You like to learn more about our training?

www.social-engineering.academy

Content for COVID-19

Strengthen your cybersecurity

Content for COVID-19

6. Deutscher IT-Sicherheitspreis
3. Preis 2016

Social Engineering Academy

Social Engineering Academy (SEA) GmbH
Eschersheimer Landstr. 42
60322 Frankfuhrt am Main
+49 (0) 69 9451952 40

info@social-engineering.academy

Interactive security awareness training for business departments

including customized
learning content and role plays

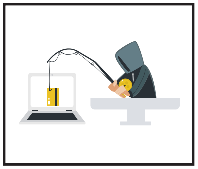
Social Engineering Academy

Preparation

Description of your work environment in a preliminary talk

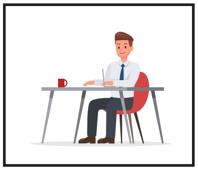
Training*)

Security awareness
and social engineering



Relevant attacks and
defense mechanisms

Exercises based on role plays



Reference to processes from
your everyday work

Follow-up

Certificate of participation, handout

*) Trainings can be conducted on-site or remotely as a webinar

Strengthen the human factor in your cybersecurity defense

Your employees as targets

In addition to your IT infrastructure, your employees are also a target for cybercriminals. In this context, a high number of attacks on the „human factor“ can be observed, with attack methods constantly evolving. For example, attacks such as spear phishing and business email compromise are tailored content-related to a targeted department. The current threat situation emphasizes the importance of employee awareness of corporate cybersecurity. Strengthen this consciousness with the help of our security awareness training.

Security awareness through practice

In our training, we provide the necessary knowledge about possible attacks relevant to a business department and train appropriate defense mechanisms. By using innovative training contents, your employees can directly apply the knowledge in their everyday work. In addition, we challenge your employees within role plays. Here, the employees are confronted with relevant attacks and have to defend the business. Constructive feedback helps them to improve their defense reactions.

Relevant training content for your business department

Since different departments are exposed to different threats, we adapt the training content to the respective threat situation. In a preliminary discussion, we determine together with you the data to be protected, the departments affected, and the communication channels and systems that could be used by attackers.