Attitude towards Cryptography: Impact on Cybersecurity

Abstract. Advancements in cyber technologies rapidly brings sophisticated attacks as well as security measures, but human error remains significant factor in cybersecurity breaches. Users with limited knowledge or unconcerned attitude may avoid data protection best practices, making sensitive information susceptible to data theft. We assume that efficient cybersecurity starts with every individual's attitude towards usage as well as knowledge of privacy preserving tools based on cryptographic solutions. We conducted two surveys among different population groups in Latvia to find out the Internet users' attitude and knowledge towards cryptographic solutions in daily use case scenarios. We reviewed results of other surveys and threat reports to identify current prime cyber threats and then we analyzed results of our surveys evaluating the current level of awareness thus attitude towards cryptography. Our aim is to emphasize the importance of cryptography as essential technical means for ensuring cybersecurity, especially when planning training opportunities for cybersecurity specialists and identifying the necessary additions to educational curriculums for future cybersecurity specialists' needs, as well as develop focused cybersecurity awareness campaigns for different groups of society.

Keywords: Cybersecurity, Cyber threats, Cryptography education, Survey.

1 Introduction

Cybersecurity is increasingly recognized as a critical component of the comprehensive national defense system, paying attention not only to improving cybersecurity management and promoting international cooperation, but also to raising the qualifications of IT specialists and raising the level of public awareness [1]. Without cryptography we would not have digital signatures and authentication, time stamping of electronic documents, electronic money, transactions and finance, secure network and messaging communications and encryption of sensitive files. Internet users' experience with cryptography often goes unnoticed because cryptographic primitives are built into various security schemes and protocols in the backend of systems, software and applications. Internet users must understand basic cryptographic principles to protect themselves, their data, and their privacy. We see that by comprehending the role of cryptography in various everyday scenarios will establish a solid foundation for overall quality of effective cybersecurity in the society. Any research, including ours, can only be a snapshot of the current situation and its problems. The results of other related surveys are analyzed in Section 2. The most popular cyber threats are reviewed in Section 3. Section 4 is devoted to analyzing the results of two of our surveys.

2 Results of related surveys

Many surveys and research in cybersecurity have been provided worldwide in recent years. While quantitative results may change, almost the same conclusions we can find in several surveys and other resources [2-5], namely:

- Phishing attacks are a major threat,
- Cybersecurity awareness training is the best defense against attacks,
- Human error accounts for 95% of all data breaches,
- 75% of cyber attacks start with an e-mail,
- The Microsoft Office formats: Word, PowerPoint, and Excel comprise the most prevalent group of malicious file extensions,
- E-mail is the primary entry point of 94% of malware attacks,
- In 2022 of 19 organizations, 84,7% were compromised by at least one successful cyber attack,
- Lack of skilled personnel and low security awareness inhibit IT security's success,
- Security is now a part of every critical business decision.

In April 2021, the Latvian Ministry of the Interior iniated public opinion telephone survey on security issues in Latvia [6]. Among 1000 respondents, cybercrime was recognized as the country's fifth most urgent security problem (behind corruption, pandemic, financial crimes, and organized crime), which worries 66% of the population. Although the emphasis in survey was on aspects of physical security, the results regarding the most important sources of information on various security issues were news portals (53% of the population obtain information on the topic of security), television (44%), social network profiles of security services (35%) and radio broadcasting (30%).

According to CERT's end-of-year study “2022 in the Latvia’s Cyberspace”, the number of incidents registered and processed by CERT.LV increased by 40%. [8] In the public administration sector, the search for vulnerabilities in IT systems has increased seven times, while the total volume of attacks has quadrupled. The year 2022 in Latvian cyberspace can rightly be considered the most challenging and cyber attack-intensive period in the entire history of CERT.LV's existence since 2011.

