ELEARNINGNEWS ARTICLE

Year 4 - number 101 Wednesday 26 february 2020

Can eLearning contribute to corporate cyber security?

How can eLearning improve the company's IT security?

Does the corporate **IT security** protocol really belong exclusively to the IT department only? Of course, the IT team is responsible for the installation and maintenance of security systems in the company, but the digital world is constantly growing and expanding and affects all company departments. And here eLearning comes into play.

According to a 2016 study, published in Information and Knowledge Management, the constant growth of the Internet has reformulated the pedagogical inclination of **eLearning**. The primary objective of online training is precisely to make learning as accessible as possible.

Online courses, tutorials and digital files can be excellent channels of internal communication and staff updating. In addition, eLearning has grown in popularity, making it the perfect vehicle for training employees on cyber security.

Involvement

The " **cyber security**" theme isn't widely treated by everyone because it brings to mind images of complexity, technicality and IT jargon inaccessible to most. ELearning allows you to approach the topic in an engaging way. There is also the possibility of basing the lessons on practical cases and putting them into real life **scenarios** (as reported by the ZDNet report).

Cyber security has a strongly interdisciplinary nature, so much so that, in the ISC2 Security Congress, has been compared to the arts.

How to spread information **security training** and updating in the company?

- messaging apps can be used to quickly inform about potential data breaches and how to avoid them;
- useful files and training videos can be stored in the cloud and easily updated;
- through the company eLearning platform, online training on the subject can be offered to all company employees;
- short video tutorials can be very useful to those who want to create password protection protocols and the like.

Cyber security is constantly evolving

The IT security protocol requires much more than the creation of complex passwords, but generally concerns all systems for preventing data theft and preserving the integrity of the data. The importance of cyber security is a concept that can be the subject of effective training, also because cyber threats are rapidly evolving. This offers managers the opportunity to engage their employees in more depth.

Clearly, the types of cyber security protocols needed will depend on the operations your company performs. Employees of technology companies, for example, require much more intense training that covers both software and hardware: **eLearning courses** can be customized and updated in this perspective, to meet specific needs.

The next steps

Employees pose a major threat to corporate IT security, especially in cases of remote workers, as it is difficult to monitor the use of the computer and the security of their devices. Gulf Business News recommends educating employees in advance so they can understand the risks.

It is important to quickly evaluate your employees' cyber security knowledge so that you can know where to start with the training. **LMS**s keep track of the levels of training completion dates and this can help to have accurate reports about employee training. These metrics can therefore be used to establish a solid safety culture within the company; By monitoring what employees already know, managers can add new modules that are based on other data and fill in the gaps either (preventing future attacks).

Article taken from InfoSecurity Manager