CyberEast+

Enhanced action on cybercrime for cyber resilience in the Eastern Partnership States

National quantitative and qualitative analysis of the attitude towards cybercrime and online security in Ukraine

Version 28 May 2026

Co-funded by the European Union
EUROPEAN UNION
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Co-funded and implemented by the Council of Europe

Disclaimer

This report has been produced as part of the CyberEast+ project co-funded by the European Union and the Council of Europe. The research report was drafted by INFO SAPIENS LLC (Ukraine) with inputs from Mr Roeland van Zeijst (Netherlands). The opinions expressed in this study are the responsibility of the authors and do not necessarily reflect the official policy of the Council of Europe.

The research publication utilized artificial intelligence (AI), specifically large language models (LLMs), in the preparation of written content, analysis, or data presentation. While AI tools were employed to assist and enhance various aspects of the publication process, all outputs were carefully reviewed, validated, and edited by the authors to ensure accuracy, clarity, and compliance with research standards. The authors take full responsibility for the final content presented herein.

Personal Data Protection

In accordance with applicable data protection regulations of the Council of Europe and applicable legislation of Ukraine, any sensitive information collected during the survey process will be fully anonymized before inclusion in this report.

Key principles of our personal data handling include:

- Anonymization: All personal and sensitive data is processed in a manner that ensures individuals cannot be identified, directly or indirectly, in any published results.
- Purpose Limitation: Data collected is used solely for the purposes described in the survey and the resulting analysis.
- Data Security: Appropriate measures are in place to safeguard information against unauthorized disclosure or use.
- Lawful Processing: Data is collected and handled in compliance with applicable data protection regulations.

If you have any questions about how your data is used, or if you believe your information has not been properly anonymized, please contact our Data Protection Officer at dpo@coe.int.

For more details on your privacy rights and our data practices, please refer to the Council of Europe Regulations on the Protection of Personal Data of 15 June 2022, available here.

Contact:

Cybercrime Programme Office	cybercrime@coe.int
Council of Europe (C-PROC)	www.coe.int/cybercrime

TABLE OF CONTENTS

List of acronyms

2FA	Two-factor authentication
AI	Artificial intelligence
APT	Advanced Persistent Threat
BEC	Business ‘Email’ Compromise
CaaS	Cybercrime as a Service
CAWI	computer-assisted web interviewing
CEO	Chief Executive Officer
CRM	Customer Relationship Management
CVV	Card Verification Value
DDoS	Distributed Denial-of-Service
EU	European Union
GDPR	General Data Protection Regulation
GDQ	Global Data Quality
ICC	International Chamber of Commerce
ESOMAR	European Society for Opinion and Marketing Research
IDPs	Internally Displaced Persons
IP	Internet Protocol
ISMS	Information Security Management System
ISO	International Organisation for Standardisation
IT	Information Technology
M.E.Doc	My Electronic Document Circulation
NBU	National Bank of Ukraine
OLX	OnLine eXchange, global online marketplace platform
OSINT	Open-Source Intelligence
PIN	Personal Identification Number
SMS	Short Message Service

1. Executive Summary

This study combines quantitative survey data and qualitative insights from focus group discussions to provide a comprehensive view of cybercrime perceptions, experience and behaviour among internet users, businesses and experts in Ukraine.

Across both research stages, the internet is clearly established as a core part of daily life, with high levels of engagement across communication, services, finance and information consumption. This widespread use is accompanied by a strong awareness of cyber risks: most users recognize cybercrime as a real and personal threat. However, this awareness does not fully translate into consistent protective behaviour. While basic security practices are common, they are often fragmented and insufficient to prevent exposure, as reflected in the high share of users reporting direct or indirect experience with cybercrime.

Phishing emerges as the most widespread and recognizable type of cybercrime across both quantitative and qualitative data. At the same time, less frequent but more severe threats—such as data breaches, identity theft and ransomware—are associated with stronger negative consequences and higher perceived seriousness. This creates a gap between prevalence and perceived impact: the most common threats are not always those considered most harmful.

A key cross-cutting finding is the central role of the human factor. All groups—general public, businesses and experts—identify user behaviour as the main vulnerability. However, responses to this differ significantly. Individuals tend to view cybersecurity as a matter of personal responsibility but act inconsistently. Businesses address this risk through structured approaches, including policies, training and technical controls. Experts frame the issue at a systemic level, pointing to institutional, regulatory and capacity constraints.

The research also highlights the growing role of artificial intelligence. Across groups, AI is seen as both an enabler of more sophisticated attacks and a tool that can support users. Its use increases the scale, speed and realism of cyber threats, making detection more difficult.

Trust in institutions is consistently low. Although survey data shows a stated willingness to report cyber incidents, especially in serious cases, qualitative findings indicate scepticism about the effectiveness of law enforcement. The reasons differ by group: the public refers to negative experience and bureaucracy, businesses prefer to rely on internal or private solutions, and experts point to systemic limitations. At the same time, there are clear expectations, especially among the public — for a stronger role of the state, which is not currently met.

Finally, the study identifies a strong demand for information, particularly regarding complex and high-impact threats such as data breaches and identity theft. Combined with mixed assessments of institutional preparedness, this indicates a gap between the scale of the problem, user needs and the current capacity of response systems.

Overall, the findings show a high level of exposure to cyber risks, uneven preparedness across groups, and the need for more systematic, coordinated and trust-based approaches to cybersecurity.

2. Quantitative Research

2.1. Summary

The quantitative survey shows that internet use is deeply embedded in daily life in Ukraine. Most users spend several hours online each day and actively use the internet for communication, information, services and entertainment. This high level of engagement is combined with a strong awareness of cyber risks: the vast majority recognize cybercrime as a real threat and see themselves as vulnerable.

At the same time, users report relatively widespread use of basic protection measures, such as avoiding suspicious websites and apps and limiting the sharing of personal data. Most also use device-level protection, including passwords, PIN codes and biometrics. Despite this, a significant number of respondents report having already experienced cybercrime, which indicates that existing behaviours do not fully prevent exposure to risks.

Phishing is the most widespread type of cybercrime and is experienced by a majority of users. Other types of incidents, such as account takeovers, data breaches, online abuse, service disruption and ransomware, are also present, though less common. However, the frequency of experience does not fully match perceived severity. Data breaches and identity theft are seen as the most serious threats and are associated with the strongest negative impact on life, even if they are reported less often than phishing. Phishing, while more common, is perceived as somewhat less severe in its consequences.

The impact of cybercrime varies by type, with identity theft, phishing and online abuse causing the highest levels of distress or harm. At the same time, there is a relatively high stated willingness to report incidents to authorities, especially in more serious cases, although this is based on perceived behaviour rather than actual reporting.

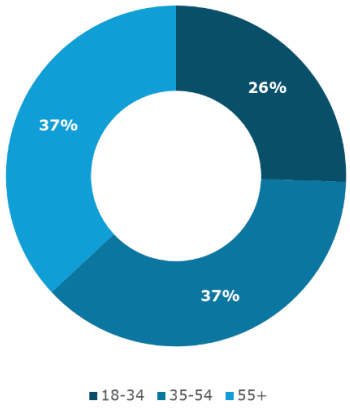
There is a clear demand for more information about cyber threats, particularly about data breaches and identity theft. Finally, assessments of the preparedness of authorities are mixed: while some users believe that institutions are at least somewhat prepared, a substantial share view them as unprepared to effectively respond to cybercrime.

2.2. Technical Information

Gender

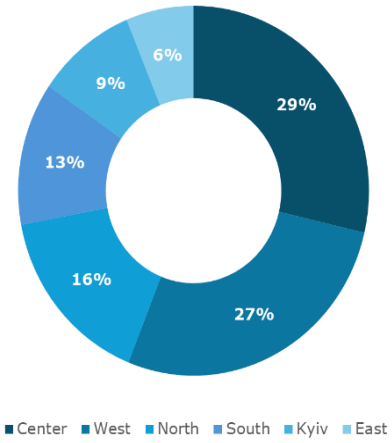
Women constitute 55% of the sample and men 45%. Overall, the sample closely reflects the gender distribution of the general population in this age group (48.2% men and 51.8% women[1]).

Figure 1. Age



Respondents aged 18-34 make up 26% of the sample, whereas the 35–54 and 55+ age groups are equally represented at 37% each (*Figure 1.* Age

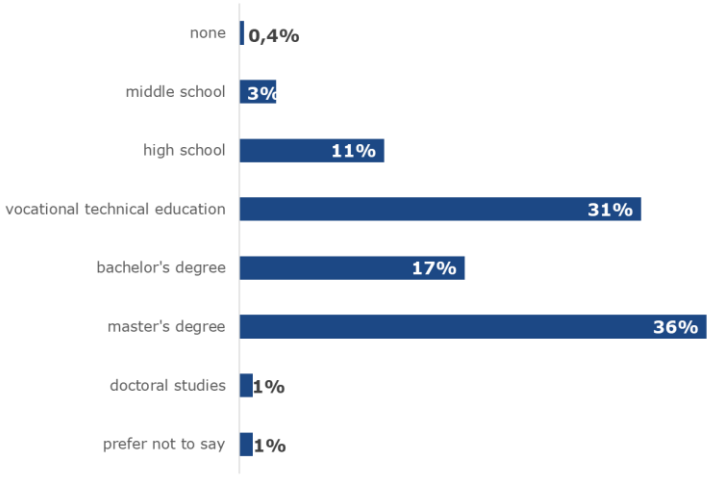
Figure *2. Region*



Respondents are most represented in the central (29%) and western (27%) regions, followed by the north (16%), south (13%), Kyiv (9%), and the east (6%) as shown in ***Error! Reference s ource not found.***.

[1] Державна служба статистики України (n.d.). Статистика населення України. Retrieved January 10, 2022, from http://database.ukrcensus.gov.ua/MULT/Dialog/statfile_c.asp

Figure 3. Highest level of education



The majority of respondents have higher or vocational education. 36% of respondents hold a master's degree and 31% have vocational technical education, while 17% have a bachelor's degree. Smaller shares report high school (11%) or middle school (3%) as their highest level of education. Only 1% have completed doctoral studies, 0.4% have no formal education, and 1% preferred not to say (*Figure*).

2.3. Research Methodology

The quantitative stage of the study was conducted using a computer-assisted web interviewing (CAWI) approach via the proprietary Sapiens Online panel. The panel includes over 100,000 active members and is managed using in-house software for panel administration, invitation delivery and questionnaire completion. This infrastructure enables efficient fieldwork, cost control and full oversight of data collection processes.

In total, 1,232 respondents aged 18 and above were surveyed, exceeding the target sample size of 1,000. The sample was constructed to reflect the structure of the adult population of Ukraine by key socio-demographic characteristics, including age, gender, region and type of settlement. The reference population structure corresponds to January 2022. To ensure comparability with the pre-war population distribution, respondents were asked about their place of residence prior to the full-scale invasion.

The panel covers all regions of Ukraine and includes both urban and rural residents, allowing for the implementation of quotas that reflect the national population structure. Panellists participate via web links accessible on both desktop and mobile devices, without restrictions by specific applications or platforms.

To bring the selected sample into line with the population structure, correction weights were applied.

Sample of the survey of individuals

Macro-region	Regions	Area	Quotas Planned	Total Collection
Centre	Vinnytsia, Dnipropetrovsk, Poltava, Cherkasy, Khmelnytskyi, Kirovohrad regions	Urban	184	237
		Rural	91	74
East	Kharkiv, Donetsk, Luhansk regions	Urban	75	175
		Rural	15	16
Kyiv	City of Kyiv	Urban	86	115
North	Chernihiv, Kyiv, Sumy, Zhytomyr regions	Urban	93	107
		Rural	53	43
South	Kherson, Mykolaiv, Odessa, Zaporizhia regions	Urban	104	157
		Rural	38	38
West	Chernivtsi, Ivano-Frankivsk, Lviv, Rivne, Ternopil, Volyn, Zakarpattia regions	Urban	131	169
		Rural	130	101
Total			**1000**	**1232**

The study adheres to international research and data protection standards. The panel complies with EU GDPR requirements. The information is stored on secure cloud infrastructure located

in Germany. The company follows ICC/ESOMAR standards as a corporate member of ESOMAR and adheres to the Global Data Quality (GDQ) initiative.

A set of quality control measures is applied to ensure data reliability. These include validation questions within the questionnaire, monitoring of interview duration, prevention of multiple submissions from the same device, and consistency checks between survey responses and panel profiling data. In addition, response patterns, including open-ended answers and distributions across closed questions, are systematically reviewed.

As with all non-probability online panels, the sample may be limited in its representation of individuals with limited internet access or lower digital literacy. This should be taken into account when interpreting the results.

2.4. Use of Internet

2.4.1. Use of electronic devices

The use of personal electronic devices was measured based on respondents' self-assessment. First, respondents were asked about the daily time they spend using their personal electronic devices online, and then – about total use (including offline activity). The most common level of online use of personal electronic devices was 3–6 hours per day; in total, 54% of respondents reported this, including 28% who spend 3–4 hours online and 26% who spend 5–6 hours daily. A somewhat smaller share (17%) used their personal electronic devices for 7–8 hours per day. At the same time, 7% of respondents spent more than 12 hours online daily. The least common is minimal use: only 1% of respondents spend less than one hour per day on this.

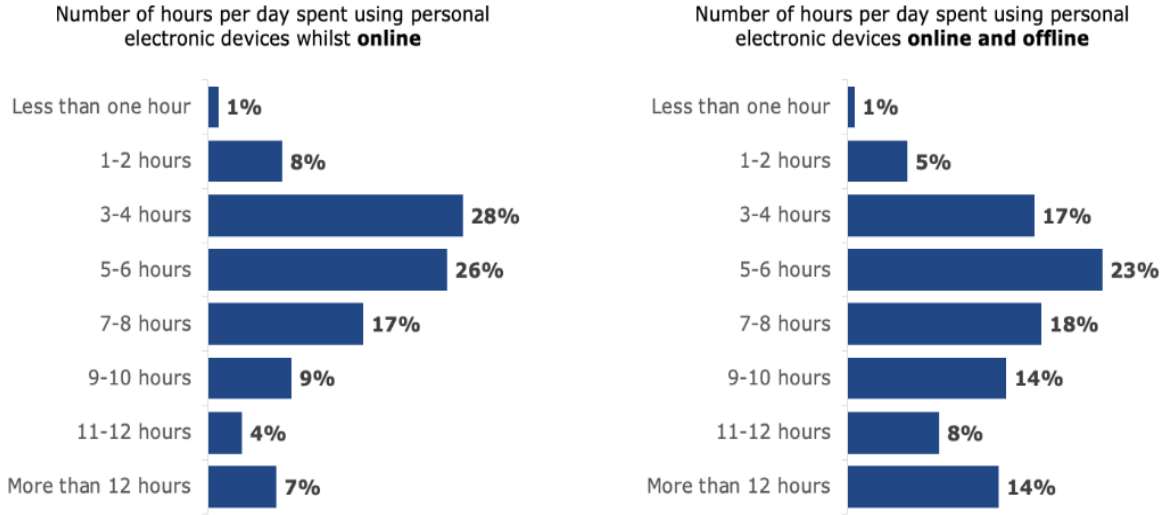
When considering the total use of personal electronic devices (online + offline), the distribution shifts towards longer usage. More than half of respondents (54%) spend 7 or more hours per day using their devices. At the same time, the 3–6 hour range, which dominates for online use, remains substantial for total device use as well (40%). Low-intensity use, as with online use, is negligible (1% less than one hour, 5% 1–2 hours).

At the same time, it should be considered that the survey was conducted online, therefore the obtained estimates may be somewhat biased towards more intensive internet use (*Figure 4*).

Figure 4. Hours using electronic devices (online vs online and offline)

Q: How many hours per day do you use your personal electronic devices ONLINE?

Q: Considering these devices, how many hours per day do you use them OVERALL?



The distribution of time spent online differs by respondents' age. Among young people aged 18–34, it is shifted towards more intensive use; they more often spend 7–8 hours online per day (21% vs. 15–16% in other age groups) and 9–10 hours (12% vs. 8%).

Shorter usage intervals are more typical for older groups: only 4% of young people spend 1–2 hours online per day, compared to 9–11% among respondents aged 35–54 and 55+. Similarly, 22% of young people spend 3–4 hours online per day, compared to 29–31% in older age groups.

At the same time, no statistically significant differences between age groups are observed either in the central part of the distribution or for the maximum values. In particular, 25–28% of

respondents across all age groups spend 5–6 hours online per day, 3–4% spend 11–12 hours, and 7–9% spend more than 12 hours per day online (Table 1).

Table 1. Number of hours per day spent using personal electronic devices online (by age group)

Hours per day (online)	Age group		
	A (18-34)	B (35-54)	C (55+)
Less than one hour	0%	**2%**(A, C)*	0%
1-2 hours	4%	**9%**(A)*	**11%**(A)*
3-4 hours	22%	**29%**(A)*	**31%**(A)*
5-6 hours	28%	26%	25%
7-8 hours	**21%**(B)*	15%	16%
9-10 hours	**12%**(B, C)*	8%	8%
11-12 hours	4%	4%	3%
More than 12 hours	9%	7%	7%

* - *statistically significant differences compared to the age group indicated in parentheses.*

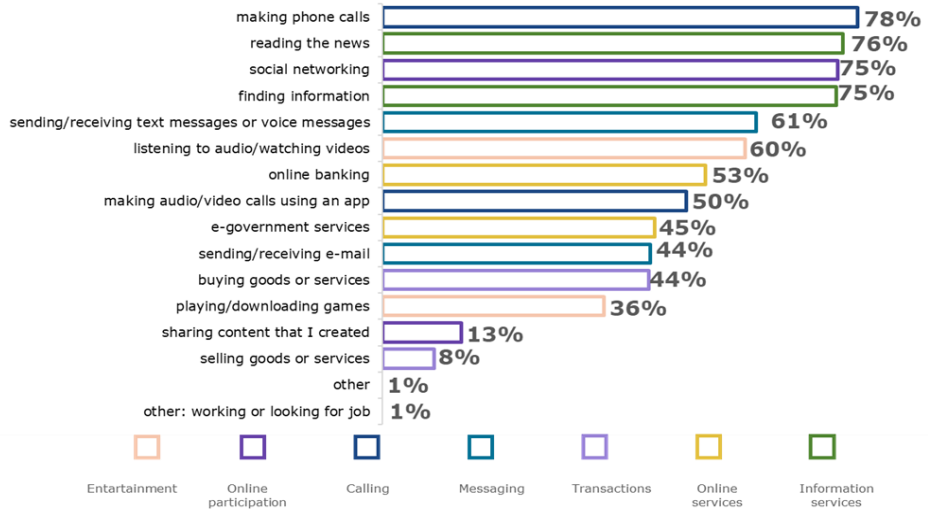
2.4.2. Online Activities

Ukrainians primarily use the internet for communication and for reading the news. In particular, 78% of respondents use the internet for making phone calls, 76% for reading the news, and around three quarters for social networking and finding information (*Figure*).

The second tier in terms of prevalence includes sending/receiving text or voice messages (61%) and listening to audio/watching videos (60%). Somewhat less frequently, respondents use online banking (53%) and make audio/video calls using an app (50%). At the same time, a substantial share also use the internet for e-government services (45%), as well as for sending/receiving e-mail and buying goods or services (44% each).

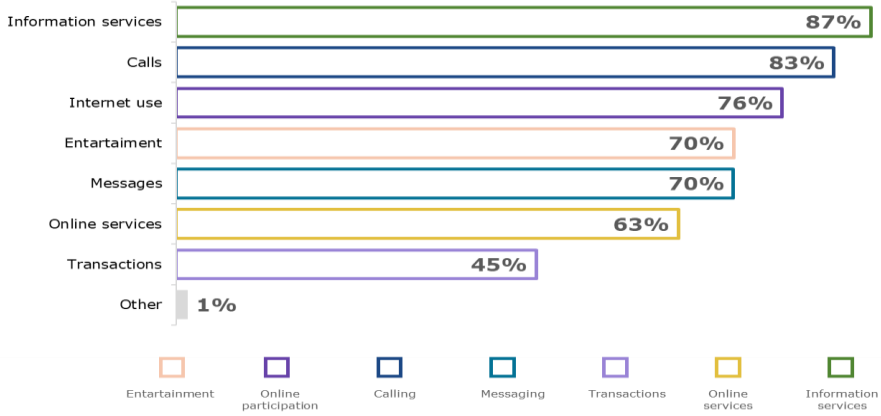
Figure 5. Activities online at least once per week

Q: Which of these online activities do you do, on average once per week or more often?



Aggregation by broader categories of internet use confirms these trends (*Figure*). The most widespread are information services (87%) and communication (calling – 83% and messaging – 70%). Overall internet use is also high (76%), as well as use for entertainment (70%). Online services are somewhat less popular – used by 63% of respondents, while the lowest index is observed in the "Transactions" category, which includes financial operations and buying goods or services (45%).

Figure 6. Activities online at least once per week (groups)



The distribution of types of online activities is relatively even across age groups, although statistically significant differences are observed for some activities (*Table 2*).Calling via the internet is common across all age groups, but the highest share is recorded among respondents aged 55+ (58%), which is statistically significant compared to those aged 35–54. Young people also demonstrate a high level of use of calling (84%). Sending/receiving messages (68–74%) and conducting online transactions (44–47%) remain consistently widespread across all age groups without statistically significant differences. The use of information services increases significantly with age: among respondents aged 55+, this indicator reaches 92% and is statistically higher compared to young people and those aged 35–54. Entertainment content, on the contrary, is more typical for younger respondents: 74% among those aged 18–34 compared to 67% among those aged 35–54 (the difference is statistically significant).

Table 2. Activities online at least once per week (by age group)

Activities	**Age group**		
	A (18-34)	**B (35-54)**	**C (55+)**
Calls	84%	79%	**85%(B)***
Messages	74%	68%	70%
Internet use	77%	73%	**79%(B)***
Information services	83%	86%	**92%(A, B)***
Entertainment	**74%(B)***	67%	70%
Transactions	47%	44%	45%
Online services	63%	59%	**67%(B)***
Other	1%	1%	3%

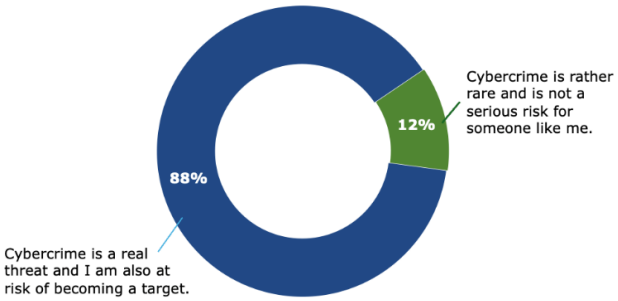
* - *statistically significant differences compared to the age group indicated in parentheses.*

2.5. Knowledge, awareness, and attitudes towards cybercrime

2.5.1. Level of knowledge

Figure 7. Awareness of cybercrime as a real threat

Q: After reading this definition, please tell me with which of these two statements you agree more.



