The Threat is Growing

Invest in an effective human firewall and cyber security awareness for your workforce with us.

It sounds like science fiction, but it's reality when cyber-attacks cripple entire communities and lock millions of people out of vital services at a stroke. The annual damage caused by phishing and data theft in Germany is now well over €200 billion - and rising. 58% of companies surveyed said they had been the victim of a cyber attack at least once (*statistica.com).

Security attacks continue to exploit the latest trends, leaving IT managers scrambling to implement new security measures and close potential gaps. But even the best IT protection is useless if the human factor fails. It all comes down to the knowledge and vigilance of your staff:

Without security knowledge and awareness, any technology is of limited use.

Unique partnership with HanseSecure

In order to build up this awareness in a targeted and sustainable way, companies should take no risks and rely on the many years of experience of experts. The unique partnership between soluzione and HanseSecure gives you the secure feeling of being in the best hands:

soluzione as an award-winning learning specialist with more than 15 years of well-founded competence in learning psychology.

Florian Hansemann of HanseSecure has already received several international awards as a leading expert in the field of IT security. With more than 15 published zero-days, he has also discovered vulnerabilities in major antivirus software such as McAfee and is listed among the top 21 most influential security experts worldwide.

HanseSecure
CHOOSE THE INTRUDER!

73.000+ Followers on Twitter

Keynote Speaker „Best of the World in Security“

Interviews and Live-Demos On TV und Radio

Tip: Together with HanseSecure, you can also book the following services with us:

Security news: Learn about security vulnerabilities before they become official

Security talks and **webcasts** with Florian Hansemann as keynote speaker

Three key takeaways to successfully future-proof your organization:

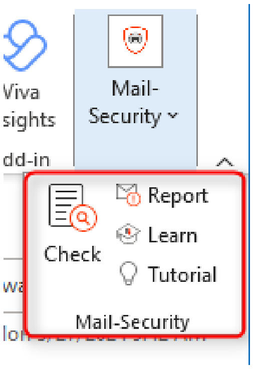
- Cyber security measures do not work in isolation – a successful strategy therefore consists of several components.
- Invest in timeliness and speed.
- Don't think of awareness training as a compliance obligation, but as an ongoing effort that empowers your workforce to become an authoritative part of the defense.

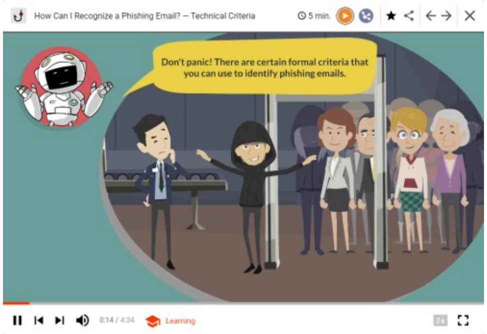
Rely on our multilayer protection

With soluzione, you will find an experienced and motivating partner for precisely these challenges. Our portfolio consists of interlocking security modules and is supported by experienced consultants:

Phishing simulations as a test for emergencies: We simulate realistic phishing attacks in different levels of difficulty on selected employees of your company (levels 1-5 including spear phishing). In the event of misconduct, they will be redirected to a social information page. Here we show how the specific attack could have been detected and offer tailor-made learning aids.

Smart Outlook Add-In: The soluzione add-in Mail Security (incl. report button) increases awareness of the topics of phishing and security in a practical way and strengthens the reporting culture. In addition, you can use statistical evaluations to assess the current probability of successful cyber security attacks more realistically.




How Can I Recognize a Phishing Email? – Technical Criteria
5 min.
Don't panic! There are certain formal criteria that you can use to identify phishing emails.
0:14 / 4:34
Learning

soluzione **e-learning** as motivating cyber security courses: Storytelling, best practices and relevant recommendations for action guarantee easy implementation in everyday work, a high level of acceptance among employees and the development of sustainable habits.

Awareness campaigns for comprehensive premium protection: Building on and in a media mix with content from the e-learning courses, we offer a 10-week awareness campaign actively supported by our security consultants, with additional awareness nuggets. This already incorporates initial results from the parallel phishing simulations. In this way, discovered vulnerabilities can be remedied in a focused and targeted manner. They close knowledge gaps and can already measure the result with upcoming simulation statistics.

Holistic and sustainable awareness training

Only through continuous training can the cybersecurity knowledge of your employees be strengthened. Promote vigilance and reporting across your organization, empowering the workforce to identify new threats and respond quickly in the event of an emergency.

- Continuing education must have positive connotations and be fun.
- Build trust by not judging employees when they report misinformation.
- Avoid stagnation - through media mix, motivating campaigns and individual learning methods.
- Analysis and continuous performance measurements allow targeted qualification measures.