ELEARNINGNEWS ARTICLE

Year 3 - number 89 Wednesday 13 november 2019

Computer security for e-learning

Today, companies that offer courses in e-learning mode must ensure that no third party can get hold of user data, which could endanger computer security and privacy.

Violations and data loss endanger user privacy: in e-learning platforms, many data are available concerning the students (demographic data, health data, date of birth, e-mail addresses, telephone numbers, Facebook profile, name and surname) that is necessary also protect in reference to the " General data protection regulation" of the European Union (GDPR). If the e-learning platform suffered a loss or data breach, all personal information could end up in the hands of a cybercriminal, who could use them for scams, phishing attacks or simply sell them for a profit.

The GDPR imposes specific rules on the treatment of personal data of employees in the context working.
If your company has offices and employees throughout the EU, you should know the specific national laws of the countries where your company is present.

In the specific case of e-learning, to comply with the GDPR it is necessary to carefully examine the GDPR compliance program, the Privacy Policy and the Terms of Use of the LMS used and sign a DPA (Data Processing Addendum) compliant with the GDPR with the LMS provider.
The DPA must clearly specify the instructions that the LMS service should follow and oblige both parties to comply with the legal obligations relating to the GDPR.

Developing a sustainable GDPR training plan will make data protection a strong value for your organization: having a continuous training plan will allow you to incorporate good data protection habits throughout the company.

If instead you are a user of an e-learning course, fortunately there are some things you can do to protect your data:

1. Use security software on all devices

Hackers often take advantage of your device's lack of security. They expose you to malware that steals your sensitive data or keeps activity logs. That's why you should use anti-virus and anti-malware programs. Make sure you keep them up to date and schedule regular scans.

2. Use a virtual private network (VPN) service

These are online services that can help you hide your IP address and encrypt your Internet traffic, which means no one can monitor it, so it will be harder to track you down. VPNs make it easy to bypass firewalls.

3. Make all your social accounts private

The manager of your company does not need to know where you celebrated last Saturday or when you go shopping. So, you should make sure that all your social media profiles are set up as private. In this way, only the people you know, and trust will be able to see your posts and access your data.