu perfil al secreto empresarial

Hasta ahora se trataba de ti en lo privado. Ahora llega la parte que te alcanzará más adelante en el trabajo.

Quien hace unas prácticas, una formación profesional o tiene su primer empleo tiene de repente acceso a cosas que no son tuyas: datos de clientes, precios, planos, historiales médicos, datos de acceso. Para eso, los atacantes casi nunca van a por la tecnología, van a por las **personas**. Y empiezan justo donde estábamos hace un momento: en el perfil público.

Importante

El método es siempre el mismo: primero reunir lo que es público. Luego escribir un mensaje que encaje exactamente. Cuando alguien te habla como si te conociera, compruebas menos.

Cómo funciona un ataque real

1. Alguien averigua dónde trabajas; basta con una foto con la camiseta de la empresa
2. Ve quién es tu jefe, cuándo son las vacaciones, cómo están formadas las direcciones de correo
3. Entonces llega un correo: «Un favor rápido, estoy en el tren, lo necesito urgentemente»



4. Y como todo cuadra (nombre, tono, momento), alguien simplemente lo hace

Esto se llama fraude del CEO y cuesta cada año sumas enormes a las empresas alemanas. Todo empezó con información visible públicamente.

El juego de la protección de datos

Tu docente desbloquea ahora el juego. Veréis el perfil público de una persona inventada. Vuestra tarea: encontrar todo lo que un desconocido podría aprovechar.

Juego didáctico

Desbloquear y proyectar el código QR. En la pizarra se ve en directo quién ha encontrado cuánto y

Complemento

Después del juego merece la pena preguntar a la clase: ¿cuáles de estos nueve datos son públicos en vuestro caso? Por experiencia, en ese momento se hace un gran silencio.

Y ahora, a la oficina: Operación ORION

El perfil era privado. Ahora, lo mismo en un puesto de trabajo. En «Operación ORION» os coláis en una oficina de lo más normal y buscáis los puntos donde un atacante podría actuar: la nota adhesiva en el monitor, el correo abierto, el pendrive del stand de la feria, la reunión en la que se habla demasiado alto.

Juego didáctico

Unos cinco minutos por partida. Sujetar el móvil en horizontal. En la pizarra verá quién



Importante

Cada hallazgo por separado parece inofensivo. Lo peligroso es la suma: una nota más una pantalla desbloqueada más una reunión escuchada por casualidad dan un acceso completo.

Lo que esto significa para más adelante

- **Lo que no es tuyo, no lo compartes:** tampoco «solo un momento» con tus amigos
- **Nada del trabajo en chats privados:** ni capturas de pantalla, ni fotos de la pantalla
- **Los datos de acceso son personales.** Quien pasa sus datos de acceso responde de lo que se haga con ellos
- **Ante la duda, preguntar:** por otro canal, no respondiendo al correo

Pregunta de quiz

Estás haciendo unas prácticas. ¿Qué puedes publicar en abierto?

Opciones de respuesta

- Que estás haciendo prácticas en una empresa
- Una foto de tu pantalla con la lista de clientes
- El nombre de usuario que te han dado
- Que te gusta el trabajo
- Capturas de pantalla del chat interno

Pregunta de quiz

Un correo de «tu jefe»: urgente, breve, supuestamente desde el móvil,





pidiendo una transferencia. ¿Qué haces?

Opciones de respuesta

Hacerlo enseguida, es el jefe

Preguntar respondiendo al correo

Comprobarlo por otra vía, por ejemplo llamando

Pedir a una compañera o un compañero que lo revise contigo



5. Perfiles falsos, catfishing e ingeniería social

Cómo los estafadores se hacen pasar por otros e intentan manipularte.

No todo el mundo es quien dice ser

Recibes una solicitud de amistad de alguien con una foto de perfil simpática, amigos en común e intereses parecidos. Todo parece auténtico. Pero ¿lo es?

¿Qué es un perfil falso?

