Chapter 4
Scanning for Scams: Local, Supra-national, and Global Events as Salient Contexts for Online Fraud

Kristjan Kikerpill

Introduction

Regardless of the verbs we use when describing our online presence, e.g., online banking, dating, gaming, or shopping, these phenomena boil down to a series of requests and responses exchanged between connected devices and servers across the globe (Kikerpill 2021a). Digital spaces and places so-called are but informational nodes signalling an active human presence and waiting to be acted upon (Maggi 2014). Communication in such environments (see Snowdon et al. 2001) connects us to other people, and the digital traces of their activities, through texts and graphical interfaces. All of our actions and interactions in mediated environments are, in fact, communicative acts and accompanying interpretations carried out via open channels and with the help of various media. In other words, people's mediated presence always constitutes action-as-communication (Kikerpill 2021a).

Since crime is a socially constructed phenomenon (Posick 2018), it goes wherever people go. Thus, the opportunities and (near-)immediate access provided by modern information and communications technologies are not always used towards positive or legal ends, but are employed instead to perpetrate cybercrimes. Put differently, some action-as-communication in mediated environments constitutes crime-as-communication (Kikerpill 2021a). In recent years, both the financial and psychological harms caused by cybercrime victimisation are on the rise (PurpleSec 2021), and especially from online scams and frauds (Button and Cross 2017). The fact that approximately 99% of cybercrime threats require human interaction, e.g., opening attachments in emails or following links (Proofpoint 2019), to be

K. Kikerpill (✉)
Institute of Social Studies, University of Tartu, Tartu, Estonia
e-mail: kristjan.kikerpill@ut.ee

D. Radovanović (ed.), *Digital Literacy and Inclusion*,
https://doi.org/10.1007/978-3-031-30808-6_4

successful makes the recipient of a mediated crime attempt the person best positioned to mitigate relevant risks and ensure their own safety from victimisation (Kikerpill 2021b).

Hence, the first step towards preventing harm from the modern social menace of cybercrime relies on a simple, but important understanding: in mediated environments, there is plenty of communication without crime, but no crime without communication. As perpetrators often manipulate the communication underlying their cybercriminal activities, i.e., socially engineer the messages in their online attacks (Hadnagy 2018; Hatfield 2018), learning to distinguish between criminal and noncriminal communication is essential. The most common general form of social engineering attacks in mediated environments is broadly referred to as "phishing" (Khonji et al. 2013), although numerous variations of phishing exist, e.g., vishing (voice phishing) and smishing (text message phishing) (Hong 2012). An important part of the larger effort of countering cybercrime comes from understanding how criminal actors exploit salient social contexts within the content of the scams and frauds they disseminate. Given that contexts have both an interpretive and a constitutive dimension (Rigotti and Rocci 2006), they help people interpret incoming messages, but can also be used to create messages that fit specific social expectations (Carter 2015). In cybercriminal endeavours, this means exploiting salient social circumstances to craft crime messages, which are more meaningful for the recipient due to a shared "lived experience" (Kikerpill 2021a).

To explore and illuminate how salient social contexts can spur online scams, and how awareness about these connections can contribute to preventing victimisation from fraud, we apply the *mazephishing* framework (Kikerpill and Siibak 2021a) to study specific events on the local, supra-national and global level. The *mazephishing* framework comprises three primary components: the social context from which specific scam messages obtain their salience, e.g., the COVID-19 pandemic (Kikerpill and Siibak 2021b) or natural disasters such as forest fires (Taodang and Gundur 2022), the media or channels used to circulate the scam messages (see above: Hong 2012), and the influencing techniques employed in the actual scam messages (Lawson et al. 2020; Kikerpill 2021a; Steinmetz et al. 2021). In this chapter, the focus will primarily be on the social context element, because we are only now beginning to learn about the true importance of social context in cybercrimes that require human interaction (Verma et al. 2018; Norris et al. 2019; Montañez et al. 2020; Kikerpill and Siibak 2021a; Steinmetz et al. 2021; Taodang and Gundur 2022), and how this emerging knowledge can be used in digital literacy education for the purposes of fraud avoidance. Scholarship and education in this area is paramount if we want to move towards dismissing the entrenched discourse of the "deficient user" that currently dominates cybersecurity discussions (Klimburg-Witjes and Wentland 2021).

