UDC 004

# *DIGITAL SECURITY AND MEDIA LITERACY*

***V. Kolesnyk,*** group KB-24
***S. Shcherbyna,*** Candidate of Pedagogical Sciences, Associate Professor
*Central Ukrainian National Technical University*

The modern world is characterized by high dependence on digital technologies, which creates new opportunities, but also new risks. Issues of digital security and media literacy have become important aspects of everyday life. According to a report by Symantec, cyber threats such as malware and phishing attacks are the main dangers for internet users, and the risks of misinformation increase the need for media literacy for all age groups[1].

Digital security covers many aspects, including personal data management, privacy and general cyber hygiene skills. According to Symantec, more than 60% of attacks start with phishing emails, highlighting the importance of being able to recognize such threats[1]. This includes skills such as creating strong passwords, using two-factor authentication, and social media privacy settings.

Media literacy is the ability to recognize fake news, determine the reliability of sources and analyze information flows. According to the Media Literacy Now Foundation, the spread of misinformation and fake news is becoming a serious problem as people are exposed to a myriad of poor quality information sources. Increasing the level of media literacy is a key tool for developing critical thinking and countering disinformation[1, 2].

Many countries, such as Finland, have developed curricula to increase the level of media literacy among schoolchildren. According to research contained in a policy paper on media education in Finland, the Finnish education system focuses on integrating media literacy into the curriculum, providing students with the skills needed to critically analyze media and recognize misinformation. Education in this area begins at an early age and encompasses both formal and non-formal education, which promotes responsible media consumption[3].

Users can take a few simple steps to improve their digital security: changing passwords regularly, using reliable antivirus programs, learning to recognize phishing attacks, and actively using media literacy resources such as online courses and webinars[1, 2].

To enhance security when using public computers, avoid logging into personal accounts whenever possible. If you must access these accounts, always log out fully afterward and clear the browser history to remove traces of your activity. Avoid connecting USB drives to these computers, as they may harbor malware that can infect your personal devices through USB connections. Public Wi-Fi networks, while convenient, lack security measures, particularly for those who frequently work while traveling, such as journalists. When using public networks, protect your data and devices by connecting through a Virtual Private Network (VPN). In addition, turn off Bluetooth and other file-sharing settings to prevent unauthorized access to your device.For safer browsing, opt for secure browsers like Chrome and Firefox, which support various security-focused extensions. Look for HTTPS in the URL bar and a lock icon to confirm secure encryption when accessing websites. Installing HTTPS-enforcing extensions can enhance this layer of security. Watch for fake domains that mimic real websites. Verify URLs carefully to ensure accuracy, particularly the HTTPS indicator, to avoid malicious sites that can install malware. Consider using browser extensions like Adblock Plus to block intrusive ads, and Privacy Badger to protect against tracking ads and enhance your online privacy[4].

Encryption is one of the most effective ways to secure sensitive information and communications. Basic encryption works by scrambling data with a mathematical formula, which can only be decoded with a unique key or passphrase. For journalists handling sensitive data, encryption

can protect information that might otherwise put them or their sources at risk. When working internationally, journalists should consider encryption laws, as some countries restrict or monitor its use. Therefore, researching local regulations and including these in a risk assessment is essential before traveling. There are encryption tools that secure messages, calls, or files during transmission, making them less vulnerable to interception. However, it's crucial to verify if the tool also encrypts data on the company's servers, as some tools store copies of communications or documents. In situations where a government could demand access to these server-stored records, encryption on the server can compromise confidentiality. Choosing the right encryption tool should account for the needs and risks of both the journalist and their sources, as well as local legal conditions. Always prioritize secure communication methods and carefully evaluate the trustworthiness and policies of the tool providers[4].

Another important consideration is metadata – information such as location, contact details, and timestamps of interactions, which some companies retain and may share with authorities. Depending on the risk level, journalists should select tools that limit metadata storage to reduce the chance of data leakage[4].

Advances in technology continue to create new cyber threats, such as ransomware and the spread of disinformation through artificial intelligence. This requires constant updating of knowledge in the field of digital security and critical analysis of information. For example, deep fake technologies are becoming increasingly difficult to recognize, which poses new challenges for users[1].

Ransomware attackers are increasingly refining their techniques and broadening the tactics, techniques, and procedures (TTPs) they use to breach systems. Traditionally, these attacks often began through phishing emails or by exploiting networks already infected by botnets. Although these methods remain prominent, an increasing number of ransomware campaigns are now taking advantage of security vulnerabilities in public-facing applications. For instance, unpatched vulnerabilities in Microsoft Exchange Server have become a primary entry point for attackers. Another major shift is the increased reliance on legitimate software tools to support ransomware operations. Attackers are increasingly using "dual-use" tools (legitimate programs introduced by attackers) and "living-off-the-land" tactics, which involve exploiting utilities already on the target network. Commonly exploited tools now include remote desktop applications like Atera, AnyDesk, Splashtop, and VNC Viewer, with some attacks employing multiple tools in tandem. Ransomware operators have also integrated tools like Rclone, which is open-source software initially intended for cloud content management but now commonly used by attackers to exfiltrate data from victims before encrypting it. Similarly, AdFind, a public tool for querying Active Directory, has become a mainstay in ransomware arsenals, assisting attackers in mapping target networks. Built-in Windows utilities such as PowerShell, PsExec, Windows Management Instrumentation (WMI), Scheduled Tasks (Schtasks), and Volume Shadow Copy Service (VssAdmin) are further leveraged to navigate networks and carry out malicious operations while remaining under the radar. The sophistication of these methods illustrates the growing adaptability of ransomware actors, who increasingly rely on dual-use and built-in tools to mask their activities and evade detection during attacks[1].

In the conditions of rapid digitization of society, the development of digital security and media literacy skills is necessary to ensure the security of personal data and awareness in the information environment. Integrating these skills into formal education will help shape a responsible and conscious society capable of effectively countering the challenges of the digital world.

**References**

1. Symantec Threat Hunter Team. Threat landscape year in the review whitepaper : підручник. 2022. URL: https://www.symantec.broadcom.com/hubfs/2022_Threat_Year_in_Review.pdf (дата звернення: 28.10.2024)
2. Media Literacy Now : веб-сайт. URL: https://medialiteracynow.org (дата звернення: 28.10.2024)
3. Saara Salomaa & Lauri Palsa. MEDIA LITERACY IN FINLAND : підручник, 2019. URL: https://medialukutaitosuomessa.fi/mediaeducationpolicy.pdf (дата звернення: 28.10.2024)
4. Rory Peck Trust. Digital Security : веб-сайт. URL: https://rorypecktrust.org/uk/how-we-help/freelance-resources/digital-security/ (дата звернення: 31.10.2024)