

Digital victimization experiences in Iceland in 2016-2022¹

Helgi Gunnlaugsson & Jónas Orri Jónasson
(*University of Iceland*)

Abstract

The web has increasingly been used as a source to target suitable victims all over the globe. By using the internet we can all be connected offering all kinds of new opportunities for deviant activities and crime. The first study in Iceland examining cybercrime victimization among the Icelandic public was conducted online in 2016 and was repeated every other year 'till 2022. According to the findings in 2016, about 13 percent of the respondents reported having been victimized by cybercrime in the past three years prior to the survey. In 2018 and 2020 close to 20% of the respondents admitted cybercrime victimization. Slightly fewer respondents admitted cybercrime victimization in 2022 compared to 2020 and 2018, or about 16%. In the paper it is shown that both the me-too movement starting in 2017, and the pandemic during 2020-2022, might have had some impact on sexual harassment victimizations and slander experiences respectively.

Key words

Cybercrime, Me-too, Covid-19 Pandemic

Introduction

Crime control agencies such as the police have in recent years detected a shift of criminal activity from the “real world” to the internet. The web has increasingly been used as a source to target victims all over the globe. Through the internet, people worldwide can be connected, giving rise to all kinds of new opportunities including deviant activities and crime. Several internet-related threats are regularly being reported

¹ An earlier version of this paper (Cybercrime victimization in Iceland) was presented at a research seminar organized by the Scandinavian Research Council for Criminology (NSfK) in Hameenlinna, Finland May 8–10, 2023.

in the mass media, e.g. consumer fraud, ID thefts, sexual harassment, cyberbullying and, more recently, cyberwarfare; all of these indicate a new type of threat to public safety in postmodernity.

Today, daily life increasingly involves online activity, particularly in Western societies. Routine tasks more frequently take place online: we pay bills, communicate with friends and family, order food, plan holidays, and book flights and hotels. According to Eurostat (2023), approximately 98% of Icelandic households had internet access in 2022, the highest share in Europe alongside Norway and Denmark; Luxembourg and the Netherlands followed closely at 97%. Icelandic users are also among the most likely to use the internet regularly: Sigurðsson (2015) reported that roughly 97% of Icelandic internet users accessed the internet at least once a week, the highest rate in Europe in 2014.

The increasing time people spend online has created numerous opportunities for criminal and deviant activities. Such risks have become part of everyday life and are increasingly recognized by the public. Reports of digital crime now occur daily. The social media team at the Reykjavík Metropolitan Police has repeatedly posted warnings on Facebook about online scams and other cybercrime-related activity (Metropolitan Police, 2025). Similarly, a local bank advisory warned customers about fraudulent offers purporting to be from the bank (Landsbankinn, 2023). Digital crime is expected to overtake drug-related offenses as perpetrators adopt increasingly sophisticated methods.

Making sense of digital crime is challenging for criminologists, primarily because there is no consistent definition. The term digital crime does not appear in the penal code, yet it is widely used in political, criminal-justice, media, public, and academic discourse (Yar & Steinmetz, 2019). Digital crime is also largely absent from official statistics: few offences are reported to the Icelandic police, and research indicates that a substantial proportion remain unreported for various reasons. Victims may be unaware that an offence has occurred, may regard the incident as insufficiently serious to contact

the police, may believe the police will not respond, or may feel embarrassed.

Another challenge of defining cybercrime is that targets can range from governments and multinational corporations to individuals. Therefore, it can be difficult to grasp digital crime as a single phenomenon, it should rather be understood as a range of illegal activities. A typical definition for different forms of digital crimes is that it has been committed using computers or other online platforms (Holt, Leukfeldt, & van de Weijer, (2020). Instead of considering digital crime a single phenomenon, it should be viewed as an umbrella term used to describe two closely related criminal activities: digital-dependent and digital-enabled crimes. As is apparent from the term, digital-dependent crimes depend on computers, computer networks, or other forms of information communications technology (ICT). Digital-dependent crimes can therefore only exist online and cannot be committed without the use of computer technology. These types of offences include hacking or spreading viruses, which are directed against computers or network resources from other computers. Digital-enabled crimes, on the other hand, are traditional crimes which are amplified in their scale with the aid of computers or computer networks. Unlike digital-dependent crimes, they can be committed without the use of the internet or computers, for example fraud, data theft, and sexual offence (Sarre, Yiu-Chung & Chang, L.Y.C., (2018).

In a recent criminological textbook (Siegel, 2023) different types of digital crime types are identified. First is *cybertheft* which involves the use of cyberspace to defraud people for quick profits such as illegal copyright infringement, identity theft, phishing, and fraud. Second is *cyber deviance* which includes distribution of illegal goods and services such as pornography and drugs. *Cyber vandalism* is the third type, involving the use of cyberspace for revenge, destruction, and to achieve malicious intent. Examples include website defacement, viruses, slander, harassment, image-based sexual abuse, cyberstalking, and cyberbullying. Finally, there is *cyberwar*, involving efforts from enemy forces to disrupt the intersection at which the virtual electronic

reality of computers meets the physical world. Logic bombs used to disrupt secure systems or networks are examples of cyberwar.

The focus in this study is on individual victims, examining victimization among the Icelandic public. Our focus is on experiences considered digital-enabled crimes and deviant activity online that can have an impact on the victim. Not much is known about how widespread digital crime is in Iceland apart from a previous study by the authors including the time range 2016-2018 (Gunnlaugsson and Jónasson, 2020). According to the findings approximately 13 percent of the respondents reported having been victimized by different types of digital crime in the past three years prior to the survey in 2016. Slander and consumer fraud were the most common types of victimization. Respondents aged 30–44 years old were most likely to have been victimized. In 2018 the number of victims had increased to 19 percent of the respondents with slander and consumer fraud again the most common types of victimization. However, respondents aged 18-29 admittedly had experienced most of the victimizations.

