ELEARNINGNEWS ARTICLE

Year 5 - number 145 Wednesday 10 february 2021

How and why to train employees on cyber security?

How to create effective training programmes that help reduce corporate cyber security breaches?

According to a study by IBM, 95% of corporate **cyber security breaches** depend on the actions of their employees.

This means that even with the most sophisticated security systems in place, failure to train employees can still expose the company to cyber risks and threats.

Adequate cybersecurity training is therefore the first line of defence against cyber crime, which in most cases is facilitated by people's own mistakes or negligence.

An untrained employee might, for example, open suspicious emails or fail to adequately protect sensitive information by adopting non-security compliant behaviour.

Which employees should attend IT security courses?

The answer to this question is very simple: if an employee uses a computer, they need **cyber security training**. Technology offers employees endless opportunities to unknowingly put company data at risk.

Computer security attacks increased dramatically during the coronavirus pandemic, as a result of the rapid spread of **remote working**. The use of personal computers and inappropriate Internet networks increases the vulnerability of companies.

Training in **cyber security** can help mitigate this exposure and contribute to a secure workforce. But how to create an effective cyber security training programme?

Tips for effective cyber security training

1. Include cybersecurity training in onboarding programmes

Creating awareness of online security threats should start on day one. Make online cybersecurity training mandatory for new employees. Incorporate cybersecurity training into your **onboarding program** and make sure it covers all the most important topics.

This way, you'll make sure they understand the importance of careful online behaviour from their first week on the job.

2. Assess your company's weaknesses

Before designing computer security training courses for your company, you need to look at the overall security you already have in place and identify weak points. Are there **security gaps** when it comes to payment processing? E-mails between offices? Attachments and document security? Identify the weakest link and focus the beginning of the course design there.

3. Continuously update your employees on new threats

One of the most important concepts to understand is that, just like technology, IT security is constantly evolving and staying up to date could mean the difference between keeping your business safe or not.

So make sure that training isn't a one-off action, but instead provide **ongoing updates** (e.g. quarterly) and send your employees constant reminders of new attacks that have developed.

4. Use the principles of microlearning

Use the power of **microlearning** to provide small snippets of essential information. This mode of training requires less effort in terms of time than traditional training (both for content creation and delivery), resulting in a higher course completion rate and an **immediately updated workforce**. For example, you can create microlearning content to update employees on new types of cyber attacks.

5. Create a sense of shared responsibility

Remember that it's better to know about a potential breach as soon as it occurs, so make sure you create an environment where sharing is encouraged and avoid a situation where someone tries to hide their mistakes and make the situation even worse.

When a threat is identified, send a company-wide email to inform employees. Being up to date will help them to keep their alert level high.

Online course on cyber security

When it comes to continuous training of workers, one of the most effective and economical solutions is online training. In this respect, we reccomend Mega Italia Media **Online course "Cyber Security: company information protection"**: to provide your employees with specific training on the risks and responsibilities related to data and information treatment via IT devices.

Translated with www.DeepL.com/Translator