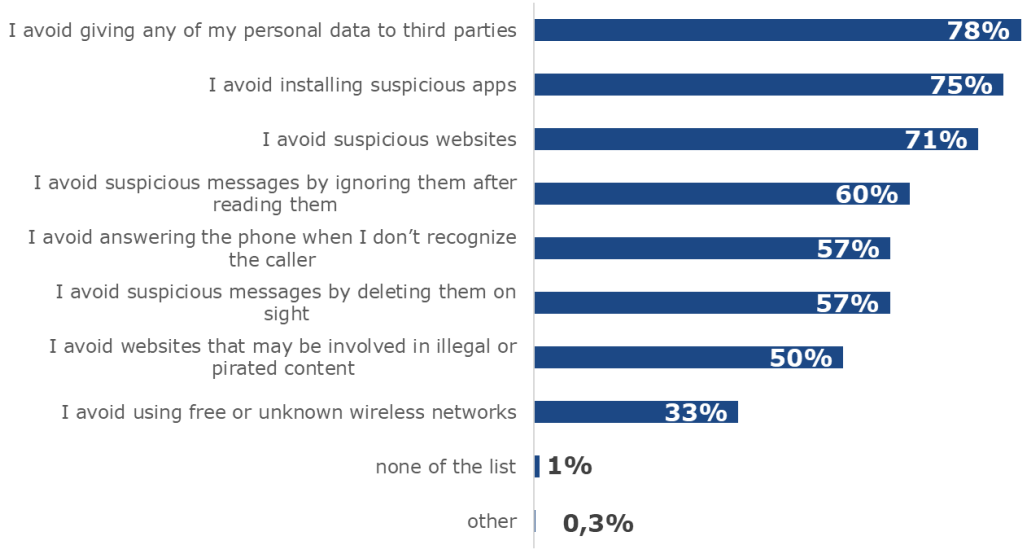
The majority of respondents (88%) recognize cybercrime as a real threat and acknowledge that they may become a target of cybercrime. Only 12% believe that cybercrime is rather rare and does not pose a serious risk to them (*Figure*).

A high level of awareness of cybercrime translates into proactive behaviour among most respondents. The most common practices include avoiding actions such as giving any of their personal data to third parties (75%), installing suspicious apps (75%), and visiting suspicious websites (71%).

Around 60% ignore suspicious messages after reading them, while 57% avoid answering the phone when they don't recognize the caller or delete suspicious messages on sight. Half of respondents avoid websites that may be involved in illegal or pirated content, while one third avoid using free or unknown wireless networks. At the same time, only 1% of respondents do not follow any of the listed protective measures (*Figure*).

Figure 8.Risks generally avoided to protect yourself from cybercrime

Q: Which of these risks do you generally avoid, to protect yourself from cybercrime?

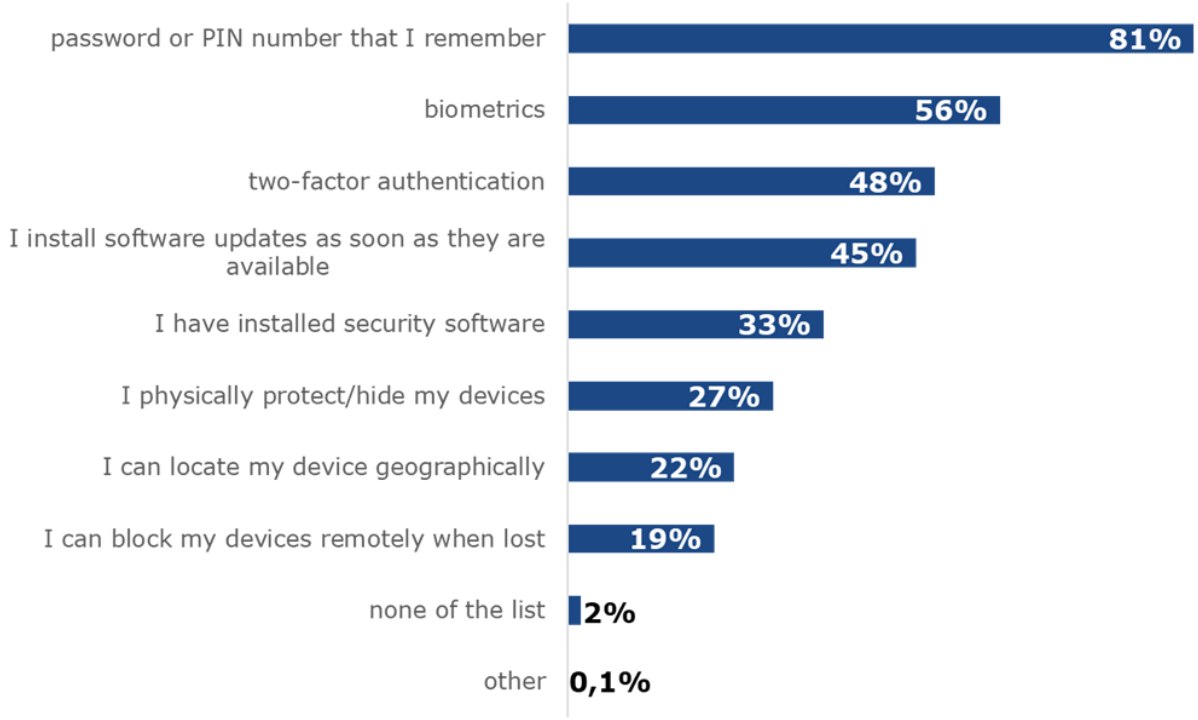


Basic tools dominate in keeping devices safe: 81% of respondents use a password or PIN number that they remember, and 56% use biometrics (fingerprint, face recognition). Two-factor authentication (an extra login step via a separate app or SMS) is used somewhat less frequently (48%).

Additional practices include the installation of software updates as soon as they are available (45%) and having installed security software (for example, anti-virus or anti-malware) (one third of respondents). Less common are physically protecting or hiding devices (27%), the ability to locate a device geographically (22%), and the ability to block devices remotely when lost (19%). At the same time, only 2% of respondents do not use any of the listed measures (*Figure*).

Figure 9. Ways of keeping devices safe

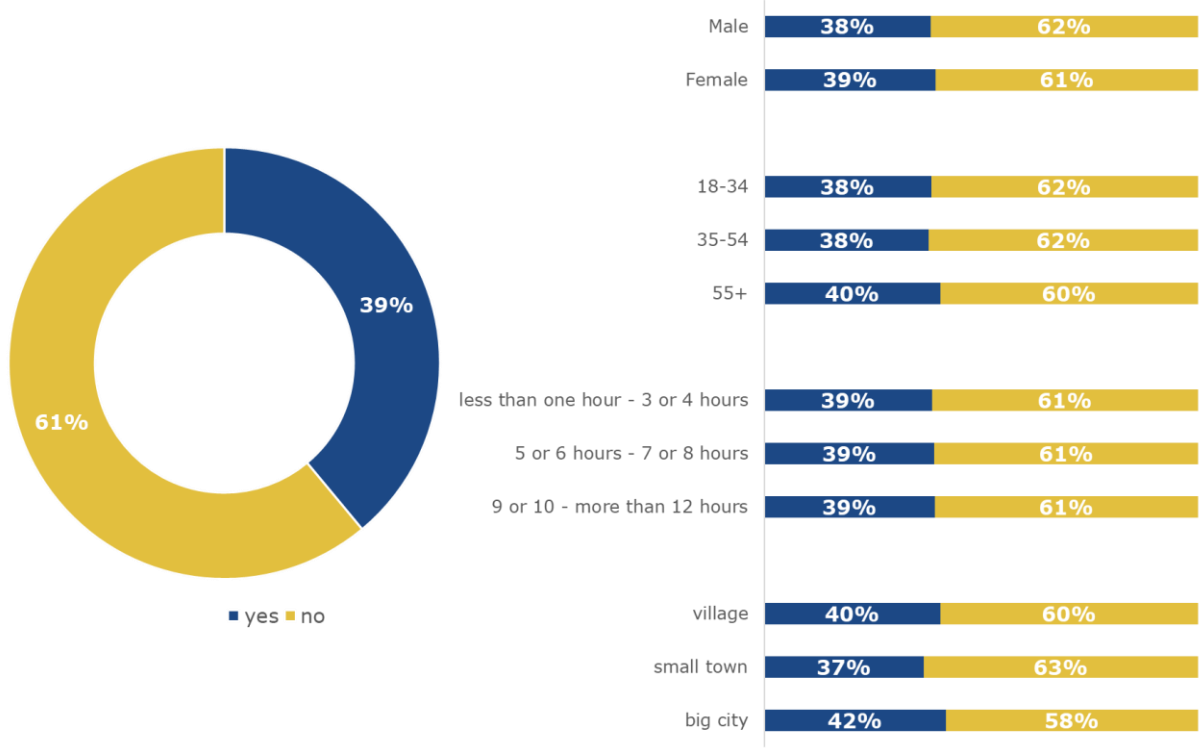
Q: How do you keep your devices safe?



The majority of respondents (61%) reported that they have never been targeted by cybercrime, while 39% indicated that they have had such an experience. At the same time, no significant differences were found by demographic characteristics or by the level of daily online use between those who reported being targeted by cybercrime and those who avoided it (*Figure 10*).

Figure 10. Awareness of being targeted by cybercrime

Q: To your knowledge, have you ever been targeted by cybercrime?

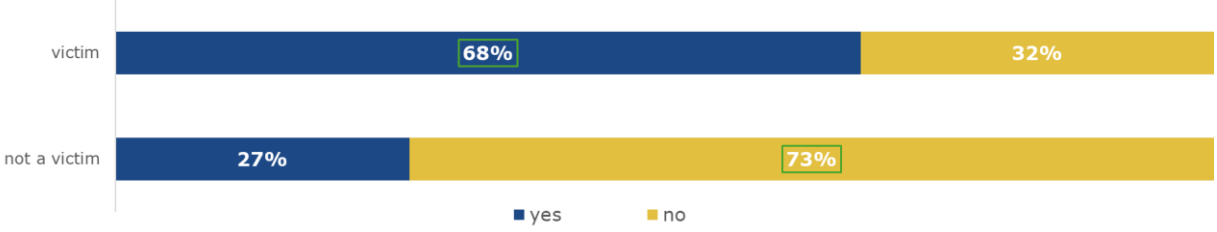


In the subsequent analysis, we do not rely solely on respondents' self-assessment. An analytical variable was constructed to classify respondents into "victims" and "non-victims" of cybercrime based on their responses to specific cybercrime situations discussed during the survey. The comparison shows discrepancies between general self-assessment and the experience captured through responses to specific cases.

Perceiving oneself as a potential target differs significantly depending on the presence of such experiences; among those who have been targeted by cybercrime, 68% consider themselves at risk, while among those without such experience, this share is only 27%. The difference between these figures is statistically significant (*Figure 21*).

Figure 21. Awareness of being targeted by cybercrime (victims vs non-victims)

Q: To your knowledge, have you ever been targeted by cybercrime?



2.5.2. Phishing

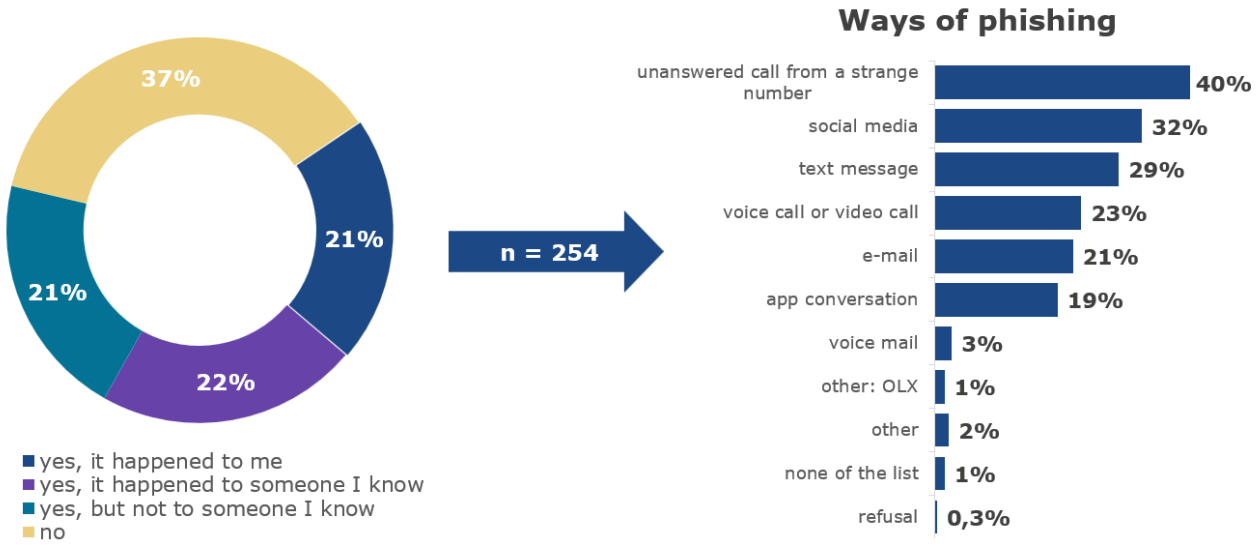
Phishing was defined to respondents as a situation in which criminals use remote contacting through phone, e-mail, messages or social networks to trick or threaten the recipient into sending them money or private information, or installing malicious software. After reading this definition, respondents were asked about their experience (*Figure 3*).

21% reported that phishing happened to them, another 22% said it happened to someone they know, and 21% are aware of such cases but not among their acquaintances. At the same time, 37% indicated that they have not had such experience.

Among those who personally experienced phishing, the most common contact channel was an unanswered call from a strange number (trying to get them to call back), reported by 40%. This is followed by social media (32%) and text messages (29%). Less frequently, phishing contacts were received via voice or video calls (23%), e-mail (21%), and app conversations (19%). Isolated cases include voice mail (3%) and the OLX app (1%).

Figure 32. Awareness of phishing happened and ways of receiving messages over the past 12 months

Q: After reading this definition, are you aware of phishing happening in the past 12 months?
Q: Please indicate in which of the following ways you may have received any phishing messages over the past 12 months, on any of your personal devices or accounts? Select everything that applies.

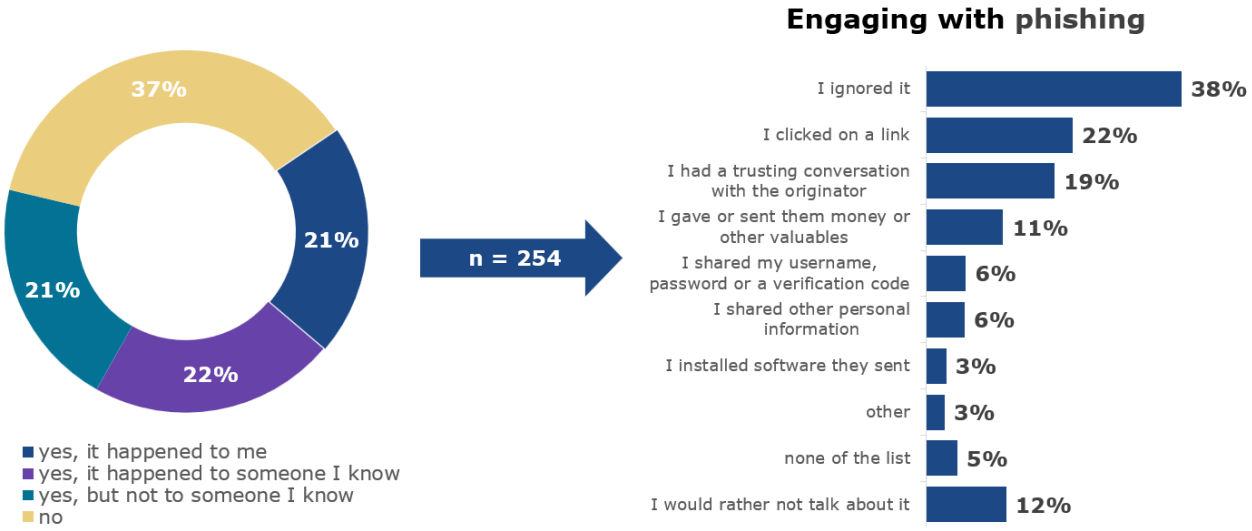


Respondents who had experienced phishing were also asked about how they engaged with such messages. The most common reaction was ignoring them – reported by 38% of respondents. At the same time, a substantial share demonstrates risky behaviour: 22% clicked on a link, and 19% had a trusting conversation with the originator. In addition, 11% reported that they gave or sent money or other valuables, while 6% each said they shared their username, password or a verification code, or other personal information. At the same time, 12% of respondents refused to answer this question, which may indicate the sensitivity of the topic or reluctance to disclose personal experience (*Figure 43*).

Figure 43. Awareness of phishing happened and ways of engaging with it

Q: After reading this definition, are you aware of any phishing attempts happening to you in the past 12 months?

Q: How did you engage with these message(s) on your personal devices? Select everything that applies.

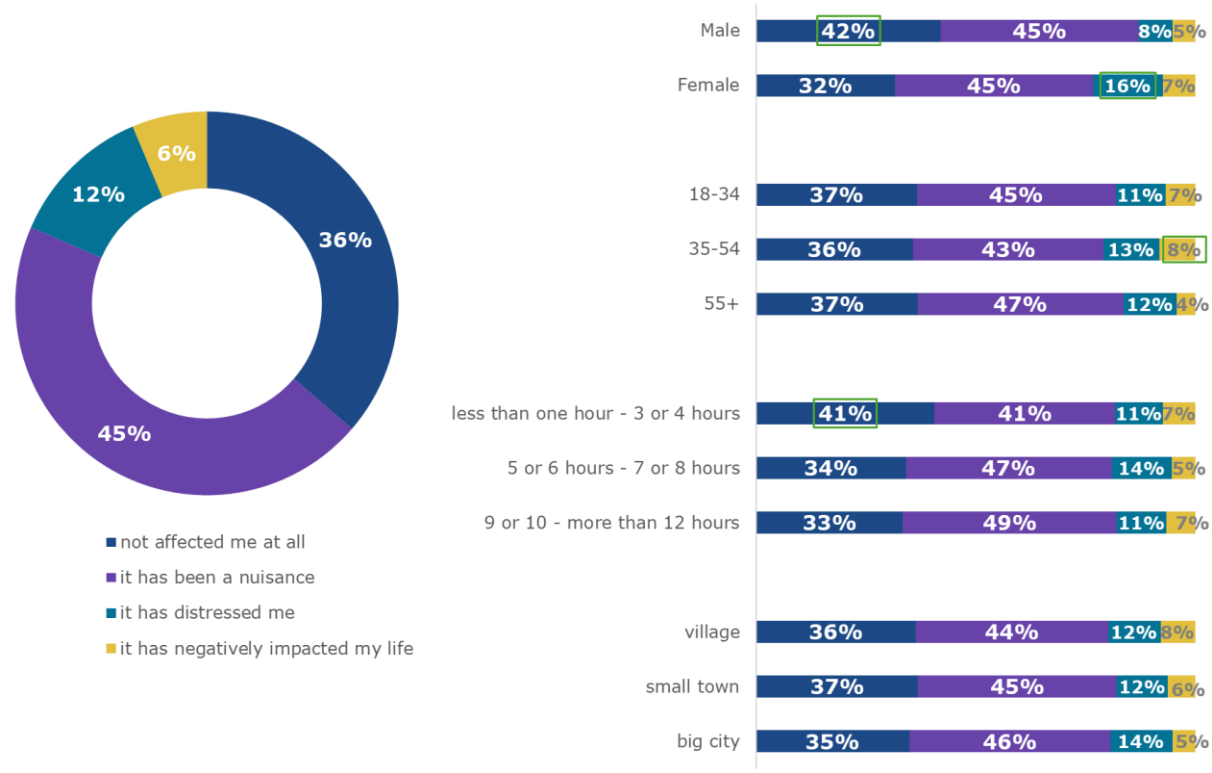


Regardless of personal experience, respondents were asked about how deeply phishing has affected their life. Most often, respondents indicated that it has been a nuisance (45%), while 36% reported that it has not affected them at all. At the same time, 12% said it has distressed them, and 6% reported that it has negatively impacted their life (*Figure 5*).

Subgroup analysis reveals a number of differences. Men were statistically significantly more likely than women to report no impact (42% vs. 32%), while women more often reported that it has distressed them (16% vs. 8% among men). Among respondents aged 35–54, a negative impact was reported more often than among younger respondents (8% vs. 4%). Respondents with lower levels of daily online use (up to 4 hours per day) more often indicated that phishing has not affected them at all (41% vs. 33–34% in other groups).

Figure 54. Impact of phishing on respondents' lives

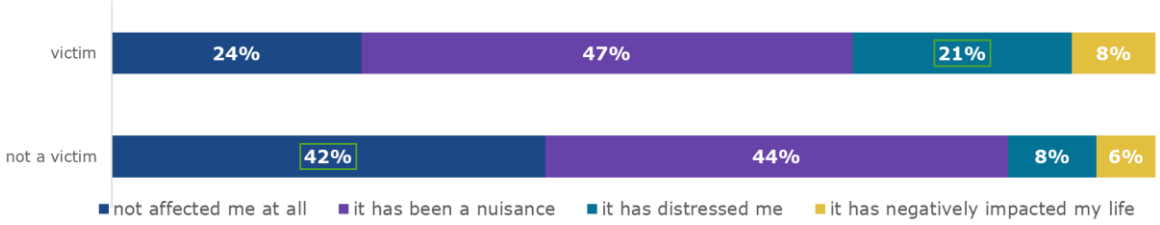
Q: How deeply has phishing affected your life over the past 12 months?



Among those who have been targeted by cybercrime, only 24% reported that phishing has not affected them at all, compared to a significantly higher share among those who were not targeted (42%). Those who have been targeted more often report more serious consequences: 21% of them said it has distressed them, which is statistically higher than the corresponding share among "non-victims" (8%), as shown in *Figure 65*.

Figure 65. Impact of phishing on respondents' lives (victims vs non-victims)

Q: How deeply has phishing affected your life over the past 12 months?