The objective of this study is to provide updated information concerning internet use in Iceland and perceived exposure to digital crime victimization. What is the actual scope and scale of such crimes in Iceland during the entire period 2016-2022? What social groups are most likely to be victimized, and what is the most common type of digital victimization in Iceland? Furthermore, we inquired survey participants about their own illegal and risky behavior online during the last three months prior to the survey. How many admitted to knowingly breaking the law by downloading illegally copyrighted material? How many admitted to visiting pornographic websites online? Does risky behavior of this type have any impact on digital crime victimization? And most importantly, has there been any change in online victimization since the 2016-2018 study mentioned above, measuring these different types of activities?

Previous Research and Theoretical Framework

According to prior research, identity theft, phishing, sexual offences, and fraud are among some of the most common types of digital crime

(e.g. Oksanen & Keipi, 2013; Wolak, Mitchell, & Finkelhor, 2006; Yar, 2013; Ybarra, 2004, and Zandt, 2023). Digital victimization tends to be low among the general population but higher among younger online users when compared to older age groups (e.g. Norton, 2016; Wolak et. al, 2006). It has also been reported that children who use social media to a great extent are more likely to be victimized than children who do not use social media as much (Staksrud, Ólafsson, & Livingstone 2013). Residents living in rural areas have also been shown to be less likely to become victims of digital crime than those living in larger cities (Glaeser & Sacerdote, 1999).

One study showed that more than three million new malicious software such as viruses and Trojans appeared in the first half of 2015 alone (G Data Securitylabs, 2015). Furthermore, data from the US indicate that approximately 10 percent of internet users in 2012 reported being victims of online scams or phishing (Norton, 2012), and in 2014, more than 348 million identities were exposed by hackers (Norton, 2016). Data from a recent National Crime Victimization survey in the United States showed that about 17 million citizens had been victims of identity theft in 2018 (IIE, 2019). In a survey by Näsi et al., (2015) about 6.5 percent of young people aged between 15 and 30 years living in Finland, the USA, Germany and UK, reported having been victims of cybercrime during the past three years. A recent US study (Fried, 2023) showed online hate and harassment increasing with more than half of Americans admitting to such an experience in the last 12 months.

Patchin and Hinduja (2016), leading experts on cyberbullying, have conducted yearly surveys using large samples of high school youth in the USA. Approximately one-third of high school and middle school students surveyed reported having been the target of some form of internet harassment. On average, approximately 25 percent of the students reported that they had been victims of cyberbullying at some point in their lifetime. It was also found that girls are just as likely, if not more likely, than boys to experience cyberbullying as a victim or an offender. Other more recent survey results also seem to support these findings. According to the data compiled by the

National Center for Education Statistics (2019), approximately 20 percent of the total student body reported being bullied during the school year. In the US the figure of bullying among teens had risen even more, to almost half of them admitting being bullied or harassed online (Vogels, 2023).

Previous research has shown that gendered communication patterns may make women more likely to experience sexual harassment online than men because of their gender (Herring, 1999; Taylor, 2003). Gender-based violence online has repeatedly been confirmed in different studies. Image based sexual abuse among youth has been examined in Denmark (Harder, Jørgensen, Gårdshus & Demant, 2020) and social media disclosures of sexual violence in Iceland (Sigurvinsdóttir, Ásgeirsdóttir & Arnalds, 2020). In this respect, women have been shown to be disproportionately more affected by online abuse than men (UN Women Broadband Commission, 2015). The same tendency has also recently been shown in Iceland with more women MP's and journalists admitting to online abuse than male MP's and male journalists (Markúsdóttir, 2022).

In 2017, the Me-too movement began as a global phenomenon sweeping through every aspect of society including Iceland. Women from different walks of life shared their stories of sexual abuse and sexual misconduct they had experienced in their professional life. While sexual abuse is not new, computer technology and social media have become new platforms for this abuse, in addition to providing new media to openly reveal these victimization experiences. Non-consensual exchange of digital sexual images online has, in this respect, repeatedly been a leading topic in the local news in Iceland (Bernharðsdóttir, 2019; Jónsson, 2021 and Helgadóttir, 2024). Politics is no exception to online sexual victimization. More than 40 percent of female MPs in Europe reported, in a recent study conducted by the Parliamentary Assembly (2019), being victims of sexual harassment online during their political tenure in parliament. Of specific interest in the wake of the Me-too confessions in 2017, it was interesting to detect in our earlier survey (Gunnlaugsson and Jónasson, 2020) that these public revelations might have had some relationship with sexual

victimization experiences reported by women in the 2018 survey. In this study we explore whether any signs of the Me-too movement can possibly still be detected in our survey results in 2020 and 2022, or how gender patterned victimization experiences play out in the findings.

The covid-19 pandemic, with its lockdowns and social distancing during 2020 and 2021, undeniably had a profound impact on the lives of those impacted. Schools, like universities, predominantly took place online and on the general labor market as well. Social isolation became the new norm for a couple of years preceding our survey in 2022. Even though it is difficult to show with certainty whether covid restrictions had any impact on victimization experiences online, it is still interesting to examine the 2022 survey results with the covid-19 social distancing measures in mind. Nevertheless, recent research has shown that cybercrime increased after the pandemic (Monteith et. al., 2021; Sorrentino, et. al., 2023).

