DriveLock
securing your digital tomorrow

Security Awareness
Strengthen your human firewall

eBook

DriveLock
securing your digital tomorrow

Cyber defence and prevention
“It’s about protecting systems and people.”

When we talk about cyber security, the first thing we think about is technically sophisticated security measures. However, the most important security measure is people.

It would be too simplistic to regard cyber defence as a purely technical challenge that can be overcome with preventive measures such as antivirus scanners, firewalls and application control: Ultimately, however, it is about protecting both systems and people, and not falling victim to attacks.

The actions of people play a decisive role here. Whether a cyberattack is successful or not depends on people, plus the majority of attacks are the result of an inside job, either knowingly or unwittingly.

If we regard people as the most important link in a holistic security strategy, then employee sensitisation is just as much a part of the spectrum of measures as the technical defence measures mentioned above, and also includes measures to prevent the potential theft of data by encrypting data, files and hard drives. It is vital to motivate and sensitise employees for IT security and to explain to them how **important they are within the chain of protective measures**.

This requires interaction between IT departments, employees and HR. A company can only build a successful security strategy if everyone involved is motivated to implement the measures and if they have **internalised protection against attacks and data misuse**.

Establishment of security awareness is a key security layer that is added to existing technical security measures.

"Humansare a gateway and also the ultimate line of defence that makes all the diff erence."

DriveLock
securing your digital tomorrow

Trend towards remote working exacerbates the security situation

People face particular challenges when working from home or remotely. Employees who work from home are at risk of doing things that could have negative cyber security consequences, sometimes due to a lack of technical control and often due to carelessness when it comes to security awareness. They may be interrupted or distracted from their work by family or visitors. These distractions can make them careless. There is a lack of direct physical contact with colleagues and the IT department, from whom they can seek advice quickly and easily.

In particular in view of the current trend for hybrid working, security awareness is becoming increasingly important.

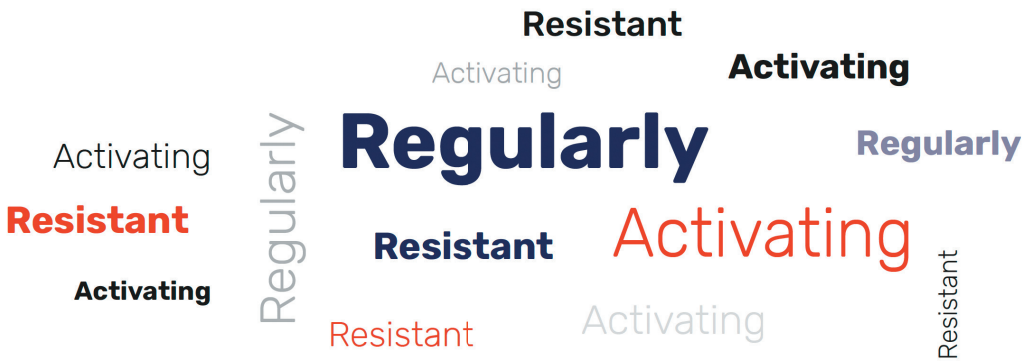
Sensitise employees through security awareness training

In companies, IT awareness training for all employees – including superiors – is now essential when it comes to establishing security awareness. It is important, however, that training sessions are not stand-alone, one-off special measures.

Regular security awareness training with context-related sensitisation measures creates an awareness that forms the basis for a sustainable security mentality. Such training should be provided to everyone, especially those who are not technically savvy.

Training sessions should appeal to their emotions.

They should aim to encourage and motivate in order to have an impact.



What are the goals of security awareness training?

- To enhance security awareness
- To permanently change user behaviour
- To comply with recommendations and legal requirements, such as ISO 27001 or the German Federal Office for Information Security (BSI) Basic Protection standard

What are the elements of security awareness training or campaigns? We would like to mention the most important topics here as examples:

- In training sessions, you will learn to recognise various forms of **social engineering**, e-mails that trick us into thinking they come from a person or entity we know or trust (e. g. bank, payment service provider) or fake versions of their website.
- You will learn to recognise suspicious **phishing mails**.
- **Malware** and **ransomware**
- You will be trained in the **proper use of USB devices** – the most common sources of virus or malware infections that may unknowingly become infected.
- You will learn to be mindful when handling **sensitive information**.
- You will learn how to use **mobile devices in your company (BYOD)** securely.
- You will learn how to **handle information in a data protection compliant manner (EU GDPR)**.
- You will learn how to handle user accounts, e-mails and passwords.
- Working in the cloud
- Working securely outside the office

How do you achieve sustainability?

Many awareness programmes fail in practice, as IT security awareness methods often don't go into interdependencies and attack chains in enough detail, and the programmes are not designed for the long term. Too many (technical) topics are taught within a very short time frame. The result is passive participation and little fun.

Sustainable security awareness campaigns address hearts and minds. Tips:

TIP 1:

Make sure that training participants are not only aware of the importance of IT security, but also understand why it is important. Without creating this connection, no amount of training will change behaviour in the long term.