To assess respondents' likely reactions and their willingness to report cybercrime, an indirect projective question was used about the expected behaviour of "neighbours" in case of an incident, in order to reduce social desirability bias. Overall, most respondents expect that cases of phishing would be reported to the authorities: 31% believe this would happen in any case, and another 34% think it would happen only in serious cases. At the same time, 30% tend to believe that reporting would probably not occur, and 5% are certain that it would not happen at all.

Subgroup analysis shows differences in the perception of such behaviour. Women are statistically significantly more likely than men to believe that reporting should happen in any

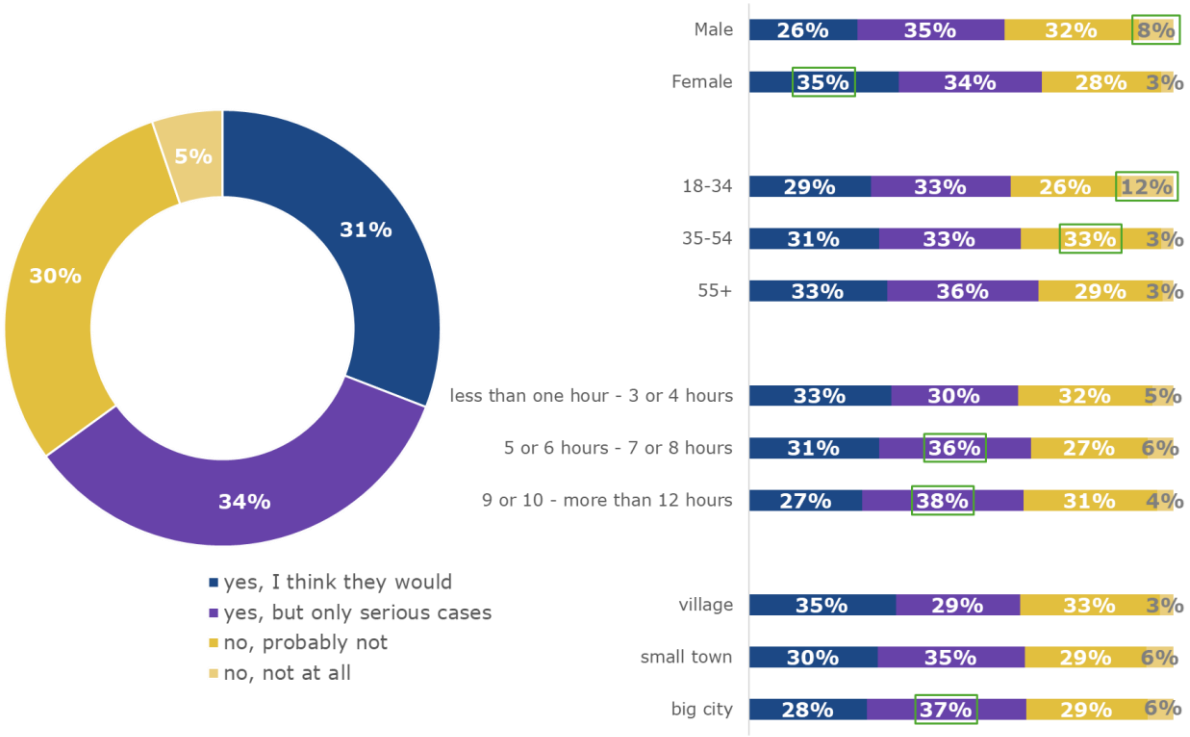
case (35% vs. 26%), while men more often assume a complete lack of reporting (8% vs. 3%). Young people under 34 more often choose the categorical position "not at all" (12% vs. 3% in older groups), while among respondents aged 35–54 the response "probably not" is more common (33% vs. 26% among younger respondents).

The level of online use is also associated with these perceptions: among those who spend 5 or more hours online per day, the position "reporting only in serious cases" is more prevalent (36% among those spending 5–8 hours and 38% among those spending 9+ hours, compared to 30% among those online up to 4 hours).

In addition, urban residents are more likely than rural residents to expect selective reporting: 37% in large cities and 35% in medium-sized cities compared to 29% in rural areas (*Figure 76*).

Figure 76. Reporting a phishing message to cyber police/government hotline

Q: If someone in your neighbourhood would receive a phishing message, and perhaps trustingly engage with it, do you think they would later report it to the cyber police, the government hotline, etc.?



2.5.3. Ransomware

Ransomware is defined as malicious software that blocks access to devices or data and demands payment to restore them. The majority of respondents (67%) reported that they have not had any experience with it, 19% said they are aware of such cases but not among people they know, and 10% reported that such cases occurred among their acquaintances. Only 3% of respondents have personally experienced ransomware.

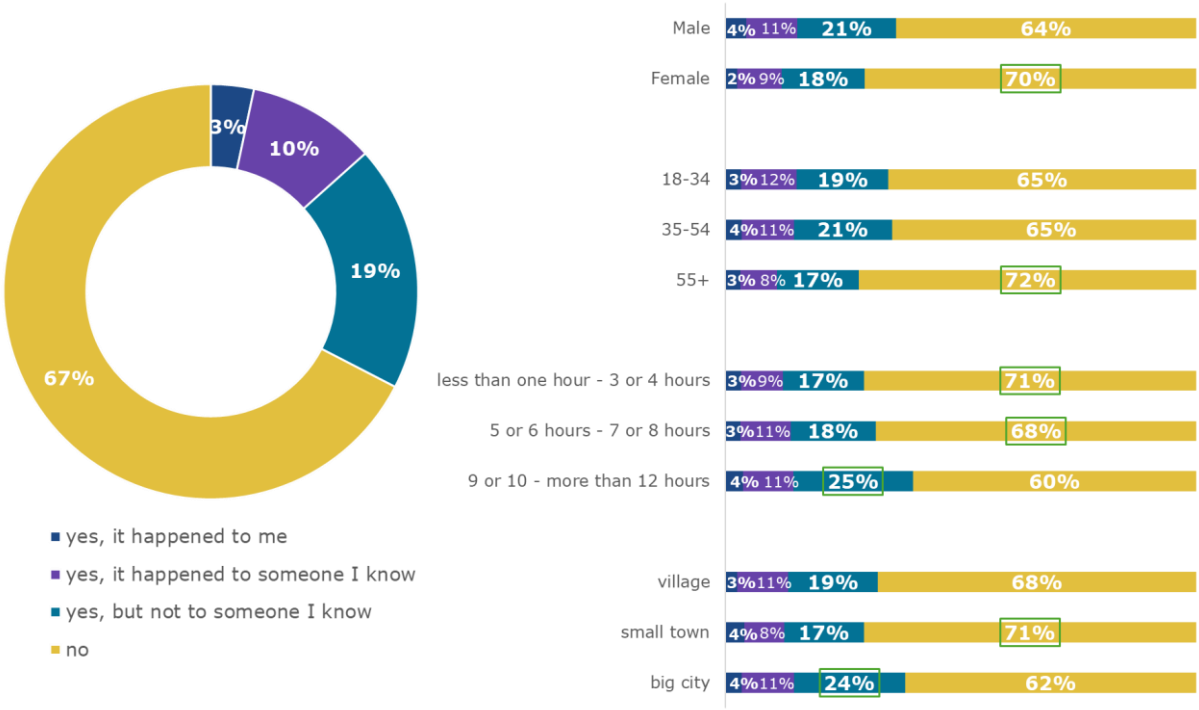
Women were statistically significantly more likely than men to report no such experience (70% vs. 64%). Respondents aged 55+ also more often than other age groups indicated that they had not heard of such cases.

At the same time, awareness increases with higher levels of online use: among those who spend 9 or more hours online per day, 25% are aware of ransomware attacks, which is statistically significantly higher compared to other groups.

By type of settlement, the lowest share of negative responses is observed among residents of large cities (62%), while in small towns this share is 71%, and in rural areas 68%, indicating a higher level of awareness in more urbanized environments (*Figure 87*).

Figure 87. Awareness of any ransomware attack in the past 12 months

Q: Are you aware of any ransomware attack in the past 12 months?

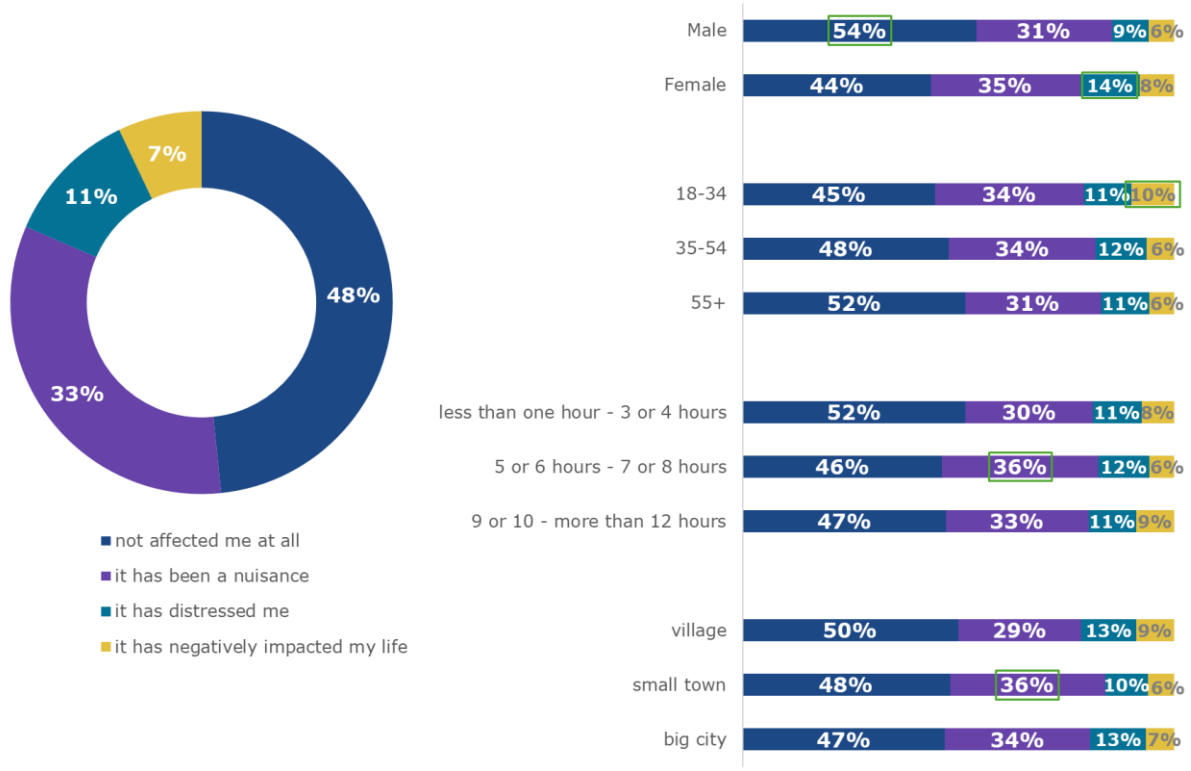


Despite the relatively low prevalence of experience with ransomware, its impact on respondents' lives is noticeable: slightly less than half (48%) reported that it has not affected them at all, while for 33% it has been a nuisance, 11% said it has distressed them, and 7% reported that it has negatively impacted their life (*Figure 9*).

Subgroup analysis shows differences in the perception of impact. Men were statistically significantly more likely than women to report no impact (54% vs. 44%). At the same time, young people more often reported a substantial negative impact (10% vs. 6% in other age groups). By type of settlement, residents of small and large cities more often indicated that it has been a nuisance (36% and 34%, respectively), which is higher compared to rural residents (29%).

Figure 98. Impact of ransomware attacks on respondents' lives

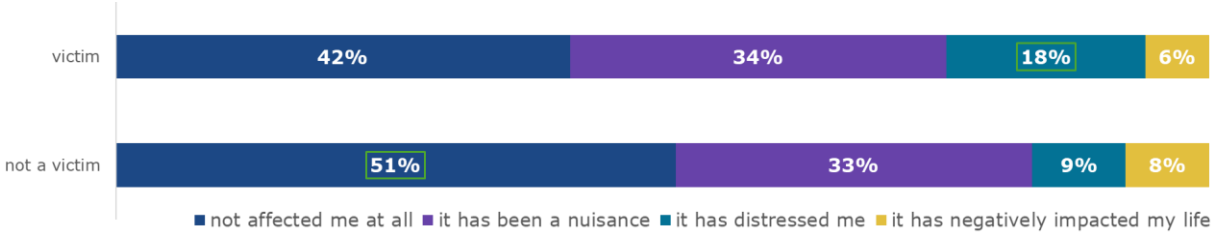
Q: How deeply has ransomware affected your life in the past 12 months?



Among those who identified themselves as victims, 42% reported that ransomware has not affected them at all (*Figure19*). However, a substantial share (18%) said it has distressed them, which is more than twice as high as among those who were not victims (9%). More than half of those who have not been targeted by cybercrime (51%) reported no impact at all. The share of those whose life has been negatively impacted by ransomware is relatively similar among victims (6%) and non-victims (8%).

Figure19. Impact of ransomware attacks on respondents' lives (victims vs non-victims)

Q: How deeply has ransomware affected your life in the past 12 months?



In response to the projective question on willingness to report a ransomware attack, most respondents show a tendency to contact the authorities: 34% believe this should be done in any case, and another 35% only in serious cases. At the same time, a quarter of respondents tend to believe they would probably not report it, while 6% are certain they would not do so.

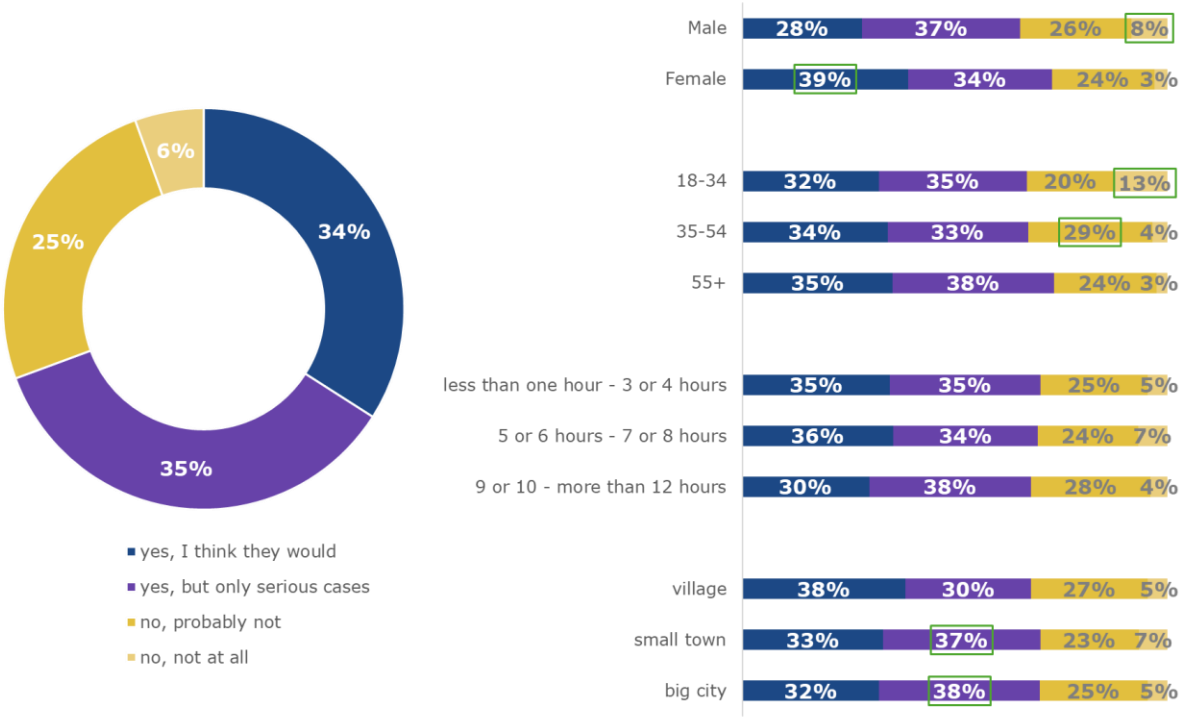
Subgroup analysis reveals notable differences. Men are statistically significantly more likely than women to state that they would definitely not report such an incident (8% vs. 3%), while women more often choose the option “in any case” (39% vs. 28%). Young people under 35 are

much more likely to take a categorical position of not reporting (13% vs. 3–4% among older groups), while respondents aged 35–54 more often lean towards "probably would not report" (29% vs. 20% among younger respondents and 24% among those aged 55+).

By type of settlement, urban residents are more likely than rural residents to consider reporting only in serious cases: 37% in small towns and 38% in large cities compared to 30% in rural areas, and this difference is statistically significant (*Figure 100*).

Figure 100. Reporting a ransomware attack to cyber police/government hotline

Q: Do you think the victim of ransomware would report it to the cyber police, the government hotline, etc.?



2.5.4. Intimidation and Abuse

In addition to phishing and ransomware, respondents were also asked about their experience with online intimidation, abuse and discrimination. The vast majority (73%) have not experienced such situations, while 16% reported that such cases happened to someone they know, and 4% each said it happened to them personally or to members of their family (*Figure*).

Subgroup analysis reveals some differences. Women were statistically significantly more likely than men to report no such experience (75% vs. 70%).

Young people and middle-aged respondents more often reported such cases among people they know (21% and 17%, respectively, vs. 12% among those aged 55+), as well as among family members (6% and 4% vs. 1%).

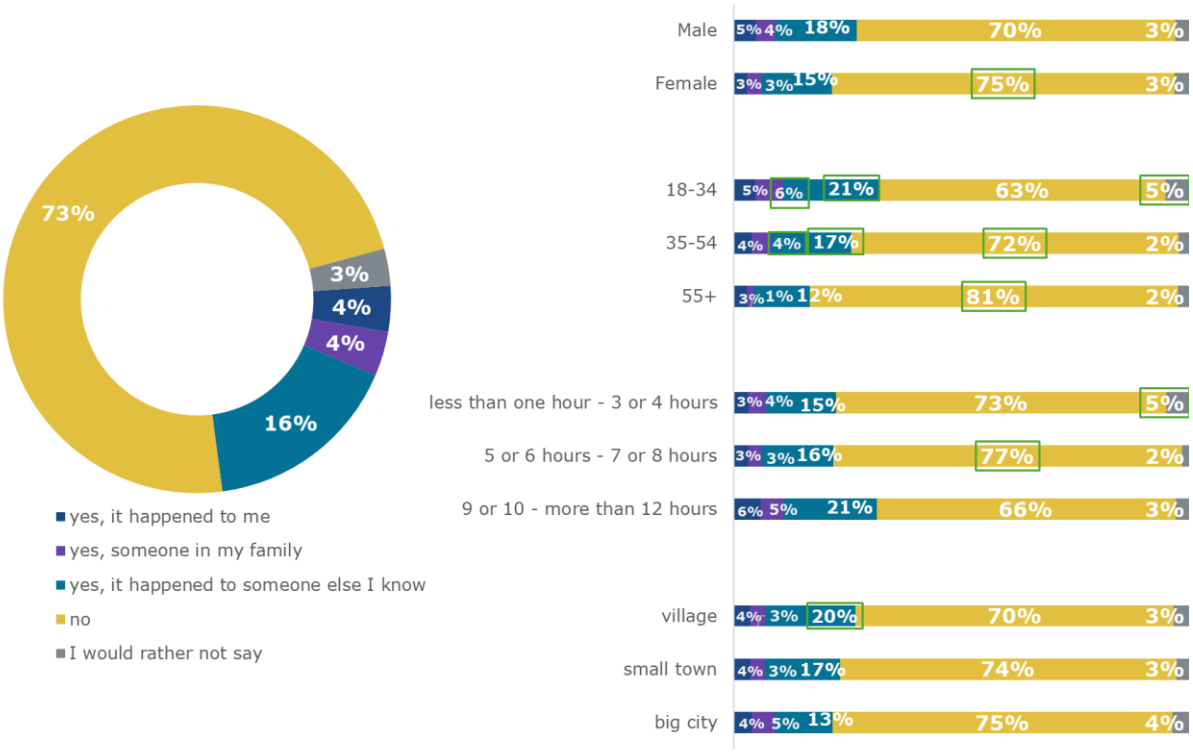
At the same time, respondents who spend 5–8 hours online per day more often than others indicated that they have not experienced such situations (77%). Young people were also slightly more likely to refuse to answer this question (5% vs. 2–3% in older groups).

Rural residents more often reported such experiences among people they know (20%) compared to residents of large cities (13%), while in small towns this share is 17%.

In addition, respondents who have been targeted by cybercrime more often indicated that members of their family had also experienced intimidation or abuse (8% vs. 2% among those without such experience), while the absence of such experience was more often reported by "non-victims" (78% vs. 60%).

Figure 21. Awareness of discrimination, abuse, intimidation or insults online in the past 12 months

Q: Some online interactions can be very intimidating. Has anyone that you personally know been insulted, discriminated against, abused or intimidated online, in the past 12 months?



Regardless of personal experience, respondents were asked about how deeply online intimidation has affected their life. Most often, respondents indicated that it has not affected them at all (43%), while 31% described it as a nuisance. At the same time, 17% said it has distressed them, and 8% reported that it has negatively impacted their life (*Figure 112*).

