Institut pro kriminologii
a sociální prevenci

Kateřina Kudrlová
Viktorie Paloušová
Jiří Vlach

# Cybercrime from the perspective of justice system and everyday users

Praha 2023

Ediční řada Studie

# Summary

**Kudrlová, K., Paloušová, V. & Vlach, J. (2023). Cybercrime from the perspective of justice system and everyday users a IKSP.**

The publication presents findings of the research conducted by the Institute for Criminology and Social Prevention „Assessment of cybercrime trends“. Team led by Dr. Kateřina Kudrlova was working on it between 2020 and 2023. The project consisted of an extensive questionnaire survey focused on selected online experiences and analysis of criminal files on cybercrimes. Results are presented to the general and professional public mainly through this publication, as well as through several articles and conference presentations.

Topics of the questionnaire are based on results of the previous analysis of criminal files related to cybercrime in 2015 (in short) and on search of publicly available statistical data relevant to cybercrime. They focus both on areas where little or no data is available (e.g. sharing of login details for different online accounts) and on improving and deepening otherwise available data (e.g. distinguishing phishing requests for money versus requests for personal data). Data collected thus include devices used for online activities and their protection, selected user skills and experiences of unjustified behaviour: ransomware, phishing, online account misuse (emails, social media profiles, e-banking, gaming accounts), online trading fraud and copyright infringement. Respondents answered both as potential victims and self-reported as potential perpetrators.

The data collection was carried out by a professional company using the CAWI method in November 2020, with the vast majority of the data relating to approximately 2020 („the past 12 months“, hereafter „2020*“). The resulting large sample of 6,811 respondents represents the Czech internet population aged 16–74 (quota sampling taking into account gender, age, education, region and size of place of residence). Data were analysed using SPSS software.

The analysis of criminal files included practically 100% of criminal proceedings on so-called computer crimes (Section 230–232 of the Czech Criminal Code), whose perpetrator was finally convicted in 2019. Dozens of features were monitored, from socio-demographic characteristics through modus operandi to selected circumstances of the criminal proceedings.

Now a few words about actual results, first with regard to the questionnaire survey. Respondents were most likely to use mobile phones, with laptops next in prevalence and desktop computers somewhat less so. By far the largest number of devices were private, with significantly fewer employee devices, and a few business devices (private devices dedicated exclusively to work related activities). Devices most commonly use Android (mobile phones) and Windows (computers) and tend to be secured with antivirus, with the exception of mobile phones. They are mostly maintained by users themselves or with the help of IT professionals (especially employee devices). Devices are most often shared with partners and close family members, while employee devices are also shared with colleagues. Some devices were attacked by ransomware in 2020* (lower percentage units), with attacks affecting computers more often than mobile phones. Men are more likely to try to resolve the situation on their own, women and young respondents are more likely to turn to the police (about 15% of those attacked).

The vast majority of respondents used email in 2020*. A fifth of them had experienced phishing requesting personal information at that time, and 40% had experienced phishing requesting money, very roughly half of the respondents in each group repeatedly. Both types of phishing appear to be more easily detected by men and university students, whereas women are more likely to be victimised. There were not many phishing scammers in 2020* (especially men and those under 29), but they acted repeatedly.

Emails tend to be secured with strong passwords, but respondents often share these passwords with others, most often with close family members and partners. Some of these people then misuse their knowledge of the password to get unauthorised access to the email, and it is also common to physically access a particular device. Overall, the experience of unauthorised access to email is in units of percentages of actors on both sides. In particular, victims detect actions that leave noticeable traces (changing passwords, deleting content, assuming identity in the form of communication on behalf of the email owner, etc.), whereas perpetrators are noticeably more likely to report simply viewing content. Victims often assume unauthorised access by an unknown hacker, but perpetrators are significantly more likely to access the online accounts of their partners or close family members, motivated by curiosity or jealousy.

When it comes to self-presentation, it is mainly men and people under 29 years of age who are confident. Respondents make extensive use of social networks, most often Facebook. Almost half of them have some idea about the dark web, young users and men often have personal experience with it. Here too, units of percentage have experience of unauthorised use of a profile on a social network, slightly more so for those under 29. The findings are strongly consistent with those in the area of email misuse: the main actors on both sides include partners and people from the close family circle, there was misuse of known passwords and physical access, and the detected behaviour differed significantly from that reported. Compared to financial motivation, virtual violence was predominant, and was expected especially by persons under 29 years of age (men were more likely to expect money motivation). Here too, curiosity and/or jealousy were predominant.

Respondents also communicated with and used fake profiles with fictitious or someone else's identity. About a tenth of them asked for something – fake profiles with someone else's identity were more likely to seek financial gain, profiles with fictitious identities were more likely to seek intimate communication. Contacted respondents were more likely to report a fake profile with a fictitious girl/female identity, but the respondents themselves were more likely to use a fictitious boy/man identity. It is possible that the fictitious boy/male identity is harder to detect or that respondents are more cautious about girl/female profiles. Profiles with someone else's identity were most often inspired by media personalities.