3 Cyber threats

The Europan Union Agency for Cybersecurity (ENISA) analyses the situation in the field of cybersecurity within EU countries, evaluates technological solutions, including cryptography, and provides recommendations for EU member states. Since 2013 ENISA has published annual report “ENISA – Threat Landscape” with summary about current state of cybersecurity in the EU [7]. According to the ENISA report of 2022, the most popular types of cyber threats today are:

- Ransomware: Type of Malicious software that take control of target’s system and blocks access to data using encryption until the owner pays a ransom.

- Malware: Broader definition of any malicious software that attacks a target's system or network to obtain sensitive information, install spyware, destroy data, or take control of a system. Traditionally, examples of different malware include viruses, worms, trojan horses. If we pay attention to technical details for cyber attacks, e-mail is still the primary entry point of malware.
- Social engineering: A technique in which attackers use psychological tricks to get a user to reveal sensitive information. Phishing is one of the social engineering techniques in which attacker send fake e-mails providing URLs (links) to fraudulent websites to obtain sensitive information such as passwords or credit card numbers. Malicious URLs (links) also are provided using various social media or messaging applications. Phishing can be highly sophisticated, utilizing methods of practical psychology to exploit human behavior.
- Threats against availability: DDoS attacks. Distributed Denial of Service attack (DDoS) refers to a network of computers or other devices utilizing the Internet to simultaneously send requests to a particular web server to overload the system and make it unavailable.

If the threats are so well-known, why are there still so many victims? One possible answer may be that cybercriminals use legal techniques for criminal purposes. For example, the explanation of threat #1 in the article by Cayley Wetzig indicates that "The general population pays no heed when clicking a link from an e-mail or a website" and "Many cyber criminals use "link bait"– enticing links that take you to malicious websites [9]". Another example is state institutions sending e-mails with usual content like monthly bills with a subject like "Invoice," and an attachment "*Invoice_R323820875_20230114_233424.PDF*".

4 Our surveys

4.1 Survey 1 – General Internet users

From October 7th to 18th, 2022, we surveyed 1034 people in an online survey. The target group was Latvian residents between 18 and 64 who use at least one device (computer, tablet, mobile phone) with an Internet connection. Respondents were from various social groups determined by gender, age, region, nationality, and family status. There was also broad coverage of respondents with employment status and affiliations: from unemployed to staff members of companies. The survey demographic profile is shown in Figure 1.

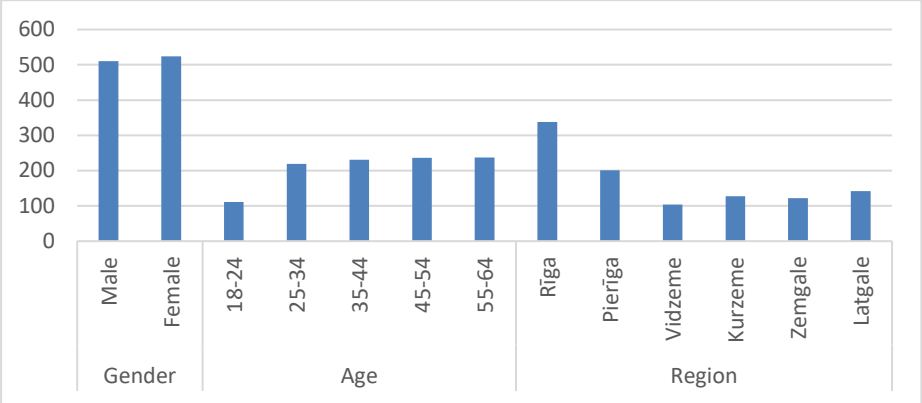

Fig. 1. The demographic profile of the survey.

One general observation was that a few questions in the survey turned out too technical to be answered meaningfully. In eight questions from the survey's 17, one answer option was "Do not know / difficult to answer." One-fifth of respondents (20.5%) never used this option. Contrarily, about a quarter (24.5%) had chosen this option for at least four questions – topics discussed in these questions are outside the scope of their interests. Looking separately at these questions with the answer option "Do not know / difficult to answer," the percentage of these answers is exceptionally high in exactly two questions about the role of cryptography in the cybersecurity and legal field – Question 4 and Question 5 (respectively, 57.8% and 60.9%, see below). The lowest number of such answers was in Question 8 about password creation habits (7%). Let us investigate answers to the particular questions in the survey (in some cases, the share of particular answers does not total 100% due to rounding):

Question 1. Do you use the mentioned devices in your work?