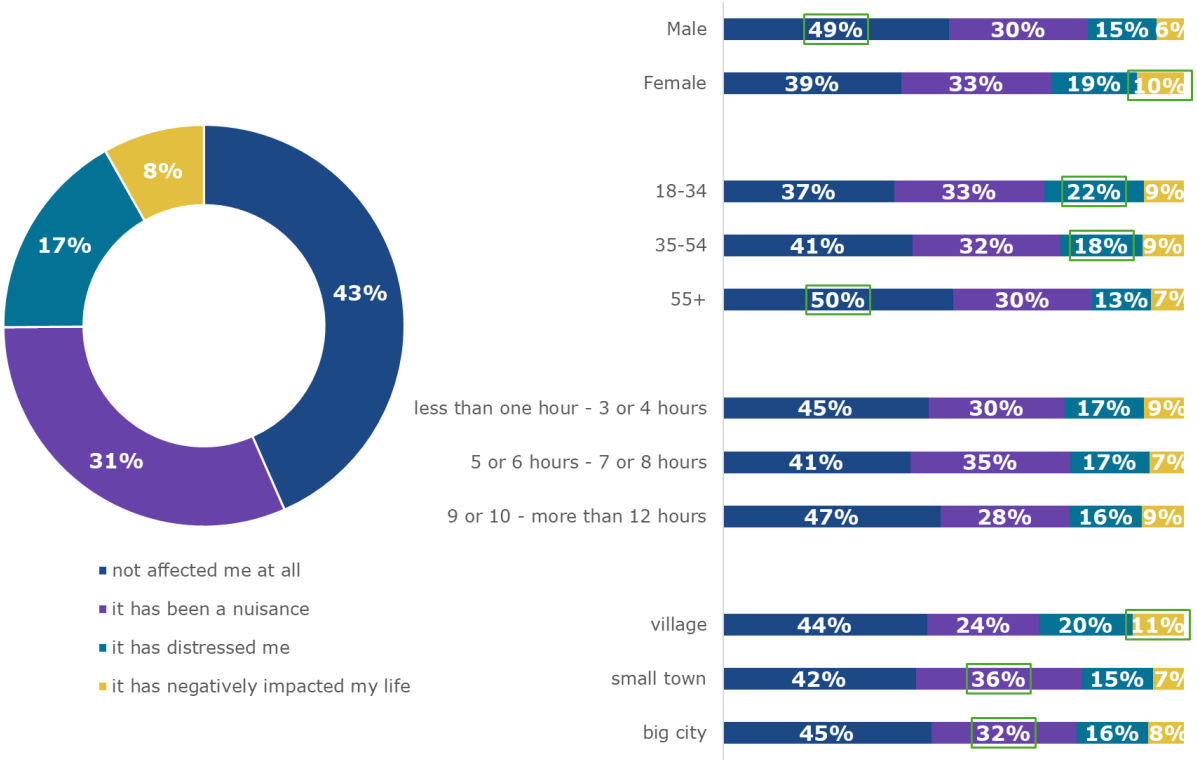
Subgroup differences are observed. Men more often than women reported no impact (49% vs. 39%) and were less likely to report a strong negative impact (6% vs. 10%).

Young people and middle-aged respondents more often reported that it has distressed them (22% and 18%, respectively, vs. 13% among those aged 55+), while the oldest age group more often indicated no impact at all (50% vs. 37% among young people and 41% among middle-aged respondents).

By type of settlement, rural residents more often reported a strong negative impact (11% vs. 7–8% in urban areas), while residents of medium-sized and large cities more often described the experience as a nuisance (36% and 32%, respectively, vs. 24% in rural areas).

Figure 112. Impact of intimidation on respondents' lives

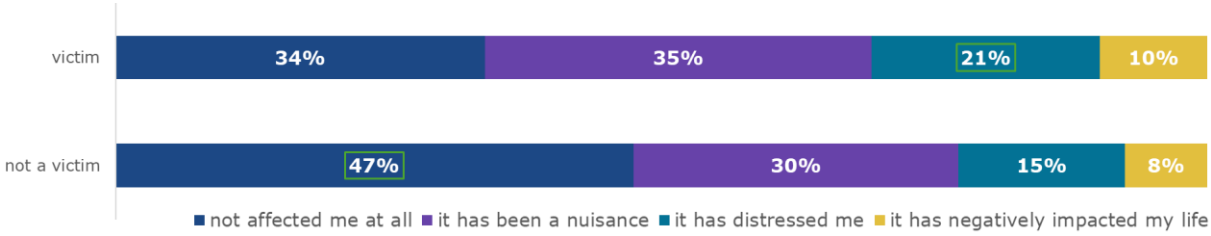
Q: How deeply has online intimidation affected your life over the past 12 months?



Those who were not targeted by cybercrime were significantly more likely to report that online intimidation has not affected them at all (47%) compared to those who have been targeted (34%). Conversely, victims of cybercrime showed a statistically higher tendency to report that such intimidation has distressed them (21%) or has negatively impacted their life (10%). For comparison, only 15% of non-victims reported that it has distressed them (*Figure 123*).

Figure 123. Impact of intimidation on respondents' lives (victims vs non-victims)

Q: How deeply has online intimidation affected your life over the past 12 months?



In response to the projective question on willingness to report online intimidation to the cyber police or a government hotline, there is an overall tendency towards reporting: 40% believe this should be done in any case, and another 37% only in serious cases. At the same time, 18% would probably not report it, while 5% are certain they would not do so under any circumstances (*Figure 134*).

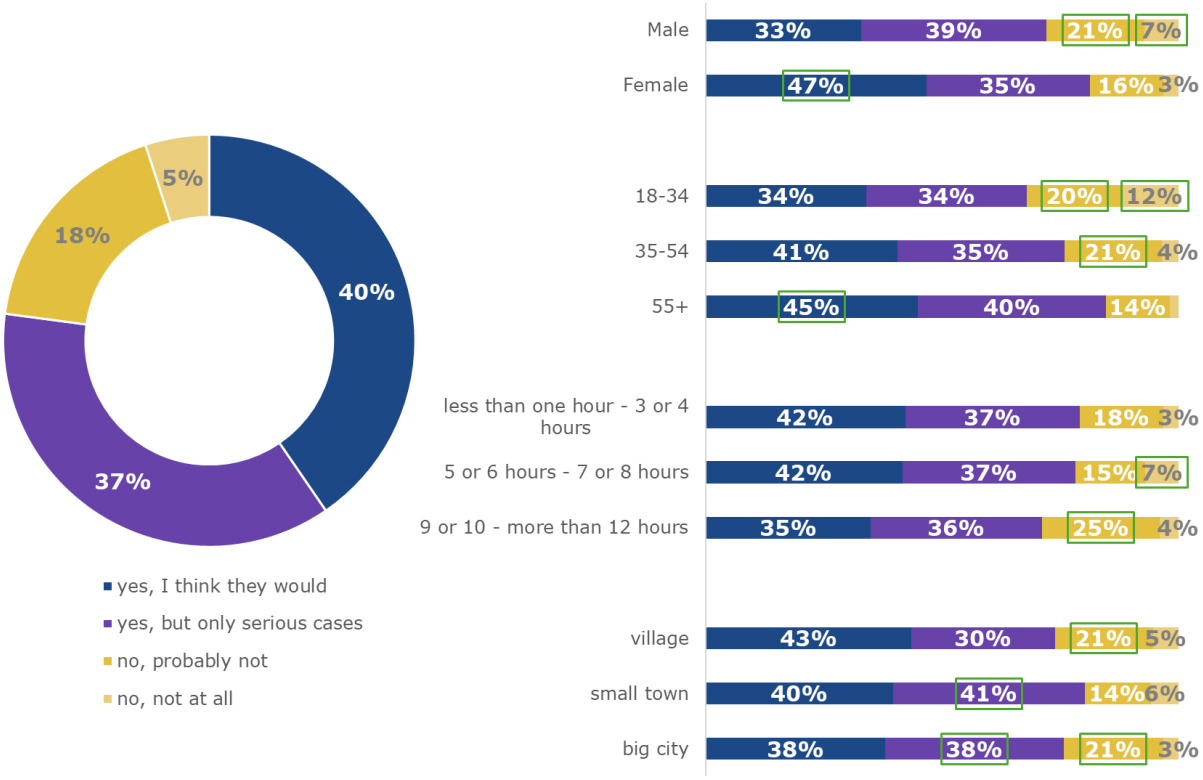
Subgroup differences are observed. Men are less inclined to report; only 33% support unconditional reporting (compared to 47% among women), while the percentage of those who would probably not report is higher (21% vs. 16%). Respondents aged 55+ more often take a proactive position (45% – "in any case") and are less likely to refuse reporting (14% vs. 20–21% among younger groups).

The level of online use is also associated with these attitudes. Among those who spend 5–8 hours online, categorical refusal to report is more common (7% vs. 3–4% in other groups), while among the most intensive users (9+ hours), the share of the response "probably not" increases (25% vs. 18% and 15% in less active groups).

By type of settlement, rural residents and those in large cities more often lean towards "probably not" (21% each), while in medium-sized cities this share is lower (14%). At the same time, residents of medium-sized and large cities more often consider appropriate to report only in serious cases (41% and 38%, respectively, vs. 30% in rural areas).

Figure 134. Reporting an online abuse to cyber police/government hotline

Q: I have asked a few questions about online abuse. If someone in your neighbourhood (or their child) fell victim to this, do you think they would report it to the cyber police, the government hotline, etc.?



2.5.5. Interference (services made unavailable)

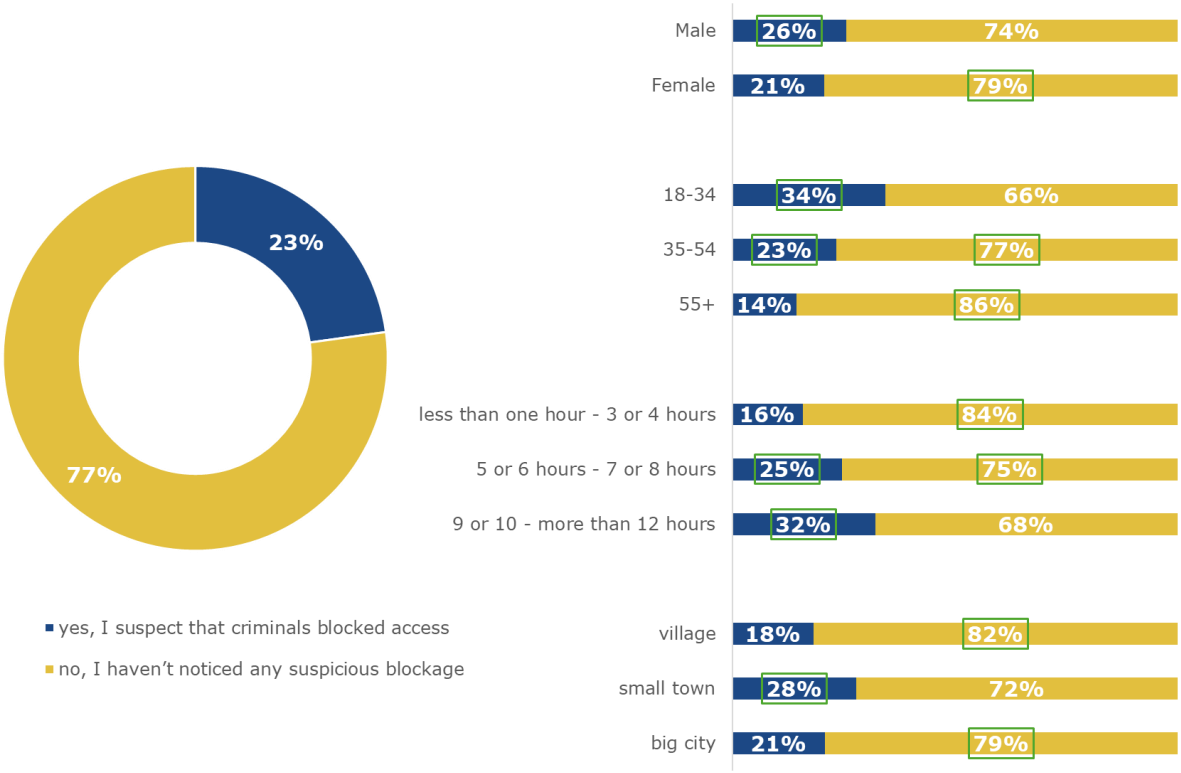
A separate question addressed the experience of online services being unavailable – whether due to technical malfunctions or deliberate blocking (DDoS attacks). The majority of respondents (77%) reported that over the past 12 months they had not experienced situations where important online services were unavailable for a prolonged period, while 23% had such experience (*Figure 14*).

Subgroup analysis shows statistically significant differences. Men were more likely than women to report such experience (26% vs. 21%). The highest share is observed among young people aged 18–34 (34%), compared to 23% among middle-aged respondents and a significantly lower share among those aged 55+ (14%), indicating a clear age gradient.

The level of online use is also associated with the frequency of such cases: among those who spend 9+ hours online per day, 32% reported service unavailability, while among users spending 5–8 hours online this share is 25%. Both figures are statistically significantly higher compared to less active users (16% among those online up to 4 hours).

By type of settlement, the highest share of such experience is observed among residents of small towns (28%), while in rural areas this indicator is the lowest (18%).

Figure 145. Reported incidents of prolonged and suspicious online service unavailability
Q19. In the past 12 months, has any of the online services that you rely on been suspiciously unreachable for a prolonged time?

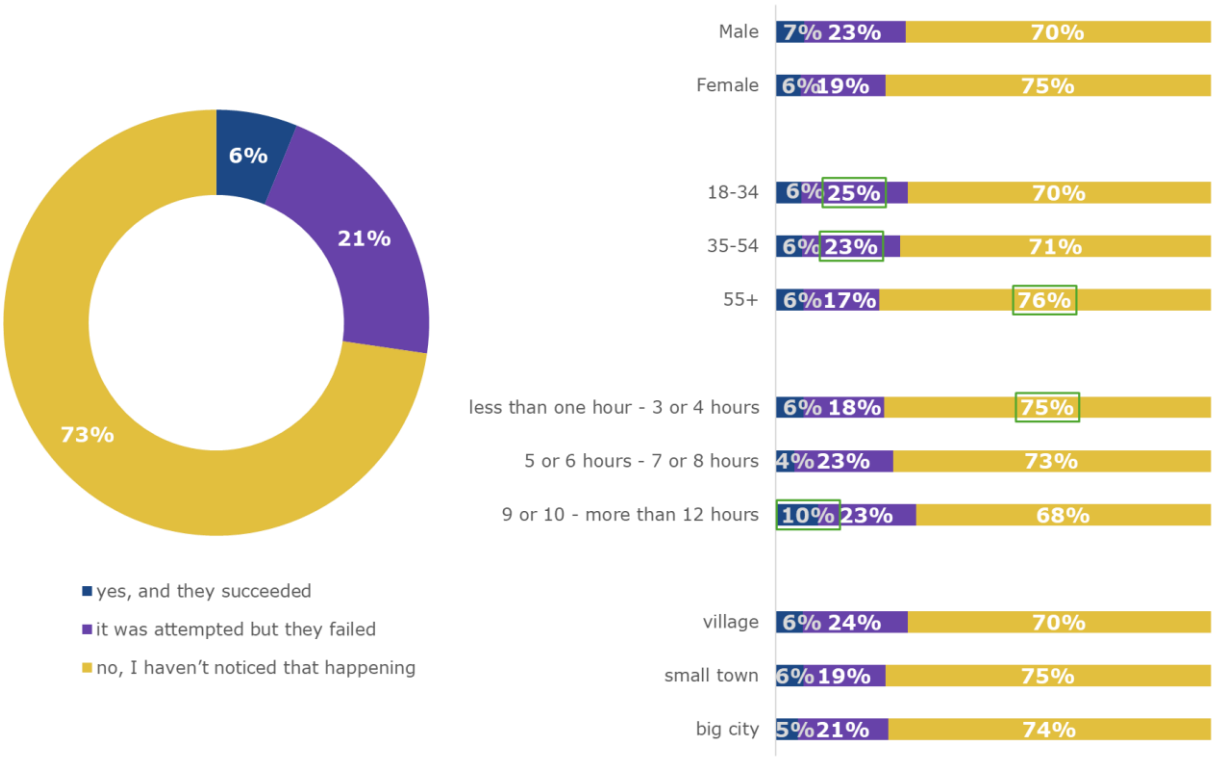


2.5.6. Data breaches and online identity theft

The next block focused on data breaches and online identity theft, which involve the unauthorized access to and use of personal information. Most of the respondents (73%) reported that they had not experienced such cases, while 21% indicated attempted access that was unsuccessful, and another 6% reported successful incidents.

Attempts of unauthorized access are more frequently reported among young people and middle-aged respondents (25% and 23%, respectively), which is statistically higher compared to those aged 55+ (17%). At the same time, this may partly be explained by a lower ability of older respondents to identify such attempts. Successful cases of access are more common among the most intensive internet users: among those who spend 9 or more hours online per day, the share reaches 10%, compared to 4–6% among less active users (*Figure 156*).

Figure 156. Awareness of unauthorized access to personal data or non-financial accounts
Q: In the past 12 months, have you become aware that any of your personal data or non-financial accounts had been used by anyone you did not allow to do it?



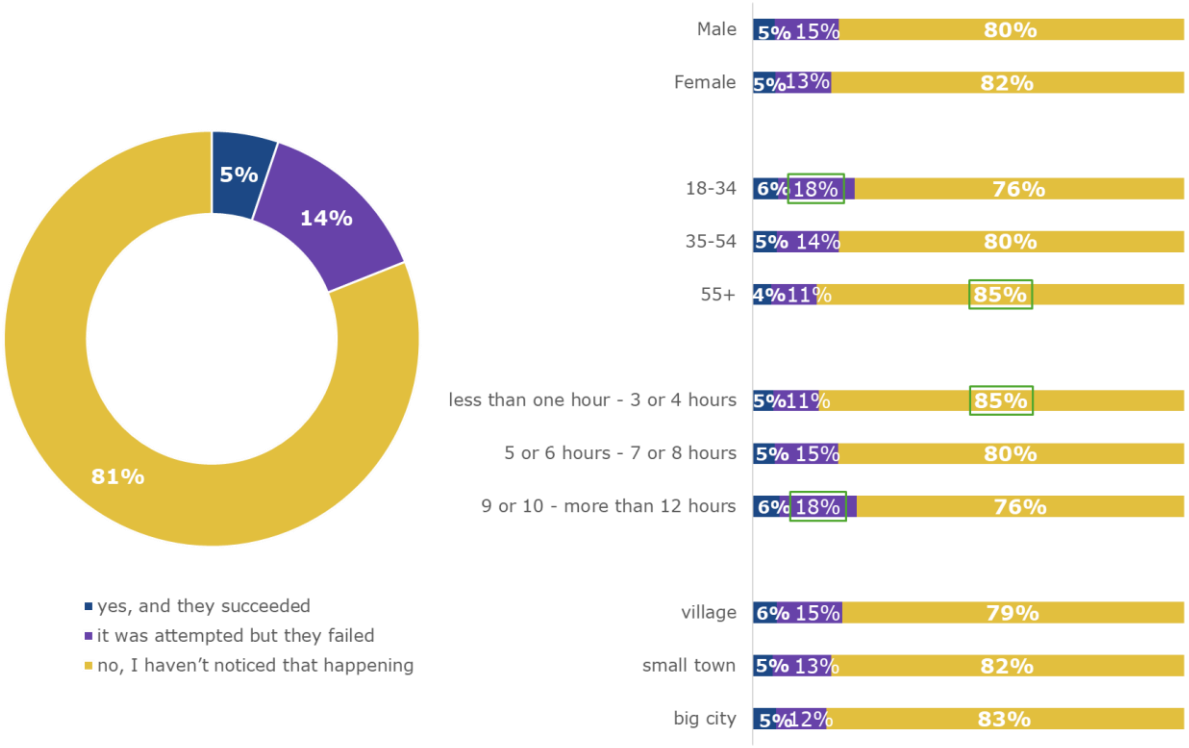
Attempts of unauthorized access to financial resources (bank accounts, online payment accounts, virtual currency wallets or credit card details) were reported by 19% of respondents, however only 5% of these attempts were successful. At the same time, 81% of respondents indicated that they had not noticed such incidents.

Unsuccessful attempts were most often reported by respondents aged 18–34 (18%), while among those aged 55+ this share is 11%. This is likely explained not only by higher awareness among younger respondents and their ability to recognize such threats, but also by more intensive use of online financial services.

A similar pattern is observed among more intensive internet users: those who spend more time online are more likely to report such attempts, although in most cases they do not result in successful attacks (*Figure 167*).

Figure 167. Awareness of unauthorized access to bank accounts, online payment accounts, virtual currency wallets or credit card details

Q: In the past 12 months, have you become aware that any of your bank accounts, online payment accounts, virtual currency wallets or credit card details had been illegally used?



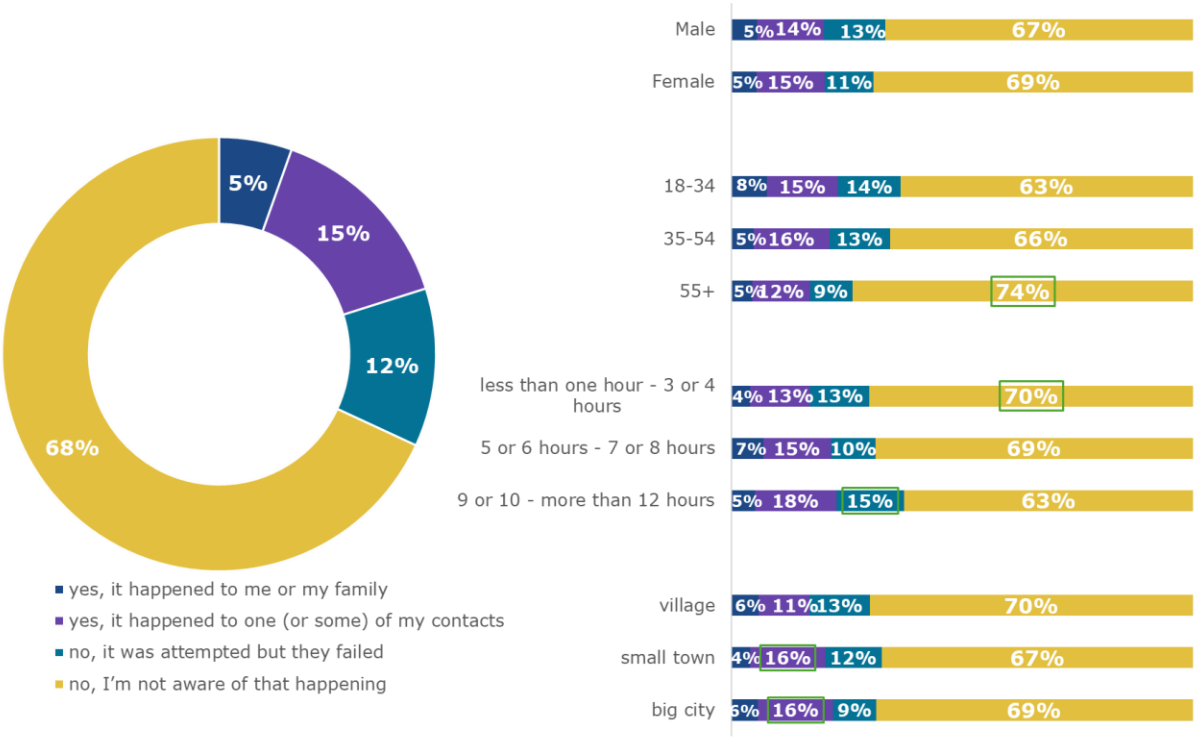
A somewhat different pattern is observed regarding attempts to take over online accounts or phone numbers for impersonation purposes. The majority of respondents (68%) indicated that they are not aware of such cases. At the same time, 5% reported personal experience or experience among family members, 15% reported cases among their contacts, and another 12% reported attempts that were unsuccessful.