Research in the field of digital crime often employs the routine activity theory (RAT) introduced by Cohen and Felson in 1979. RAT has been used to analyze various forms of criminal behavior including burglary and violent behavior, but also to shed light on patterns of online victimization (Leukfeldt & Yar, 2016). This theory has been shown to have a relationship with digital victimization and the likelihood of becoming a victim of deviant behavior online (e.g. Näsi et al., 2015; Marcum, Higgins, & Ricketts, 2010; Pratt, Holtfreter, & Reisig, 2010, Cook et. al., 2023). Prior social behavior is believed to influence the likelihood of victimization according to RAT. Those who engage in risky behaviors, are poorly guarded, or are exposed to groups of motivated offenders, are more likely to be victimized than others (Holt and Bossler, 2008).

In this study, one element of RAT will be examined, i.e. prior online social behavior and online victimization. Those who report using the internet frequently, according to the theory, are more likely to become victims of deviant or illegal behavior online than users who use the internet less (e.g. Reyns & Henson, 2015; Näsi et al. 2014; 2015). Moreover, according to RAT, we expect those who use the

internet for risky activity such as using pornographic material or illegally downloading copyrighted material to be more likely to become victims of digital crime (e.g. Buzzell, Foss, & Middleton, 2006). However, not all scholars agree. Yar (2005) has, for example, argued that digital crime is substantively different from traditional victimization in that virtual environments are spatially and temporally disconnected and relatively unstable unlike physical space. In this study, an empirical opportunity will be provided to analyze the extent to which the concepts of an established theory (RAT) can be used to understand the new reality of online victimization in Iceland.

Data and Methods

The data of this study was derived from web-based surveys with participants older than 18 years old from Iceland. The questionnaire was only available in Icelandic thus only Icelandic-speaking participants could take part in the research. Data collection was administrated by the Social Science Research Institute affiliated with the University of Iceland and the data was collected in April and May in 2016, 2018, 2020 and 2022. All participants had agreed to be members of the institutes' panel. We used a stratified sample mirroring for the population in terms of basic socio-demographic variables of age, gender, residence, education level, and income. The sample size was 1800 members of the panel and the response rate was satisfactory or between 40 to 50 percent on all occasions.

First, we examined how many had knowingly broken the Icelandic law by downloading copyrighted material or visited pornographic websites during the last three months prior to the survey. The primary purpose was to distinguish between legal and illegal online activity. According to RAT, we would expect those who engage in risky activities online to be more likely to become victims of cybercrime in general.

The second objective of the study was to examine how many of the respondents had been victims of digital crime. This was measured by asking the respondents the following question: "Have you been the victim of any of the following offences online in the past three years?"

The options given were slander or defamation of character, threat of violence, identity theft, sexual harassment, blackmail, consumer fraud, or photos being shared online without permission. With the last question, we wanted to grasp the extent of sexual harassment in Iceland. As noted above, it was interesting to detect in our earlier survey (Gunnlaugsson and Jónasson, 2020) that these public revelations might have had some relationship with sexual victimization experiences reported by women in the 2018 survey. Therefore, an intriguing question for the two surveys conducted in 2020 and 2022 is whether this relationship still holds or not. Similarly, we explore if any changes in victimization experiences in 2022 from previous measurements might have anything to do with the socially restrictive measures following the covid-19 pandemic.

The period under investigation covers three years prior to the survey in 2018 like the first study in 2016. Therefore, in part, the surveys in 2018, 2020 and 2022 might include victimization experiences occurring during the same time-period as the previous survey. If respondents had been victims of multiple victimization crime experiences, they could mark more than one crime type.

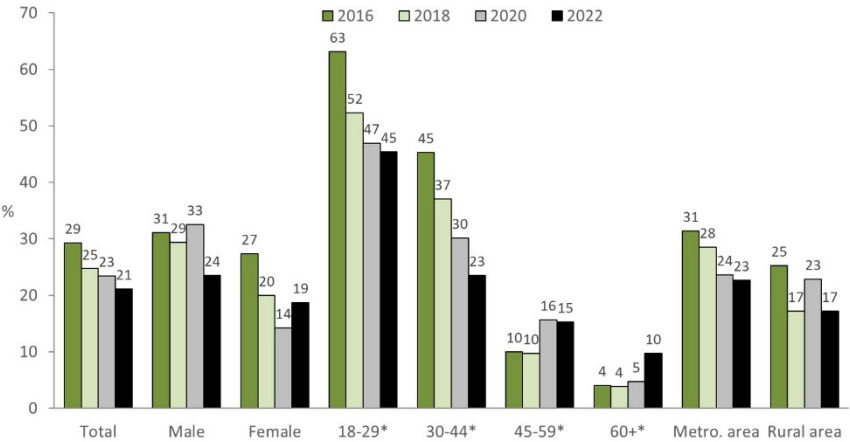
Finally, it was examined how different background variables influenced the likelihood of becoming a victim of online crime. Several different independent variables were included such as gender, age, and residency, i.e., if participants lived in or outside the Reykjavik capital area. Participants were divided into four age groups, 18–29 years old, 30–44 years old, 45–59 years old, and 60 years old and older. Slightly fewer younger members of the panel answered the survey and more participants with university degrees also participated. Therefore, the data had to be weighted for age, gender, education level, and residency to satisfactorily reflect the Icelandic population.

