

DOI 10.5817/MUJLT2019-1-3

## LIVING IN A SPAMSTER'S PARADISE: DECEIT AND THREATS IN PHISHING EMAILS

*by*

KRISTJAN KIKERPILL\*, ANDRA SIIBAK\*\*

*The prevalence of using email as a communication tool for personal and professional purposes makes it a significant attack vector for cybercriminals. Consensus exists that phishing, i.e. use of socially engineered messages to convince recipients into performing actions that benefit the sender, is widespread as a negative phenomenon. However, little is known about its true extent from a criminal law perspective. Similar to how the treatment of phishing in a generic manner does not adequately inform the relevant law, a case-by-case legal analysis of seemingly independent offences would not reveal the true scale and extent of phishing as a social phenomenon. The current research addresses this significant gap in the literature. To study this issue, a qualitative text analysis was performed on (N=42) emails collected over a 30-day period from two email accounts. Secondly, the phishing emails were analysed from an Estonian criminal law perspective. The legal analysis shows that in the period of only one month, the accounts received what amounts to 3 instances of extortion, 29 fraud attempts and 10 cases of personal data processing related misdemeanour offences.*

### KEY WORDS

*Criminal Law, Cybercrime, Legal Analysis, Phishing Emails, Qualitative Text Analysis*

---

\* kristjan.kikerpill@gmail.com, Independent Researcher.

\*\* andra.siibak@ut.ee, Professor of Media Studies, Institute of Social Studies, University of Tartu, Estonia.

## 1. INTRODUCTION

It is suggested that more than 281 billion emails were exchanged daily in 2018.<sup>1</sup> Recent malicious online activity reports suggest that about one in every 2000 of these emails is an attempt at phishing,<sup>2</sup> i.e. a cyber-attack which utilises socially engineered messages to convince recipients into performing actions that benefit the sender. Phishing does not generally constitute a separate offence under substantive criminal law<sup>3</sup> but is an umbrella moniker for the collection of offences initiated or committed, among other channels, via email.<sup>4</sup> Therefore, in addition to facilitating legitimate communication in the email ecosystem, the inbox also acts as a honeypot and staging ground for various forms of criminal offences.

Research from different fields provides a rich background to the study of phishing. For example, phishing has been studied extensively by scholars working in the fields of behavioural sciences, psychology and criminology.<sup>5</sup> However, disciplines external to law treat phishing and other computer-related criminal activities as generic negative phenomena without providing an accompanying legal assessment. Applying the *nullum crimen sine lege* principle, findings from disciplines researching phishing as a phenomenon thus do not enable the effective informing of the relevant law. The central problem here is a lack of connection between phishing attacks and the compendium of formally established offences the attacks

---

<sup>1</sup> Radicati Group. (2018) *Executive Summary*. Available from: <https://www.radicati.com/wp/wp-content/uploads/2018/05/Email-Market-2018-2022-Executive-Summary.pdf> [Accessed 20 November 2018].

<sup>2</sup> Symantec. (2018) *Internet Security Threat Report*. Available from: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf> [Accessed 20 November 2018].

<sup>3</sup> In the European Union, this notion might be subject to change and harmonisation depending on future developments (see European Commission Proposal for a Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA. (2017/0226) 13 September, Recital 9. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0489:FIN> [Accessed 20 November 2018]).

<sup>4</sup> While email-based attacks are more common, phishing also appears in other forms such as *smishing* or SMS-phishing and *vishing* or voice-phishing.

<sup>5</sup> For example, in psychology and behavioural sciences see Rajivan, P. and Gonzalez, C. (2018) Creative Persuasion: A Study on Adversarial Behaviors and Strategies in Phishing Attacks. *Frontiers in Psychology*, 135 (9); Williams, E. J., Beardmore, A. and Joinson, A. N. (2017) Individual Differences in Susceptibility to Online Influence: A Theoretical Review. *Computers in Human Behavior*, 72, pp. 412–421; Vishwanath, A. et al. (2011) Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model. *Decision Support Systems*, 51 (3), pp. 576–586; in criminology see Hutchings, A. and Hayes, H. (2009) Routine Activity Theory and Phishing Victimization: Who Gets Caught in the ‘Net’? *Current Issues in Criminal Justice*, 20 (3), pp. 433–451; Reyns, B. W. (2015) A Routine Activity Perspective on Online Victimization: Results from the Canadian General Social Survey. *Journal of Financial Crime*, 42 (4), pp. 396–411.

