

Cybersecurity Month in the Workplace: Employee Skills Under the Spotlight

2 October 2026 – As the workplace becomes increasingly digitalised, organisations and their employees must address digital risks and manage them effectively.

Is the workplace cybersecure?

ENISA's new Cybersecurity Threat Landscape report, based on an analysis of more than 8,000 incidents, presents the main threats across all economic sectors. As many as 73% of the organisations targeted are essential and important entities as defined by the NIS2 Directive. Public administration remains the most frequently targeted sector (32% of cases), followed by business services (8%), transport (8%), manufacturing (7%), and finance and banking (6%).

The latest ENISA report highlights the following threats:

- Fraudsters continue to use social engineering techniques. They exploit users' trust primarily through phishing campaigns and the ClickFix technique.
- Ransomware operators continue to disrupt organisations across different sectors by encrypting data, stealing data and extorting victims.
- During the reporting period, cybercrime remained one of the main threats in the EU and globally, accounting for 36% of all cyber incidents. In 2025, ransomware represented the largest share of financially motivated activity (40% of analysed incidents), followed by data breaches (31%) and fraud and impersonation (19%).
- Fraud is enabled by compromised data and credentials. Websites such as "Baiting News Sites" (BNS) are designed to attract and deceive individuals with promises of quick earnings while appearing credible and legitimate.
- The use of artificial intelligence by malicious actors is increasing. AI systems are being used to enhance and scale their activities. The number of AI-supported foreign information manipulation and interference (FIMI) campaigns rose from 41 to 147 in one year, an increase of 259%.

[The European Commission's Eurobarometer survey](#) on employees' cybersecurity awareness and preparedness provides insight into the level of exposure to cyber risks in the workplace and into employee practices across the EU.

Why conduct a survey on cybersecurity in the workplace?

Cyber threats in the workplace are widespread. In the six months preceding the survey, three quarters of employees were exposed to suspicious emails, messages or links at work. The survey measured how employees perceive cyber risks and how familiar they are with threats such as phishing, fraud, identity misuse, ransomware and AI-generated scams.

The survey aimed to assess employees' ability to recognise and report suspicious activities and incidents. The questions also examined whether organisations have appropriate security measures, rules, reporting channels, and awareness and training programmes in place.

Key survey findings

- Only 18% of employees state that no incident occurred in their organisation, while 74% received suspicious email, text or voice messages or links.
- Phishing remains the most common threat. 39% of employees report receiving phishing or fraudulent emails, while 18% report attempts to steal personal data.
- Reported incidents also include malware attacks, password theft attempts, AI-enabled scams, ransomware and other forms of attack.

- 83% of respondents believe that the consequences of a cyberattack would be serious for their organisation.
- 82% of employees consider their organisation's digital systems and tools effective in defending against cyberattacks.
- Cybersecurity is regarded as an important area, with employees attaching even greater importance to it than organisational leadership.
- Only 45% of employees report that their organisation regularly provides cybersecurity information or updates.
- Around half of organisations already have key cybersecurity measures in place, while one quarter plan to introduce them in the future.

Do employees have sufficient knowledge, and how are organisations investing in training?

Improving employees' awareness and preparedness is essential to protecting organisations from cyber incidents. Continuing to build knowledge is therefore an unavoidable next step.

However, the survey shows that strong demand for cybersecurity skills is accompanied by several barriers:

- lack of time at work (26% of employees),
- high training costs (16%),
- lack of information about training opportunities,
- insufficient support from employers.

Nevertheless, 85% of surveyed employees expressed an interest in improving their cybersecurity knowledge and skills.

Strengthening skills through the SRC-EDIH 2.0 project

The SRC-EDIH 2.0 project, in which the Chamber of Commerce and Industry of Dolenjska and Bela krajina (GZDBK) participates, also recognises the importance of cybersecurity and employee awareness of digital risks. One of the project's areas of activity is cybersecurity and data technologies, through which it supports companies in strengthening digital competences and safely introducing new digital solutions.

Companies are invited to follow the activities of the SRC-EDIH 2.0 project, which will offer a range of free or subsidised activities, including expert workshops, webinars, training courses and information campaigns aimed at strengthening digital security and cyber hygiene. By acquiring up-to-date knowledge and best practices, companies can reduce cyber risks more effectively, increase the resilience of their information systems and build a culture of safe digital technology use.

More information about upcoming events, training courses and other opportunities to develop digital competences is available on the [SRC-EDIH 2.0](#) project website.



Source and photo: ENISA