The overall distribution of answers (multiple options were allowed) was:

- Computer with Internet access (85%),
- Tablet with Internet access (16%),
- Smartphone with Internet access (72%),
- Other (6%).

Question 2. How would you describe your interest in cybersecurity issues?
The overall distribution of answers was:

- Not interested (20%),
- Interested occasionally (64%),
- Interested regularly (17%).

The most significant differences from the average indicators "not interested" and "interested regularly" are observed among people with basic education (respectively, 44% and 6%), trade workers (31% and 8%), and widows (36% and 13 %)(see Fig. 2).

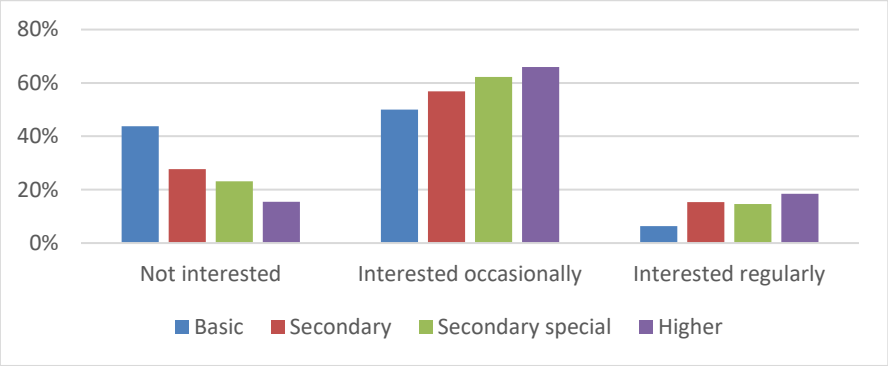

Fig. 2. Correlation between interest in cybersecurity and educational attainment.

Question 3. Do you think that attention paid to cybersecurity in Latvia is sufficient?

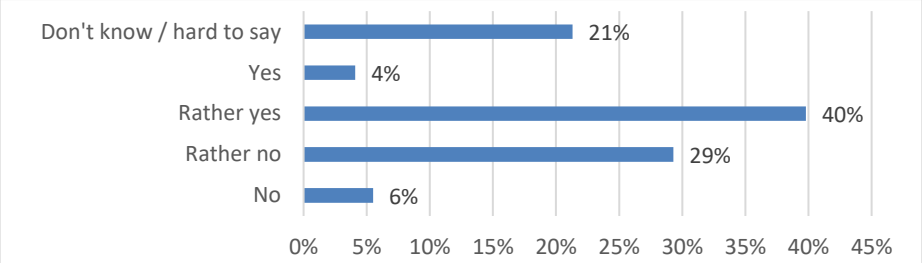

Fig. 3. Distribution of overall answers to Question 3.

Question 4. How would you rate the role of cryptography in cybersecurity today? Among the answers, the option "Do not know / difficult to answer" was the most chosen (58%). Other options:

- Cryptography plays an essential, but not decisive, role in ensuring cybersecurity (29%),
- Cryptography plays a role in cybersecurity, but other areas are much more important (7%),
- Cryptography plays a critical role in cybersecurity (7%).

There is a difference in the answers of women and men: the answer "Cryptography plays an essential, but not decisive, role in ensuring cybersecurity" is chosen by 34% of men and 23% of women. Women chose the answer option "Do not know / difficult to answer" in 65% of cases, and men – 50%. Respondents with basic education chose this option significantly more often (88%).

Question 5. How do you assess the current regulatory framework in Latvia in the field of cryptography?