Background and Approach

Since fraud is a crime of interaction (Harrington 2012: 396), both its offline and online manifestations are always rooted in and dependent upon communication (Kikerpill 2021a). While all cybercrime depends on communications technology, the concurrent communicative aspects of the same crimes are often overlooked if not diminished in lieu of more technical discussions (Kikerpill 2021a), e.g., "to a computer scientist, the solution to a bug is often just more computer science" (Borel 2018). Taking this into account, the chapter decidedly focusses on the equally important communicative and interpretive underpinnings of cybercrime by presenting a series of examples (Simons 2014) of specific salient events or circumstances that have enabled criminals to use the entailing social context as input for their socially engineered fraud messaging. Where contexts are not primarily created within a fraudulent interaction, e.g., in longer running online dating and romance scams (Carter 2021) or cold-call type "one-off" fraud attempts such as phishing attacks (Khonji et al. 2013; Atkins and Huang 2013; Kikerpill and Siibak 2019), criminals can decrease their deviant workload and increase the credibility of the crime messages, by relying on events or circumstances that are important in a geographically, culturally or temporally restricted, semi-open or open manner.

Acknowledging that not all events are of equal importance for different communities in various parts of the world at any given moment, we use cases with local (geographically and temporally restricted), supra-national (geographically and culturally semi-open, temporally restricted) and global (culturally and geographically open, temporally semi-open) significance. The categories of geographical, cultural and temporal openness and/or restrictions are used as guidelines for better understanding the connection between social occurrences and fraud proliferation, including why some types of scam content may be relevant for some and not others. The reasoning is that interpretations of scam believability can depend on where we live, which cultural practices we observe and what we consider as desirable or necessary at any given moment (Kikerpill 2021a). The *mazephishing* framework was chosen as a lens for exploring the aforementioned categories because it provides a structured backdrop with respect to what people should look for in scams in general, i.e., the (social) timing of particular scams, the relevance and comprehensibility of scam messages depending on the current "lived experience" of a person as well as how we engage with modern mediated environments in general.

While the chapter does not directly include temporally unrestricted cases, these would mainly involve malicious exploitations of the human experience and people's vulnerabilities rather than the amplification provided by any single event or specific circumstances (Kikerpill 2021a), e.g., as it often occurs in scams perpetrated in the context of intimate relationships and romance (Carter 2021). Yet, it must be noted that while these opportunities are available to scammers without particular temporal restrictions, the prevalence of romance scams is also known to increase during Valentine's Day (Fowler 2022). Even so, the examples in this chapter focus on events or circumstances with an element of temporal restriction to also explore the idea of "criminal event calendars", i.e., how (cyber)criminals may be perceiving, or telling, time in accordance with specific opportunities for criminal exploitation based on salient social contexts.

On the local level, we present a case study of scams circulated during the respective tax seasons in Estonia and the United States. For the supra-national level, we provide examples from widely recognised commercial sales events, i.e., Amazon Prime Day and Black Friday. For the global level, we chose the current phenomenon of gaming console unavailability and restocking issues that have been caused by a shortage in microchips required for the production of said consoles. These examples represent (1) instances where an obligation necessitates certain practices, and the context of this obligation creates opportunities for scammers; (2) instances where cultural and commercial developments have created certain opportunities for scammers, and (3) instances where a combination of unexpected circumstances create opportunities for scammers.

It is important to note that the examples presented in the chapter are not geared towards bringing about or recommending substantive changes in the events or circumstances as such – which, as will become clear, would be very difficult if not entirely impossible – but are meant as illustrative examples on how the realities of the social world become reflected in mediated crimes, and how being aware of these connections can aid in avoiding becoming a victim of fraud.

Online Scam Ecosystem During Tax Season in Estonia and the United States

In this chapter, the previously mentioned categories of geographically and temporally restricted contexts mean that a similar or identical event occurs on different set dates or date ranges in different countries, which makes it possible to explore how the event or circumstances impact the dissemination of contextually fitting scams. For instance, the so-called tax season begins in January in the United States, but in mid-February in Estonia, with respect to private individuals' tax declarations. Given the vast differences in tax filing complexity between the two countries (e-Estonia 2021), the following exemplifies how opportunities for fraudulent offers made by scammers may differ in scope and intensity.

The starting point for tax-related frauds comes from the importance of the institution as such and people's willingness to pay their taxes. Attitudes towards paying taxes vary significantly across different countries, where tax morale is influenced by numerous factors such as cultural differences and trust in one's government (Torgler and Schneider 2007). In Estonia, 91% of people consider paying taxes their essential obligation (ETCB 2021), 98% of personal income declarations are made electronically (e-Estonia 2022) and the Estonian Tax and Customs Board's e-tax system is viewed as the most convenient public service being offered (Kantar Emor 2020). Furthermore, the average personal income tax declaration takes approximately three to five minutes to file (Work in Estonia 2022), which makes tax compliance easy. In contrast, the tax preparation and filing process in the United States can take approximately 13 hours for an individual (Kessler 2013), and about 44% of Americans are bothered "a lot" by the complexity of the tax system (Pew Research 2015). From the perspective of scammers, who are known to be opportunistic in their exploitation of people's vulnerabilities (Kikerpill and Siibak 2021b), the more complexity a particular system presents, the more opportunities there are for interjecting bogus offers for seemingly relevant services, including for the speeding up or simplification of the process.