Subgroup analysis shows that respondents aged 55+ (74% vs. 63–66% in younger groups) have the highest percentage when reporting that no such experience is observed. Unsuccessful attempts are more often noticed by the most intensive internet users (15% among those who spend more than 9 hours online per day), which may be related both to higher exposure to risks and to a better ability to identify them.

By type of settlement, cases among people they know are more often reported by urban residents (16% in both medium-sized and large cities vs. 11% in rural areas), which is likely linked with broader social networks (*Figure 178*).

Figure 178. Incidence of online account and phone number takeovers for impersonation purposes

Q: In the past 12 months, have you become aware that your own, or someone else's, online account or phone number had been taken over by a stranger for impersonation purposes?

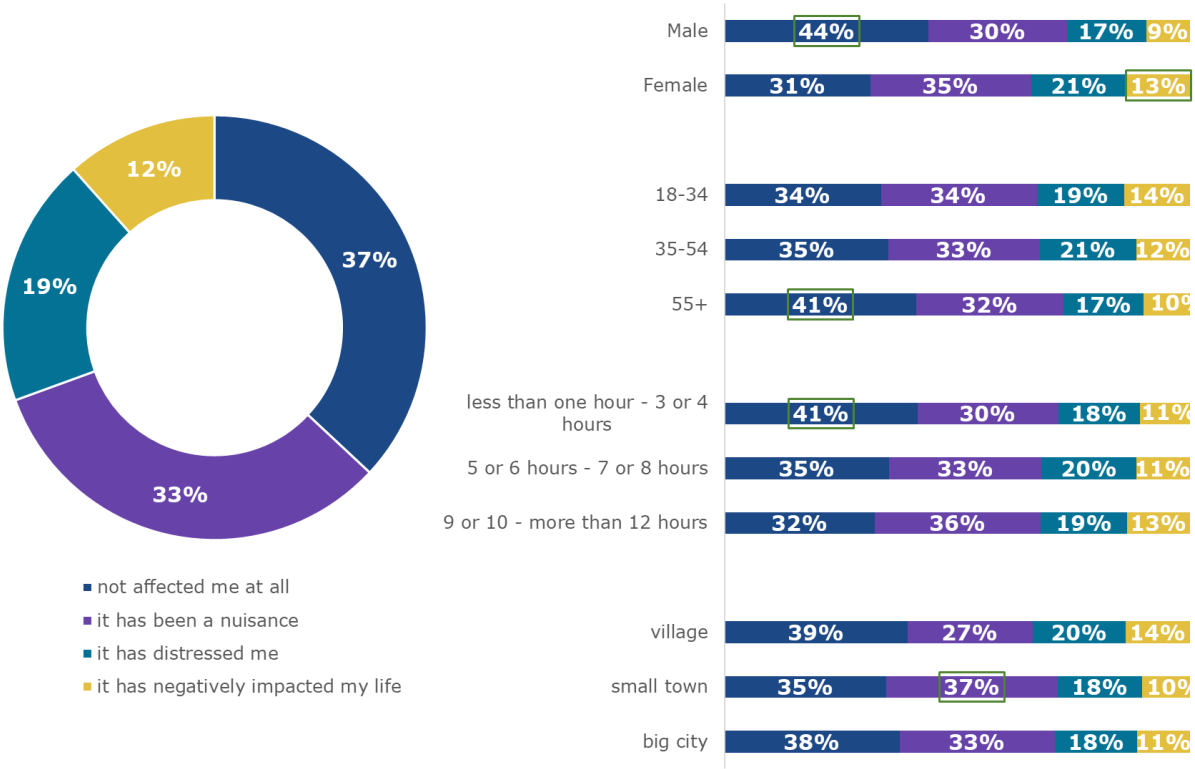


Regardless of personal experience, respondents were asked about how deeply online identity theft has affected their life over the past 12 months. Most often, respondents indicated that it has not affected them at all (37%), while for 33% it has been a nuisance. At the same time, 19% said it has distressed them, and 12% reported that it has negatively impacted their life (*Figure29*).

Men more often than women reported no impact at all (44% vs. 31%), while women more often reported negative consequences (13% vs. 9%). Respondents aged 55+ also more often indicated no impact (41% vs. 34–35% among younger groups). In addition, the highest share of responses indicating no impact is observed among those who spend the least time online (up to 4 hours per day).

Figure 29. Impact of online identity theft on respondents' lives

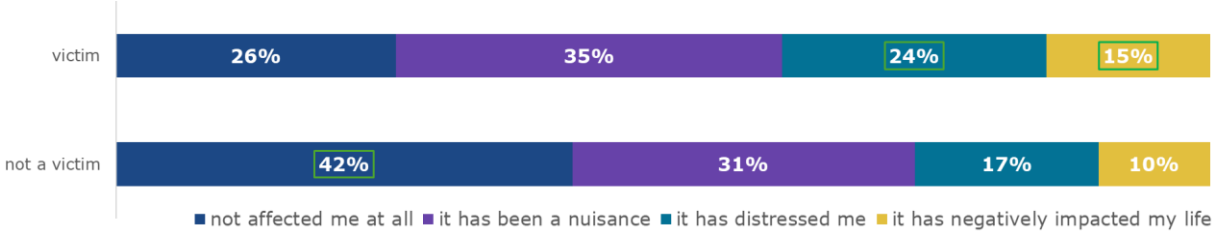
Q: How deeply has online identity theft affected your life over the past 12 months?



A statistically significant difference is observed between respondents who have been targeted by cybercrime and those who have not (*Figure 18*). Among those who were not victims of cybercrime, 42% reported that online identity theft has not affected them at all – a figure substantially higher than the 26% among victims. Conversely, victims of cybercrime experience a much deeper impact. They are statistically more likely to report that online identity theft has distressed them (24% vs. 17% among non-victims) or has negatively impacted their life (15% vs. 10%).

Figure 180. Impact of online identity theft on respondents' lives (victims vs non-victims)

Q: How deeply has online identity theft affected your life over the past 12 months?



Regarding willingness to report online identity theft, 36% of respondents believe this should be done in any case, while another 39% think it should be done only in serious cases. At the same time, 21% tend to believe that reporting would probably not be appropriate, and 5% are certain they would not do so under any circumstances.

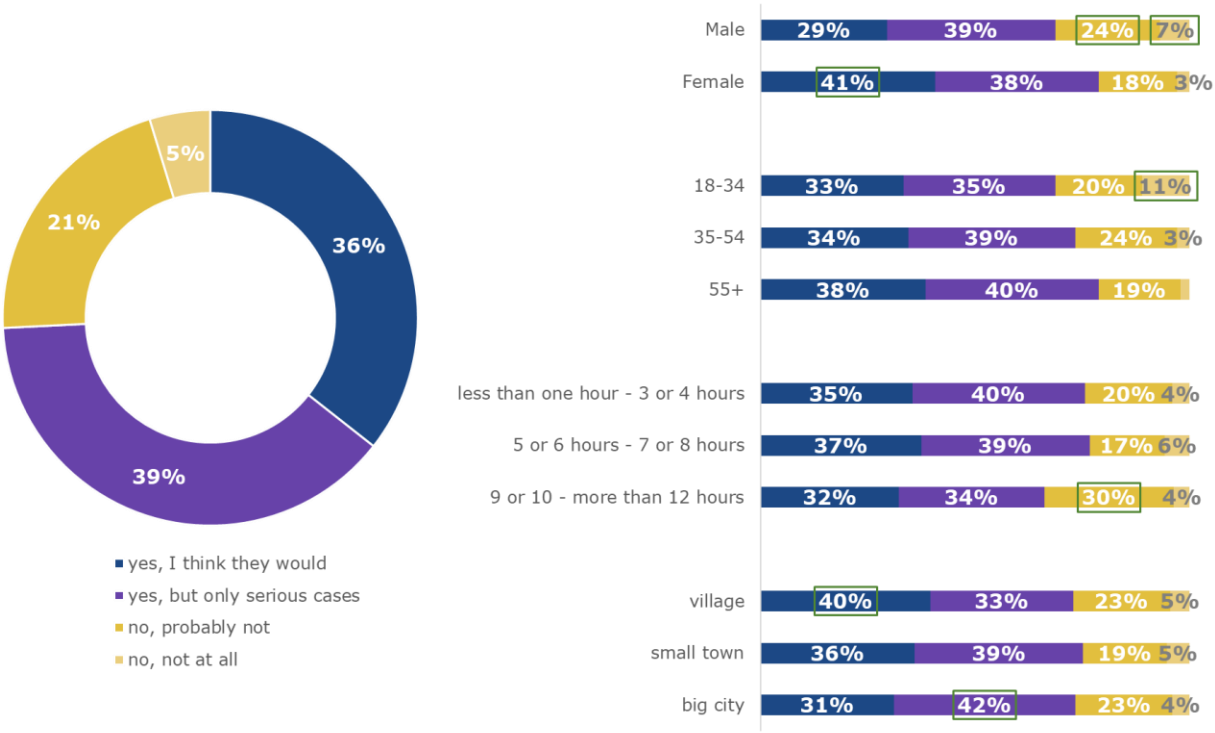
Subgroup analysis shows that women are more likely than men to support unconditional reporting (41% vs. 29%). Young people demonstrate the highest share of categorical refusal

(11% vs. 2–3% in older age groups). Among the most intensive internet users, a higher share tends towards the response "probably would not report" (30%).

By type of settlement, urban residents are more likely to consider reporting only in serious cases appropriate (42% vs. 33% among rural residents), and this difference is statistically significant (*Figure 19*).

Figure 191. Reporting an online identity theft or a scam abuse such a stolen identity to cyber police/government hotline

Q: If someone in your neighbourhood falls victim to online identity theft, or to a scam abusing such a stolen identity, do you think they would report it to the cyber police, the government hotline, etc.?



2.5.7. Cybercrime – concerns and expectations

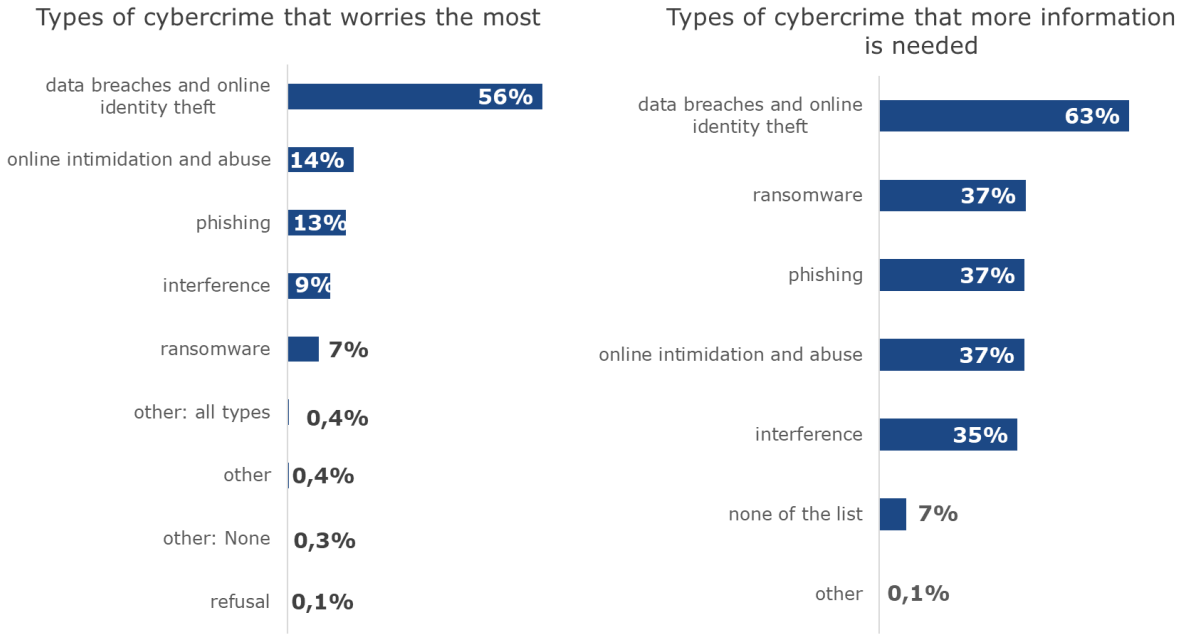
Among all types of cybercrime, data breaches and online identity theft cause the greatest concern among respondents – reported by 56%. Other types of threats lag significantly behind in perceived importance: online intimidation and abuse were mentioned by 14%, phishing by 13%, interference (services made unavailable) by 9%, and ransomware by 7% (*Figure 202*).

The need for additional information is also highest for data breaches and online identity theft, as reported by 63% of respondents. For other types of cybercrime, this share is lower and relatively similar; 37% for ransomware, phishing, and online intimidation and abuse, and 35% for interference (services made unavailable).

Figure 202. Most concerning types of cybercrime vs Areas requiring additional public information

Q: Which of all these types of cybercrime would you say worries you most?

Q: For which types of cybercrime do you feel that you need more information to be able to protect yourself and your family against them?

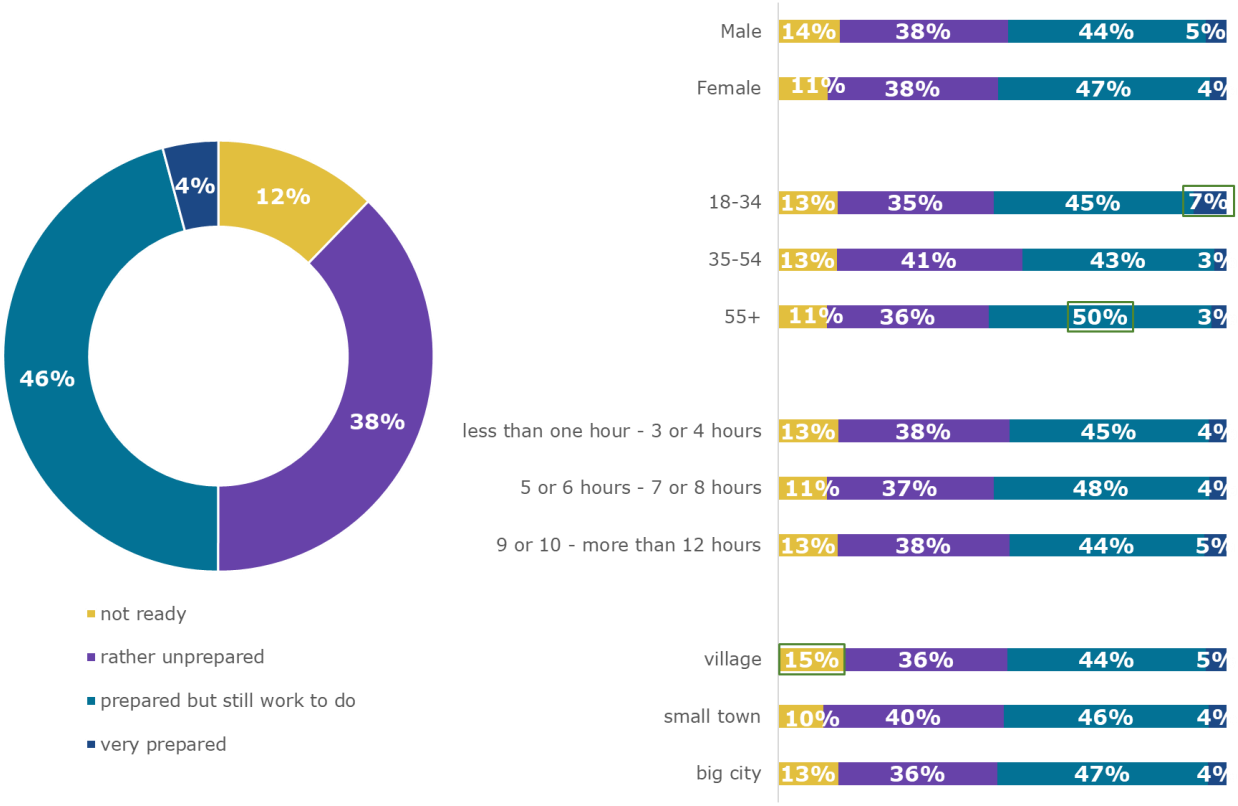


At the end of the survey, respondents were asked to assess how prepared the authorities are to take on cybercrime. Opinions are evenly divided: 50% believe that the authorities are not ready (including 12% who consider them not ready at all and 38% rather unprepared). At the same time, the other half holds the opposite view, although mostly with cautious assessments: 46% stated that the authorities are prepared but still have work to do, and only 4% believe that the authorities are very prepared to effectively address cybercrime (*Figure 213*).

Young people aged 18–34 are statistically more likely to consider the authorities very prepared (7% vs. 3% in older age groups), while among respondents aged 55+ the share of those who assess them as “prepared but still need to improve” is significantly higher compared to those aged 35–54 (50% vs. 43%).

The share of those who consider the authorities not ready at all is highest among rural residents (15%) and is statistically significantly higher than among residents of small towns (10%).

Figure 213. Public perception of law enforcement preparedness to combat cybercrime
Q: How prepared do you feel are the authorities to take on cybercrime?



2.6. Conclusions

Based on the results of the quantitative survey among internet users in Ukraine aged 18 and above, the following conclusions can be drawn.

- **The internet is an integral part of everyday life**: 62% of Ukrainians spend 3 to 8 hours online per day, another 20% spend 9 or more hours, while only 1% use the internet for less than one hour daily.
- The internet is most commonly used for **communication**, **reading the news**, **finding information**, and **accessing online services and entertainment**.
- A high level of digital engagement is accompanied by **awareness of risks**: 88% of respondents consider cybercrime a real threat and acknowledge their own vulnerability.
- At the same time, **most take basic protective measures**: 75% avoid giving any of their personal data to third parties and installing suspicious apps, while 71% avoid visiting suspicious websites.
- In terms of **keeping devices safe**, the most common tools are a password or PIN number (81%), while more than half also use biometrics (56%). Only 2% do not use any protective measures.
- Despite this, 39% of respondents believe they have already been **targeted by cybercrime**.

- **The most widespread type of cybercrime is phishing** – in one way or another, 64% of respondents have encountered it over the past 12 months. Other types of experience include taking over online accounts or phone numbers for impersonation purposes (32%), data breaches of non-financial personal data (28%), online intimidation and abuse (24%), interference (services made unavailable) (23%), ransomware (22%), and unauthorised access to financial resources (19%).
- In terms of **impact on quality of life** (nuisance, distress, or serious harm), different types of cybercrime show substantial differences. The most significant impact is observed for online identity theft and phishing – 63% of respondents reported negative consequences. Online intimidation and abuse affected 56%, while ransomware affected 51% of respondents.
- **Willingness to contact the cyber police** or a government hotline (assessed through perceptions of neighbours' behaviour) is relatively high and increases with the severity of the incident. 77% of respondents expect reporting in cases of online intimidation and abuse (at least in serious cases), 75% would report in cases of online identity theft, 69% would report in cases of ransomware, and 65% would report in cases of phishing.
- The structure of concern does not fully correspond to the prevalence of experience. Data breaches and online identity theft are perceived as **the most serious threats** (56%), while other types of cybercrime have significantly lower shares. Online intimidation and abuse were mentioned by 14%, phishing by 13%, interference (services made unavailable) by 9%, and ransomware by 7%. This aligns with the assessment of consequences: although experience with data breaches is relatively less widespread, this type of cybercrime has one of the strongest impacts on life, according to 77% of respondents. By comparison, the more widespread phishing (encountered twice as often) has a lower (though still substantial) level of negative impact according to 63%.
- There is also a clear **need for information**. 63% of respondents report needing more information about data breaches and online identity theft, while for other types of cybercrime this share is 35–37%.
- Assessments of **how prepared the authorities are to take on cybercrime** are mixed. Half of respondents believe that the authorities are at least somewhat prepared (of which only 4% consider them very prepared), while 38% tend to think the authorities are rather unprepared and another 12% are convinced they are not prepared at all.

3. Qualitative Research

3.1. Summary

Focus group discussions show that cybercrime is perceived as a widespread and growing phenomenon, but its meaning depends on the group.

3.1.1. The general public

Cyberspace is part of everyday life. People use it for communication, content, banking and public services. This creates a mixed perception: active use and partial trust coexist with a constant sense of risk. The main concerns are financial loss, account hacking, data theft and psychological pressure. Phishing is the most common and best understood threat, while more complex attacks are less clear. Artificial intelligence is seen both as a useful tool and as a source of new risks, especially due to realistic fakes. Protection behaviour is inconsistent: people recognize the importance of basic security but do not follow clear routines, often due to fatigue and information overload. Cybersecurity is seen as a personal responsibility, but there is also an expectation that the state should play a leading role. This expectation is not met, as trust in law enforcement is low. The reasons include negative experience, bureaucracy and the belief that incidents are not investigated. Banks and service support are trusted more, but they are not seen as responsible for overall protection.

3.1.2. Business and IT specialists

Cybercrime is a constant operational risk that affects business continuity and reputation. Threats are understood in a structured and technical way. Respondents clearly distinguish between phishing, DDoS, data breaches, ransomware and insider threats. Phishing is the most common threat and often the entry point for more complex attacks. Ransomware and infrastructure attacks are seen as critical because they can stop operations. Past large-scale incidents, such as Petya, strongly shape risk perception. The human factor is seen as the main weakness — this is common for all groups, but in business it is addressed through policies, staff training and technical controls. Companies use complex approaches, including standards and technical tools. Artificial intelligence is seen as increasing both risks and vulnerabilities, including data leakage through public tools. Trust in the state is low, but for different reasons: businesses prefer to rely on internal resources or external experts. There is also a shortage of qualified specialists.

3.1.3. Subject matter experts

This refers to government officials responsible for combating cybercrime. Cybercrime is viewed at the state level as part of national security. The focus is on attacks against government systems, critical infrastructure and long-term intrusion and espionage. Experts also highlight that many incidents are not reported, so official data underestimates the real scale. Their assessment of the state system is similar to other groups: it is seen as not effective enough. However, experts explain this through systemic issues, such as gaps in regulation, organisation and staffing. Unlike the public, they do not focus on individual behaviour, but on system-level constraints.

3.1.4. Common patterns across all groups

Cyber threats are seen as increasing. Phishing is the most widespread type of attack. The human factor is the main vulnerability. Artificial intelligence makes attacks more advanced and harder to detect. There is also low trust in law enforcement in all groups.

At the same time, there are clear differences. The public focuses on personal financial risks and reacts situationally. Businesses focus on continuity, data protection and reputation, and use structured approaches. Experts focus on systemic risks and the need for institutional change. Views on digital literacy also differ: the public sees itself as generally aware but not always careful, while experts consider the level of cyber hygiene insufficient. Expectations also differ: the public expects action from the state, businesses rely on their own systems, and experts point to the need for reforms and stronger institutions.