Members of the youngest group of respondents (18-24 years old) are more confident in their competence: the latter was given by 41% of respondents.
Answers:

- Such regulation is not necessary (3%),
- The existing regulatory acts of Latvia, which affect the use of cryptography, are entirely sufficient and comply with international standards (8%),
- Regulatory acts are needed in Latvia, which would more precisely regulate the use of cryptography and introduce good practices (18%),
- In Latvia, it is necessary to modernize the cryptographic solutions used to correspond to the internationally recognized (11%),
- Do not know / difficult to answer (61%).

Question 6. In your opinion, is the exchange of information with state and local government institutions in e-services safe?

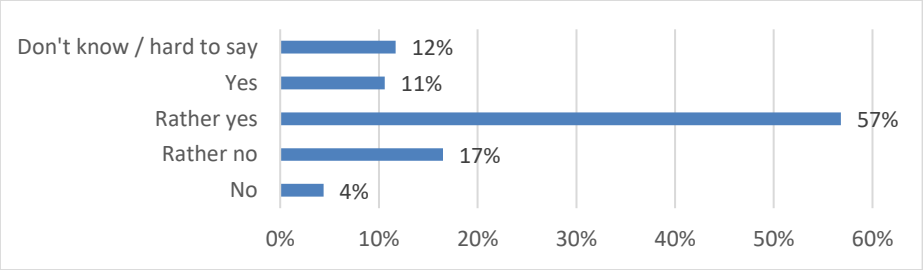

Fig. 4. Distribution of overall answers to Question 6.

Unqualified workers are the most skeptical – only 50% ("Yes" and "Rather yes") as opposed to 68% on average (see Fig. 4).

Question 7. Do you trust the security of electronic identification and trust services (e.g., e-signature)?

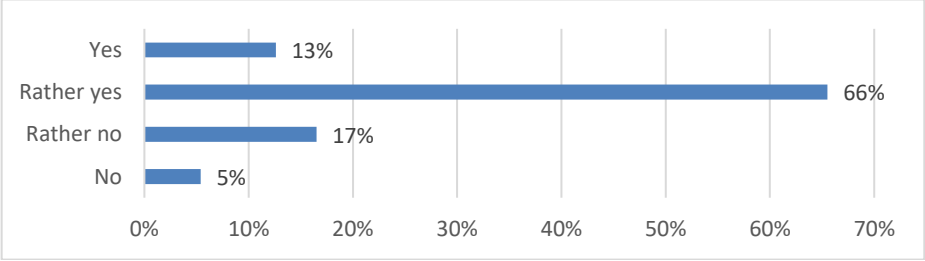

Fig. 5. Distribution of overall answers to Question 7.

There is no answer option "Do not know / difficult to answer" since it is assumed that any adult in Latvia should be able to use electronic identification services (see Fig. 5). More suspicious were respondents from:

- Vidzeme (30% of answers are “No” and “Rather no”),
- rural residents (29%),
- service and trade workers (31%),
- unemployed people looking for work (36%).

Question 8. How would you describe your text password creation habits?
Overall answers:

- I use simple and easy-to-remember passwords, as long as the system allows it (29%),
- I use hard-to-remember passwords that also contain special symbols (36%),
- I use computer-generated passwords (4%),
- I use several approaches of the above (25%),
- Do not know / difficult to answer (7%).

Against the average, those with a basic education stand out (63% use simple passwords, against the average of 29%), and unqualified workers (50% use simple passwords). Among widows/widowers, only 19% use hard-to-remember passwords, and 10% use entirely computer-generated passwords.

Question 9. Do you trust the security of online stores?
Question 10. Do you trust the security of online banking?
Trust in the security of online stores is significantly lower than in the security of online banks – 69% of respondents trust online stores completely or rather, and 89% trust online banks (see Fig. 6.). The most significant difference is among the unemployed searching for a job – 100% complete or partial trust in online banks, but only 68% in online stores .

The reasons for such difference may be the following:

- Banks, in the eyes of the public, are more reliable. There are legal procedures to get a license, and licensed bank customers have some state guarantees. The same attitude also applies to online banks.
- Almost anyone can start selling goods on the Internet.
- Bad previous experience using online stores, like an unsuccessful attempt to reach online store representatives via mobile phone or e-mail using credentials on the webpage.