Results

Figure 1 shows that fewer respondents admitted to downloading copyrighted material in 2022 than in previous years. Approximately one-fifth of the participants reported doing so in 2022, compared to around one-third in 2016. Males consistently had a higher likelihood

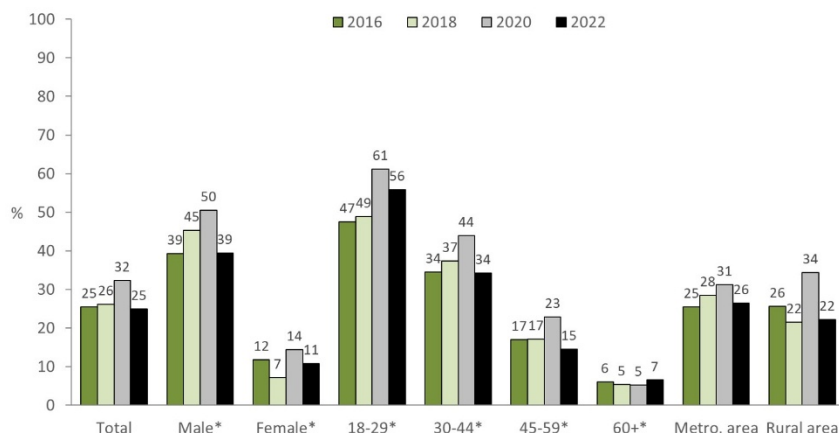
of admitting to downloading copyrighted material than females, although the gender gap has narrowed over time. However, there was no significant difference between the two genders in the 2022 survey. Younger respondents are much more likely to admit to downloading copyrighted material than older respondents, but even in the youngest age group (18-29), the percentage has decreased over time. In 2022, there was a significant difference between the age groups, with around 45% of the youngest group admitting to downloading copyrighted material, compared to only about 23% of participants aged 30 to 44 years old. Interestingly, about 10% of the oldest group admitted to downloading copyrighted material in 2022, compared to only 5% in 2020. Respondents from rural areas consistently have a lower likelihood of admitting to downloading copyrighted material than those from metropolitan areas. However, the gap between the two groups has narrowed during the time-period in question 2016-2022.

Figure 1. *Percentage of participants who reported having downloaded copyrighted material in the past three months based on gender, age, and residency in 2016, 2018, 2020 and 2022.*



* marks significant difference between groups (p < 0,05)

Figure 2 This figure shows the percentage of participants who have deliberately visited adult websites in the past three months in 2016, 2018, 2020 and 2022.



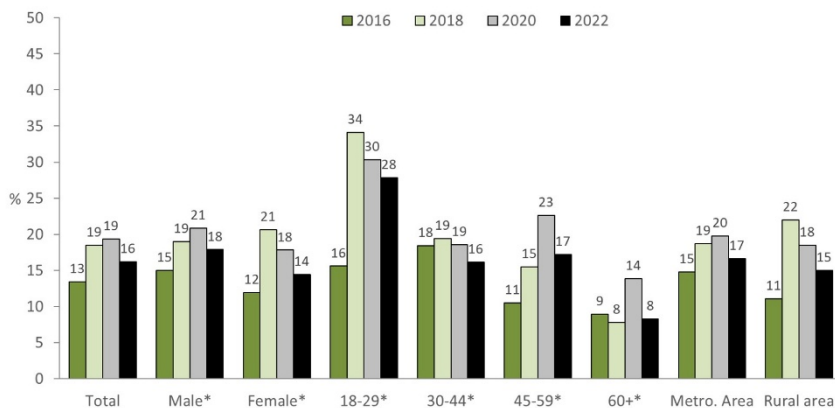
* marks significant difference between groups ($p < 0,05$)

As shown in Figure 2, the percentage of all respondents who admitted to having visited websites containing adult material has remained relatively stable over the years. About one in four admitting to doing so in the past three months, except in 2020, when one-third of the participants admitted to visiting adult websites. Males are consistently more likely to admit to having visited websites containing adult material than females, and the difference is statistically significant. However, the gap between the two genders has fluctuated somewhat. With the men's percentages decreasing after 2020 after a steep increase while women's percentages have remained more or less stable the whole time. Yet, noteworthy to see the decrease among women in 2018 compared to 2016. In 2022, around 39 percent of men admittedly visited adult websites compared to 11 percent of women. Younger respondents were significantly more likely to admit to having visited websites containing adult material than older respondents. However, even among the youngest age group (18-29), the percentage of respondents admitting to this behavior has decreased slightly over

time. In 2022, around 56 percent of the youngest respondents admittedly had visited these websites compared to 34 percent of respondents aged 30 to 44. The difference between urban and rural areas in Iceland was not significant and has been similar for all the years.

As shown in Figure 3, cybercrime victimization rates were lowest in our first survey in 2016 with 13 percent admitting victimization. Since then, the rate increased and has remained relatively stable in 2018, 2020 and 2022. In 2022, 16% of respondents reported being victims of cybercrime within the previous three years. This represented a slight decrease from 19% in 2018 and 2020. Males are more likely than females to report being victims of cybercrime, with a statistically significant difference in 2022. Around 18% of men reported being victims of cybercrime in the past three years prior to the study, compared to around 14% of women. Younger respondents are also more likely to report victimization than older respondents, with the highest percentage among the 18-29 age group on all occasions except for the first survey in 2016. The difference has always been statistically significant. Respondents aged 60 and older were the least likely to have been victimized in 2022 as on previous occasions. In most years, respondents living in the Reykjavik Metropolitan area have been more likely to have been victimized by cybercrime than those living outside the metropolitan area, except for 2018, when more respondents living outside the metropolitan area reported being victims. However, the difference in 2022 was not statistically significant.