Following from the above, there were only a very limited number of tax season scams available for further analysis with respect to Estonia. With the exception of 2018, there was at least one reported tax scam from 2014 to 2020 and the time of reporting ranged from late January to mid-March. The outlier was a tax refund scam reported at the end of December (Sobak 2014), which requested people to submit their credit card information for an expedited tax return. As also noted in the relevant scam report (Sobak 2014), the circulated fraud message was mistimed by the criminals, because personal income tax declarations are filed starting from February 15. Hence, examples from other years appear on and around February 15 and in March. There were two main types of scams disseminated: phishing emails that request the recipient to provide additional information to receive their tax refund quicker (Pihlak 2017) or which provide a link that leads the recipient to a faked website of the local tax authority for the purposes of entering one's credit card number and the relevant security code (Raamatupidaja 2016). Interestingly, a scam circulated in 2016 (Rapp 2016), which used bad Estonian and notified recipients that the tax authority was unable to process their respective tax refund and, thus, requires additional information, also promised the return to be made in Estonian kroons, i.e., the currency used in Estonia prior to 2011 and the Euro. Hence, not only can temporally restricted scams be noticed and reported due to mistimed dissemination and poor use of local language, but also when the scams fail to take into account local changes and social context. From a technical perspective, since credit card numbers and security codes are only used to initiate payments (Walter 2019), and not to receive them, providing the tax authority with one's relevant respective information lacks purpose entirely.

In comparison with the Estonian examples, the scam ecosystem of the US tax season is a completely different phenomenon. Firstly, tax season scams are so widespread in the United States each year that it has become commonplace to release general warnings beforehand (Rafter 2022). In contrast, the scam reports were few in Estonia and reported only after the scams actually occurred. Furthermore, the complexity of the tax filing process (e-Estonia 2021) reveals that tax preparation services are common in the United States, but virtually unheard of for private individuals in Estonia. As mentioned previously, the complexity of a process, i.e., the number of steps a person has to take in order to complete the process, presents opportunities for scammers to interject bogus offers or threats. Thus, it is not surprising that one of the more common types of tax season scams in the United States relates to fraudulent tax preparation services (Rafter 2022). A related issue concerns taxpayer advocate scams in which recipients receive a call and are asked for personal information that would allow the perpetrators to successfully commit identity theft (Rafter 2022). Provided that tax advocates aid taxpayers with the more difficult tax issues, this further shows how the complexity of a process can increase the variety of scams it potentially enables. In comparison, since the majority of Estonian personal income declarations are pre-filled and the process takes only some minutes in the official online environment of the local tax authority (see e-Estonia 2021), a significant number of scam opportunities are avoided through this solution.

Digital Hallmark Holidays Mark a Rise in Scams: Amazon Prime Day and Black Friday

Originating from the United States, the term "hallmark holidays" broadly refers to the celebration or observance of dates primarily for commercial purposes. In the digital sphere, this has come to include "commercial holidays" such as Amazon Prime Day, which has been in effect since 2015 to celebrate the 20th anniversary of the company Amazon (Johnston 2022), as well as Black Friday that arrives yearly at the end of November. Commercial events like Amazon Prime Day and Black Friday are geographically and culturally semi-open due to the increasing reach of Amazon's activity, and the adoption of Black Friday sales events in countries other than the United States Since crime, including scams, goes where people go (Posick 2018; Kikerpill 2021a), geographically and culturally semi-open contexts for scams can expand over time insofar as new communities take up the practice of "following" certain dates or events.

For instance, Black Friday was historically restricted primarily to the United States (Marcos 2021), but the opportunity for financial gain from set-date steep sales has made the observance of this commercial event spread to other countries via globalisation (Dumoulin 2019). Although the aforementioned Black Friday sales events take place in different countries, each location still observes the original date for the event, i.e., late November, which makes it temporally restricted. Similar to Black Friday, the initial reach of Amazon Prime Day has also expanded in unison with the company's increasing sphere of activities – while Prime Day began as a 24-h sales event that included 9 countries, it has since grown into a 48-h event spanning 20 countries (Johnston 2022). The dates of such temporally restricted but culturally and geographically semi-open sales events are, therefore, prime targets for scammers to present their fraudulent offers alongside legitimate offers from stores and online merchants. It is important to note here that Amazon Prime Day has usually occurred in the month of June or July, but took place in October in 2020 due to the COVID-19 pandemic (Johnston 2022). The importance of such a shift is revealed in the corresponding warnings circulated in the media concerning "Amazon Prime scams" (Tompor 2021; Whitney 2021), i.e., the scams follow the dates of an event even if the date is changed due to exceptional circumstances, which also provides some support for the notion of so-called criminal calendars.