Un perfil falso es una cuenta creada por alguien que se hace pasar por otra persona. Ocurre en **todas** las plataformas:

- **Instagram:** fotos de perfil copiadas, identidades inventadas
- **Snapchat:** cuentas que se hacen pasar por compañeros de clase
- **Discord:** desconocidos que se ganan la confianza en servidores de juegos
- **TikTok:** comentarios de cuentas falsas que te atraen a otras plataformas

Catfishing: cuando alguien falsifica una identidad entera

Catfishing significa que alguien construye una identidad falsa durante mucho tiempo, a menudo con fotos robadas, historias inventadas y mucha paciencia. El objetivo:

- Sacarte **información personal** (dirección, centro, rutina diaria)
- **Ganarse tu confianza:** para luego exigirte dinero o imágenes
- **Manipuarte:** llevarte a hacer cosas que nunca harías

Importante

El catfishing no es un caso aislado. Según un estudio, uno de cada tres jóvenes ya ha tenido que ver con perfiles falsos. Cuanto más joven es el grupo al que apuntan, más agresivos son los autores.

Ingeniería social: el arte de la manipulación

Se llama ingeniería social cuando alguien usa trucos psicológicos para que hagas o reveles algo. Las palancas más habituales:

Truco	Ejemplo
Prisa	«¡Rápido, van a bloquear tu cuenta!»
Ganas de ayudar	«¿Me pasas un momento tu contraseña? Estoy probando una cosa».
Autoridad	«Soy el admin de este servidor, necesito tus datos».
Curiosidad	«Oye, ¿eres tú el de este vídeo?» + enlace
Miedo	«Tengo capturas tuyas. Paga o las publico».

Cómo protegerte

- **Ningún desconocido necesita tu contraseña.** Nadie. Ni un admin, ni el soporte, ni un amigo
- **Comprobar por otro lado:** ¿conoces de verdad a esa persona? Pregunta por otro canal
- **Revisar las imágenes:** clic derecho → búsqueda de imágenes. Las fotos de perfil robadas suelen aparecer varias veces
- **Nada de imágenes privadas a desconocidos:** tampoco a «amigos» que solo conoces de internet
- **Bloquear en vez de discutir:** si algo te parece raro, bloquea enseguida

Consejo

Una prueba sencilla: pide a la persona que, en una videollamada, escriba una palabra concreta en un papel y lo enseñe. Los perfiles falsos fallan siempre.



Cuestionario: ¿auténtico o falso?

Alguien te escribe en Instagram: «Hola, soy nuevo en tu instituto y todavía no conozco a nadie. ¿Me das tu número para que quedemos?».

¿Qué haces?

- ☐ Mandar mi número, parece majo
- ☒ Preguntar: «¿En qué clase estás?» y comprobarlo con compañeros
- ☐ Ignorarlo
- ☒ Revisar el perfil: ¿desde cuándo existe? ¿Cuántas publicaciones y seguidores tiene?

Nube de palabras

¿En qué notas que un perfil podría ser falso?

Pregunta de quiz

Un perfil nuevo te escribe. ¿Qué te hace desconfiar?

Opciones de respuesta

- | |
|---|
| Pocas publicaciones, pero muchísimos seguidores |
| Quiere pasarse enseguida a otra app de mensajería |
| Tiene foto de perfil |
| Pregunta muy pronto por detalles personales |
| Todas las fotos parecen sacadas de un catálogo |



6. Deepfakes y voces falsas: no te fíes de todo lo que ves y oyes

Cómo la IA falsifica vídeos y voces que parecen auténticos, y cómo no dejarte engañar.

Cuando tus ojos y oídos te engañan

Antes valía: un vídeo o un mensaje de voz es una prueba. Hoy ya no. La inteligencia artificial puede falsificar caras y voces tan bien que casi no se ve ni se oye la diferencia. Esto se llama **deepfake** (vídeo/imagen falsificados) y **clonación de voz** (voz clonada).

Dónde te lo encuentras

- **Vídeos falsos de famosos:** una estrella o un streamer anuncia supuestamente un «sorteo gratis», pero en realidad es un montaje con IA que te lleva a una web de estafa.
- **Voces clonadas:** con unos pocos segundos de un mensaje de voz, la IA crea una copia de tu voz. Luego «tu amigo» llama y pide ayuda urgente.
- **«Mamá, tengo un móvil nuevo»:** un mensaje o una llamada con una voz conocida pide dinero o una contraseña. Un truco viejísimo, ahora mucho más convincente con IA.

Importante

Una voz o una cara **ya no es una prueba** de quién escribe o llama de verdad. No te fíes de eso, sino del camino por el que te llega el mensaje.