constitute. In contrast, mere case-by-case legal analysis of handpicked examples of seemingly independent offences would only succeed in attaching existing criminal law provisions to objective facts, i.e. solving a clearly delimited criminal case. This approach fails to reveal the scale and impact that phishing as a phenomenon entails in society. For the above reasons, the current paper takes a socio-legal approach to explore the phenomenon of phishing. Firstly, a qualitative text analysis was performed on emails (N=42) received over the course of a month, which had initial indications of being phishing attempts. The analysis focused on how perpetrators craft stories and insert influencing techniques into their text for the purposes of manipulating the recipients' will to act or respond. Secondly, the paper provides a legal assessment regarding the results with an aim to fill the gap currently present in phishing literature as well as provide some insight into the real scale of online crime commission.

## 2. CONTEXTUAL BACKGROUND

To the detriment of the public at large, conventional anti-crime efforts are falling short when it comes to cybercrime, including the phenomenon of phishing. In 2013, a study published by the *United Nations Office on Drugs and Crime* suggested that perhaps only 1 % of actual cybercrime victimisation is reported to law enforcement.<sup>6</sup> The underreporting was stated to derive from a lack of awareness about victimisation and of reporting mechanisms, but also victim shame and embarrassment.<sup>7</sup> Perpetrators increasingly choose to take advantage of their potential victims' natural inclination towards deception and threat susceptibility rather than wasting time and resources on overcoming complex technological barriers. As recent literature suggests, criminal actors often employ social engineering techniques to motivate recipients into giving out personal information or performing specific acts.<sup>8</sup>

In general, influencing techniques,<sup>9</sup> or urgency cues, in fraudulent emails are used for two main reasons. Firstly, the senders aim to elicit emotional

---

<sup>6</sup> United Nations Office on Drugs and Crime. (2013) *Draft Comprehensive Study on Cybercrime*. p. 119. Available from: [https://www.unodc.org/documents/organized-crime/UNODC\\_CCP\\_CJ\\_EG.4\\_2013/CYBERCRIME\\_STUDY\\_210213.pdf](https://www.unodc.org/documents/organized-crime/UNODC_CCP_CJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf) [Accessed 20 November 2018].

<sup>7</sup> Op. cit., p. xxi.

<sup>8</sup> See also Williams, E. J., Beardmore, A. and Joinson, A. N. (2017), op. cit.

<sup>9</sup> Williams, E. J., Hinds, J. and Joinson, A. N. (2018) Exploring Susceptibility to Phishing in the Workplace. *International Journal of Human-Computer Studies*, p. 120.

reactions from the recipients by evoking feelings such as fear or threat,<sup>10</sup> which would inhibit the recipients' ability to process the information under review.<sup>11</sup> Secondly, urgency cues are used to draw the recipients' focus away from other aspects of the text, e.g. spelling errors, which could aid the user in determining the email's authenticity.<sup>12</sup> Previous analyses have also shown the prevalence of urgency cues<sup>13</sup> and visceral appeals, such as money, love or sorrow, in eliciting compliance from the targets.<sup>14</sup> Vishwanath and others also found that attention to urgency cues is positively related to the potential victim's likelihood of responding to the fraudulent email.<sup>15</sup>

The approach is certainly well-founded as the rates of users clicking on links directing them to fake websites or opening attachments infected with malware contained in phishing emails hovers around 10 % on average.<sup>16</sup> These high success rates rank phishing emails as the top attack vector used to bypass technology-centred security efforts and attack the human factor instead. Human beings are not considered particularly adept at detecting deception<sup>17</sup> and their abilities are further inhibited with text-based, less rich media such as email.<sup>18</sup> The issue is compounded by the fact that the people being preyed upon by criminal actors consider themselves to be poorly informed about phishing and other malicious activities facilitated by information technology.<sup>19</sup> Additionally, the way modern electronic communications enable access to potential victims plays right into the hands of the perpetrators. Criminal actors employ mass-

<sup>10</sup> Workman, M. (2008) Wisecrackers: A Theory-grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security. *Journal of the American Society for Information Science and Technology*, 59 (4), pp. 662–674.