Furthermore, although Amazon Prime Day is still only geographically semi-open in its reach, the significance of the sales event is expansive enough to prompt "preparatory" scams (Bolster Blog 2021), i.e., scams that are perpetrated even before the actual event begins. For instance, these preparatory scams include offers for early deals as well as attempts to entice incoming users to become Amazon members, including with various fraudulent offers for coupons and discounts, and set up their respective payment accounts (Bolster Blog 2021). Given the sales frenzy of the actual event, perpetrators are able to intensify their otherwise regular efforts and exploit people with ruses that are built on non-existent problems with a person's Amazon account, on bogus payment and shipping receipts that are meant to make the person submit additional personal information, as well as on the "verification" of payment methods used in an Amazon purchase (ITRC 2019). Moreover, even after the event-proper has passed, the online sales ecosystem's general reliance on product reviews provides scammers with a further opportunity for perpetrating fraud (ITRC 2019), i.e., criminals are able to make bogus monetary offers in return for writing reviews that are only a smoke-screen for stealing a person's personal and payment information.

Scammers' approach to Black Friday sales is similar to those employed with respect to Amazon Prime Day. Potential buyers are presented with offers that are "too good to be true", asked for personal information or payment details under the guise of fraudulent delivery messages, and lead to enter their payment information into very real-looking fake websites of online merchants (Smith and Aguilar 2021; Osborne 2021). Of note with Black Friday events is their increased sphere of influence due to globalisation (Dumoulin 2019), which is also represented in how the scam ecosystem of fake websites is created alongside the efforts of legitimate vendors trying to take advantage of the sales dates (Bischoff 2020). As Bischoff (2020) showed, the registration of new websites skyrockets in the period preceding Black Friday and Cyber Monday, which is a sibling event to the former, and these websites are spread out globally. Thus, what was historically an event primarily observed in the United States, has expanded throughout most of the world because of its potential for bringing in buyers that are looking for discounts and probably also making materialistic preparations for Christmas. In effect, the salience of the Amazon Prime Day and Black Friday events comes from their regular and relatively reliable occurrence each year, which allows scammers to prepare crime messages, lures and dissemination tactics beforehand. Moreover, the further the occurrence and the legitimate exploitation of such events reaches, the more salient context "room" there is for fraudsters to operate (Dumoulin 2019; Bischoff 2020; Osborne 2021). Even though the aforementioned sales events are temporally restricted to one or two days, the events carry enough significance and have created certain expectations, for buyers that the pre- and post-event periods are also marked in the respective "criminal calendars". Moreover, since Black Friday is itself a commercial prelude to Christmas, the last months of the year are dotted with legitimate commercial events that are as busy for scammers as they are for retailers.

Different from the first example of tax season, which focussed on how certain demands for services are created by specific obligations that people are subject to, the criminal exploitation of commercial holidays often comes down to criminal actors “piggybacking” on gain-based incentives already present for those interested in discounts and deals. As long as people are sufficiently incentivised to engage in practices that involve transfers of funds, the source of the specific demands for goods and services, i.e., whether legally prescribed or culturally created, is less important in mediated fraud.

Non-existent Stocks Can Never Run Out: The COVID-19 Microchip Shortage and Gaming Console Scams

Scammers tend to create their main ruse based on one of two communicative approaches, i.e., either a gain-based “Good Samaritan”, i.e., offering items or services currently in demand, or a loss-based “Shock and Awe” approach, i.e., threatening to cause financial or reputational harm to persons (Kikerpill and Siibak 2021b). Since the social context of frauds has been shown to significantly impact the content of crime messages circulated to the public (Kikerpill 2021a; Taodang and Gundur 2022), the content of such scams, in turn, also reflects the opportunities that the particular context allows for. For instance, scams disseminated in the first four months of the COVID-19 pandemic relied more on a gain-based approach (Kikerpill 2021a), because the pandemic circumstances themselves better facilitated fraudulent offers of potential gain more so than threats of loss. These included bogus offers for difficult-to-obtain personal protective equipment, various untested cures and remedies and even vaccines (Naidoo 2020; Kikerpill and Siibak 2021a). Therefore, when the social context created by an event or salient circumstances is more open to offering recipients something that they need or want rather than threatening to take away something that people already have, then this notion can be expected to be reflected in the types of online scams being circulated.