Cómo reconocer el truco

No por cómo se ve, eso cada vez está mejor hecho. Sino por **cómo se desarrolla**:



- De repente es **superurgente**.
- Tienes que **guardar el secreto** («no se lo digas a nadie»).
- Llega por una **vía poco habitual**.

Así te proteges

- **Acordar una palabra clave:** pacta con tu familia y tus amigos una palabra secreta para emergencias. Quien no la sepa no es quien dice ser.
- **Devolver la llamada:** al número que ya conoces, no al del mensaje.
- **No creerte nada solo porque parezca real:** las imágenes, los vídeos y las voces se pueden falsificar.

Pregunta de quiz

Recibes un mensaje de voz. La voz suena exactamente como tu mejor amigo y te pide con urgencia tu contraseña. ¿Qué haces?

Opciones de respuesta

Mandar la contraseña, la voz es la suya

Devolver la llamada al número conocido o preguntar en persona

Desconfiar si es «urgente» y tiene que quedar en secreto

Hacer enseguida lo que dice la voz

Juego didáctico

¿Real o falso? Mirad juntos ejemplos de imágenes, vídeos y mensajes y decidid qué es real y qué no.



7. Videojuegos: robo de cuentas, estafas y cómo protegerte

Por qué tu cuenta de juegos vale mucho y cómo intentan robarla los estafadores.

Tu cuenta vale dinero de verdad

Has invertido cientos de horas en tu juego. Skins, rangos, objetos, quizá incluso cosméticos raros. Lo que a lo mejor no sabes: en el mercado negro, estas cuentas tienen un valor real en dinero. Una cuenta de Fortnite con skins raras se vende por 50-500 €. Un inventario de CS2 con skins de cuchillo puede valer miles.

Y justo por eso las cuentas de juegos son un objetivo muy buscado.

Las estafas más habituales

1. «V-Bucks / Robux / monedas gratis»

Ves una web o un vídeo de YouTube que promete moneda del juego gratis. «Solo» tienes que introducir tu nombre de usuario y tu contraseña. Lo que pasa de verdad: tu cuenta desaparece.

Importante

No existen V-Bucks, Robux ni otra moneda de juego gratis fuera de las tiendas oficiales. Toda web que lo promete es una estafa.

2. Estafas de intercambio

«Te cambio mi objeto raro por el tuyo». El intercambio empieza, pero en el último momento cambian el objeto o manipulan el trato. Muy extendido en: Rocket League, CS2, Roblox.



3. Soporte falso

Recibes un mensaje: «Tu cuenta ha sido denunciada por hacer trampas. Haz clic aquí para verificarla o será bloqueada». El enlace lleva a una página de inicio de sesión falsa.

4. Phishing por Discord

«Oye, me falta uno para mi equipo. ¡Apúntate en esta web de torneos!». El enlace parece una plataforma de eSports real, pero es una copia que intercepta tu contraseña.

Cómo entran los atacantes en tu cuenta

Método	Cómo funciona
Enlace de phishing	Página de inicio de sesión falsa que parece auténtica
Adivinar la contraseña	Porque usas la misma en todas partes
Robar el token de sesión	Mediante extensiones del navegador manipuladas
Ingeniería social	«Soy mod, necesito tus datos de acceso»

Así te proteges

- **Activar la autenticación de dos factores (2FA):** en Steam, Epic, Riot, Blizzard, donde se pueda
- **Una contraseña única** para cada cuenta de juegos
- **Nunca compartir tus datos de acceso en Discord, TeamSpeak ni en el chat**
- **Usar enlaces oficiales:** no buscar en Google, sino escribir tú mismo la dirección
- **Revisar las extensiones del navegador:** instalar solo lo que de verdad necesitas

Consejo

Activa la 2FA. Ya. En serio. Tardas dos minutos y tu cuenta pasa a ser muchísimo más segura. En Steam se llama «Steam Guard», en Epic «autenticación de dos



factores», en Riot «aplicación de autenticación».

Acertijo: descubre la estafa

Recibes este mensaje en Discord de alguien que conoces de un servidor de juegos:

«¡Tío, he encontrado un patrocinador para nuestro equipo! Solo tenemos que registrarnos todos en esta web: esport-turniere.net/anmelden. ¡Date prisa, que las plazas son limitadas!»

¿Cuáles son las señales de alarma?

Pregunta de quiz

Una web te promete moneda del juego gratis si inicias sesión. ¿Qué es cierto?