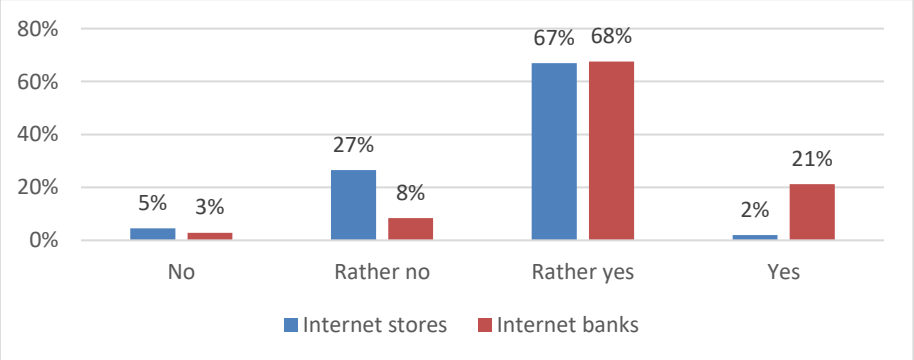

Fig. 6. Distribution of overall answers to Questions 9 and 10.

Question 11. Do you encrypt the information sent by e-mail (e.g. create archives with a password, use PGP/GPG)?

Overall answers: "Never" (52%), "In rare cases" (26%), "Often" (5%), "Always" (1%), "Do not know / difficult to answer" (16%).

Unqualified workers differ the most from the average (67% never encrypt the information sent) and managers, who significantly more often (10%) than average encrypt the information sent in e-mails.

Question 12. Do you encrypt backup data?

Overall answers: "No" (57%), "Sometimes" (21%), "Yes" (6%), and "I do not create backups" (16%). Men always or sometimes encrypt data more often than women - 31% and 23% of respondents, respectively. Compared to the average, those with primary education (12%), unqualified workers (11%), and widowers/widowers (13%) are the least likely to encrypt backups, at least sometimes.

Question 13. Are you using the latest cryptographic solutions for data storage?

Together with positive answers "Always" (1%), "Often" (4%), and "In rare cases" (24%), there was a high proportion of "Do not know / difficult to answer" and "never" responses to this question (29% and 43%, respectively). There were especially many "Never" answers among the 55-64-year-old group (50%), among respondents of Russian nationality (51%), among the group of those with primary education (69%), and among the self-employed (52%). The answer "Do not know / difficult to answer" was given more than average by residents from Kurzeme (37%), service and sales workers (50%), and divorced people (36%).

Question 14. Are you evaluating the security risks of storing unencrypted data?

Overall answers: "No" (32%), "Yes" (39%), "Do not know / difficult to answer" (29%).

18-24-year-old respondents (49%), students (50%), and representatives of other (unspecified) professions (52%) evaluate security risks more than average.

Question 15. When browsing websites, do you react to security warnings (e. g "Your connection is not private")?

Overall answers:

- I ignore such warnings (10%),
- I ignore such warnings for known sites (31%),
- I evaluate the potential risk and act depending on the content of the warning (42%),
- Yes, I never visit such sites (18%).

More than average, safety warnings are ignored by the young respondents aged 18-24 (14%), self-employed (18%), and unemployed jobseekers (16%). On the other hand, 55-64-year-old respondents (4%), residents of Pierīga (7%), pensioners (5%), and divorced people (5%) are more careful.

Question 16. Have you encountered phishing (fraudulent attempts to obtain confidential information)?

Overall answers:

- Never encountered (44%),
- Yes, but I have recognized fraudulent activity early (51%),
- Yes, I have fallen victim to such scammers at least once (5%).

Less than the average victims of phishing became residents of Pierīga (3%), residents of large cities (3%), managers (3%), office workers (2%), students (2%), and pensioners (2%). On the other hand, significantly more - those who have obtained primary education (13%), unemployed looking for work (12%), unemployed and not looking for work (11%), and self-employed (10%).