3.2. Technical Information and Research Methodology

The qualitative component of the study encompassed three target audiences: (1) members of the general public who had experienced cybercrime, (2) representatives of micro, small, medium, and large businesses and organisations responsible for cybersecurity, and (3) representatives of public authorities engaged in countering cybercrime.

In total, the qualitative sample included 7 participants from the general public, 13 participants from the business sector, and 4 representatives of public authorities.

Data collection was conducted through online focus group discussions. One focus group was conducted with participants from the general public. For the business audience, three mini focus groups (4–5 participants each) were organized instead of a single large group. These groups were stratified by business size (micro and small; small and medium; medium and large), which allowed for more homogeneous discussions and facilitated deeper exploration of participants' experiences while preserving group dynamics.

Participants from the general public and business sectors were recruited to ensure geographical coverage across all regions of Ukraine. The expert group did not follow a regional distribution principle and was formed based on institutional relevance.

Recruitment of business participants was designed to ensure diversity, not only in terms of company size, but also across sectors of activity. A key screening criterion was the participant's involvement in cybersecurity within their organisation. Only those who were personally responsible for, or jointly involved in, organizing information or cybersecurity systems were included in the study, while those without such involvement were excluded.

Participants from the general public were recruited from the quantitative survey sample, specifically among respondents who reported having experienced cybercrime and agreed to take part in further research. Recruitment of representatives of public authorities was conducted with the support of the Council of Europe, which provided access to relevant experts.

All discussions were conducted in an online format and recorded with the informed consent of participants. The recordings were used solely for analytical purposes. All data presented in the report, including quotations, have been anonymized. Video recordings were deleted upon completion of the analysis.

Detailed profiles of participants in each target audience are provided in the relevant sections of the report.

3.3. General population: Cybercrime Victims

Stories of focus group participants who have been victims of or targeted by cybercriminals, along with their demographic profiles:

R1, Male, 34, Dnipropetrovsk Oblast A food production technologist by training, he worked as a call centre operator.	He received phishing messages in an online game where he was pressured to deposit funds ("top up his balance") in order to supposedly claim a prize. He also had his Facebook account hacked and received phishing links via email. He once lost 1,000 hryvnias by paying for a fake work permit on a fraudulent website.
R2, Male, 32, Chernivtsi Works remotely in the tourism industry; he holds a degree in power engineering.	He has repeatedly encountered messages about fake car giveaways and calls from the "bank's security service" regarding an allegedly blocked card. He described a case of extortion where, after he refused to pick up unwanted goods at the post office (which he had ordered using fake information to test the scammers), he was threatened with criminal charges.
R3, Female, 55, Kyiv Oblast Engaged in creative work and blogging.	For several months, she endured phone harassment and threats after refusing to make a deposit on a crypto exchange. The most traumatic incident involved the theft and illegal disclosure of her personal data by an acquaintance seeking revenge, which led to her receiving offensive messages from men around the world.
R4, Female, 65, Poltava Oblast Works as a nursing assistant	She has been a victim of scammers twice. The first incident involved a Viber hack via a phishing link disguised as an ad activation on OLX; scammers requested money in her name, and her friend transferred 10,000 UAH to them. The second incident involved an online job scam, where she was defrauded of a large sum. She also experienced attacks from bots sending threats over an unpaid seminar.
R5, Female, 55, Zhytomyr IDP from Severodonetsk, accountant	She received messages about fake winnings of money and cars. In the fall of 2025, her husband's Telegram account was hacked due to a fake poll; requests to lend 10,000–20,000 hryvnias were sent to all his contacts in his name. She also faced psychological pressure from debt collectors who demanded repayment of someone else's loan, claiming that she was the guarantor.

R6, Male, 65, Kharkiv Retiree	Due to carelessness, he clicked on a suspicious link, which led to his Viber account being hacked and spam being sent out in his name.
R7, Male, 72, Kyiv Researcher, entrepreneur, and blogger.	His first experience with this occurred between 2008 and 2010, when he lost money playing an online game. He recently became the target of a phishing attack and intimidation via Viber. He also regularly receives messages about fake winnings.

3.3.1. Trust in the evolving online landscape

Participants are active internet users, spending anywhere from 4–5 hours to 12 hours a day online. For many, the internet is a space they inhabit constantly, checking for updates from early morning until late at night.

For those who work or are involved in creative pursuits, a single Internet session can last 3–4 hours straight. Others describe their style as "log in and log out," but do so throughout the day (such people often describe themselves as Internet-addicted).

The range of respondents' online activities is extremely broad—from professional work and education, to daily chores and entertainment.

- Communication and social media: This is one of the main purposes. Messengers (Telegram, Viber, WhatsApp) and social media platforms (Facebook, Instagram, LinkedIn) are used.
- Several respondents are bloggers; some create content, videos, and the like. All respondents shop online—this is a common practice for people of all ages.
- Work and creativity: Respondents work remotely (tourism, call centres), maintain blogs, and edit video and audio.
- Education and self-development: Learning foreign languages (English), mastering new editing software, and searching for information on pet care.
- Entertainment: Watching videos on YouTube and TikTok, movies, listening to audiobooks and podcasts, playing online games, and playing solitaire.
- Government and everyday services: Active use of the Diya app, banking apps (PrivatBank, Monobank), the Helsi medical system, and the Tabletki.ua service.
- Shopping and services: Using marketplaces (Rozetka, Prom, OLX, Kasta), booking train tickets (Ukrzaliznytsia), requesting a taxi, and ordering food delivery.
- Artificial Intelligence: All participants already have experience using AI (ChatGPT, Gemini, Copilot) for comparing products, analysing texts, legal consultations, or even composing music.

> I'm kind of addicted to the internet. As soon as I wake up: 'What's going on in the world?' All those apps, every single one. If I wake up in the middle of the night: 'Oh, right. Is there an alert?' I have to check the alerts. Log in, log out. Maybe six hours.

> Just not constantly, all the time. You log in, look at something, log out, log in again. (**R5**)

> I'm online pretty much from early morning until late at night. Mostly for entertainment. YouTube, to learn something. TikTok too. I mean, TikTok as well. And I play games from time to time, but very rarely. (**R2**)

Respondents are aware that the online space is fraught with dangers and that there are many scams.

Respondents' level of trust in online platforms varies significantly depending on the type of resource: from high trust in government services to complete suspicion of social networks and messaging apps.

Trust in government resources, including banking apps, is higher, but participants realise that even these are not completely secure. According to respondents, the most dangerous platforms are messaging apps and email, as phishing messages often arrive there. Respondents are alarmed that their phone or computer quickly displays ads for products or services that they are discussing aloud—this is also perceived as a threat, misuse of data, and so on

Respondents spontaneously mentioned the following threats:

- Dishonest merchants—the risk of not receiving goods when shopping online if payment is made in advance.
- Hacking of bank accounts, theft of banking data—particularly the risk of fraudsters using credit funds on a bank card with no funds.
- Hacking social media and messaging app accounts.
- Receiving phishing messages.
- Calls made in the name of the bank, attempts to obtain banking data.

Respondents recognize that they are personally responsible for their own security and for assessing risks.

> You always need a safety net. But when it comes to our online activities, it's a matter of consciously viewing these platforms as a risk. That's why everyone should choose the method they believe will keep them safe. (**R7**)

> I know about two-factor authentication. But I only use it on one platform. Actually, my daughter-in-law jokes that your trust in the universe is endless. And I feel that I'm too carefree myself. That I trust people, give (laughs) everyone my passwords, my card numbers. (**R4**)

Overall, participants' main concerns relate to **the vulnerability of personal data** and technical flaws in systems:

- Risk of hacking: Even reliable state-owned banks or platforms can be targeted, leading to data theft.
- Credit risks: Banks may automatically increase credit limits without the customer's consent, leaving the user vulnerable in the event of a banking breach; fraudsters can withdraw credit funds, which the account holder will then have to repay.

- Eavesdropping and surveillance: Respondents note that apps (particularly Google) 'eavesdrop' on conversations to serve targeted advertising, which is perceived as a violation of privacy rights.

Participants cited numerous examples of how popular platforms are being used by criminals:

- Messaging apps (Viber, Telegram): Used to hack accounts via phishing links (e.g., 'vote for the child') followed by sending requests for money on behalf of the account holder.
- Classifieds platforms (OLX, Prom): Creation of fake listings to extract card details or obtain prepayment for non-existent goods.
- Social engineering and AI: Using artificial intelligence to create realistic fake videos and photos that are difficult to distinguish from the real thing. Psychological pressure is also exerted via messaging apps: threats on behalf of debt collectors or 'security services'.

As online shopping is one of the most popular activities on the internet, the issue of secure payments is a concern for respondents. The main requirement is a combination of convenience and security. Services such as Google Pay are widely used, as well as specialized payment services on the most popular platforms (Nova Pay at Nova Poshta, Prom Oplata on the Prom.ua marketplace). For certain services, such as requesting a taxi, respondents use linked cards from which funds are debited automatically. It is not uncommon for respondents to have a separate card for online payments, containing a small amount of funds, in case the details are stolen. They also set a limit on the card for online payments and purchases. Respondents only enter their payment card details (number, expiry date and CVV code) on trusted platforms.

All respondents use artificial intelligence; this is the main change in online behaviour noted by respondents. Over the past year, artificial intelligence has become a widespread and frequently used tool. In particular, artificial intelligence is used for security in the online environment. Respondents check whether certain websites and platforms are secure, particularly for entering personal data.

> I interact with artificial intelligence. I take a screenshot or copy something, send it and write: 'Can I trust this platform or not?'. It checks and tells me yes or no, giving a specific percentage of trust, say per cent. And then, when I ask 'why?', it explains everything to me: what the signs of fraud are and so on. It helps me a lot. (**R3**)

Overall, over the last six months, artificial intelligence has become an integral part of the respondents' lives. They use it for video translation, text generation, analysing financial documents, medical consultations and advice on pet care, and even for technical support for old equipment.

> I used Gemini. I took a photo of my ECG and said, 'Give me an analysis. What's going on here?' And it analysed it and said there were heart problems, tachycardia, something like that. You don't need to go to the doctor. But it's not accurate. It's better to see a doctor. (**R1**)

According to respondents, it is a useful tool, but it cannot be fully trusted; one must take a critical approach to the results. Respondents note that it is becoming increasingly difficult to

distinguish content created by AI. For example, it now creates extremely realistic videos and photos, and this misleads even experienced users.

> It is not always appropriate to trust artificial intelligence. Because many times it has been wrong, it tells lies. That is why you need to check the information. I use it more for simple questions, to get an answer. For drafting text, when I need to write a letter or a complaint. And it formats that text beautifully. (**R2**)

However, despite statements about the need to verify AI responses, respondents did not provide clear algorithms that they use for such verification.

Regarding changes in online behaviour recently, some respondents indicated that over the past year they have become more attentive and careful about protecting their accounts and data. This change in behaviour occurred, in particular, due to an awareness of vulnerability (as fraudsters exploit human overconfidence and take advantage of stressful situations). The war has also brought additional risks linked to cyberterrorism and attempts by hostile intelligence services to recruit citizens via the internet to carry out unlawful acts.

3.3.2. Cybercrime

Respondents' spontaneous associations with cybercrime relate to actions that lead to the loss of money or property via the Internet through the extortion of information or funds. On a larger scale, this is associated with the hacking of websites belonging to banks, government institutions, military structures and the Pension Fund. Cybercrime is also perceived as the exploitation of people's digital illiteracy for financial gain.

According to respondents, all people and institutions are equally vulnerable to cybercrime, including ordinary people and business representatives. The threat is equally present for both companies and the general public. Respondents consider job seekers and people with medical conditions seeking treatment to be a more vulnerable group – such people are easier to deceive. Older people are also at risk due to lower levels of digital literacy. However, respondents do not feel constant anxiety but acknowledge that danger lurks at every turn and that immunity to it comes only from previous negative experiences.

According to respondents, the main type of crime is data theft and extortion for that data. Cyberterrorism organized by Russia is also widespread. The main defence against criminals is vigilance. Basic knowledge of cybersecurity and the ability to avoid acting impulsively are also important.

Respondents realise that their safety online/in the digital space is their personal responsibility. According to participants, the information that requires protection above all is that which allows access to finances or enables the manipulation of a person's identity:

- Financial details, such as bank card numbers, expiry dates and CVV codes.
- Passport details and identification number.
- Passwords and usernames for social media (Facebook) and messaging apps (Viber, Telegram), which fraudsters hack to send requests for money in the victim's name.
- Mobile phone number, as it is the key to banking apps, 'Diya' and other services.

- Personal photos, videos and correspondence, which could be used for revenge, blackmail or harassment if unlawfully disclosed.

In general, to protect themselves, respondents use a combination of technical and behavioural methods. The following technical protection methods were mentioned:

- Two-factor authentication (2FA) — cited as the most important step for protecting all accounts.
- Password management: Using complex passwords, avoiding standard combinations (such as '12345') and storing them in notebooks or special apps.
- Using biometric data to log in to your phone.
- Setting limits on online payments and using separate online payment cards with a minimum balance for suspicious websites.
- Linking your phone number to your passport with your mobile operator to prevent it from being stolen.
- Restricting app permissions for microphone and camera use.

Information hygiene measures include the following:

- Checking suspicious numbers or platforms via Google or using artificial intelligence (ChatGPT, Gemini).
- Adhering to the 'one-hour rule': do not make decisions immediately under pressure, but take time to think things through and verify the information.
- Completely avoid clicking on any unfamiliar links.

3.3.2.1. Phishing

Most focus group participants and people in their social circles had received phishing messages or fallen victim to them. Respondents described a variety of schemes: from hacked messaging apps to fake prize notifications and forged official documents. However, it is worth noting that, apart from phishing, respondents do not always identify different types of crime well, even after being read the definitions. The authors of the report presented the respondents' cases in the order in which the respondents identified them during the discussion. Some cases can be classified under different categories of crime, and the respondents also discussed this.

Respondents gave the following examples of phishing messages:

- A request to vote for a child's entry in a competition, account hacking and the sending of requests to borrow money to all numbers. The victims' reaction is to call and inform all their acquaintances about the account hacking; acquaintances also call the victim.
- A message in response to an advert posted on OLX, account hacking and sending out requests to borrow money to all numbers. The recipient of the message abroad did not realise it was phishing and transferred the funds. Messages also came into the work chat; colleagues found this unpleasant, and there were comments from management.
- Messages about a large win; if the person responds, they are told they must pay tax (a fairly large sum), given bank details, the person transfers the money and is added to a

blacklist. The respondent spoke about a friend's experience, a situation he was involved in and tried to prevent the crime.

Respondents emphasize that fraudsters use psychological pressure, a sense of urgency and a person's vulnerable states (sleepiness, stress, the need for work) to lower their guard. Recovering accounts after such attacks often requires providing passport details to technical support and takes from a few days to six months.

3.3.2.2. Ransomware

This is a less familiar form of cybercrime to respondents; only one respondent had encountered ransomware, and the incident involved an acquaintance. The woman had attempted to download a paid program for free from a dubious website. After restarting her computer, her hard drive was found to be encrypted, and the program demanded payment. Access was only restored thanks to an antivirus website, where they found the unlock code and instructions on how to remove the utility via safe mode.

3.3.2.3. Intimidation and abuse

This is a common crime. More than half of the respondents had encountered various situations. One respondent was even invited to work at a call centre involved in fraud and extortion.

Situations described by respondents:

- A respondent signed up for a paid seminar but did not attend and did not pay for it. For several months, she received calls with persistent requests (and psychological pressure) to pay for her participation.
- A demand to pay for goods the respondent had not received. In response to a phishing call about a prize and an offer to place an order for goods as a condition for receiving the prize, the respondent placed a fake order using incorrect details. After that, calls began with accusations and demands to collect the goods.
- While looking for work, the respondent was offered a job at a cryptocurrency exchange, but she had to deposit funds to start. The woman realised it was a scam, and for the next month she received calls containing requests, demands and threats to pay the money. Only after she threatened to contact the police did the calls stop.
- Prolonged calls from a bank demanding payment of a loan on behalf of a third party, as the respondent was listed as a guarantor. In response, the respondent eventually threatened to contact the police, and the calls stopped.
- There are widespread fake calls from the bank demanding that banking details be provided. The person is gradually asked for all their details, starting with their card number and expiry date. They let their guard down and disclose confidential information that bank staff would never ask for and are warned that it is forbidden and dangerous to provide this information to third parties.

Respondents describe such actions as psychological pressure and extortion, carried out via the internet or telephone using personal data. Participants cite the following as the main characteristics of such abuses:

- Rudeness and brutality: communication often takes place in an aggressive manner, using foul language ('a string of swear words').
- Systematic nature: attacks can last from a few days (intensive calls from bots) to several months.
- Manipulation through fear: perpetrators threaten criminal prosecution, the police or physical violence.

3.3.2.4. Identity theft

Focus group participants had not only heard of identity theft but also described the phenomenon in detail through the lens of their own experiences and observations. Generally, they understand it as the unlawful acquisition or use of personal information without the individual's consent for the purpose of gaining an advantage or causing harm. For example, when applying for a job, a respondent suspected that a potential employer was collecting their personal data under the pretext of an interview for subsequent unlawful use.

Respondents are also aware of major data leaks from government databases (such as Diya and the electoral register). Such incidents are also perceived as threatening. The situation is complicated by the fact that there is no countermeasure available to the average citizen. The causes of such leaks are unknown – according to respondents, this could be either a targeted cyberattack or unlawful actions by officials who have access to the data and sell it.

The installation and use of apps such as GetContact (which have access to the user's address book) is also perceived as the unlawful acquisition of subscribers' personal data.

3.3.3. Cybercrime - concerns and expectations

Of all the crimes discussed, respondents are mostly concerned about phishing calls, which can last for several days, cause significant disruption and exert pressure. At the same time, this is the most common type of cybercrime.

Among the crimes not mentioned, respondents highlighted cyberterrorism as a pressing issue, where intelligence services of an enemy state recruit Ukrainians via social media and messaging apps for small sums of money to carry out bombings of buildings and vehicles, resulting in innocent people suffering.

Participants are deeply concerned by the fact that the cyber police do not effectively investigate minor crimes against ordinary citizens. Respondents feel vulnerable, as reports are often 'fobbed off', whilst offenders (particularly those calling from prisons) go unpunished and continue their activities for years. This leads to an ambivalent attitude towards law enforcement agencies, which should be providing support to victims and investigating cybercrimes. During the discussion, scepticism was expressed regarding the ability of law enforcement agencies to carry out this work, particularly due to negative personal experiences of interaction. Among the reasons why people are reluctant to report cybercrimes, the following can be highlighted:

- Psychological barriers and victim-blaming: respondents' relatives and acquaintances have faced situations where the police mocked them, calling them 'fools' and claiming that they were 'themselves to blame' for what happened.

- Scale of the crime: there is a belief that law enforcement agencies only handle cases involving large sums of money (from $50,000), whilst they are 'not interested' in petty thefts involving ordinary citizens.
- Bureaucracy and evading accountability: Reports are often redirected from the cyber police to local police stations that lack the relevant expertise, resulting in letters of refusal to open an investigation.

Among the reasons that may prompt citizens to report cybercrimes, the following can be highlighted:

- To stop the pressure, a desire to stop the criminals: even simply informing the perpetrators that a report had been filed with the police and the prosecutor's office helped to stop the stream of threats and calls.
- An attempt to restore justice: respondents noted that people sometimes file reports spontaneously under the influence of stress. However, this there is often a lack of feedback from investigators.

However, the participants' overall conclusion is that the current system for protecting the public from cybercrime is inadequate, and contacting the authorities is often seen as a waste of time.

Banking institutions and the technical support services of messaging apps and social networks enjoy greater public trust, as the specialists working for these services provide genuine support to those affected.

According to focus group participants, the fight against cybercrime in Ukraine should be addressed by both existing specialized bodies and state institutions responsible for digitalization in general. Respondents highlight the following key institutions and the rationale for their roles:

- **The Ministry of Digital Transformation**:

It is seen as the main actor responsible for the state's digital policy. Consequently, this ministry should also be responsible for digital security issues.

> And who is responsible for digital policy in the country? There is a dedicated Ministry of Digital Transformation. It is clear that this Ministry should be the main body determining policy, including in the fight against cybercrime. This is a very specific type of crime that needs to be given greater priority. And it seems to me that the central body here should be the Ministry of Digital Transformation. Although I am not in favour of taking functions away from the National Police. There needs to be some type of partnership, some type of cooperation. But it needs to be more effective. (**R7**)

- **The Cyber Police**

Currently, the Cyber Police are part of the National Police, which, according to respondents, undermines their effectiveness, as outdated methods used by ordinary police stations are applied to specific digital crimes.

➢ A Centralized Analytical Centre

It was proposed to form this Centre which could analyse mass reports, helping to prevent more serious crimes at an early stage.

In addition to law enforcement agencies, respondents see an important role for state media (for example, 'Public Radio') and schools in crime prevention through public awareness and the development of digital literacy. Public awareness is a crucial step in combating cybercrime, as criminals' methods are constantly evolving. Awareness-raising should be directed primarily at children (through the education system) and older people (through the media and other public education channels).

Overall, participants are seeking a shift from a reactive approach to individual complaints towards a comprehensive national cybersecurity system. Citizens feel a need for support and protection, as currently the responsibility for their own cybersecurity lies entirely with the user.

3.4. Organisations: IT professionals

Respondents' profiles

FGD 1 (micro and small business)

R1.1. Kharkiv, microbusiness, construction, accountant
R1.2. Kyiv, microbusiness, software development, cybersecurity specialist
R1.3. Odesa region, microbusiness, logistics, director
R1.4. Kyiv, small business, law firm, information security specialist
R1.5. Zhytomyr, small business, auto parts sales, IT department head

FGD 2 (small and medium business)

R2.1. Zhytomyr, medium-sized business, IT, team lead
R2.2. Kyiv, medium-sized business, IT, head of information security
R2.3. Odesa, small business, manufacturing, director
R2.4. Rivne, medium-sized business, manufacturing, computer systems engineer

FGD 3 (medium and big business)

R3.1. Lviv, large business, banking sector, information security specialist
R3.2. Odesa, medium-sized company, humanitarian organisation, head of security department
R3.3. Kharkiv, large business, banking sector, IT systems administrator
R3.4. Kyiv, large business, transportation, head of IT department

3.4.1. The risk of cybercrime

The spontaneous mention of cyber threats evokes a wide range of associations among business representatives, from specific technical threats to large-scale attacks on national infrastructure. The main associations can be divided into several groups:

- Technical attacks and malicious software;
- Fraud and social engineering;
- Threats to data and business processes; and
- Large-scale attacks on critical infrastructure and government institutions.