Opciones de respuesta

Siempre es una estafa

A veces funciona

Después tu cuenta habrá desaparecido

El correo electrónico vinculado también está en peligro



8. ¿Dónde está ahora mi mensaje? Cómo funciona internet

Nodos, routers, servidores: qué camino sigue un mensaje, qué son un cliente y un servidor, y por qué el lugar de almacenamiento decide quién puede ver tus datos.

No es un cable, es una red

Mucha gente se imagina internet como un cable: de tu móvil al móvil de tu amiga. En realidad es una **red mallada** de millones de nodos: tu móvil, el router wifi, el proveedor, ordenadores de conmutación, cables submarinos, centros de datos, otro proveedor, un router, un móvil.

Tu mensaje se divide en pequeños paquetes. Cada paquete salta de nodo en nodo, y cada nodo solo decide: «¿Adónde ahora?». Si un camino falla, los paquetes toman otro. Por eso la red sigue funcionando aunque se rompa un cable en algún sitio.

Importante

Por el camino, tu mensaje pasa por **muchos ordenadores ajenos** que no conoces. Justo por eso el cifrado no es un capricho, sino lo que impide que otros lo lean.

Cliente y servidor

Tu móvil **pregunta** («Enséñame el vídeo», «Envía este mensaje») y un gran ordenador en un centro de datos **responde**. El que pregunta se llama **cliente**; el que responde, **servidor**. Cada app, cada página web, cada juego funciona así, aunque parezca que todo está «en tu móvil».

Y al revés: el servidor ve todo lo que le envías. Quien gestiona el servidor tiene tus datos. No es la técnica la que decide sobre la protección de tus datos, sino **el**





operador.

¿Dónde están tus cosas?

Lugar de almacenamiento	Ejemplo	¿Quién puede acceder?	Cuando lo borras
Tu dispositivo	Fotos en la galería	Tú, o quien tenga tu móvil en la mano	Desaparece (salvo las copias de seguridad)
Servidor de la red del centro	Archivos en el servidor del centro	Tú, el profesorado, el servicio informático del centro	Según las normas del centro
Servidor del proveedor	Mensajes de chat, publicaciones	Tú, los destinatarios, el proveedor	Tu copia desaparece, las de los demás se quedan
Nube	Almacenamiento en línea, copias de seguridad	Tú, el proveedor y, en su caso, las autoridades del país del servidor	A menudo solo de forma definitiva tras un plazo

Al comparar cuentan cuatro cosas: **disponibilidad** (¿puedo acceder desde cualquier sitio?), **colaboración** (¿pueden participar otros?), **seguridad** (¿quién puede leerlo o robarlo?) y **operador** (¿de quién es el servidor, en qué país está, qué normas rigen allí?).

Pregunta de quiz

¿Qué es cierto sobre el camino de un mensaje en internet?

Opciones de respuesta

Se divide en paquetes que pasan por muchos nodos

Si un camino falla, los paquetes toman otro

Hay una línea directa de móvil a móvil





Técnicamente, solo el destinatario puede ver los paquetes

Pregunta de quiz

Quieres hacer un trabajo con tres compañeros de clase. ¿Qué lugar de almacenamiento encaja mejor y en qué te fijas?

Opciones de respuesta

La nube o el servidor del centro, porque todos pueden trabajar a la vez

Mirar antes quién gestiona el servicio y dónde está el servidor

Solo en mi móvil, es lo más seguro para trabajar juntos

Da igual dónde, lo importante es que sea gratis

Nube de palabras

**¿Qué dispositivos hay en el camino entre tú y un amigo cuando chateáis?
Una palabra por respuesta.**

Consejo

Si quieres saber dónde tiene sus servidores un servicio: la política de privacidad suele indicarlo en «Alojamiento» o «Lugar de almacenamiento». Alemania o la UE significa: se aplican las normas europeas de protección de datos (el RGPD).



9. Cifrado: el candado del navegador y el truco de César

Por qué WhatsApp y el candado del navegador te protegen, qué significa «de extremo a extremo» y cómo cifrar y descifrar tú mismo con el truco de César.

¿Quién lo está leyendo?

Cada mensaje que envías pasa por decenas de ordenadores ajenos: tu wifi, el router de la cafetería, el proveedor, servidores en cualquier parte del mundo. Sin cifrado, cualquiera de ellos podría leerlo, como una postal.