Following from the above, and considering how much of today’s world “runs” on microchips, i.e., smartphones, laptops and even cars (Feder 2021), the final example provides an initial glimpse into what happens in terms of online fraud if there is suddenly a shortage in the supply of such objects of desire or need. Here, the culturally and geographically open social context for scams originally emerged from a combination of at least two important developments during the COVID-19 pandemic: the increased number of people working from home and using smart devices for work, school and entertainment (Vargo et al. 2021) as well as the issues with and limits to the process of manufacturing microchips (Kamasa 2021). Items such as gaming consoles fall under both of the aforementioned categories, i.e., consoles require microchips and are an increasingly important part of home entertainment (Muriel and Crawford 2018). Thus, when the newest Xbox and PlayStation 5 released only two days apart in November 2020, it was a global cultural event that occurred in the midst of the COVID-19 pandemic (Frank 2020). Even though Sony, i.e., the manufacturer of PlayStations, did not expect the COVID-19 pandemic to derail the new console's release plans (Powell 2020), keeping the gaming consoles in stock, including in online stores, was highly problematic from the beginning (Smith 2020). As already shown previously, deficits concerning in-demand products or services are a quintessential opportunity for scammers to defraud people (Kikerpill and Siibak 2021b). Furthermore, the fluctuating availability of gaming consoles can also be considered as a temporally semi-open event, i.e., a reoccurring salient social context that becomes more scam-inducing when stocks are low.

Ultimately, the combination of a sought-after product and severe issues in its production establishes the social context within which scammers are able to successfully operate. Recognising the emergence of similar circumstances is an important aspect of digital literacy and fraud avoidance. Understanding how the presence of demand and a lack of supply (Kikerpill and Siibak 2021b) provide opportunities for fraud, in particular in online venues where the environment is easily further manipulated (Kikerpill 2021a), is a general skill requirement for staying safe in online environments. Whether the object of desire is some product, service, or even just content, e.g., free streaming of popular TV series or movies, the scam rules are broadly the same: the presence of demand can always be satisfied with pretend supply. With respect to the current example of gaming consoles, the primary aim is to acknowledge the different ways in which the overall cultural importance of certain items and activities intensified the acuteness of an already existing unavailability of products. Social context, in this sense, seems to act as a strengthening agent for underlying wishes and desires. Unlike the commercial holidays example, which incentivises people on the basis of temporal restrictions, the microchip shortage and subsequent gaming console scams placed the focus on objects of desire the demand for which comes and goes as social trends shift.

Discussion and Conclusion

The main objective of the previously presented examples was to explore and explain the ways in which events and social circumstances, i.e., salient social contexts, are or can be used in the dissemination of credible-sounding or looking online scams. In the temporally and geographically restricted comparative tax seasons example, the complexity of the tax system itself and the ease with which people can file their taxes played an important role in terms of the extent of a relevant scam ecosystem (see Kikerpill 2021a). The "criminal calendars" are fixed to the date ranges in which taxes are prepared, filed and returns received. Where the tax filing is made simple for citizens (see e-Estonia 2021), scams appear scarcer as there are fewer points in the process into which scammers can interject their bogus offers. However, when the preparation of taxes is complex enough so as to require the provision of relevant services, scammers will find ways of exploiting this weakness in the system, including how people handle their personal and financial information in the process

(Rafter 2022). Referring to the social context element of the *mazephishing* framework (Kikerpill and Siibak 2021a), the event itself, e.g., the upcoming or ongoing tax season, decreases scammers' workload, because it already provides a seemingly credible reason for contacting people. Hence, knowledge of such processes, including who might be expected to contact a person in these circumstances, is important for fraud avoidance in cases of crime-as-communication.

In the case of Amazon Prime Day and Black Friday sales events, scams follow a well-trodden path of promised gains and a type of fear-of-missing-out experience (Kikerpill and Siibak 2021b), i.e., not buying a product during the sales event means a person would have to wait for the next one. What was particularly important with respect to advancing digital literacy in the area of fraud avoidance, is the fact of how scams follow the well-known social context even if the particular date of the temporally restricted event is changed due to exceptional circumstances (see Johnston 2022). Furthermore, as the observance of such events extends to new areas and communities, the social context that enables respective scams extends along with it. In other words, the more culturally shared (or open) an event is, the larger the geographical range for the dissemination of increasingly believable scams. The application of the first element of the *mazephishing* framework, i.e., the social context element, is relatively easy with well-established "hallmark holidays". Even so, future research could inquire whether this also holds true for culturally restricted events or circumstances, e.g., local fairs that are organised regularly, or other celebrated dates that involve a local commercial element.

