



This is a translation for your convenience. Only the German version is legally binding. [Go to the German version](#)

Template for the school, version as of 09.10.2026 · insert the school letterhead, fill in the blanks

(school) · Class · (date)

Teaching unit “Digital self-defence”: information for parents

Note for the teacher: this letter belongs to the course “Digital self-defence” (grades 8 to 10), the only course that includes phishing training. For “Starting out safely online” and “Media literacy”, an information letter without a consent form is sufficient.

Dear parents and guardians,

over the coming weeks, the class will learn how to protect themselves online: recognising phishing, passwords and two-factor authentication, what apps collect about us, fake profiles, deepfakes and how to use AI tools. The unit is aligned with the Baden-Württemberg curriculum (Bildungsplan; computer science and media education, guiding perspective “Living and learning in a digitalised world”) and is taught by .

The material comes from secureIT, a small provider of security training from the Breisgau region, and is made available to schools free of charge. It contains no advertising and no intention to sell.

How the lessons work

- The teacher shows the lesson on the board. The class takes part in quiz questions and learning games on their own smartphones; anyone without one joins in with their neighbour.
- A first name is all that is needed to take part. **There is no pupil account, no app and no registration by email.**
- **Phishing training at the end, only with your consent:** pupils who take part receive, after the lessons, three simulated, harmless emails from secureIT that look like professional fraud attempts. This shows whether your child recognises a staged fraud attempt. Anyone who clicks lands on a page that explains what happened; only your child sees the result, nobody else. An email address is needed for this.
- **Certificate:** the certificate confirms successful participation in the phishing training. It is therefore only given to those who take part in the training. Without taking part, your child joins in the lessons as normal but does not receive a certificate.

Data protection: the data is stored on servers in Germany, is not passed on and is not used for advertising. Passwords entered during the simulation are never stored. Certificate data is deleted automatically after 60 days. A detailed description for the data protection officer is available at secureit.icu/schulen/datenschutz; the school has a data processing agreement with the provider.

What you can do at home: ask your child about the “5-second check” (Who is sending this? Where does the link lead? Is there time pressure?). Agree on a family code word for calls from a supposedly familiar voice. And switch on two-factor authentication together for your most important accounts. You can read the course materials yourself: secureit.icu/schulen.

If you have any questions, please do not hesitate to contact me.

Kind regards

Teacher

School management (optional)





Please detach this section and return it to the teacher

Consent form for the phishing training

School: . Teacher: .

Child's name: . Class: .

☐ **Yes**, my child may take part in the phishing test scenario of secureIT UG (haftungsbeschränkt). This tests their ability to recognise a staged, professionally made fraud attempt by email (phishing training). My child may provide an email address for this purpose. If the training is carried out, my child will receive a certificate of successful participation.

☐ **No**, my child will not take part in the phishing training. They will take part in the lessons, will not provide an email address and will not receive a certificate.

Date, signature of parent/guardian

Template by secureIT UG (haftungsbeschränkt), free of charge for schools. Adaptations are expressly welcome. Source: secureit.icu/schulen