Respondents mention technical attacks first and foremost. In particular, these include DDoS attacks, where servers stop responding to requests due to overload. Also mentioned among technical attacks are programs that block access to information or encrypt company documents, demanding a ransom for unlocking them (ransomware). Many respondents also mentioned the Petya virus (2017) – an incident that became a symbol of cybercrime for many, as it paralyzed the operations of numerous businesses due to vulnerabilities in the M.E.Doc software.

Respondents classify phishing (sending fake messages via email or instant messengers to obtain data and access) as falling within the realm of fraud and social engineering. The activities of 'call centres' are classified as social engineering, as they are directed more towards the general public. Respondents also classify the theft of funds from bank accounts – belonging to both businesses and individuals, particularly through the forgery of a manager's account – as falling within the realm of fraud.

Data threats are perceived as being specific to the business community. The most frequently mentioned crimes are database leaks, theft of intellectual property, or theft of confidential company information. A related crime is industrial espionage, which is carried out through cyber access to company data. In general, as modern business is fundamentally dependent on IT, any cybercrime is perceived as a threat to the shutdown of all company processes.

Among examples of larger-scale cybercrime, respondents mention cyberterrorism and attacks on critical infrastructure, as well as cyber warfare. The most frequently mentioned of such attacks is the 2023 attack on Kyivstar (when hackers destroyed the network core, leaving millions of users without communication and internet access for several days).

Among the crimes mentioned, respondents consider the following to be the most critical for businesses and organisations:

- **Phishing** is considered the number one threat for virtually all organisations due to its frequency and its focus on the weakest link, the human factor.
- **Ransomware** is critically dangerous for companies whose operations depend entirely on databases (for example, 1C accounting software or banking registers). A successful attack can lead to the complete collapse of a company if there are no backups.
- **DDoS attacks** are most relevant for online services, e-commerce sites and infrastructure facilities (banks, telecoms), as downtime leads to direct financial loss. For large companies and banks, DDoS attacks and data breaches are more critical due

to public exposure — even a few hours of downtime or news of a breach can seriously undermine customer trust.

- **Data breaches** are a key risk for organisations handling customers' personal data or humanitarian aid.

Thus, the significance of a cybercrime is determined not by its complexity, but by the scale of potential losses (financial or reputational) and the likelihood of its successful execution due to staff error.

According to respondents, the rise in cybercrime is inevitable alongside the digitalization of business and everyday life.

However, business representatives do not consider themselves the most vulnerable target for cybercriminals. In their view, the most vulnerable section of the population is the elderly (respondents are unanimous on this point). In second place are Internally Displaced Persons (IDPs) and people seeking humanitarian aid. Criminals exploit their difficult emotional and financial situation by creating fake chatbots and 'payment' websites to extract money under the guise of 'processing fees' or to steal personal data.

Representatives of organisations and 'offended' employees rank only third in terms of vulnerability. Experts agree that the weakest link in any company's security system is the human factor. People fall victim to phishing due to inattention, fatigue or disregard for 'digital hygiene' rules (for example, opening suspicious attachments or links). This applies equally to management and key staff – the entire organisation can suffer due to mismanagement or negligence. As for 'disgruntled' employees, it is far easier for criminals to 'buy' access from a current employee (such as a system administrator) than to mount a complex hacking attack. Employees may therefore deliberately steal or destroy customer databases out of revenge or for their own gain.

3.4.2. Cybercrime experiences

Respondents had their first experience of cybercrime under various circumstances. Some encountered cybercrime whilst studying at university. Others had heard of hacker DoS attacks on websites as far back as their school days, which influenced their choice of career.

For some participants, their first serious encounter with cyber threats came through a large-scale incident, primarily the Petya virus (2017).

Older respondents, with over 20 years' experience in the IT sector, associate their first exposure to cybercrime with the onset of digitalization.

Overall, participants note that interest in cybersecurity has risen sharply over the last 3–5 years, as the market began to address system protection more systematically and at a legislative level. It is also noted that digitalization (in particular government services such as 'Diya') simultaneously creates new risks and drives the development of protective measures.

3.4.2.1. Phishing

Respondents describe phishing as one of the most widespread and dangerous forms of cybercrime. It encompasses a wide range of methods — from simple emails containing links to sophisticated automated social engineering schemes. Attacks are carried out via email,

instant messaging apps, social media and phone calls. Attackers use fake payment accounts, links for 'voting', offers of humanitarian aid or malicious attachments.

> To give you an idea, phishing targeting our bank, for example, involves a colossal number of emails – simply colossal. For every 100 legitimate emails, there might be 50, 60 or 70 phishing emails. The percentage is simply colossal. Most of them, of course, are filtered out at the entry point (**R3.1**)

Companies' experience shows that phishing messages arrive regularly and in large numbers. Some attacks have led to serious consequences: server infections, loss of corporate funds, and account hijacking in financial transactions. In addition to financial losses, respondents highlight reputational risks when fraudsters spread false information on behalf of organisations.

Some examples of successful attacks:

- A phishing email infected all the computers and the server of a logistics company and also took its website offline.
- At a humanitarian organisation, by clicking a link in a phishing email, attackers gained access to the database and deleted lists of people who were due to receive aid.

To combat phishing, companies employ a range of measures: technical (anti-spam, anti-virus systems, backups, two-factor authentication) and organisational (staff training, security policies, attack simulations). Participants emphasize that effective protection is only possible through a combination of technological solutions and high staff awareness. In particular, a range of strategies has been developed to combat phishing for organisations of all sizes (from micro-businesses to large corporations):

- The 'if in doubt, don't open it' principle: The main rule in many companies prohibits employees from opening emails, downloading attachments or following instructions if the message raises even the slightest doubt, regardless of any claimed 'urgency'.
- Verification in an isolated environment: In companies with their own IT departments, suspicious emails are forwarded to specialists who open links or files in an isolated environment for analysis. If a threat is confirmed, the domain and sender are blocked.
- Verification via alternative channels: If a suspicious request arrives from a manager (for example, regarding a funds transfer or the provision of data), the standard procedure is to call that person directly to confirm the instruction verbally.
- Technical filtering: Large organisations and banks use anti-spam systems that automatically block up to 99% of phishing traffic at the point of entry, so that the average employee does not even see these messages.
- Training tests: Some companies conduct simulated attacks: they send their own fake phishing emails to employees. Those who 'fall for the trick' undergo additional training.
- Action when a brand name is used: If phishing is carried out in the name of the organisation itself (for example, fake humanitarian aid payments), companies issue official denials and press releases and contact the cyber police to shut down malicious websites.

Modern technologies, particularly artificial intelligence (AI), significantly complicate the detection of phishing and scale it up. In particular, AI enables the automated creation and distribution of personalized phishing messages, as well as the faster identification of vulnerabilities in companies' infrastructure.

Overuse of tools such as ChatGPT creates new risks: employees may upload confidential documents (financial reports, legal papers) to open neural networks for analysis, effectively making them publicly accessible.

The increased use of cloud services expands the attack surface and creates a dependency on external providers, whose vulnerabilities could be exploited to gain access to customer data.

3.4.2.2. CEO fraud, sometimes called Business 'Email' Compromise (BEC)

A rare type of crime; respondents cited only a few instances. In both cases, respondents had no idea how such situations could have occurred – there must have been a data leak, and the attackers were privy to the organisations' internal affairs.

In the first instance, the organisation was awaiting an invoice for payment and received a letter containing an invoice with its details but featuring a false account number; the email address was also different. The errors were detected during verification, and the organisation suffered no loss.

The second example describes how a message was sent from a fake Telegram account claiming to be the manager's, requesting 16,000 UAH to be transferred to the fraudster's card. Similar requests from the manager had been made before, so the employees were not surprised. The fraudster created a fake Telegram account using the name and photo of the real boss, who was on holiday abroad at the time. The fraudster used phrases and jokes characteristic of the director, which lulled the employees into a false sense of security. The money was transferred, and two employees compensated the company's losses from their salaries.

Modern technologies significantly increase the effectiveness of attacks, making them harder to detect. AI allows for the creation of extremely realistic voice and video forgeries, making social engineering as convincing as possible. Criminals can simulate 'poor connection' to mask the flaws in the synthesized voice. The use of OSINT tools allows attackers to analyse workplace photographs, reports and employees' social media to learn about management's holiday schedules, the company's internal structure and communication style.

AI also enables criminals to communicate with many potential victims simultaneously on an automated basis, increasing the scale of attacks.

3.4.2.3. DDoS (interference attack)

DDoS attacks are seen as part of the digital environment in which businesses must operate, requiring investment in protection and continuous infrastructure improvements. This type of cybercrime is one of the most common threats to modern businesses, particularly in the context of digital transformation and military operations.

Some participants noted that their companies had not directly encountered attacks, whilst others emphasised that the absence of monitoring does not mean there are no attacks — they may simply go unnoticed.

Participants consider the main motives for such attacks to be extortion or blackmail, unfair competition where a competitor's website is 'overloaded' to poach customers, as well as political and military objectives aimed at destabilising critical infrastructure (for example, attacks on power grids or telecoms operators).

To protect the company, comprehensive solutions are employed: monitoring systems, Cloudflare, WAF, Firewall, bot filtering, as well as upgrading to more powerful hosting plans. The emphasis is on preventing data leaks in the event of an active attack.

Modern technologies have a dual impact on this type of crime. From the attackers' perspective, the use of artificial intelligence allows hackers to automate bot actions, find vulnerabilities more quickly and accelerate the attack processes. From a security perspective, AI is being actively integrated into DLP systems and monitoring tools to detect anomalies and enable automated responses to threats at the very outset.

The proliferation of cloud infrastructure expands security capabilities but creates a critical dependency on external providers. The failure of a single major security service could bring thousands of organisations worldwide to a standstill.

3.4.2.4. Data breach

This is a common threat to businesses and organisations. The main channels are phishing, social engineering and insider threats. Participants emphasized that even technically skilled employees can fall victim to deception due to fatigue, haste or inattention.

Companies' vulnerabilities are often linked to inadequate data storage systems (such as using spreadsheets instead of a CRM), a lack of proper access controls, and weak organisational processes.

To counter this, companies employ both technical and legal measures:

- The 'Zero Trust' concept. A model in which no device or user is considered trusted by default, and access is granted only upon verified request.
- Restriction of access rights. Ordinary employees should not have administrator rights, and access to databases must be segmented.
- Legal protection. Signing non-disclosure agreements (NDAs) and confidentiality undertakings, which enables companies to combat insider threats within the legal framework.
- Technical measures. Use of two-factor authentication (2FA), disk encryption (e.g. BitLocker) and regular backups.
- Mandatory reporting. Banks, in accordance with NBU requirements, are obliged to report breaches of banking secrecy or personal data to the regulator and the Ukrainian Parliament's Commissioner for Human Rights.

Security breaches or data leaks are perceived by Ukrainian businesses as one of the most critical threats, which can lead to reputational damage or the complete cessation of a company's operations.

3.4.2.5. Ransomware

Respondents perceive ransomware as a widespread cyber threat to business. Ransomware is seen as a threat capable of paralyzing a company's operations, but effective technical and organisational measures can significantly reduce the risks.

The main channels of intrusion are phishing messages, outdated software and the physical introduction of viruses via storage media. Hidden remote control programs pose a particular danger, as they can remain undetected for months and be activated at any moment.

The consequences of such attacks include complete data encryption, ransom demands and the disruption of business processes. A typical ransomware program offers to restore data in exchange for money. Respondents frequently mentioned the Petya virus, which caused damage to many businesses. Its aim was not to extort money, but to cause maximum damage; data was encrypted without the possibility of recovery. Respondents are sceptical that paying the ransom leads to data recovery.

Respondents emphasise that the key vulnerability factors are human error and the lack of regular software updates. They stress the importance of backups, which allow data to be restored after an attack. Staff training is essential to help avoid phishing traps.

3.4.2.6. Other cybercrimes

Among other cybercrimes, apart from those discussed, respondents highlighted the following:

- Insider threats.

These are considered among the most difficult crimes to detect and prevent. They involve malicious actions by the company's own employees (often senior staff) who have legitimate access to systems and can steal customer databases, destroy data before leaving the company, or pass on confidential information to competitors.

- Creation of mirror sites (clone websites).

Attackers completely copy the design and information from the company's official website but replace the phone numbers with their own to intercept orders and customer funds.

- OSINT threats

Criminals gather information about the company, its employees and managers from social media, photos, or public reports, to meticulously plan further attacks.

- Crypto fraud.

Criminals use phishing links for payments or the provision of services in cryptocurrency, leading to the complete emptying of victims' crypto wallets.

- Industrial espionage, i.e. the theft of intellectual property or trade secrets.
- Attacks on critical infrastructure.

Cyberterrorism which is aimed at destabilizing energy supply systems (blackouts) or communications (for example, the attack on Kyivstar).

3.4.3. Concerns and expectations

Based on the discussion, several key types of cybercrime can be identified that cause the greatest concern among representatives of Ukrainian business. The main factors of concern are not only the technical complexity of the attacks, but also the scale of potential damage — ranging from financial loss to a complete collapse of reputation.

Participants are most concerned about the following threats:

1. Phishing and social engineering. This type of crime is cited as the most widespread and pressing by virtually all groups of participants. Phishing is often the first link in a chain of planned cyberattacks. The main vulnerability is the 'human factor', the impact of which is amplified using AI to create deepfakes, making the deception extremely convincing.

2. Leakage of databases and confidential information. As customer and/or supplier databases are the most valuable assets for many companies, their leakage or loss is perceived as a critical threat. Furthermore, the information obtained may be used by competitors or adversaries for military purposes. Furthermore, the disclosure of internal information can undermine customer trust and carries reputational risks.

3. DDoS attacks. Participants note that DDoS attacks on infrastructure (particularly banking infrastructure) are virtually continuous.

4. Insider threats. Representatives of large organisations consider insider threats to be the most serious security challenge. After all, it is almost impossible to protect against the actions of one's own employee who has legitimate access to the systems. It is far easier and cheaper for a cybercriminal to 'buy' an insider than to devise a complex hacking scheme to infiltrate a bank or a large corporation.

5. Ransomware. Such viruses remain a symbol of a total threat to business data. After all, the threat of complete destruction of information with no possibility of recovery can lead to the company's demise if it has no backups.

6. OSINT and risks from neural networks. Modern experts highlight a new threat — excessive openness of information online and the use of public AI services (such as ChatGPT).

3.4.3.1. Trust in state institutions

Trust in state bodies (particularly the cyber police) as a source of practical assistance or professional personnel remains low:

- Experts believe that cyber police placements for students are often merely a formality ('for show') and do not provide real-world experience.
- If problems arise, businesses are more likely to turn to trusted colleagues from other private companies than to police representatives.

Generally, organisations' decisions on whether to report cybercrimes depend on their size, field of activity and the existence of legal obligations. Participants in the discussions expressed differing views on whether to contact state authorities. For example, the banking sector is obliged to report certain incidents (such as breaches of banking secrecy or personal data) to the National Bank of Ukraine, as well as to the Verkhovna Rada Commissioner for Human Rights.

Humanitarian and large organisations are more likely to contact law enforcement agencies, particularly when cybercriminals use their name for phishing. This is done to swiftly shut down malicious websites and protect their reputation.

Small and medium-sized businesses, on the other hand, often avoid reporting incidents. Representatives of these business segments prefer to resolve issues independently with the help of external specialists, focusing on restoring the system's functionality as quickly as possible, rather than on the investigation. After all, there is a fear that state authorities' interference with a company's internal data could cause more harm to the business than the hacking attack itself.

Furthermore, many entrepreneurs consider the work of law enforcement agencies to be ineffective ('results are close to zero') due to a lack of qualified personnel, bias, or an over-reliance on paperwork.

Overall, trust in state institutions regarding the protection of private businesses remains low, and only strict regulation (as in the banking sector) or a critical threat to the brand compels companies to seek official assistance.

3.4.3.2. Cybersecurity frameworks and standards

Organisations employ various methodological approaches to building defences. Large companies and banks follow international standards such as ISO/IEC 27001. This helps to structure information security management (ISMS) not only on paper but also in practice. In mature organisations, cybersecurity is a continuous cycle of policy improvement, technical controls and ongoing staff training.

In particular, organisations seek to utilize modern access models:

- Zero Trust. A model in which no user or device is considered trusted by default, and access is granted on a least-privileged basis.
- Identity-First Security. An approach where the central element of protection is digital identity management and multi-factor authentication.

Large and international humanitarian organisations widely apply local and corporate policies, such as global standard operating procedures, adapted to the Ukrainian context.

Respondents note that the organisation's internal environment often determines the effectiveness of technical security. As has been noted on numerous occasions, participants unanimously consider the human factor to be the weakest link. Inattention, fatigue or low digital literacy lead to successful phishing attacks. Vulnerability does not depend on age, gender or position within the company. To strengthen this link, organisations conduct regular training sessions and phishing tests to check employees' vigilance, and use internal knowledge bases and educational portals for staff certification.

To reduce the vulnerability of the 'human factor', organisations implement technical restrictions. In particular, the security culture of some organisations involves denying administrator rights to standard users, which blocks 90% of viruses. There is evidence of a ban on the use of public messaging apps (Telegram, Viber) for business correspondence.

The core technical solutions for organisations include data backups, two-factor authentication (2FA), the use of firewalls, antivirus software and specialized traffic filtering services to protect against DDoS attacks, and data encryption.

However, the implementation of cybersecurity standards in organisations faces a shortage of qualified personnel. According to respondents, the issue of finding cybersecurity specialists and investigating cybercrimes in Ukraine is quite acute. The situation is characterized by a shortage of personnel, a mismatch in qualifications and the high cost of professional experts' services.

Respondents noted that there are many specialists on the market who possess only basic theoretical knowledge gained at universities or on courses but lack practical experience. Their training may be limited to an internship with the cyber police 'for the sake of it', which does not provide real-world skills for handling incidents. Specialists often provide superficial consultations, offering simple solutions such as moving data to a 'secure' cloud environment that is not actually well-protected. Specialists distinguish between 'paper' security and real technical work:

- 'Paper' specialists: There are plenty of people on the market capable of dealing with methodology and paperwork, but finding an analyst who can professionally analyse logs or system vulnerabilities is extremely difficult.
- Superficial knowledge: Business representatives complain that many experts only discuss security superficially and struggle when it comes to in-depth technical questions.

Respondents emphasize that combating cybercrime requires systematic measures at both the state and corporate levels. For the state, the key requirements are:

- Revising approaches to security in the context of digitalization ('the country in a smartphone', 'Diya', digital banking).
- Establishing a clear regulatory framework for new challenges (crimes involving cryptocurrency and the use of artificial intelligence).
- Reforming the cyber police, as most participants consider the work of law enforcement to be ineffective due to bias, a lack of specialists and a focus on paperwork.
- International cooperation between law enforcement agencies and the creation of joint investigation mechanisms.
- Development of our own server infrastructure and data centres to avoid the risks of storing citizens' data abroad.
- Stepping up the fight against organised criminal groups (call centres, fraudulent offices).
- Developing cybersecurity education — from school level to training specialists with practical skills.

The following actions are important for business and society:

- Increasing budgets. Many cybersecurity solutions are expensive, and management does not always understand the need for such expenditures until a real incident occurs.

- Overcoming the ‘human factor’. Employees often resist inconvenient security measures (such as mandatory 2FA or complex passwords), so work needs to be done on corporate culture.
- Regular audits and penetration tests. Engaging external specialists to professionally assess system vulnerabilities.
- Information sharing. Creating platforms for the rapid exchange of data on new threats between companies (similar to how this works in the banking sector via the NBU).

Respondents describe the outlook for cybercrime and defence measures as a ‘race between the sword and the shield’. Technological advancements are driving growth in both criminals’ capabilities and defence tools. In particular, artificial intelligence is already being used both as an attack tool and a defence mechanism. Complete security is impossible to achieve, but the country and businesses must keep ‘up to date’ to understand new threats and respond to them appropriately.

> As progress advances, so will everything else. And that includes cybercrime tools. But security measures will also advance in parallel. In principle, I don’t think one can say that anyone can be 100 per cent protected, but it is a process—a process that will continue, encompassing both defence and attack. (**R3.2**)

3.5. Authorities

Respondents' profiles

R1. Representative of the Office of the Prosecutor General
R2. Representative of the Security Service of Ukraine
R3. Representative of the Cyber Police Department
R4. Representative of the State Bureau of Investigations

3.5.1. Cybercrime

The list of cybercrimes spontaneously mentioned by representatives of the authorities partly coincides with the perceptions of the public and businesses. In particular, respondents rank online fraud, such as the activities of so-called 'call centres' and the use of phishing, as the top concern. Other cyber threats mentioned include:

- Interference with systems, unauthorized network intrusion, and the corruption, destruction or theft of data.
- Malicious software: the development, sale and distribution of viruses, in particular ransomware.
- Complex cyberattacks targeting government bodies and critical infrastructure: DDoS attacks, supply chain attacks or man-in-the-middle attacks.
- Crimes involving crypto-assets: transnational crimes where cryptocurrency is used to conceal financial flows.

The assessment of the relevance of these crimes is based on threats to national security, the scale of financial loss and the difficulty of documentation. Experts therefore prioritize state-sponsored terrorism and attacks on critical infrastructure, which are predominantly carried out by an aggressor state. APT (Advanced Persistent Threat) groups affiliated with the Russian Federation's intelligence services are involved in such attacks. The attacks often exploit 'zero-day' vulnerabilities, which are not detected by countermeasures. The 2023 attack on Kyivstar was cited as an example.

Social engineering and online fraud have been ranked second, as the most widespread types of cybercrime targeting the general public. In particular, the Office of the Prosecutor General reports over 700 searches in the last six months, which indicates the industrial scale of this type of crime. Ordinary people are targeted by 'mass hacking' — the mass distribution of phishing messages (for example, disguised as 'eSupport' payments) with the aim of stealing bank details. In social engineering schemes, the trend of using AI to spoof voices and images is also gaining popularity, making phishing and telephone scams extremely convincing.

Experts have ranked the use of crypto-assets third in terms of relevance, due to the anonymity of transactions and the lack of clear regulation, which makes this area particularly problematic.

Over the past two years, coinciding with the period of the full-scale invasion, the cybercrime landscape in Ukraine has undergone significant transformations. Experts note changes not only in the volume but also in the strategic objectives and methods of attackers.

