27.08.2026

Often, the greatest vulnerability are humans themselves

Criminals increasingly resort to psychological tricks nowadays to obtain confidential information. Instead of exploiting vulnerabilities, they use fake e-mails, telephone calls or messages to specifically manipulate people.

Internet scammers use convincing stories and psychological pressure to persuade their victims to disclose their passwords, click on malicious links or pass on sensitive data. Such manipulative types of attack go by the term of “social engineering”.

In the process, their methods are becoming ever more sophisticated. Thanks to artificial intelligence, messages and telephone calls appear more authentic than ever before. Increasing use is also made of faked voices, photos, videos and identities.

It is crucial to become aware of such tactics and apply a healthy dose of suspicion to recognise social engineering attacks early and react in an appropriate manner.

Would you like to learn more about current methods of attack and protective measures? Then why not take part in our webinar on “Social Engineering – Betrugsmaschen erkennen und sicher handeln” (Social Engineering – how to recognise scams and act safely)? With the help of hands-on examples, our experts will demonstrate how to effectively protect yourself, your data and your assets against brazen scamming attempts:

- Tuesday, 20th October at 1 pm (https://events.teams.microsoft.com/event/1071392a-6e09-4c1a-bcea-13e520e64d77@75a34008-d7d1-4924-8e78-31fea86f6e68)
- Wednesday, 21st October at 7 pm (https://events.teams.microsoft.com/event/545297b9-ae92-45bc-ac13-5238eaa06794@75a34008-d7d1-4924-8e78-31fea86f6e68)

Register now und improve your security skills!

Copyright – All rights reserved. Lucerne School of Information Technologies