

Information Security

To implement information security in an organization in a structured way, an Information Security Management System (ISMS) is needed. This is not a "finished" system that updates or builds itself automatically, but a systematic approach for how information security is to be built up.

An ISMS regulates and manages the planning, steering, and control tasks required to establish a well-thought-out and effective process for creating information security, and to continuously implement and improve it.

*Fabian Amon
Informationssicherheitsbeauftragter (ISB)
of Trier University of Applied Sciences*

Phishing Attacks

A supposed email from the president, a supposed call from a supplier... This is often how attackers make first contact. Through social engineering, trust is built to gather further contact details and then launch a targeted attack.

Recognizing Phishing (Email)>>>

For every email you receive, first check the sender address. Internal email addresses always contain the domain hochschule-trier.de or umwelt-campus.de. Example: you receive an email with the sender address praesidentin@hotmail.com and the display name of the president. What stands out here is the external domain: hotmail.com. This is not a university-internal domain, so this email is a phishing email. Please note that this is only an example domains such as @gmail.com etc. are also possible. Do not be misled by the display name. Even if the display name

matches the name of a university employee, the sender's email address may still be external to the university. For external email addresses, pay attention to the email address, subject line, and content. Under no circumstances click on a link in an email that seems suspicious to you. If you are unsure, you can contact the email address below at any time.

Support? Yes, gladly!>>>

Phishing attacks are not limited to emails, they can also occur by phone. Callers often pose as suppliers, service providers, or similar,

usually with a request to change bank details or addresses.

IMPORTANT! Do not disclose any personal data over the phone. Have any changes to bank details or similar confirmed by email. Check the [requested] changes against the existing master data, and contact the supplier, service provider, or similar and have the changes confirmed again by them. Use the already stored and verified contact details to do so.

Have You Fallen Victim to a Phishing Attack?>>>

If you are the victim of a phishing attack, stay calm. Immediately contact your supervisor and the Information Security team. Break off contact with the attacker immediately.

Please also refer to the following content on the university's website:

[Email Hygiene](#)
and

[Protection against Phishing emails](#)



Emergency Contact for IT Incidents

In the event of **information security incidents**, please immediately contact us by phone: +49 651 8103-777 or by mail: informationssicherheit@hochschule-trier.de