El **cifrado** convierte tu texto (el **texto en claro**) en un **texto cifrado** ilegible. Solo quien tiene la **clave** correcta puede volver a hacerlo legible.

Importante

Codificar no es cifrar. Un código QR o el morse los puede traducir **cualquiera** que conozca la regla. El cifrado necesita además una **clave** que solo tienen las personas adecuadas.

Dos tipos que usas cada día

Cifrado del transporte: el candado del navegador (el «https»). Entre tu móvil y la página web nadie puede leer nada, ni siquiera en una wifi abierta. Pero: el operador de la página ve todo lo que escribes en ella.

Cifrado de extremo a extremo: WhatsApp, Signal, Threema. El mensaje se cifra en tu móvil y solo se descifra en el móvil de la destinataria. Ni siquiera el proveedor puede leerlo.





Consejo

¿No hay candado en el navegador o el navegador te advierte sobre la página? Entonces **nunca** escribas ahí una contraseña ni datos bancarios. Da igual lo auténtica que parezca la página.

El truco de César

Julio César ya cifraba mensajes: cada letra se desplaza en el alfabeto un número fijo de posiciones. La clave es ese número.

Con la clave **3**, la A se convierte en D, la B en E, la H en K:

Texto en claro: H O L A

Texto cifrado: K R O D

Pruébalo: cifra tu nombre con la clave 3 (usa el alfabeto de 26 letras, sin la Ñ). Al final del alfabeto se vuelve a empezar: la X se convierte en A.

Pregunta de quiz

Interceptas el texto cifrado **VHJXUR****. Sabes que es César con la clave 3. ¿Qué pone?**

Opciones de respuesta

SEMANA

SEGURO

SALIDA

SILLAS





Por qué César ya no sirve hoy

Solo hay **25 claves posibles**. Un atacante simplemente las prueba todas. Eso se llama **fuerza bruta**: no es listo, pero es rápido. Un ordenador lo consigue en menos de un segundo.

Aún más rápido es el **análisis de frecuencias**: en español, la E es la letra más frecuente. Así que la letra más frecuente del texto cifrado es muy probablemente la E desplazada, y ya se conoce la clave.

Importante

Exactamente lo mismo pasa con las **contraseñas cortas**: un ordenador prueba todas las posibilidades. Cuantas más claves posibles, más tarda. Por eso ganan las contraseñas largas y el cifrado moderno, con claves de cientos de cifras.

Pregunta de quiz

¿Qué es cierto?

Opciones de respuesta

Con el candado del navegador nadie puede leer nada en la wifi, pero el operador de la página sí

Con el cifrado de extremo a extremo ni siquiera el proveedor puede leer el mensaje

Un código QR es un cifrado seguro

César es seguro porque ya casi nadie lo conoce

Nube de palabras

¿Dónde te encuentras el cifrado en el día a día? Basta una palabra.



10. Contraseñas y cuentas: lo que es tuyo y lo que nunca compartes

Por qué cada contraseña tiene que ser única y qué aporta la autenticación de dos factores.

Tu contraseña es la llave de tu casa

Imagina que tienes una sola llave que abre la puerta de tu casa, tu taquilla, el candado de la bici y el vestuario. Parece práctico, hasta que la pierdes. Entonces lo pierdes todo.

Eso es justo lo que pasa cuando usas la misma contraseña en todas partes.

Por qué no basta con una contraseña

Cuando hackean una web (y pasa constantemente), los nombres de usuario y las contraseñas acaban en la dark web. Los atacantes prueban entonces esas combinaciones automáticamente en cientos de webs. Esto se llama **credential stuffing** (relleno de credenciales).

Así que si usas la misma contraseña en Instagram, en tu correo y en tu cuenta de juegos, y hackean Instagram, **las tres cuentas** están en peligro.

Importante

La regla es sencilla: **Una cuenta, una contraseña**. Ninguna contraseña puede usarse en dos servicios a la vez.

Qué hace segura una contraseña

Mala	Por qué	Mejor
JuanPerez2009	Nombre + año de nacimiento = adivinable	Correcto-Caballo-Batería-Grapa
123456789	La contraseña más común del mundo	Combinar palabras al azar
Verano2024!	Patrón que usan millones de personas	Usar un gestor de contraseñas

Una buena contraseña:

- Tiene al menos 12 caracteres
- No se puede adivinar (ni nombre, ni fecha de nacimiento, ni mascota)
- Es única para cada cuenta

El método más sencillo: coge cuatro palabras al azar y únelas: «Jirafa-Piano-Nube-Siete». Larga, fácil de recordar, segura.