Question 17. How would you describe your experience in data encryption using cloud computing?

Overall answers:

- I do not care about data encryption (28%),
- If necessary, I use simple data encryption methods (28%),
- I use the best-known cryptographic solutions (5%),
- I do not use cloud computing (39%).

Respondents aged 55-64 (50%), unskilled workers (50%), and representatives of other (specifically unspecified) professions (62%) chose the answer "I do not use cloud computing" significantly more than the average. On the other hand, the most active users of cloud computing are the youngest respondents aged 18-24 (23% do not use, 77% use), students (22% and 78%), and those who are not working and not looking for work (22% and 78%).

4.2 Survey 2 – Students of the Faculty of Computing of the University of Latvia

We conducted the online survey using Google Forms. We surveyed 80 first-year students of the year 2022 of the Faculty of Computing of the University of Latvia. The survey was aimed to evaluate students' level of awareness and interest in privacy-preserving applications and security mechanisms based on cryptography.

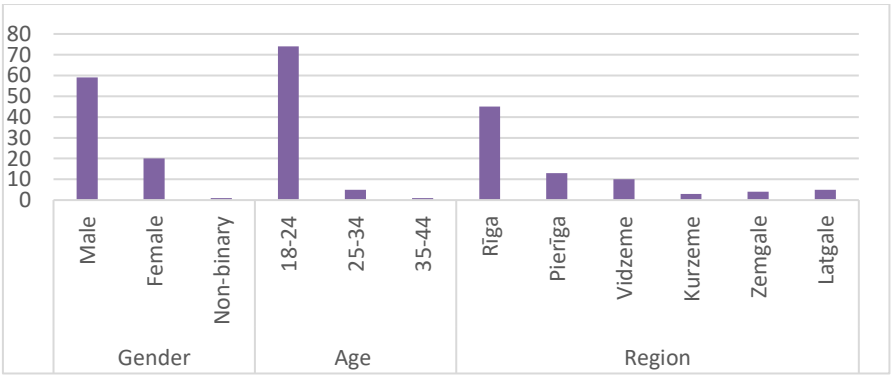

Fig. 7. The demographic profile of the survey

The survey contained 22 questions, of which eight were devoted to general statistics and 14 questions related to cryptography. The survey demographic profile is shown in Figure 7.

Let's look at some questions and answers. The following figures (Fig. 8., 9.) show the acknowledgment of privacy-preserving applications and security mechanisms based on cryptography.

Secure Boot is a security standard that ensures that a device boots using only software trusted by the original manufacturer [10]. A virtual private network (VPN) extends a corporate network through encrypted connections made over the Internet to ensure that traffic between the device and the network remains private as it travels. [11].

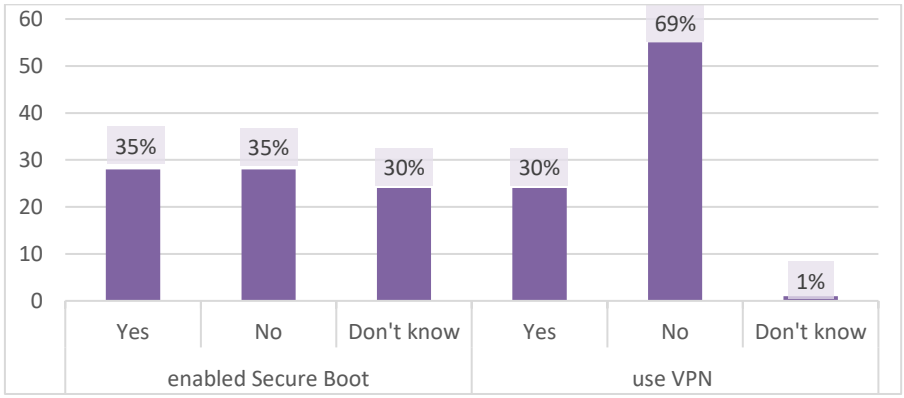

Fig. 8. Acknowledgement and usage of Secure Boot and VPN

Pretty Good Privacy (PGP) is an encryption system for sending encrypted e-mails, ensuring certification of identity and providing encryption, and digital signing [12].

