Materiales del curso para el docente

Digitale Selbstverteidigung Klasse 9/10: Angriffe erkennen

6 lecciones · aprox. 90 minutos de clase · 15 actividades interactivas · Versión: 23/11/2026

Fake-Profile, geklonte Stimmen, Betrug in Spielen, Datenschutz im Praktikum und Phishing, mit Praxistest zum Schluss.

Cómo funciona el curso

Usted dirige el curso en la pizarra y decide cuándo tratar cada lección. El curso no caduca. Este curso incluye el entrenamiento contra el phishing: una gran oportunidad para practicar lo aprendido en el propio dispositivo, en el propio buzón. Solo para ello la clase se apunta mediante un código QR en la primera hora; para participar basta el nombre. Las actividades se activan una a una: en la pizarra aparece un código QR, la clase responde desde el móvil y con «Resolver» aparece la respuesta correcta a la vez en la pizarra y en todos los móviles. Las soluciones de todas las preguntas están en su panel; este PDF abierto no las incluye a propósito para que no lleguen antes a la clase. Al final cierra el curso y con ello arranca el entrenamiento contra el phishing: tres intentos de estafa simulados por correo electrónico durante las semanas siguientes. Solo pueden participar quienes tengan el consentimiento de los padres (plantilla: carta a los padres) y una dirección de correo guardada. El certificado acredita la participación con éxito en este entrenamiento y solo se expide a quienes participan.

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

Klassen 9 und 10 (etwa 14 bis 16 Jahre) · Duración: zwei Doppelstunden plus Praxistest in den Wochen danach · Versión de 03.10.2026

Angriffe erkennen: Fake-Profile und Social Engineering, Fake-Stimmen, Betrug in Spielen, Datenschutz im Praktikum und Phishing. Schließt mit dem Phishing-Praxistest ab, mit Einverständnis der Eltern. Ámbitos de acción de la perspectiva rectora «Vivir y aprender en un mundo digitalizado»: Verantwortungsvoll handeln und schützen, Digital kommunizieren, kooperieren, handeln, Informationen sammeln, verstehen, bewerten.

Ámbito	Competencia (guía de lectura de Informática y Educación Mediática 2026/27 o plan de estudios 2016)
Digitalität und Partizipation	Akteure und Interessen; Vertrauenswürdigkeit; Desinformation und Deepfakes Lecciones: Fake-Profile, Deepfakes und Fake-Stimmen
Leitperspektive Medienbildung	Jugendmedienschutz, Informationelle Selbstbestimmung und Datenschutz, Kommunikation und Kooperation
Aufbaukurs Informatik, 3.1.4 Informationsgesellschaft und Datensicherheit	(6) Anfall personenbezogener Daten, Nutzen und Risiken

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.	**Perfiles falsos, catfishing e ingeniería social** Curso 9/10 · Digitalität und Partizipation Cómo los estafadores se hacen pasar por otros e intentan manipularte.	Quiz, Nube de palabras, Quiz
2.	**Deepfakes y voces falsas: no te fíes de todo lo que ves y oyes** Curso 9/10 · Digitalität und Partizipation Cómo la IA falsifica vídeos y voces que parecen auténticos, y cómo no dejarte engañar.	Quiz, Juego: faktencheck
3.	**Videojuegos: robo de cuentas, estafas y cómo protegerte** Complemento · Praxis Betrug im Alltag Por qué tu cuenta de juegos vale mucho y cómo intentan robarla los estafadores.	Nube de palabras, Quiz
4.	**Protección de datos en el trabajo: por qué los secretos valdrán dinero más adelante** Complemento · Praxis Datenschutz (BP 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.	**Reconocer el phishing, aunque parezca tu juego favorito** Complemento · Praxis Phishing Así reconoces mensajes y enlaces falsos antes de pulsar en ellos.	Quiz, Juego: phishing-duell, Quiz
6.	**Resumen: tu caja de herramientas digital** Complemento · Zusammenfassung 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. 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
- **Manipularte**: 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?».

Pregunta de quiz

¿Qué haces?

Opciones de respuesta
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

2. 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.

3. 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!»

Nube de palabras

¿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

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 suyas: 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. 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: steamcommunlty.com/verify»

¿Ves el error? Pone «steamcommunlty» 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]»

Pregunta de quiz

¿Cuáles de estos mensajes son phishing?

Opciones de respuesta
Netflix: suscripción cancelada, actualizar el pago
SMS de DHL: pagar 1,99 € de aduana mediante un enlace

Centro: nuevos horarios de actividades en el portal
Mensaje de Discord: «¿Eres tú el de la foto??» con 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

6. 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.