Gestor de contraseñas: tu llavero digital

Un gestor de contraseñas guarda todas tus contraseñas cifradas. Solo tienes que recordar **una** contraseña maestra. El gestor genera y rellena todas las demás automáticamente.

Opciones gratuitas: Bitwarden, KeePassXC, la función de llavero de Apple/Google.

Autenticación de dos factores (2FA)

2FA significa: aunque alguien conozca tu contraseña, necesita además un segundo factor, normalmente un código en tu móvil.

Dónde deberías activar la 2FA ya mismo:

1. Tu correo electrónico (es la llave de todas tus demás cuentas)
2. Tus cuentas de juegos (Steam, Epic, Riot)
3. Redes sociales (Instagram, TikTok, Snapchat)

4. Todo lo que tenga que ver con dinero

Lo que es tuyo y lo que nunca compartes

☐ Puedes compartir	☐ Nunca compartes
Tu nombre de jugador	Tu contraseña
Tu película favorita	Tu cumpleaños con el año
Tu perfil público	Tu dirección
Capturas de pantalla (sin datos sensibles)	Tu DNI / carné de estudiante
Tu servidor de Discord	Tus datos de acceso al correo

Consejo

Tampoco con tu mejor amigo. Las amistades cambian. Las contraseñas que has compartido no se pueden «recuperar». Y a tu amigo pueden hackearlo sin que se dé cuenta, y entonces el atacante también tiene tu acceso.

Acertijo: revisión de contraseñas

¿Cuáles de estas contraseñas son seguras?

1. Futbol2009 → ☐ (palabra + año de nacimiento)
2. kT9\$mP2!xR4# → ☐ (aleatoria, pero difícil de recordar)
3. Elefante-Ketchup-Tambor-42 → ☐ (larga, aleatoria, fácil de recordar)
4. TeQuiero → ☐ (entre las 20 contraseñas más comunes)
5. qwerty → ☐ (patrón de teclado)

Juego didáctico

Inventad una contraseña y mirad cuánto aguanta. Solo se transmite el



patrón,

Pregunta de quiz

¿Qué hace realmente fuerte una contraseña?

Opciones de respuesta

La longitud

Un signo de exclamación al final

Que solo se use para un único servicio

Que la puedas recordar bien porque es tu cumpleaños

Que no aparezca en ningún otro sitio



11. Proteger tu smartphone: PIN, apps y permisos

Por qué tu móvil es tu dispositivo más importante y cómo protegerlo bien.

Tu móvil es la llave de todo

Tu smartphone no es solo un teléfono. Es tu cuenta bancaria, tu correo, tu álbum de fotos, tu GPS y tu documento de identidad, todo en uno. Quien tiene acceso a tu móvil tiene acceso a toda tu vida digital.

Protección básica: bloqueo y biometría

Método	Seguridad	Recomendación
Sin pantalla de bloqueo	Ninguna	Nunca
Patrón	Muy débil (las marcas de grasa delatan el patrón)	No
PIN de 4 cifras	Débil (10.000 posibilidades)	Mínimo
PIN de 6 cifras	Mejor (1 millón de posibilidades)	Bien
Huella dactilar	Fuerte + rápido	Recomendado
Face ID / reconocimiento facial	Fuerte (en dispositivos recientes)	Recomendado

Importante

Los **PIN más habituales** en Alemania: 1234, 0000, 1111, 2580 (línea vertical), el año de nacimiento. Si el tuyo está entre ellos: cámbialo ya.

Permisos de las apps: ¿quién puede hacer qué?

Cada app pide permisos. Pero no todas necesitan lo que piden:



- **Cámara:** Instagram la necesita, una app de linterna no
- **Micrófono:** una app de voz lo necesita, un juego no
- **Contactos:** WhatsApp los necesita, una app del tiempo no
- **Ubicación:** Google Maps la necesita, una calculadora no

Seguridad wifi: las redes abiertas son peligrosas

El wifi gratis en el tren, en una cafetería o en la estación suena genial. Pero en las redes abiertas cualquiera puede ver lo que haces. Esto se llama **ataque de intermediario** (man-in-the-middle): alguien se pone entre tú e internet y lo lee todo.