Multifactor authentication (MFA), where the most known version is two-factor authentication (2FA), is a security mechanism that requires more than one form of identification to verify user identity and gain access to a system, account, or service [13].

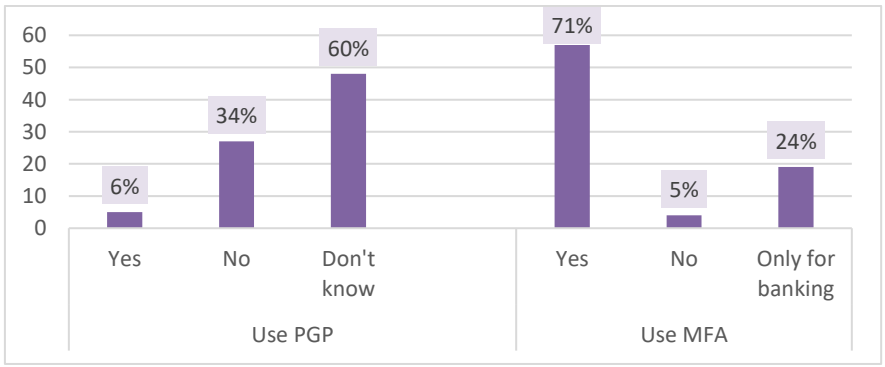

Fig. 9. Acknowledgement and usage of PGP and MFA

Question 14. While sending a request for a website, the browser warns that the connection to the server is not secure. Why is that?

The question was provided with a free-form answer. Investigating all responses, we can summarized that a quarter of students could explain the problem. Let us look at the examples for answers that could indicate the comprehension of the given problem:

- Invalid TLS certificate. (expiration date, outdated TLS version, or incorrect certificate parameters vs. domain),
- No certificate,
- The home page contains links that use HTTP,
- The certificate is signed by an unknown certificate authority (CA) (there is no such CA entry in the browser library).

Question 15. What is SSL/TLS, and what is its purpose?

TLS/SSL allows client - server applications to communicate over the Internet in a way that to prevent eavesdropping, tampering, and message forgery. [14]

The question was provided with a free-form answer. Most students acknowledge SSL/TLS protocol and understand its importance.

Question 16. You have decided to change your computer's operating system to one of the Linux distributions. You find the installation file on the official website and download it. How can you prove that the downloaded installation is the original file?

Several answers were provided, and 50% of students chose the answer: Checking whether the service provider offers the checksum file of the selected software and its digital signature. That also was the expected answer.

Question 17. Do you check the authenticity of downloaded files, if possible?

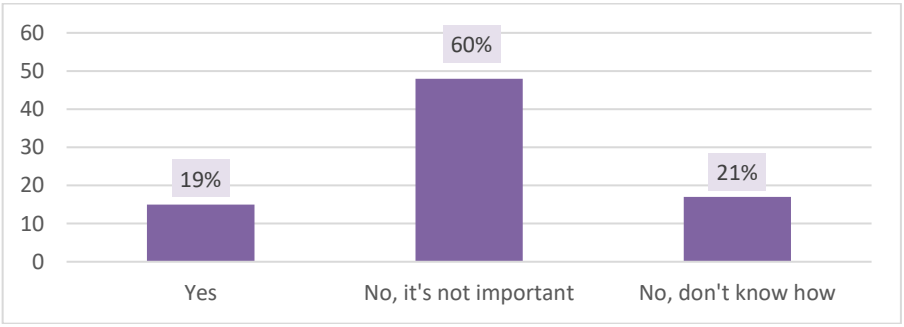

Fig. 10. Verification of downloaded files.

Question 18. Describe the steps involved in verifying the authenticity of a downloaded file.