E-banking misuse evokes a clearly financial motivation compared to social networks and emails, but in fact mere curiosity is a strong motivation for perpetrators. Here again, a considerable amount of unauthorised activity enabled by shared login credentials comes into play. From the point of view of actors, e-banking misuse also bears a strong resemblance to experiences with emails and social networks.

Overall, the online accounts appear to be subject to a number of undetected unauthorised accesses. Actors are current partners, driven by curiosity and taking advantage of previous knowledge of a password or sharing a device with a partner, or physical access to a particular device, while their activity remains hidden as they ‚only' view otherwise hidden content.

The picture is somewhat different for gaming accounts. While there is also a disproportion between the respondents' answers on the victims' and the perpetrators' side, the predominant motivation is gaming itself (except for gambling).

The majority of respondents (over 90%) shop online on e-shops, and around a fifth of them have experienced a defective goods delivery in 2020* caused by the e-shop, mostly worth up to € 80. Three quarters of them have subsequently requested a correction from the e-shop, and about three quarters of them have actually obtained a remedy. Nearly half of the respondents shop on online marketplaces, while nearly a fifth also had defective goods delivered in 2020* (again, mostly in the value of up to € 80). Here too, about three quarters turned to the seller, but only less than half of the respondents obtained a full remedy (another fifth obtained at least a partial remedy). A few dozen respondents sold the goods themselves via e-shops and less than a third via advertising portals, but most of them avoided delivery of defective goods (three quarters of e-shops and over 90% of sellers on advertising portals).

Around two-thirds of respondents had downloaded some content in 2020*, with around a quarter reporting infringing music or films and a tenth reporting infringing software (e.g. computer games). Some respondents (less than a tenth) had also made infringing content available to others in 2020*. The prevailing motivation was excessively high cost of legal access, and for software, enjoyment of one's own skills was almost as common. The prevailing age category was under 24, and in total under 34 (roughly three quarters).

Among employees with access to an otherwise non-public information system, several dozen individuals were found to have misused their access beyond their authority or misused a colleague's access in 2020*. In addition, roughly one-fifth of respondents found an unknown storage medium and nearly half of them used it, including nearly half without any prior checking for possible hidden malware. However, they did so mostly on private devices.

While studying perpetrators and victims, we created a victimization index and a perpetration index. Younger individuals are concentrated among the perpetrators, however, digital piracy may have a significant impact. Victimization occurs most often on social media and through the misuse of private email, but in general it is not possible to point to any particular sociodemographic or other characteristics specific to victims of cybercrime. Rather, the relationships found are only weak indications. Young people appear to be more at risk, but they are also significantly more likely to use digital technologies on a regular basis. The level of self security has no major impact on victimisation. In addition, detected attacks (e.g. unauthorised use of an online account) may say more about the ability to detect such attacks than about their prevalence.

It was confirmed that there is a substantial latency of the phenomena observed, overall at the level of about one tenth of the cases reported to the police. The tendency to report at least some of attacks is particularly evident among polyvictimized individuals. Those who do contact the police tend to be satisfied with their work.

As for the results of the analysis of criminal files for 2019, it follows previous findings from 2015. Among those convicted, men predominate, in half of the cases tried for the concurrence of a computer and another crime. More than half of those convicted were first-time offenders. The age structure has changed slightly from 2015, with a decrease in the overall proportion of younger offenders. The distinction between older generations and those already growing up in a digital environment is (and will continue to be) gradually blurring. The level of sentences imposed is largely influenced by the concurrency of offences, usually more severely punished. Of the 158 cases monitored, 50 involved the tampering with tachographs.

However, the findings from the analysis of the criminal files must be taken with reservation of the wording of the elements of computer crimes. In our opinion, it does not correspond adequately to social reality, but it is based on international obligations. Nevertheless, there could be some space for a limited decriminalisation. This is particularly desirable in order to ensure that the use of criminal sanctions does not apply to relatively common activities with little harm to the victim, while more serious cases would still be punishable.

Virtual violence, especially between intimate partners, appears to be an important topic for future research on cybercrime within the Institute for Criminology and Social Prevention. They represent a specific group that has unexpectedly come to the fore in the context of online account misuses motivated by motivations other than money.

**Cybercrime from the perspective of justice system and everyday users**

Autoři: Kateřina Kudrlová
Viktorie Paloušová
Jiří Vlach
Vydavatel: Institut pro kriminologii a sociální prevenci
Nám. 14. října 12, 150 00 Praha 5
Určeno: pro odbornou veřejnost
Design: addnoise.org
Sazba: Lukáš Pracný, sazbaknih.cz
Tisk: Reprocentrum, a. s., Blansko
Vydání: první, prosinec 2023
Náklad: 200 ks

www.iksp.cz

**ISBN 978-80-7338-204-9**