The microchip shortage, and the unavailability of popular gaming consoles that the shortage has entailed, shows that a combination of cultural and commercial elements can emerge to enable widespread scams. While these scams are temporally semi-open, i.e., the circumstances that underlie the scams fluctuate, they are concurrently the category that requires the most attention in future research. In comparison with fixed-date (or date range) events such as tax seasons or "hallmark holidays", fluctuating social contexts may be the most difficult to predict in terms of salience for online scams, because current trends in objects of desire or necessity can change quickly and be very different in different parts of the world. Put another way, while we are beginning to learn more about the importance of social context in the dissemination of scams (Carter 2015; Kikerpill and Siibak 2021a; Kikerpill 2021a, Steinmetz et al. 2021), we still lack sufficient information as to what exactly causes some events or circumstances to become salient enough so as to enable the circulation of scams reliant on said context. The gaming console scams are a lone example of how the combination of different circumstances can make for a scam-inducing environment, but more information is required about other similar combinations, i.e., temporal, cultural and geographical aspects that comprise a basis for social circumstances conducive to circulating scams. Given that not all events and circumstances are equally important for members of different communities, and such circumstances are also lived and experienced differently, an important future effort in digital literacy and fraud avoidance must come from employing local knowledge to detect, record and report how salient social contexts create opportunities for scammers. In fact, adopting the *mazephishing* framework for classroom instruction may facilitate this process on a local level in different types of digital literacy courses. By looking at scams that are already detected, it opens the possibility for a more in-depth scrutiny of their timing (e.g., set dates or all-year-round circulation), content and context (e.g., the themes and references to events used in the scams), as well as the channels used for spreading them (e.g., emails, text messages, social media, or bogus websites created for the specific purpose). As it is incredibly difficult to uniformly determine what different people might consider as desirable or necessary under varying circumstances, digital literacy in fraud avoidance is key to mitigating the myriad of crime (as communication) threats that are circulating now or will be circulated in the future.

References

Atkins B, Huang W (2013) A study of social engineering in online frauds. Open J Soc Sci 1(3):23–32. https://doi.org/10.4236/jss.2013.13004

Bischoff P (2020, November 25) 5,000+ Black Friday and Cyber Monday scam sites registered in November. Comparitech. Retrieved February 27, 2022, from https://www.comparitech.com/blog/vpn-privacy/black-friday-scam-website-research/

Bolster Blog (2021, June 16) Amazon scams up 7X leading up to Prime Day. Retrieved February 27, 2022, from https://bolster.ai/blog/amazon-scams-up-7x-leading-up-to-prime-day/

Borel B (2018, October 1) Clicks, lies and videotape. Scientific American. Retrieved July 22, 2022, from https://www.scientificamerican.com/article/clicks-lies-and-videotape/

Button M, Cross C (2017) Cyber frauds, scams and their victims. Routledge

Carter E (2015) The anatomy of written scam communications: an empirical analysis. Crime Media Cult Int J 11(2):89–103. https://doi.org/10.1177/1741659015572310

Carter E (2021) Distort, extort, deceive and exploit: exploring the inner workings of a romance fraud. Br J Criminol 61(2):283–302. https://doi.org/10.1093/bjc/azaa072

Dumoulin I (2019, November 25) The development of Black Friday as a global sales phenomenon. Diggit Magazine. Retrieved February 27, 2022, from https://www.diggitmagazine.com/papers/black-friday-global-sales-

e-Estonia (2021, March 17) Estonian simplicity, American complexity: a tale of two very different tax systems. Retrieved February 27, 2022, from https://e-estonia.com/a-tale-of-two-very-different-tax-systems/

e-Estonia (2022) e-Tax. Retrieved February 26, 2022, from https://e-estonia.com/solutions/ease_of_doing_business/e-tax/

ETCB (2021, December 14) Eesti elanike maksutahe kasvas kolmandat aastat järjest. Estonian Tax and Customs Board. Retrieved February 27, 2022, from https://www.emta.ee/uudised/eesti-elanike-maksutahe-kasvas-kolmandat-aastat-jarjest

Feder S (2021, October 12) Understanding the global chip shortage, a big crisis involving tiny components. Popular Science. https://www.popsci.com/technology/global-chip-shortage/

Fowler B (2022, February 14) Valentine's Day romance scams: don't fall for them. CNET. Retrieved February 27, 2022, from https://www.cnet.com/tech/services-and-software/valentines-day-romance-scams-dont-fall-for-them/

Frank A (2020, November 19) Why the new PlayStation and Xbox are such a big deal. Vox. Retrieved February 26, 2022, from https://www.vox.com/culture/21551062/playstation-5-xbox-series-x-price-games-release-date-explained-next-gen

Hadnagy C (2018) Social engineering: the science of human hacking. Wiley

Harrington B (2012) The sociology of financial fraud. In: Cetina KK, Preda A (eds) The Oxford handbook of the sociology of finance. Oxford University Press, pp 393–410

Hatfield JM (2018) Social engineering in cybersecurity: the evolution of a concept. Comput Secur 73:102–113. https://doi.org/10.1016/j.cose.2017.10.008