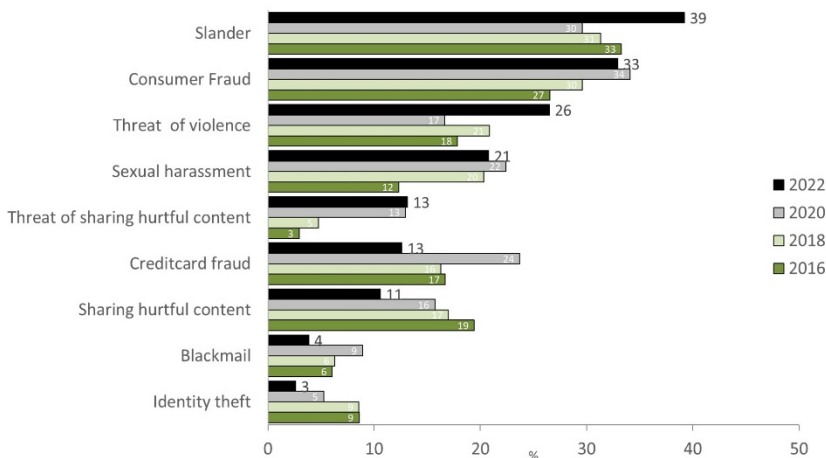
Figure 3. *Percentage of participants who reported having been victimized by digital crime in the past three years, based on gender, age and residency in 2016, 2018, 2020 and 2022.*



* marks significant difference between groups ($p < 0,05$)

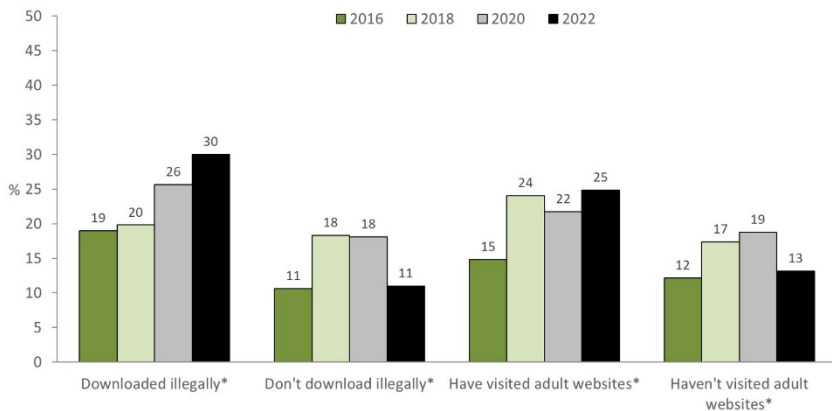
According to the results shown in Figure 4, the most common type of cybercrime reported by victims was slander or defamation, in total 39% of all of the victim reports in 2022, which represents a steep increase from previous years. Consumer fraud, such as receiving the wrong product or unauthorized credit card charges, was the second most frequently reported type of victimization, with one-third of the offenses reported falling into this category. Sexual harassment was reported by approximately one in five of victim respondents in 2022, with an increase from 12% in 2016. About 13% of respondents reported being threatened with the sharing of hurtful content about them, while 11% had actually experienced hurtful content being shared. Although the numbers rose between 2018 and 2020, there was a decrease in the sharing of hurtful content in 2022. Furthermore, fewer respondents reported being victims of credit card fraud in 2022 than in 2020. Only 13% reported being victims of credit card fraud in 2022 compared to 24% in 2020. Similarly, reports of blackmail and identity theft have decreased from previous years.

Figure 4. *The percentage of digital crime types reported by victims for a period of three years prior to the surveys in 2016, 2018*, 2020 and 2022.*



*it was possible to mark more than one crime
** marks significant difference between groups ($p < 0,05$)

Figure 5. *The percentage of participants who reported having been victimized by digital crime in the past three years based on illegal and risky behavior activities online in 2016, 2018, 2020 and 2022.*



* marks significant difference between groups ($p < 0,05$)

Figure 5 shows that participants who illegally downloaded copyrighted material in the past three months were more likely to have been victims of cybercrime. The difference between those who downloaded illegally and those who did not was statistically significant. Around one in three participants who downloaded copyrighted material had been victimized, compared to about one in ten who had not. Cybercrime victimization among those who downloaded copyrighted material increased from around 19% in 2016 to 30% in 2022. In Figure 5, we can also observe a significant difference between those who visited adult websites and those who did not. In 2022, around 25 percent of those who visited adult websites had been victimized, compared to around 13% of those who did not.

Summary and concluding remarks

The number of households with internet access has increased drastically in the past few years. Currently, almost every Icelandic household is connected to the internet (Eurostat, 2023). With increased internet use, online victimization, apparently, has also increased from the first survey in 2016. Previous research had shown that roughly 10 percent of internet users in the US have reported to have been victims of online scams or phishing (Norton, 2012). Our data showed that approximately 16-19 percent of Icelandic internet users had been victimized by digital crime of some sort during the last three years before the three surveys conducted in 2018, 2020 and 2022. However, these figures cannot be fully compared because our survey inquired about a wider range of victimization experiences than the US survey.

The figures for the Icelandic surveys conducted a total of four times during 2016-2022 are all comparable. Here, we see an increase in online victimization between 2016 and 2018, but the rates have apparently levelled off since then. Only about 13 percent of respondents admit to digital victimization in 2016, increasing significantly to 19 percent in 2018, and has remained close to that figure since. The relative share of each victimization type remained

similar on all occasions, with slander and consumer fraud being the most frequent victimization types. However, notable differences can be detected. Fewer respondents admit being a victim of credit card fraud in 2022 compared to previous years, possibly due to more cautious use of credit cards and to actions taken by banks to prevent fraud. Similarly, fewer admit being victim of blackmail, hurtful content being shared and identity theft in 2022 than in previous years. However, more respondents admit to being threatened with violence and hurtful content being shared in 2022 than before.