Normas para el wifi público:

- Nada de banca online ni de iniciar sesión en cuentas importantes
- Usar una VPN (hay versiones gratuitas)
- Desactivar la conexión wifi automática

Consejo

Ve a los ajustes de wifi y borra todas las redes que ya no necesites. Si no, tu móvil se conecta automáticamente a cualquier red con el mismo nombre, y un atacante puede falsificar fácilmente un «Starbucks WiFi».

Actualizaciones: la protección más aburrida y la más importante

Cada actualización cierra agujeros de seguridad conocidos. Si aplazas las actualizaciones, dejas abierta una puerta que los atacantes saben que existe.

- Instalar enseguida las **actualizaciones del sistema operativo**
- Hacer con regularidad las **actualizaciones de las apps**
- **Borrar las apps** que ya no usas: menos apps significa menos superficie de



ataque

Cuestionario: ¿qué tan seguro es tu móvil?

Compruébalo ahora en tu dispositivo:

1. ¿Tienes activado un PIN o la biometría? ☐ / ☐
2. ¿Está tu sistema operativo actualizado? ☐ / ☐
3. ¿Tienes instaladas apps que no usas desde hace meses? ☐ / ☐
4. ¿Alguna app usa permisos que no necesita? ☐ / ☐

Cada ☐ en la 1-2 y cada ☐ en la 3-4 suma un punto. Quien tiene los cuatro puntos está bien protegido.

Juego didáctico

Seis apps, seis permisos. Que vote la clase y luego comparar en la pizarra.

Pregunta de quiz

¿Qué permiso es sospechoso sin duda en una app de linterna?

Opciones de respuesta
Ubicación
Contactos
Flash de la cámara
Micrófono

12. Reconocer el phishing, aunque parezca tu juego favorito

Así reconoces mensajes y enlaces falsos antes de pulsar en ellos.

¿Qué es el phishing?

Phishing es cuando alguien se hace pasar por otra persona para conseguir tus datos. Normalmente por correo electrónico, pero también por SMS, WhatsApp, Discord o incluso como mensaje dentro de un juego.

El nombre viene de «fishing» (pescar, en inglés): el atacante lanza un cebo y espera a que alguien pique.

Así es el phishing en tu día a día

Ejemplo 1. La trampa de Steam:

«Tu cuenta de Steam ha sido suspendida por actividad sospechosa. Verifica tu identidad en un plazo de 24 horas: [steamcommuntly.com/verify](https://steamcommunity.com/verify)»

¿Ves el error? Pone «steamcommuntly» en lugar de «steamcommunity». Una sola letra de diferencia, pero acabas en una web totalmente falsa.

Ejemplo 2. El mensaje de Instagram:

«Oye, alguien ha subido un vídeo tuyo 📺 míralo: bit.ly/3xK9mP»

Los enlaces acortados ocultan adónde llevan de verdad. Y el mensaje juega con la

curiosidad y un poco de pánico.

Ejemplo 3. El correo de Spotify:

«Su método de pago ha caducado. Actualice sus datos para no perder su cuenta».

Spotify sí envía correos así, pero el correo auténtico enlaza a spotify.com, no a spotify-account-update.com.

La comprobación de 5 segundos

Antes de pulsar un enlace, detente cinco segundos y comprueba:

1. **¿Quién lo envía?** ¿Conozco de verdad a esa persona/empresa?
2. **¿Hay prisa?** «Inmediatamente», «en 24 horas», «ahora»: eso casi siempre es manipulación
3. **¿Adónde lleva el enlace?** Mantener el dedo encima (¡sin tocar!) muestra la dirección real
4. **¿Tiene sentido?** ¿Me contactaría así Steam/Instagram/Spotify?
5. **¿Pide datos de acceso?** Los servicios auténticos nunca te piden la contraseña por mensaje

Importante

Ningún servicio serio te envía un mensaje con un enlace en el que tengas que introducir tu contraseña. Si tienes dudas: abre la app o la web directamente, no a través del enlace.

¿Qué hacer si has pulsado?