Hong, J. (2012). The state of phishing attacks. Communications of the ACM, 55(1). https://doi.org/10.1145/2063176.2063197

ITRC (2019, July 11) Scored on Amazon Prime Day? Watch now for scams. Identity Theft Resource Center. Retrieved February 26, 2022, from https://www.idtheftcenter.org/post/scored-on-amazon-prime-day-watch-now-for-scams/

Johnston B (2022, January 4) Prime Day 2022: everything you need to know. Retrieved February 26, 2022, from https://www.expertreviews.co.uk/amazon-prime-day

Kamasa J (2021) Microchips: small and demanded. CSS Analyses in Security Policy 295. https://doi.org/10.3929/ethz-b-000517399

Kantar Emor (2020) Riigiportaali eesti.ee kasutaja rahulolu analüüs: koondaruanne. Retrieved February 27, 2022, from https://www.ria.ee/sites/default/files/kantar_emor_riigiportaali_eesti.ee_rahuloluanaluus_koondaruanne.pdf

Kessler G (2013, April 13) Claims about the cost and time it takes to file taxes. The Washington Post. https://www.washingtonpost.com/blogs/fact-checker/post/claims-about-the-cost-and-time-it-takes-to-file-taxes/2013/04/13/858a97fc-a455-11e2-9c03-6952ff305f35_blog.html

Khonji M, Iraqi Y, Jones A (2013) Phishing detection: a literature survey. IEEE Commun Surv Tutor 15(4):2091–2121

Kikerpill K (2021a) Crime-as-communication: detecting diagnostically useful information from the content and context of social engineering attacks. University of Tartu Press

Kikerpill K (2021b) The individual's role in cybercrime prevention: internal spheres of protection and our ability to safeguard them. Kybernetes 50(4):1015–1026. https://doi.org/10.1108/K-06-2020-0335

Kikerpill K, Siibak A (2019) Living in a spamster's paradise: deceit and threats in phishing emails. Masaryk Univ J Law Technol 13(1):45–63. https://doi.org/10.5817/MUJLT2019-1-3

Kikerpill K, Siibak A (2021a) Mazephishing: the COVID-19 pandemic as credible social context for social engineering attacks. Trames J Humanit Soc Sci 25(4):371–393. https://doi.org/10.3176/tr.2021.4.01

Kikerpill K, Siibak A (2021b) Abusing the COVID-19 pan(de)mic: a perfect storm for online scams. In: Pollock JC, Kovach DA (eds) COVID-19 in international media: global pandemic perspectives. Routledge. https://doi.org/10.4324/9781003181705-25

Klimburg-Witjes N, Wentland A (2021) Hacking humans? Social engineering and the construction of the "deficient user" in cybersecurity discourses. Sci Technol Hum Values 46(6):1316–1339. https://doi.org/10.1177/0162243921992844

Lawson P, Pearson CJ, Crowson A, Mayhorn CB (2020) Email phishing and signal detection: how persuasion principles and personality influence response patterns and accuracy. Appl Ergon 86:103084. https://doi.org/10.1016/j.apergo.2020.103084

Maggi R (2014) Toward a semiotics of digital places. In: Resmini A (ed) Reframing information architecture. Human–computer interaction series. Springer, pp 85–102. https://doi.org/10.1007/978-3-319-06492-5_7

Marcos CM (2021, November 26) How Black Friday got its name. The New York Times. https://www.nytimes.com/2021/11/26/business/how-black-friday-got-its-name.html

Montañez R, Golob E, Xu S (2020) Human Cognition Through the Lens of Social Engineering Cyberattacks. Front Psychol 11:1755. https://doi.org/10.3389/fpsyg.2020.01755

Muriel D, Crawford G (2018) Video games as culture: considering the role and importance of video games in contemporary society. Routledge

Naidoo R (2020) A multi-level influence model of COVID-19 themed cybercrime. Eur J Inf Syst 29(3):306–321. https://doi.org/10.1080/0960085X.2020.1771222

Norris G, Brookes A, Dowell D (2019) The psychology of internet fraud victimisation: a systematic review. J Police Crim Psychol 34:231–245. https://doi.org/10.1007/s11896-019-09334-5

Osborne H (2021, November 25) Black Friday: how to avoid scams when shopping for deals. The Guardian. Retrieved February 27, 2022, from https://www.theguardian.com/money/2021/nov/25/black-friday-scams-deals-save-money-tips

Pew Research (2015, April 10) 5 facts on how Americans view taxes. Pew Research Center. Retrieved February 25, 2022, from https://www.pewresearch.org/fact-tank/2015/04/10/5-facts-on-how-americans-view-taxes/

Pihlak A (2017, March 12) Petturid saadavad maksuameti nimel õngitsuskirju. Õhtuleht. https://www.ohtuleht.ee/792799/petturid-saadavad-maksuameti-nimel-ongitsuskirju