The percentage of sexual harassment victimization experiences has apparently increased substantially after 2016. Up to a total of 20 percent of such victimization reports surfaced in 2018, 2020 and 2022 compared to only 12 percent in 2016. This statistically significant increase of sexual harassment reporting comes mostly from women. In 2016, fewer women admitted to digital victimization than men. In 2018, more women, or 21 percent, admitted to victimization with 19 percent men. Gender difference is however not statistically significant. On the other hand, it is noteworthy that the percentage of women reporting victimization increased from 12 percent in 2016 to 21 percent in 2018, while the increase for males was somewhat less, or from 15 percent to 19 percent.

How can this almost twofold increase in women reporting online victimization and the increase of those reporting sexual harassment be explained? A plausible explanation, as was discussed in our earlier research (Gunnlaugsson and Jónasson, 2020), might have to do with different social circumstances in 2018 compared to 2016. New social movements appeared after 2016 in which experiences of women played a central role. More specifically, a movement linked to Me-too emerged in Iceland in 2017. Women in different professional groups stepped forward in Iceland with stories of sexual harassment they had experienced in their professional life. These women came from different walks of life such as arts, academia, sports, banks, restaurants, immigrants, etc. Thousands of anonymous stories were accumulated and published online (Beck, 2017). Understandably, these confessions created an uproar in the public discourse and the

sheer volume came as a surprise to many. A social revolt against sexual discrimination became prominent in Icelandic public life and social awareness of this behavior both increased and deepened. Possibly, this movement has something to do with how more women came forward in our study in 2018 and again in 2020 and 2022, admitting to digital victimization, especially sexual harassment. Not necessarily reflecting an actual increase for this type of victimization but perhaps suggesting more social awareness among women with respect to recognizing certain unwanted behavior as sexual harassment than before. Harassing communications previously perceived as nothing more than a nuisance, increasingly being interpreted more as sexual harassment in the aftermath of Me-too, and its impact apparently has continued in the years following (see also Fontaine, 2021). However, this aspect needs to be explored further in new studies. Similar studies in the US have in this respect shown that hate and sexual harassment toward women in particular has increased as well (Friar, 2023) as was pointed out in the literature review here above.

The Me-too confessions might also be linked to why fewer women admitted to visiting pornographic websites in 2018 compared to 2016. In 2016, a total of 12 percent of the women admitted to this use during the last three months before the survey was conducted; dropping to seven percent in 2018. Thus, this behavior was probably not as accepted anymore among women immediately after the Me-too movement confessions, pornography being considered more as a sexist expression of male dominance and sexual objectification of women. In 2020 and 2022 however, the use of porn online by women apparently had returned to similar levels as in 2016. Interestingly, this shift in behavior toward pornographic material did not appear to have the same impact on males and their use of porn online in 2018. Their use of porn online moved to a different direction, increasing markedly from 39 percent admitting to visiting pornographic websites in 2016, to 45 percent in 2018. Since 2018 however use of porn online has apparently levelled off among men.

Another notable change in 2022 compared to previous surveys can also be observed regarding slander. Even though total

victimization rates have remained relatively stable during the time-period in question, slander victimization experiences in 2022 are an exception. More respondents admitted slander victimization online in 2022 than ever before. A total of 39 percent of the victimizations included slander in 2022 compared to earlier surveys around 30 percent. A possible explanation might perhaps have something to do with the covid-19 pandemic restrictions between our two surveys in 2020 and 2022. Various preventive measures were put in place in both 2020 and 2021, mass public gatherings for example were forbidden (Reuters, 2020). Many social activities on the labor market including schools were transferred to the internet and face to face interactions only allowed with your close ones. Being isolated for a long period of time with only online communication with others possible, might have triggered some frustration, resulting in more aggressivity online, for instance in slander toward others. Increased polarization has in this respect been detected in recent years in Iceland (Egilsson, 2023), with less tolerance felt toward minorities (Hjaltadóttir, 2023). Thus, maybe not surprising to see more slander victimization experiences in our 2022 survey, compared to previous years. However, this impact is suggestive at best and more studies need to be conducted to back up this observation.

The finding that one in three respondents who downloaded copyrighted material had been victimized in 2022 appears to support the Routine Activity Theory's (RAT). The proposition that illegal downloading makes individuals more vulnerable to cybercrime can accordingly be shown in the results. The same is true for individuals who visit adult websites. The possible explanations for this vulnerability include a higher likelihood of malware being present on such websites, less cautious online security practices among those engaging in this type of behavior, and targeting by cybercriminals, due to the perceived stigma associated with adult content. Therefore, as Holt and Bossler (2008) have previously shown, we found support for the RAT proposition. Risky behavior online seems to be correlated with digital crime victimization. Engaging in deviant lifestyles online may expose individuals to motivated offenders, thereby increasing the

risk of victimization. More online activity, especially online visits of pornographic sites, tends to increase online victimization according to this study.

The number of respondents admitting illegally downloading copyrighted material decreased in 2022 compared to previous years. In 2016, one-third admitted illegal downloading but in 2022 the rate was only about one-fifth. The downward trend may be attributed to the increased enforcement of copyright laws, including the shutdown of illegal sites, as well as the availability of legal streaming options such as Netflix and Spotify. More males admitted illegal downloading in 2016-2022, yet the data does not show a significant gender difference, unlike the 2016 findings, when the gender difference was statistically significant.

