



Esta traducción se facilita a título informativo. Solo la versión alemana es jurídicamente vinculante. [Ver la versión alemana](#)

Formación en phishing y prueba de phishing: lo que le espera al claustro

Información para todos los docentes · Versión 09.10.2026

En las próximas semanas realizaremos juntos una breve formación en línea sobre phishing y seguridad informática. A continuación llegarán al buzón profesional tres correos de phishing **simulados**, para que cada persona pueda poner a prueba con calma lo aprendido. Esta hoja explica qué ocurre y qué, expresamente, no ocurre.

¿Por qué lo hacemos?

Los centros escolares son un objetivo frecuente: correos falsos del «titular del centro» (Schulträger), supuestos mensajes de la dirección del centro, un «Su contraseña del portal escolar está a punto de caducar». La tecnología intercepta mucho, pero no todo. El resto depende de nosotros. Y quien reconoce el phishing por sí mismo puede enseñárselo a la clase de forma creíble. La formación encaja con la perspectiva rectora «Vivir y aprender en un mundo digitalizado».

¿Cómo se desarrolla?

- **Primero la formación:** cada persona recibe un enlace personal al curso en línea. Duración aproximada de 45 minutos, a su propio ritmo, computable como tiempo de servicio.
- **Después la prueba:** tras el curso, en el plazo de algunas semanas, llegan tres correos de phishing simulados. Parecen auténticos, pero son inofensivos.
- **Si hace clic:** se abre una página explicativa que muestra en qué se podría haber reconocido la falsificación. Eso es todo. Un clic en falso es un momento de aprendizaje, no un fallo.
- **Certificado:** tras el curso y la prueba, usted descarga su certificado de formación personal (persona, tema, contenido, duración), para su portfolio de cualificación.

Lo que ocurre

- La dirección del centro ve quién ha finalizado el curso y cuántas personas han terminado la prueba.
- Usted ve su propio resultado.
- Su nombre y su dirección de correo electrónico profesional se guardan para el envío y el certificado, en servidores en Alemania.

Lo que no ocurre

- Nadie recibe una lista de quién hizo clic.
- Nada pasa al expediente personal, a evaluaciones del desempeño profesional ni a entrevistas sobre el rendimiento.
- Ninguna exposición ante el claustro, ningún «ranking».
- Ninguna supervisión del resto de su correo electrónico; en la simulación nunca se guarda una contraseña.

¿Qué debo hacer si un correo me parece extraño?

Exactamente lo que también sería correcto ante un ataque real: no hacer clic, no responder, notificarlo. Cómo y a quién se notifica se explica en el curso y vale tanto para los correos reales como para la prueba.

¿Preguntas? Persona de contacto en el centro: · Junta de personal (Personalrat):

La formación y la simulación las realiza secureIT UG (haftungsbeschränkt) por encargo del centro escolar, de forma gratuita para los centros. Más información sobre el desarrollo y la protección de datos: secureit.icu/schulen/datenschutz