TIP 2:

Also incorporate serious topics, e. g. during a workshop, in a fun way and with humour.

TIP 3:

Use modern learning methods (micro-learning) and motivate users with concise content.

TIP 4:

Use experimental learning and playful elements (gamification) to promote understanding, e. g. using a simulated phishing e-mail.

TIP 5:

Think about who you are training: Everyone has a different perception of security, and therefore a different sense of relevance.

TIP 6:

People learn through repetition. Our forgetting curve shows us how memory decreases over time. That is why repetition of simple slogans is important.

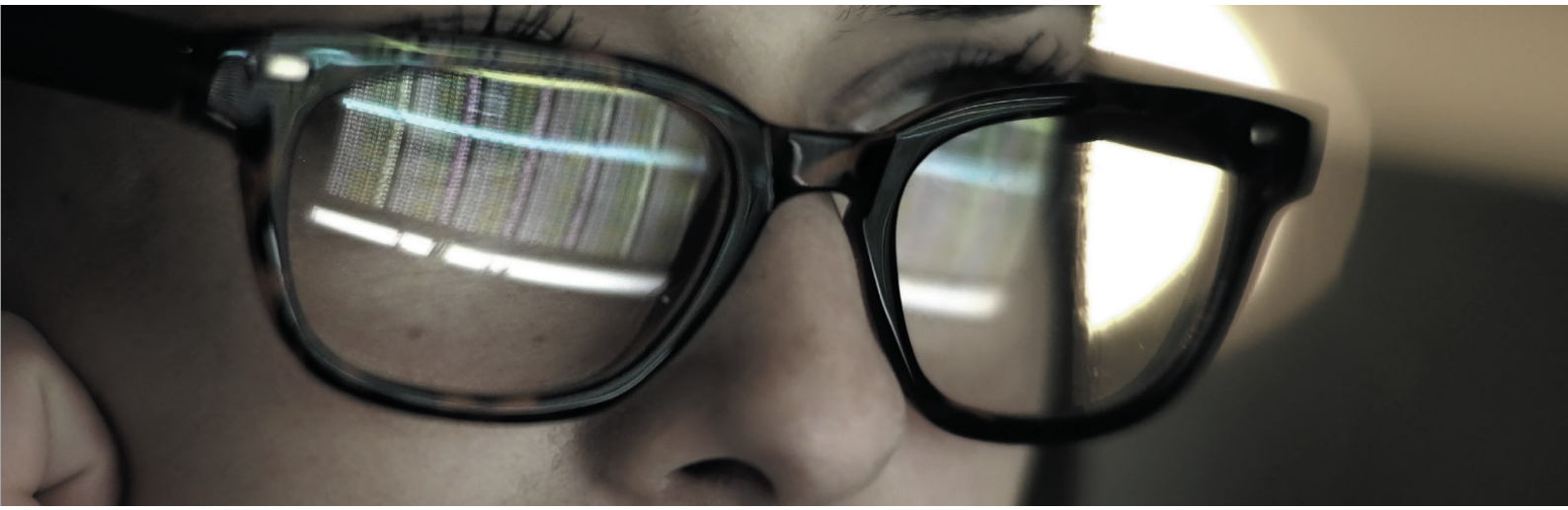
TIP 7:

Create a relaxed atmosphere, instead of publicly criticising employees for clicking the wrong link during your phishing training simulation.

DriveLock
securing your digital tomorrow

You want to get started. What can you do straightaway?

Practical tips in times of critical cyber threats.



TIP 1:

Distrust all e-mails that ask you to take urgent action. Never disclose your passwords and never click on any links or attachments in suspicious e-mails.

TIP 2:

Always check the sender's e-mail address first, as the sender name displayed can be very easily faked. This also applies to e-mails from family, friends or your employer.

TIP 3:

Establish processes for reporting anomalies and security incidents within the company. Set up a company address to which suspicious mail can be directed. You should collect phishing e-mails here. For example, set up an intranet or WIKI page with these mails.

TIP 4:

Make employees aware of the current threat situation (warnings from the German Federal Office for Information Security (BSI) and German Federal Office for the Protection of the Constitution (BfV) etc.) in order to establish risk awareness.

TIP 5:

Ensure you create secure, complex passwords that need to be changed regularly. To protect confidential information, all employees should use secure, complex passwords for their devices. You should also protect data carriers with passwords (hard drives, files, removable media).

TIP 6:

Dare to take the step to multi-level authentication. This secure protective mechanism makes it difficult for attackers to penetrate internal company systems and gain access to sensitive information. Where more than a password is required, cyber criminals have a harder time. Also consider other factors for identity & access management (IAM) (tokens, biometrics).

TIP 7:

Grant individual or group-based access rights: Apply the principle of least privilege (POLP). Users' access rights should be limited to only those that they strictly require to do their job.

TIP 8:

Encourage your employees to check the update status of their devices and software regularly and to carry out any necessary updates.

Contact us!

DriveLock SE
+49 (89) 546 36 49-0
info@drivelock.com

www.drivelock.com