Posick C (2018) The development of criminological thought: context, theory and policy. Routledge

Powell S (2020, May 29) PlayStation 5: sony confident coronavirus won't change release plans. BBC News. Retrieved February 26, 2022, from https://www.bbc.com/news/newsbeat-52851506

Proofpoint (2019) Human Factor Report 2019. Proofpoint, Inc

PurpleSec (2021) 2021 Cyber security statistics: the ultimate list of stats, data & trends. Retrieved February 27, 2022, from https://purplesec.us/resources/cyber-security-statistics/

Raamatupidaja (2016, January 21) Liikvel on tuludeklaratsiooni petukirjad. Retrieved February 26, 2022, from https://www.raamatupidaja.ee/uudised/2016/01/21/liikvel-on-tuludeklaratsiooni-petukirjad

Rafter D (2022, January 26) 5 IRS scams to watch out for this tax season. Lifelock. Retrieved February 25, 2022, from https://www.lifelock.com/learn/identity-theft-resources/irs-tax-scams-to-watch-out-for

Rapp J (2016, January 31) Rahalubaduse varjus peitub pettus. Lõuna-Eesti Postimees. https://lounapostimees.postimees.ee/3075893/rahalubaduse-varjus-peitub-pettus

Rigotti E, Rocci A (2006) Towards a definition of communication context. Foundations of an interdisciplinary approach to communication. Stud Commun Sci 6(2):155–180

Simons H (2014) Case study research: in-depth understanding in context. In: Leavy P (ed) The Oxford handbook of qualitative research. Oxford University Press, pp 455–470

Smith C (2020, November 25) PS5 stock: sony offers hope of more consoles before end of 2020. Retrieved February 27, 2022, from https://www.trustedreviews.com/news/ps5-stock-sony-offers-hope-of-more-consoles-before-end-of-2020-4110995

Smith D, Aguilar N (2021, November 21) Don't fall for these clever Black Friday scams this year. Retrieved February 27, 2022, from https://www.cnet.com/tech/services-and-software/dont-fall-for-these-clever-black-friday-scams-this-year/

Snowdon D, Churchill EF, Munro AJ (2001) Collaborative virtual environments: digital spaces and places for CSCW: an introduction. In: Churchill EF, Snowdon DN, Munro AJ (eds) Collaborative virtual environments: digital places and spaces for interaction. Springer, pp 3–20

Sobak K (2014, December 30) Järjekordne petuskeem üritab maksu- ja tolliameti nimel raha välja petta. ERR. Retrieved February 25, 2022, from https://www.err.ee/527151/jarjekordne-petuskeem-uritab-maksu-ja-tolliameti-nimel-raha-valja-petta

Steinmetz K, Pimentel A, Goe WR (2021) Performing social engineering: a qualitative study of information security deceptions. Comput Hum Behav 124:106930. https://doi.org/10.1016/j.chb.2021.106930

Taodang D, Gundur RV (2022) How frauds in times of crisis target people. Vict Offenders. https://doi.org/10.1080/15564886.2022.2043968

Tompor S (2021, June 15) Amazon scammers are slick, good at what they do: here's what to watch for. Detroit Free Press. https://eu.freep.com/story/money/personal-finance/susan-tompor/2021/06/15/amazons-scammers-good-what-they-do-heres-what-watch/7633895002/

Torgler B, Schneider F (2007) What shapes attitudes toward paying taxes? Evidence from multicultural European countries. Soc Sci Q 88(2):443–470. https://doi.org/10.1111/j.1540-6237.2007.00466.x

Vargo D, Zhu L, Benwell B, Yan Z (2021) Digital technology use during COVID-19 pandemic: a rapid review. Hum Behav Emerg Technol 3(1):13–24. https://doi.org/10.1002/hbe2.242

Verma R, Crane D, Gnawalli O (2018) Phishing during and after disaster: hurricane Harvey. Resilience Week (RWS):88–94. https://doi.org/10.1109/RWEEK.2018.8473509

Walter D (2019, January 25) Card number, CVV, expiry date are not knowledge elements – or maybe they are? OsborneClarke. Retrieved February 26, 2022, from https://www.osborneclarke-fintech.com/2019/01/25/card-number-cvv-expiry-date-are-not-knowledge-elements-or-maybe-they-are/

Whitney L (2021, June 17) Amazon Prime Day scams resurface for 2021. TechRepublic. Retrieved February 25, 2022, from https://www.techrepublic.com/article/amazon-prime-day-scams-resurface-for-2021/

Work in Estonia (2022, February) Taxes in Estonia. Retrieved February 27, 2022, from https://www.workinestonia.com/working-in-estonia/taxes/