WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
BOSNIA AND HERZEGOVINA

Evolution of Cybersecurity

Jovana Ostojić

Youth Ambassador at Women4Cyber Bosnia and Herzegovina

WOMEN 4CYBER

EUROPEAN CYBER SECURITY ORGANISATION

BOSNIA AND HERZEGOVINA

How is cybersecurity changing and why must we shift our mindset?

Research indicates that the number of cyberattacks is growing exponentially, but the rise in their sophistication is truly alarming. According to an article on TechRadar, Artificial Intelligence is becoming a double-edged sword: both a friend and an enemy in cybersecurity. Hackers are leveraging AI for personalized phishing emails, deepfake videos, and automated attacks that bypass traditional defenses *(TechRadar, 2024)*. Artificial Intelligence has fundamentally changed the rules of the game; we are no longer looking for obvious spelling mistakes or suspicious tones. Today's AI-generated phishing is linguistically flawless and psychologically precise. This is because algorithms learn how to perfectly mimic the writing style of our colleagues or banks, making the deception almost invisible to the average user.

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
BOSNIA AND HERZEGOVINA

The ENISA report predicts that by 2030, quantum computing and AI-generated malware will significantly threaten existing cryptographic systems, turning cybersecurity into a strategic discipline rather than just an IT task *(ENISA, 2024)*. The number of cyberattacks on organizations is growing significantly; according to research by Check Point, organizations were exposed to an average of 1,968 cyberattacks per week during 2025, representing a substantial increase compared to previous years *(Check Point, 2026)*. Cyber threats are becoming increasingly complex and diverse. ENISA emphasizes that among the most significant modern threats are ransomware, malware, social engineering, and attacks on system availability such as DDoS attacks.

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
BOSNIA AND HERZEGOVINA

Furthermore, there is an increasingly prominent trend of attacks targeting the public sector and critical infrastructure, including healthcare systems and government institutions. These trends point to an evolution from isolated technical attacks toward complex and combined threats that utilize various techniques and attack vectors *(ENISA, 2023)*. This evolution of cyber threats requires a growing number of highly qualified experts capable of understanding, analyzing, and responding to complex attacks in a timely manner. As someone who recently graduated and entered this professional world, I witness daily the massive gap between technological progress and actual digital literacy.

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
BOSNIA AND HERZEGOVINA

Through business conversations, as well as private gatherings, I notice that general awareness of these dangers is at a worryingly low level. People often neglect even the most basic elements of cyber hygiene, believing that attacks only happen to 'someone else'. Cybersecurity is no longer just a technical challenge; it has become an existential threat to individuals, companies, and nations. In this era of rapid digital development, the nature of threats is shifting, demanding a completely new approach. We can no longer rely solely on firewalls and antivirus programs; we need a mindset shift from a reactive to a proactive model, and from individual solutions toward collective responsibility.

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
BOSNIA AND HERZEGOVINA

WOMEN 4CYBER

EUROPEAN CYBER SECURITY ORGANISATION

BOSNIA AND HERZEGOVINA

Does most cyberattack activity start with phishing?

Phishing remains one of the most common initial attack vectors, with the majority of organizations reporting phishing incidents every year *(ProofPoint, 2024)*. The report is based on a survey of 7,500 users, 1,050 security experts, and an analysis of 183 million simulated phishing messages. Verizon's Data Breach Investigations Report shows that the human factor was involved in 68% of data breaches, confirming that attackers still largely utilize social engineering, user errors, and credential theft as an effective means of initial system compromise *(Verizon, 2024)*.

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
BOSNIA AND HERZEGOVINA

This data indicates that phishing and social engineering remain the dominant forms of attack, which further emphasizes the importance of education and the readiness of organizations and educational institutions to respond to modern cyber threats. However, technology is only one piece of the puzzle; the more important piece is us — *the people*.

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
BOSNIA AND HERZEGOVINA

As a young woman who has focused her education on this field and as a Youth Ambassador, I feel a responsibility to speak out about what I see on the ground. I believe that we must not view cybersecurity as an isolated IT task, but rather as an essential life skill in the 21st century. Our mission must be digital literacy, from the classroom to the office, because in a world where threats evolve at the speed of artificial intelligence, our strongest line of defense remains an educated and cautious individual. It is time to elevate cyber hygiene to a priority level before another costly lesson forces us to do so.

WOMEN 4CYBER
EUROPEAN CYBER SECURITY ORGANISATION
BOSNIA AND HERZEGOVINA