The question was subsequent to the previous and provided as open-ended. Students who answered Question 17 (see Fig. 10.) among them 19% answered Question 18 close to the expected:

1. Obtain the file's original hash or signature,

2. Calculate the downloaded file's hash,
3. Compare the hashes or verify the signature,
4. Ensure that the original hash or signature is obtained from a trustworthy and reliable source.

Question 20. What is the difference between encryption and hashing?

The majority of students (64%) do not know the difference between both, but 36% could explain the main differences briefly. The expected answer was close to the following: encryption is a method that ensures the transformation of information into its incomprehensible representation, which can be decrypted using certain keys. Hashing is done with hash functions and differs in that the information transformation cannot be returned to the original representation.

5 Conclusions

Our surveys results indicate that:

- Two-thirds do not use privacy-preserving applications and security mechanisms.
- The majority knows the importance of the TLS protocol.
- One-third of respondents understand the difference between a hashing and encryption.
- One part is aware of the possibility of verifying the authenticity of downloaded files, while just part of them is practicing it.
- Almost everyone uses multifactor authentication.
- Technical questions should be included in surveys very carefully since there is a great risk of obtaining "Do not know" type answers.

After analyzing the survey responses, we concluded that the public needs to be better informed about fundamental cybersecurity issues regarding cryptography. Cryptography is not confined only to the realm of experts – cryptographers and cybersecurity specialists but is also a set of tools that empower everyday internet users to protect their digital presence. Our aim is to improve cybersecurity in Latvia, by bringing up to date the use of cryptographic best practices and raising the issue of educational opportunities. However, due to the limits of the questionnaires it was impossible to get deep and comprehensive answers to all the questions of interest to us, so further analysis of the situation in some aspects would be necessary. The results of our study can be used to create more focused research to promote educational opportunities for cybersecurity professionals and those working in IT as well as possibilities for students. The question of how to promote the general public's interest and knowledge about cryptographic solutions in everyday life is also relevant. Cryptographic solutions might not be the silver bullet for stopping all cyber attacks but it can mitiage the impact of adversaries.

References

1. Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R0694, last accessed 2023/09/16
2. 15 Alarming Cybersecurity Facts and Statistics, https://thrivedx.com/resources/article/cyber-security-facts-statistics?referrer=cybint, last accessed 2023/09/16
3. 20 Frightening Cyber Security Facts and Stats, https://www.dbxuk.com/statistics/cyber-security, last accessed 2023/09/16
4. Triebes, K.: Insights from 2023 Cyberthreat Defense Report, https://www.imperva.com/resources/resource-library/webinars/insights-from-2023-cyberthreat-defense-report/, last accessed 2023/09/16
5. Meeting Data Security Challenges in the Age of Digital Transformation, https://www.imperva.com/resources/resource-library/white-papers/meeting-data-security-challenges-in-the-age-of-digital-transformation-wp-ty?lang=EN&asset_id=3944, last accessed 2023/09/16
6. "Latvijas Fakti" survey, http://petijumi.mk.gov.lv/sites/default/files/title_file/Drosiba_PETIJUMS.pdf, last accessed 2023/09/16
7. ENISA – Threat Landscape 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022, last accessed 2023/09/18
8. CERT 2022 end-of-year study, https://cert.lv/lv/2023/01/2022-gads-latvijas-kibertelpa, last accessed 2023/09/18
9. Wetzig, C.: 9 Most Important Cybersecurity Tips for Your Employees, https://thrivedx.com/resources/article/cyber-security-tips-for-your-employees, last accessed 2023/09/18
10. Microsoft – Secure Boot, https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot, last accessed 2023/09/18
11. CISCO – What is VPN, https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html, last accessed 2023/09/18
12. Pretty Good Privacy (PGP), https://www.techtarget.com/searchsecurity/definition/Pretty-Good-Privacy, last accessed 2023/09/18
13. NIST – Multifactor Authentication, https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication, last accessed 2023/09/18
14. The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446, https://datatracker.ietf.org/doc/rfc8446/, last accessed 2023/09/18