ELEARNINGNEWS ARTICLE

Year 6 - number 197 Wednesday 6 april 2022

E-learning and cybersecurity: skills to be transferred

When designing a format for eLearning courses, at least three competences to be administered to users must be taken into account. Let us find out what they are

One of the main requests from customers, especially large organisations, is to identify the main risks associated with the use of company devices.

The identification of risks is, more and more often, linked to the company security policy but, in my experience, it is possible to structure a format based on basic rules that you can then adapt to the specific case.

In this article, however, we will not investigate all the possible skills to be transferred to the learners of eLearning courses on computer security but, in an analytical and structured way, we will define the setting of a format starting from some topics that, in the past, I happened to face with some customers.

An excellent and immediate online course for the cybersecurity training of company employees is certainly **Cyber Security - Protection of company data and information - 1 hour**.

Protecting devices

You'll agree with me that every aspect of cyber security deserves its own article. However, as I said before, the creation of an eLearning course format necessarily requires the identification of a starting topic.

I have therefore selected one of the topics most requested by the companies I have worked with: device protection.

When designing a format for courses in eLearning mode, you must therefore take into account at least three skills to be administered to the users of a course: **creating complex passwords, combating phishing (defence against online fraud), and installing an antivirus program**.

Already from the first structure of the synopsis of a course in eLearning mode, it will be necessary to identify the constant information and the variable information: let us analyse the first of the skills and identify which will be the training variables to be offered to our client.

Creating complex passwords

Using a password has become a daily habit, whether it is to access e-mails or to purchase a product online. For this reason, strong passwords are an essential element of our protection: if an attacker managed to obtain one of your passwords, he could take possession of your identity, transfer money and gain access to your personal information.

Of course, there are a few steps you can take to improve the **security of your passwords** to protect your accounts, physical devices and online operations.

These are the constants to consider when creating eLearning courses, the famous best practices or, in Italian, **good practices** that everyone should adopt when it comes to IT security.

We include a generic list here, but yours may have many more items:

- Employ a different password for each account you have. Don't use the same password everywhere: if a hacker discovers it, he will try it on all the websites you might be registered to in order to get as much information as possible.

- Use complex passwords, never trivial ones: choosing an easy-to-guess word like your first or last name is not a good idea.
- Choose passwords of the right size, at least 14 characters, and with a certain level of complexity with special characters and capital letters.

These may be our constants in the structure of a corporate IT security format. However, for internal policy or simply for market evaluation, there may be variable elements to include in your eLearning courses.

Here's an example:

Long and complex passwords can be difficult to remember and, if the user has many accounts, it would be impossible to remember them all. For this reason, there are many password managers, both free and paid, which also provide information on the level of robustness of account passwords;

The creation of a course in eLearning mode, in this case, needs to be adapted to the conditions of use of company devices: is it possible to install third-party software? Is there a software catalogue available that we can mention in the course? Which users are most affected by this type of error? Is it necessary to mention a tutorial for installation?

All these variables can make a difference not only to the wealth of information in eLearning courses, but also to the offer to be sent to the customer: the greater the possibilities of being adherent to their needs and customising the product on a solid basis, the greater market success your product can have.

We can then move on to the second topic.

Defending against online fraud

Email and messaging apps are the main tools with which we communicate in both family and business environments: it is one of the ways in which companies provide their services online and, above all, communicate any tax demands.

It is one of the ways in which companies provide their services online and, above all, communicate any tax requests. For this reason, these tools are among the most attacked by malicious attackers and, obviously, defence techniques against phishing, the name of this particular attack, are among the most popular topics.

Read also **What are the 8 most common attacks on a company's cybersecurity system?** and **Corporate Cybersecurity: attack data**.

Falling victim to these attacks results in the theft of sensitive information or the compromise of your devices, computers or smartphones, through the installation of software called malware.

You will therefore understand the sensitivity of such a subject and the need for companies to equip themselves with shields that are not only computer-based but also **informational and educational**.

Again, there are general guidelines or, best practices to be adopted, in any case:

- attachments and links contained in all emails and messages on social networking sites should be read carefully; if you are suspicious, check the sender and see if the link is real.
- Be careful with attachments, especially those you don't expect: invoices, receipts from online purchases and requests for money.
- Always use up-to-date antivirus software to detect viruses in your email.
- Be wary of emails asking you to update your antivirus software and requesting you to click on them.

And so on.

Again, it is necessary to check what should be included in a format and what should be offered to the customer as a variable to be adjusted to the company policy.

The client may already have a security suite installed on the company email that filters these kinds of requests and puts them directly into the junk mail folder. Similarly, and this is something that happens to me with some customers, there may be an internal service for reporting discrepancies that, with a certain timeliness, is able to resolve any doubts on the subject: just make a phone call or send an email with a screenshot of the offending email and wait for a response.

Once again, the advice is to have an integration management scheme: it may be useful to offer the client a basic package of best practices and then integrate other information on which to customise the content.

Very often, in order to match the client's requirements to the budget, it may be useful to already have information content available that is only offered under licence.

This information security content will not be for the exclusive use of the client but can be formatted for general use and contracted for annual or, if desired, lifetime use but without copyright.

This choice will allow you to reduce the effort required to produce the content, at least the textual content, and to propose a lower offer than the competition, with rapid scalability and industrialisation of your eLearning courses.

We can now move on to our third topic, perhaps the one most subject to a certain variability of content.

Antivirus installation

Our smartphones, our tablets and, above all, our PCs are bought for the most disparate uses: they are used to send communications, to fill in worksheets, we use them to listen to music, access our bank account or to post photos of our holidays at the seaside.

For this reason, it is impossible to imagine that the data they contain could not be of interest to a number of malicious persons who could, quite simply, manage to appropriate sensitive information.

To avoid this danger, there are some good practices that every person or worker should implement to ensure the security of their devices.

- Insert a strong password in case your computer is lost or stolen, so that it is not at the complete disposal of an attacker.
- Pay attention to the apps installed on smartphones and tablets, but especially on PCs. Downloading software illegally may lead to the download of malicious software such as viruses and malware.
- Avoid using USB keys without checking them
- Avoid accessing public Wi-Fi

And so on.

Again, there are best practices that may depend directly on the internal policy of a company, which may partner with a vendor to install a certain anti-virus software that protects all company devices.

An anti-virus will scan your smartphone, tablet or personal computer for known malware: if a file is found to be infected, it will be deleted to neutralise the threat.

However, you will understand that not all customers are familiar with this kind of solution and may choose to entrust you with the task of explaining the potential of generic anti-virus software.

In that case, you need to be prepared in the best possible way: introduce in the format a package of features common to most anti-virus software on the market and don't go into detail.

In any case, cybercriminals are developing new and increasingly sophisticated solutions to avoid detection attempts, so anti-virus manufacturers are constantly updating them with new features.

Ask your client to show you case studies, any incidents that have already occurred, and build your original instructional design proposal around that event. In this way, you will be able to propose a unique training concept from more general topics.

You can start designing eLearning courses that are a little more specific, such as animated courses, from a format that you have already created.

What will be your next production?