According to the SBU's assessment, complex cyberattacks are distributed as follows: 40% target the military (specific units or even individuals); 30% target critical infrastructure (energy, logistics, etc.); 30% target state authorities.

The trend in the number of offences is twofold, depending on their complexity. In particular, the Security Service of Ukraine has recorded over 14,000 cyberattacks over the last four years of active aggression. Interestingly, the number of complex attacks, specifically, has decreased slightly on an annual basis: whereas previously 3–4,000 were recorded per year, the figure is now less than 500. However, this does not indicate a decline in activity, but rather a shift in approach towards quality and preparation. Whilst at the start of the invasion the enemy attempted to massively destroy information or 'wipe' servers, the focus has now shifted to a sustained presence on networks for gathering intelligence. In other words, the aim of the attacks has shifted from destructive actions to long-term espionage within critical systems.

Since the 'human factor' is one of the greatest vulnerabilities of any system, assessing the digital literacy of both ordinary citizens and employees of companies and organisations is the most sensitive metric of the state of a cyber defence system.

Ukrainian experts assess the population's level of digital literacy as gradually increasing, yet it remains insufficient to counter modern threats. Poor cyber hygiene is a critical issue even in professional environments. For example, around 40% of sophisticated cyberattacks on the military succeed precisely because of poor cyber hygiene: the use of unlicensed software or opening unverified files in messaging apps.

> There will always be people who open a malicious file not out of malice, but out of curiosity and trust. (**R2**)

Furthermore, citizens often fall for attackers' 'emotional traps', particularly in situations requiring quick decisions (for example, notifications regarding 'eSupport' payments). Overall, according to experts, the situation is characterized as a 'two-way street': as public awareness grows, criminals proportionally make their attack methods more sophisticated.

> Over the last five years, we have seen an increase in the population's IT expertise or IT literacy, and this has consequently led to a more sophisticated nature of the attacks. (**R3**)

The measures proposed by the experts in order to improve the public's technical protection have remained unchanged for at least the last five years: using two-factor authentication, regularly updating software or removing programs that are no longer in use; avoiding pirated software; using different passwords for each website and changing them periodically.

Despite the consistency of basic cyber hygiene rules, the path to their adoption lies in the continuous education of the general public. To this end, both state resources (for example, cyber hygiene courses on the Diya portal) and employer resources must be utilized. According to experts, IT directors of organisations should regularly conduct training sessions for employees on the risks of social engineering. According to experts, organisations are far better informed and prepared to operate in an environment of cyber risks than the general public.

In particular, experts note that cybersecurity measures are improving within government bodies and at the level of critical infrastructure sites. Evidence of this is that complex cyberattacks, which were successful at the start of the full-scale invasion, now often fail because we have "learned from our mistakes." However, there is a significant gap between central bodies and regional units (for example, Administrative Service Centres or Ministry of Internal Affairs service centres). Locally, there is often a lack of specialist staff capable of configuring specific equipment (such as Cisco) and continuously monitoring threats. That said, even in professional organisations poor cyber hygiene among individual employees (use of unlicensed software and opening files from messaging apps) remains the main cause of successful attacks.

One approach to gathering information on cybercrimes is to encourage the public and businesses to report such incidents (as shown earlier, the general public is generally unwilling to spend time reporting, whilst businesses do so only under regulatory pressure).

> Not all victims report incidents or contact law enforcement agencies, so we note that these crimes have a high level of latency. And the statistics held by government bodies and law enforcement agencies represent only a fraction of the actual facts. (**R3**)

Experts assess the level of hidden (latent) cybercrime as extremely high and significant, noting that official statistics reflect only part of the real picture. According to experts, victims (both the general public and organisations) do not report incidents to law enforcement agencies for a number of reasons:

- High reputational risks for organisations and government bodies, which fear publicity surrounding a successful cyberattack.
- A lack of confidence that the crime will be investigated and the perpetrators found.
- Distrust in the system and concerns about the low competence or even dismissive attitude of rank-and-file police officers on the ground.
- The disproportion between the financial loss and the time involved. If the amount stolen is small, citizens often prefer not to spend time on legal proceedings.
- Problems with assessing damages, specifically the lack of methodologies for assessing material damage resulting from data breaches or reputational losses, which complicates criminal proceedings.

> If we consider the provisions of Article 361 of the Criminal Code of Ukraine, it states, among other things, that damage is one of the qualifying elements. However, no expert body in our country can specify, for example, damage in the form of reputational losses, or in the form of information leaks, which constitute material damage as an expression and consequence of the aforementioned unlawful acts. (**R1**)

In general, experts tend to believe that the number of hidden cybercrimes is increasing. This is explained by a mathematical proportion: as the total number of attacks and instances of IT being used for criminal purposes increases, the latent portion grows proportionally.

To reduce the gap between actual crimes and official statistics, the following measures are proposed:

- Legislative changes. Further implementation of the Convention on Cybercrime (Budapest Convention), which will strengthen the capabilities of investigative authorities.

- Training for law enforcement officers. Training is necessary, not only for cyber experts, but also for prosecutors, investigators and judges, so that they understand the specifics of digital evidence.
- Development of damage assessment methodologies. It is advisable to create a standardized methodology for determining the losses caused by cyberattacks, which will enable criminals to be brought to justice more effectively.
- Awareness and prevention. Regular coverage of successful cases of apprehending offenders is expected to boost public confidence, as well as delivering courses on cyber hygiene.
- Work at the local level. There is a need to address the staff shortage in regional units so that citizens receive professional assistance even in small towns.

A distinct category of cybercrime comprises offences committed against state authorities in Ukraine. According to experts, cybercrime is indeed deeply intertwined with state structures, particularly in the context of modern warfare. This link manifests itself both in external aggression by enemy intelligence services and in the internal workings of state bodies. In particular, the Security Service of Ukraine has recorded cases of deliberate actions by state officials who provide information or access to networks to enemy intelligence services. In addition to these deliberate actions, there is also professional negligence. For instance, a representative of the State Bureau of Investigation notes that their work involves responding to cases where officials fail to take the necessary measures to protect critical infrastructure, which may constitute negligence. These factors are compounded by the fact that state structures themselves are often the target of sophisticated cyberattacks (according to the SBU, in up to 30% of cases). For example, attackers specifically target government resources, such as the Ministry of Justice's registries, causing immense damage to the state that is difficult to quantify in monetary terms.

3.5.2. Offenders

Based on the discussion, it is possible to identify several key types of individuals and groups behind cybercrimes, as well as to understand their motivations and methods of operation. Experts classify cybercriminals by skill level and objectives:

- **APT groups** (Advanced Persistent Threat). These are the most highly skilled hacker groups, operating on behalf of intelligence services (such as the FSB or GRU of the Russian Federation). They carry out complex, covert attacks on government bodies and critical infrastructure.
- **Hacktivists** are politically motivated individuals whose aim is not so much to cause serious harm as to gain publicity (for example, defacing websites or placing banners).
- **Financially motivated criminals** — organized groups specializing in fraud (for example, 'call centres') or ransomware.
- **Script kiddies**: amateurs who use ready-made instructions from the internet to carry out simple attacks.

- **Insiders**: employees of government bodies or companies who deliberately provide information or access to networks to malicious actors.

The motivation of cybercriminals is based on the following factors, or a combination thereof.

- **APT groups** pursue political objectives and state-sponsored missions. They focus on gathering intelligence and engaging in destructive activities to the detriment of a hostile state. They are rarely motivated by financial gain and never by public notoriety
- **Financially motivated criminals**, as the term suggests, expect financial gain if their cybercrime is successful. This may involve making a profit through fraud, selling stolen data on the Darknet, or demanding a ransom. Such groups as Script kiddies and Insiders are also motivated by financial gain.
- **Hacktivists** seek widespread publicity and the enhancement of their reputation and status within the criminal underworld. For criminals in this group, it is important to make a name for themselves. Script kiddies may also be interested in the publicity their actions generate.

Experts point out that sophisticated attacks are almost never carried out by a single individual — they are the work of groups with a clear division of roles. Criminals coordinate via specialised websites and forums on the Darknet. Registration often requires financial contributions, recommendations or 'vouching' from reputable members (guarantors). In addition to 'customized' cyberattacks, there is also a 'Cybercrime as a Service' (CaaS) model. One can buy access to a specific company's network, purchase a 'zero-day' vulnerability, or commission the writing of malicious code. A certain specialisation among criminals is observed in this market: one group may steal data, another will resell it, and a third will use it to take out loans or steal funds.

As for the profile of a cybercriminal in terms of the methods used, experts believe it is not static. Experts note a constant evolution of methods. First and foremost, this involves the use of artificial intelligence. AI is already being actively used to create convincing phishing messages, voice spoofing (deepfakes) and image manipulation. Criminals are becoming more professional, using unique tools that antivirus software cannot detect. Experts note that the criminal world adopts new technologies faster than the state system or ordinary users, as it views this as an investment in future profits.

> Cybercrime is, in general, extremely dynamic. What was relevant yesterday may not work at all today. (**R2**)

The following methods used by criminals against both ordinary citizens and organisations and businesses can be identified. Criminals use a combination of technical vulnerabilities and psychological manipulation:

- Social engineering and phishing. This is one of the most common methods. Criminals create fake resources (for example, websites imitating 'eSupport' payments) or use emails and messages in instant messengers to extract data. In the workplace, criminals use employees' work or personal email accounts to send malicious links or files. Modern attacks even include emulating the voices of management or colleagues in voice messages using artificial intelligence.

- Technical vulnerabilities and malware. Criminals gain access via unpatched apps on phones or by downloading pirated (hacked) software that already has malicious code 'embedded' within it for tracking or stealing credentials. This mechanism is relevant for both the general public and organisations.
- Compromised websites (used against the general public). When booking hotels or shopping on little-known websites, proxy settings may be in place that secretly record bank card details along with the CVV code.
- Supply chain attack (used against businesses). The breach occurs via third-party software products used by the organisation.
- Purchasing data on the Darknet (relevant for both the general public and businesses). Criminals often buy ready-made databases containing citizens' phone numbers, addresses and bank details, or access to specific companies' networks. The price of such access can reach tens of thousands of dollars.
- Mass scanning (relevant to everyone). Attackers scan ranges of IP addresses to identify vulnerable network equipment (routers, switches) with open ports.

Once access is gained, attackers can proceed according to several scenarios, which vary depending on who exactly was the target of the attack. For instance, in the case of an attack on the general public, one should primarily expect direct theft of funds from bank cards, an increase in the credit limit followed by the withdrawal of funds, or the taking out of loans in the victim's name. Less commonly, the victim's computer may be covertly incorporated into a network to carry out DDoS attacks on other resources. The device owner may not even be aware of this. If the target of the attack was a well-known or media-profile figure, the stolen data may be used to compromise the individual, blackmail them, or carry out media attacks by spreading false information.

If the target of the attack was a business or organisation, the access gained could be used for espionage or data exfiltration (particularly if the victim is a critical infrastructure facility). The organisation's systems may also be encrypted, with a ransom demanded for their release (ransomware). In some cases, this leads to a complete halt in production processes. However, experts emphasise that such attacks are more prevalent in the 'wealthy' countries of Western Europe, and Ukrainian companies are more likely to be targeted by mistake.

> But I can say unequivocally that ransomware attacks are not widespread, because typically these attacks are directed only at wealthy countries – specifically at companies in wealthy Western nations, Europe and elsewhere. In Ukraine, ransomware attacks are extremely rare. (**R2**)

Depending on the objectives of the attack, criminals may resort to destructive activities, namely data deletion, the destruction of government registers, or the wiping of servers. The aim of the attack may also be to steal confidential information for its subsequent distorted publication or blackmail with the aim of exerting political or corporate influence, or to intercept financial flows, or to use the organisation's resources for mining or DDoS attacks.

Experts note that criminals take measures to remain anonymous and complicate the work of law enforcement agencies. Criminal organisations often have a hierarchical structure, where organizers, operators, 'mules' (individuals to whose bank accounts money is transferred) and

the victims themselves are located in different countries, creating bureaucratic obstacles for the investigation. They use server chains, IP addresses from other countries and crypto assets to conceal financial traces. Coordination takes place on Darknet forums, where a system is in place to minimize the risk of infiltration by security services. Furthermore, in the case of complex attacks, malicious software can remain in the system for years after infiltration without causing any damage, merely extracting information. This is particularly true of the most sophisticated groups (APTs), which operate as covertly as possible, without revealing their presence, in order to collect data for as long as possible.

According to experts, cybercrime rarely ends with a single incident. One crime (such as email breach) often leads to a series of others — selling the data on the Darknet, using it to hack the victim's other accounts via the 'forgot password' feature, or reselling the database in a slightly modified form to other attackers. If the criminals have gained access to a computer, they may wait until the device is switched on, but the user is inactive (for example, during lunch) to make remote purchases on marketplaces on the victim's behalf. The original attackers may simply sell access to the network or device to other 'specialists' for a percentage of the future ransom. They often expect to receive this ransom twice: first for decrypting the data, and then a separate payment to ensure that the stolen confidential information is not published.

In recent years, there has been a significant evolution in the profile of those committing cybercrimes. The main trend is the professionalization of attackers and their adaptation to the population's growing level of digital literacy. For example, whereas phishing used to rely on simple, visually similar websites, attackers now use full-scale resource proxying to intercept traffic in real time. As already mentioned, in social engineering schemes (particularly when compromising business email or making calls), criminals have begun actively using artificial intelligence to spoof voices (deepfakes), images and phone numbers. Criminals undertake in-depth open-source intelligence, studying the family structure and behaviour of a specific victim to create the most convincing scenarios possible.

According to experts, the criminal underworld reacts to technological innovations faster than law enforcement, as it views new technologies as a direct investment in future profits.

3.5.3. Activities, needs and expectations

Ukrainian state bodies are involved in combating cybercrime at all key stages — from prevention to bringing perpetrators to justice — with functions allocated according to specialization. In the area of prevention, the main focus is on improving cyber hygiene among the public and organisations. In particular, the Cyber Police Department is involved in creating educational courses on the 'Diya' platform, whilst the Office of the Prosecutor General provides information on exposed schemes, raising awareness of the methods used by cybercriminals. However, increased public awareness is making attacks more difficult to carry out.

At the stage of detecting and stopping attacks, law enforcement agencies carry out real-time monitoring and response. The Security Service of Ukraine utilises a network of regional cyber centres, whilst the Office of the Prosecutor General conducts large-scale operations, including raids, aimed at dismantling fraudulent call centres. These activities are driven by the need to protect national security and critical infrastructure.

Incident response includes providing technical support to affected organisations to ensure the rapid restoration of their operations. Specialists from the relevant departments worked on restoring systems following large-scale attacks on major state and private entities, which required a high level of expertise, including knowledge of telecommunications infrastructure. The need for rapid restoration is driven by the risks of significant economic losses and disruption to the provision of critical services.

The procedural unit focuses on identifying those responsible and bringing them to justice. The Office of the Prosecutor General provides procedural oversight and utilises mechanisms of international cooperation, in particular joint investigation teams, to investigate transnational crimes. The State Bureau of Investigations, for its part, deals with cases of professional negligence that have led to vulnerabilities. At the same time, some complex cyberattacks linked to the activities of organised groups are beginning to be classified as war crimes.

A separate focus is on enhancing the resilience of systems and preventing future attacks. This includes readiness checks on critical infrastructure facilities, as well as participation in the drafting of legislation, particularly in the context of implementing international standards. Cooperation with international technology partners plays a vital role in analysing new threats, particularly malware and zero-day vulnerabilities.

International cooperation has become one of the key elements of the cybercrime response system. Ukraine actively engages with foreign partners both through bilateral relations and within the framework of international organisations and projects. It utilizes joint investigation teams, Council of Europe mechanisms and information-sharing networks. At the same time, Ukraine's experience in countering complex cyberattacks is in demand at the international level, owing to the unique context in which the country has effectively become a testing ground for the latest cyber threats.

According to experts, internal cooperation between state bodies is well-developed, particularly at the level of central structures, where joint working groups operate and information exchange is well-established. A network of cyber centres operates at the regional level, though there is a shortage of qualified personnel. Public-private cooperation is also of significant importance, particularly in the form of technological partnerships with international companies and the involvement of experts on a voluntary basis, although this is constrained by confidentiality requirements.

Several critical gaps in the capacity to combat cybercrime can be identified, covering both technical and organisational aspects. The most critical issue is human resources, which include staff shortages, competition with the private sector, and uneven levels of training, particularly at the local level. Indeed, government bodies are not competitive in the labour market due to low salaries compared to the IT industry. Experts state quite clearly: 'there is always a shortage of staff'.

Whilst high-calibre specialists work at central government level, regional offices (Administrative Service Centres, service centres) often lack specialists capable of even performing basic configuration of equipment (for example, Cisco). Furthermore, there are very few certified experts in Ukraine capable of conducting computer forensic investigations, which leads to delays in investigations. Moreover, it is impossible to train an expert 'once and for all',

as there is no such thing as a 'sufficient' level of knowledge in the cyber sphere — any pause in training means immediately falling behind the attackers.

Limited funding affects technical capabilities, as cybersecurity is viewed as a cost centre. In contrast, for criminals, new technologies represent an investment in future revenue, so they acquire tools (such as zero-day vulnerabilities) more quickly. Hardware requirements depend directly on the legal provisions governing the preservation of digital evidence. The legislative framework does not fully reflect reality. There are no clear mechanisms for assessing non-material damage, nor are there specialist judges. Additional challenges include the slowness of international procedures for obtaining evidence and the high level of latency in criminal cases.

> It must be understood that cyber security is always a cost centre. As a purely cost-driven activity, it cannot generate profit. And businesses worldwide operate on the premise that there is no need to fix something that is already working. (**R3**)

Cybercrime is expected to become even more sophisticated in the coming years. Attackers are quick to adapt to new technologies, using them as a tool to increase the effectiveness of their attacks. Artificial intelligence will play a particular role, as it is already being used to create convincing fraudulent schemes. Risks associated with attacks on supply chains, the exploitation of zero-day vulnerabilities and the potential development of quantum technologies will increase. At the same time, defensive approaches will also evolve, requiring constant system updates and the upskilling of specialists.

Overall, there is a shift from mass and relatively simple attacks to complex, targeted and often long-term operations, in which a covert presence within systems and the exploitation of technological advantages play a key role.

4. Conclusions

In focus groups with the public, cyberspace emerges as an everyday environment with high usage intensity, combining a wide range of practices — from communication and content consumption to financial transactions and interaction with government services. This creates an ambivalent perception: a high level of engagement and partial trust (primarily in banking and government services) is combined with a sense of constant vulnerability. The main threats are interpreted through the prism of personal experience and boil down to financial losses, account hacking, theft of personal data and psychological pressure. Phishing is the most recognizable and widespread form of cybercrime, whilst more complex types of attacks remain poorly understood.

Artificial intelligence occupies a distinct place in perceptions: it is simultaneously used as a tool for verification and analysis, while also being perceived as a source of new risks due to the possibility of creating convincing fakes. Behavioural protection strategies remain unsystematic: the importance of caution and basic security measures is emphasized, but there are no established protocols for action, partly due to fatigue, stress and information overload.

At the same time, the notion of cybersecurity as **a personal responsibility** is clearly articulated. Despite this, there is a noted public need for the familiar paternalistic approach, where a state body is responsible for cybersecurity. This need remains unmet due to low trust in law enforcement agencies in the field of cyber defence. The reasons for this low trust include experiences of ineffective interaction, bureaucracy, and the belief that most incidents are not investigated. Banks and digital service support teams inspire relatively greater trust, but paternalistic expectations cannot be shifted onto them.

In focus groups with business representatives and IT specialists, cybercrime is viewed as a systemic characteristic of the digital environment that directly affects business continuity and reputation. The perception of threats is structured and technically differentiated: respondents clearly distinguish between types of attacks (phishing, DDoS, data breaches, ransomware, insider threats) and assess them in terms of potential financial and reputational losses. Phishing is identified as the most basic and widespread threat, often serving as the initial stage of more complex attacks. Ransomware and attacks on infrastructure occupy a special place, as they are perceived as capable of completely paralysing an organisation's operations. The impact of previous large-scale incidents (notably the Petya virus) is significant, as these have cemented the perception of cyber threats as systemic and potentially catastrophic. Central to this is the notion of the 'human factor' as the primary vulnerability. This is a common trend across all groups, but in business it is operationalized through security policies, staff training and technical restrictions. Organisations adopt comprehensive approaches to protection (international standards, access models, technical solutions), which differ fundamentally from the individualised and unsystematic practices of the general public.

The use of AI is viewed as a double-edged sword: it simultaneously enhances attack capabilities (automation, personalization, deepfakes) and creates new vulnerabilities through data leaks to public services.

Trust in state institutions is low, but of a different nature: businesses pragmatically avoid engagement, preferring to rely on their own resources or private experts; a shortage of skilled personnel acts as an additional constraint.

In focus groups with experts, cybercrime is predominantly interpreted at the macro level — as a component of national security, encompassing both widespread fraudulent practices and targeted attacks on government systems and critical infrastructure. The emphasis is shifting from individual and corporate risks to systemic threats, in particular cyberterrorism and sustained attacks aimed at gaining access to data and espionage. At the same time, experts acknowledge the high latency of cybercrime, which implies a significant gap between official statistics and the actual prevalence of incidents. Assessments of the effectiveness of the state system partly coincide with those of other groups: **there is a shared perception across all FGDs that institutional mechanisms for combating cybercrime are insufficiently effective**. At the same time, unlike the general public, experts do not reduce the problem to individual behaviour but view it as a consequence of systemic constraints — regulatory, organisational and staffing-related, including a shortage of specialists and relative lack of analysis as to damages.

In summary, all three groups share common perceptions regarding the rise of cyber threats, the dominance of phishing as the most widespread type of crime, and the decisive role of the human factor as a key vulnerability—these are the basic common trends. Furthermore, all groups recognize the transformative impact of artificial intelligence, which simultaneously complicates the detection of fraud and escalates attacks. Additionally, low trust in the law enforcement system is a common feature, although the reasons for this vary.

Differences between the groups are evident in the level of analysis and priorities. The general public focuses on the risks of personal financial loss and acts on a case-by-case basis. Businesses focus on process continuity, data protection and reputation, implementing systematic approaches. Experts focus on state-level threats and the need for institutional change.

Assessments of digital literacy also differ: the general public tends to acknowledge their own awareness whilst behaving cautiously, whereas experts assess the level of cyber hygiene as insufficient. Expectations regarding the response also differ: the public looks to the state as a source of protection, businesses concentrate on internal resources and standards, and experts emphasise systemic reforms and the development of institutional capacities.