The findings in this study clearly demonstrate the need for including both age and gender in the analysis of cybercrime victimization. Young people appear to be most vulnerable to cybercrime victimization and women more so than men. Previous research has shown women to experience more sexual harassment than men as revealed in this study. In countering cybercrime preventive measures therefore need to especially target younger age groups and including women's vulnerability to harassment. Still cybercrime concerns all age groups and different genders and needs to be tackled on a broad societal level. For this task, the research community must regularly update the nature and volume of online crime and victimization experiences in general. Equally important is tracking down online perpetrators and curbing this harmful behavior resulting in cybercrime victimization.

References

Beck, B.H. (2017). *Tími þagnarinnar liðinn – sögurnar allar (Time of silence has passed – all the stories included here)*. Kjarninn. Retrieved from <https://kjarninn.is/skyring/2017-12-11-konur-islandi-segja-fra-kynferdisofbeldi-areitni-og-kynbundinni-mismunun-sogurnar-allar/>

Bernharðsdóttir, B. (2019). *Viða vandi vegna stafræns ofbeldis og nektamynda* (Widespread concern about digital violence and nude photos). Visir.is. Retrieved from

<https://www.visir.is/g/2019191028818/vida-vandi-vegna-stafræns-ofbeldis-og-nektamynda>

Buzzell, T., Foss, D., & Middleton, Z. (2006). Explaining use of online pornography: A test of self-control theory and opportunities for deviance. *Journal of Criminal Justice and Popular Culture*, 13(2), 96–116.

Cook, S., Giommoni, L., Trajtenberg Pareja, N., Levi, M., Williams, M.L., (2023). Fear of Economic Cybercrime Across Europe: A Multilevel Application of Routine Activity Theory, *The British Journal of Criminology*, Volume 63, Issue 2, March, Pages 384–406.

Egilsson, E.P. (2023). Skautun í íslensku samfélagi (Polarization in Iceland). *Víkublaðið*, March 14, 2023. Retrieved February 26, 2024: <https://www.vikubladid.is/is/frettir/skautun-i-islensku-samfelagi-1>

Eurostat (2023). *Digital economy and society statistics – households and individuals*. Luxembourg: Publications Office of the European Union. Retrieved November 9, 2023 from: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital-economy_and_society_statistics_-_households_and_individuals

Fontaine, A.S. (2021). Iceland's MeToo movement: Breaking the cycle. *Grapevine*. Retrieved February 26, 2024: <https://grapevine.is/mag/feature/2021/06/04/icelands-metoo-movement-breaking-the-cycle/>

Fried, I. (2023). Online and harassment continue to rise. *Technology*, June 28, 2023. Retrieved February 26, 2024: <https://www.axios.com/2023/06/28/online-hate-harassment-rise-adl>

G Data Securitylabs. (2015). *G Data Securitylabs Malware Report: Half-year report January-June 2015*. Bochum: G Data Software Inc.

Glaeser, E.L., & Sacerdote, B. (1999). Why is there more crime in cities? *Journal of Political Economy*, 107, S225–S258.

Harder, S.K., Jørgensen, K.E., Gårdshus, J.P. & Demant, J. (2020). In Heinskou, M.B., Skilbrei, M.L., & Stefansen, K. (eds.) (2020). *Rape in the Nordic countries: Continuity and change* (pp. 205-223). Routledge Research in Gender and Society.

Harrell. (2015). *Victims of identity theft, 2014*. Washington: Bureau of Justice Statistics.

Herring, S.C. (1999). The rhetorical dynamics of gender harassment online. *The Information Society*. 15(3), 151-167.

Holt, T.J. and Bossler, A.M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior*, 30(1), 1-25. Accessed December 12, 2019: <https://www.tandfonline.com/doi/full/10.1080/01639620701876577>

IIE (2019). Retrieved from <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime>.

Landsbankinn Homepage. (2023). Svikaskilaboð send í nafni Landsbankans (Fraud message in the name of Landsbankinn) Retrieved November 9, 2023 from <https://www.landsbankinn.is/frettir/2023/07/07/svikaskilabod-send-i-nafni-landsbankans>

Helgadóttir, R. (2024). Tengslin hafa áhrif á tegundir stafræns ofbeldis (Digital violence impacted by social relations). *Heimildin*, p. 26. Retrieved February 23, 2024: <https://heimildin.is/blod/heimildin/43/lesa/#page=26>

Hjaltadóttir, J.V. (2023). Finnur fyrir auknum stuðningi þrátt fyrir bakslag (More support despite a backlash). *RÚV*, August 14, 2023. Retrieved February 27, 2024: <https://nyr.ruv.is/frettir/innlent/2023-08-14-finnur-fyrir-auknum-studningi-thratt-fyrir-bakslag-389774>

Holt, T.J., Leukfeldt, R., & van de Weijer, S. (2020). An Examination of Motivation and Routine Activity Theory to Account for Cyberattacks Against Dutch Web Sites. *Criminal Justice and Behavior*, 47(4), 487-505. <https://doi.org/10.1177/0093854819900322>

Jónsson, S.G. (2021). Hrelli- og barnaklámi dreift á síðu sem lögreglan nær ekki til (Revenge and child porno shared on a page police cannot track). *Heimildin*, May 21, 2021. Retrieved February 27, 2024: <https://heimildin.is/grein/13332/hrelli-og-barnaklami-dreift-sidu-sem-logreglan-naer-ekki-til/>

Marcum, C.D., Higgins, G.E., & Ricketts, M. L. (2010). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, 31, 381–410.