Ha pasado: has pulsado un enlace de phishing y quizá incluso has introducido datos. No



hay motivo para el pánico, pero actuar rápido es importante:

1. **Cambiar la contraseña enseguida:** en el servicio afectado y en todos los sitios donde usabas la misma contraseña
2. **Activar la 2FA:** si todavía no lo has hecho
3. **Avisar a alguien:** a tus padres, a un docente, al responsable de informática. No es ninguna vergüenza, es un incidente de seguridad
4. **Avisar al banco:** si hay datos de pago afectados

Consejo

No has hecho nada mal si notificas un phishing. Haces algo mal si lo callas. Notificarlo ayuda, a ti y a los demás.

Cuestionario: ¿phishing o auténtico?

Clasifica estos mensajes. ¿Phishing o auténtico?

1. Correo de Netflix: «Tu suscripción se cancelará mañana. Haz clic aquí para actualizar tu pago».
2. SMS de DHL: «Su paquete no ha podido ser entregado. Tasa de aduana: 1,99 €. Pague aquí».
3. Correo de tu centro: «Ya están en línea los nuevos horarios de las actividades extraescolares. Mira el portal del centro».
4. Mensaje privado de Discord: «Oye, ¿eres tú el de la foto?? [\[enlace\]](#)»

Juego didáctico

Cinco mensajes, cada uno auténtico o falso. Después del juego, repasar las señales en la pizarra.





Pregunta de quiz

¿En qué reconoces con más seguridad un mensaje de phishing?

Opciones de respuesta
Te mete prisa
La dirección del remitente no coincide con el supuesto remitente
Está escrito en español
Pide tu contraseña o tus datos de pago
Tiene un logotipo

13. Resumen: tu caja de herramientas digital

Todo lo importante de un vistazo y la preparación para la prueba práctica de phishing.

Lo que has aprendido en este curso

Ahora tienes los conocimientos para protegerte mucho mejor en internet. Aquí tienes un resumen de los puntos más importantes:

Tus datos son tuyos.

- Decides tú quién ve qué
- Los datos publicados en abierto se pueden usar para estafas y manipulación
- La protección de datos es un derecho, no un lujo

Las redes sociales no son tus amigas, son un modelo de negocio.

- Las apps recopilan más datos de los que crees
- Perfil privado, ubicación desactivada, permisos revisados
- No todo lo que ves en internet es real

En los videojuegos hay dinero real y peligros reales.

- La moneda de juego gratis no existe
- Activar la 2FA, usar contraseñas únicas
- Ningún enlace de Discord o TeamSpeak es 100 % fiable

Tu móvil merece protección.

- PIN/biometría, actualizaciones, permisos de las apps
- Wifi abierto = libro abierto
- Borrar las apps viejas

Una contraseña, una cuenta.



- Usar un gestor de contraseñas
- Activar la autenticación de dos factores en todas partes
- No compartir nunca las contraseñas, tampoco con amigos

Reconocer el phishing = pensar cinco segundos.

- ¿Quién lo envía? ¿Adónde lleva el enlace? ¿Hay prisa?
- Ante la duda: no pulsar, sino abrir la web directamente
- Notificar no es una debilidad, protege a todos

Importante

La seguridad perfecta no existe. Pero con lo que sabes ahora, eres **mucho más difícil** de engañar que antes. Y de eso se trata.

Y ahora: la prueba práctica

En los próximos días recibirás **tres correos de phishing simulados** en tu dirección de correo del centro. Parecen auténticos, pero vienen de este curso.

Tu tarea: **Reconócelos y no pulses en ellos.**

Después recibirás tu resultado como informe personal. Y: aquí no se «suspende». Quien cae con un correo aprende de ello. Quien no abre ninguno ha superado el curso.

Consejo

Aplica la comprobación de 5 segundos. En cada correo sospechoso. A partir de ahora. No solo con los correos de prueba.



**Cuestionario final: 10 preguntas, ¿cuántas aciertas?**

1. ¿Cuántas contraseñas deberías usar en total?
2. ¿Qué es la 2FA?
3. ¿Qué es el catfishing?
4. ¿Por qué es peligroso el wifi público?
5. ¿Qué haces si has pulsado en un enlace de phishing?
6. ¿Puede alguien publicar una foto tuya sin preguntarte?
7. ¿Qué significa ingeniería social?
8. ¿A partir de qué edad eres penalmente responsable en Alemania?
9. ¿Cuál es la forma más segura de crear una contraseña?
10. ¿Cuál es el consejo más importante contra el phishing?

Quien acierte al menos 7 está bien preparado para la prueba práctica.

Nube de palabras

¿Qué te llevas de este curso? Basta con una palabra.