Markúsdóttir, E.M. (2022). Stjórnmalafólk og fjölmiðlafólk reynir að draga úr áhrifum áreitni á netinu (Politicians and mass media personnel downplay impact of digital harassment). *Heimildin*. December 21, 2022. Retrieved February 27, 2024: <https://kjarninn.is/skyring/stjornmala-og-fjolmidlafolk-reynir-ad-draga-ur-ahrifum-areitni-a-netinu/>

Metropolitan Police, (2025). Home page on Facebook accessed March 19, 2025: https://www.facebook.com/logreglan?locale=is_IS

Monteith, S., Bauer, M., Alda, M. *et al.* (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Curr Psychiatry Rep* 23, 18.

National Center for Education Statistics (2019). Indicators of school crime and safety: 2018 APRIL 2019. Retrieved from <https://nces.ed.gov/pubs2019/2019047.pdf>.

Näsi, M., Oksanen, A., Keipi, T., & Räsänen, P. (2015). Cybercrime victimization among young people: A multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 16(2), 203–210.

Näsi, M., Räsänen, P., Oksanen, A., Hawdon, J., Keipi, T., & Holkeri, E. (2014). Association between online harassment and exposure to harmful online content: A cross-national comparison between the United States and Finland. *Computers in Human Behavior*, 41, 137–145.

Norton. (2012). Norton cybercrime report 2012. Retrieved from: <http://now-static.norton.com/now/en/pu/images/>

Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf.

Norton. (2016). Norton cybersecurity insights report. Retrieved from <https://us.norton.com/norton-cybersecurity-insights-report-global>.

Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. *Vulnerable Children and Youth Studies*, 8(4), 298–309.

Parliamentary Assembly. (2019). *Promoting parliaments free of sexism and sexual harassment. Report*. Council of Europe. Retrieved from <http://assembly.coe.int/nw/xml/XRef/Xref-DocDetails-en.asp?FileID=27477&lang=en>

Patchin, J.W. & Hinduja, S. (2016). *Bullying today: Bullet points and best practices*. Thousand Oaks, CA: Sage Publications.

Pratt, T.C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, 47, 267–296.

Reuters, (2020). Iceland further tightens measures to curb covid-19. Retrieved February 26, 2024: <https://www.reuters.com/article/us-health-coronavirus-iceland/iceland-further-tightens-measures-to-curb-covid-19-idUSKBN27F29J/>

Reyns, B.W., & Henson, B. (2015). The thief with a thousand faces and the victim with none: Identifying determinants for online identity theft victimization with routine activity theory. *International Journal of Offender Therapy and Comparative Criminology*. Retrieved from <http://ijo.sagepub.com/content/early/-2015/02/26/0306624X15572861-.refs#cite-by>.

Sarre, R., Yiu-Chung, L. & Chang, L.Y.C., (2018). Responding to cybercrime: current trends, *Police Practice and Research*, 19:6, 515-518, DOI: 10.1080/15614263.2018.1507888

Siegel, L. J. (2023). *Criminology*, Eighth Edition. Boston: Cengage Learning.

Sigurvinsdóttir, R., Ásgeirsdóttir, B.B. & Arnalds, S. (2020). Breaking the silence: Social media disclosures of sexual violence in Iceland. In Heinskou, M. B., Skilbrei, M.L., & Stefansen, K. (eds.) (2020). *Rape in the Nordic countries: Continuity and change* (pp. 224-240). Routledge Research in Gender and Society.

Sigurðsson, Á.F. (2015). Computer and Internet usage in Iceland and other European countries 2014. *Statistical Series – Tourism, transport and IT*, 100(1), 1–20.

Sorrentino, A., Sulla, F., Santamato, M., di Furia, M., Toto, G.A., & Monacis, L. (2023). Has the COVID-19 pandemic affected cyberbullying and cybervictimization prevalence among children and adolescents? A systematic review. *International Journal of Environmental Research and Public Health*, 20, 5825. Retrieved from: <https://pmc.ncbi.nlm.nih.gov/articles/PMC10218135/>

Staksrud, E., Ólafsson, K., & Livingstone, S. (2013). Does the use of social networking sites increase children's risk of harm? *Computers in Human Behavior*, 29, 40–50.

Taylor, P.A. (2003). Maestros or misogynists? Gender and the social construction of hacking. In Dot.cons: *Crime, Deviance and the Identity on the Internet* (Jewkes, Y. ed.). Portland, OR: Willan Publishing.

UN Women Broadband Commission (2015). *Executive Summary: Cyber Violence Against Women and Girls. A Worldwide Wake-Up Call*. A Discussion Paper From the UN Broadband Commission For Digital Development Working Group on Broadband and Gender. Accessed January 16, 2020:

<https://www.broadbandcommission.org/Documents/reports/bb-wg-gender-discussionpaper2015-executive-summary.pdf>

Vogels, E.A., (2023). Teens and Cyberbullying 2022. Pew Research Center. Accessed November 10, 2023: <https://www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/#fn-28924-1>

Wolak, J., Mitchell, K. J., & Finkelhor, D. (2006). *Online victimization of youth: Five years later*. Alexandria: National Center for Missing & Exploited Children.

Yar, M. and Steinmetz, K.F., (2019). *Cybercrime and society* (3rd edn.). London: Sage.

Ybarra, M. L. (2004). Linkages between depressive symptomatology and Internet harassment among young regular Internet users. *Cyberpsychology & Behavior*, 7(2), 247–257.

Received: August 11, 2024

Accepted: September 8, 2024