<sup>11</sup> Vishwanath, A. et al. (2011), op. cit.

<sup>12</sup> Jakobsson, M. (2007) The Human Factor in Phishing. *Privacy & Security of Consumer Information*.

<sup>13</sup> Atkins, B. and Huang, W. (2013) A Study of Social Engineering in Online Frauds. *Open Journal of Social Sciences*, 1 (3), pp. 23–32.

<sup>14</sup> Button, M. et al. (2014) Online Frauds: Learning from Victims Why They Fall for These Scams. *Australian & New Zealand Journal of Criminology*, 47 (3), pp. 391–408. See also Langenderfer, J. and Shimp, T. A. (2001) Consumer Vulnerability to Scams, Swindles, and Fraud: A New Theory of Visceral Influences on Persuasion. *Psychology and Marketing*, 18, pp. 763–783.

<sup>15</sup> See Vishwanath, A. et al. (2011), op. cit., p. 582.

<sup>16</sup> Verizon. (2017) *Data Breach Investigations Report, 10th Ed.*

<sup>17</sup> Burgoon, J. K. et al. (1994) Interpersonal Deception: Accuracy in Deception Detection. *Communication Monographs*, 61, pp. 303–325.

<sup>18</sup> Burgoon, J. K. et al. (2003) Detecting Deception Through Linguistic Analysis. In: Hsinchun Chen et al. (eds.). *Intelligence and Security Informatics*, Springer.

<sup>19</sup> European Commission. (2017) *Special Eurobarometer 464a: Europeans' Attitudes Towards Cyber Security*, p. 6.

-targeting not exclusive to a single jurisdiction and are satisfied with relatively insignificant gains per successful action due to the scale of the operation. Using these tactics often ensures little interest from law enforcement as the latter generally have high thresholds before they consider launching an investigation.<sup>20</sup> When an investigation is ultimately launched, problems immediately arise concerning international cooperation mechanisms for accessing evidence in foreign jurisdictions.<sup>21</sup> Acting across jurisdictional borders and the ensuing complexities regarding law enforcement efforts is part of what allows perpetrators to commit computer-related offences with impunity.<sup>22</sup>

### 3. METHODS AND DATA

In order to investigate the prevalence of email-based crime commission in depth, with direct legal relevance, the authors carried out a socio-legal study related to phishing. The phishing emails were received via two email accounts from the sample of the study. The emails were gathered over a 30-day period from mid-August to mid-September in 2018. To study emails received on two accounts, a single email client was used. The second email account provided email data to the email client through forwarding. Employing a single email client, or mail user agent, is justified by considering how an individual interacts with the email ecosystem. Although people use or may use multiple email accounts for different purposes, e.g. personal, work or school, it is common to collect the influx of messages and subsequently view them using a single email client<sup>23</sup> or a single device<sup>24</sup>. This allows to view the client, or device, as the “end-of-route” collection point to which a person receives most, if not all, messages sent to them via email. Hence, the chosen method of data collection

---

<sup>20</sup> Button, M. et al. (2014), op. cit., p. 400.

<sup>21</sup> Osula, A.-M. (2015) Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data. *Masaryk University Journal of Law and Technology*, 9 (1), pp. 43–64.

<sup>22</sup> Cromwell, C. R., Narvaez, D. and Gomberg, A. (2005) Moral Psychology and Information Ethics: The Effects of Psychological Distance on the Components of Moral Behavior in a Digital World. In: Lee Freeman and A. Graham Peace (eds.). *Information ethics: Privacy and intellectual property*. Hershey, PA: Idea Group, pp. 19–37.

<sup>23</sup> Email client market shares suggest *Apple iPhone, Gmail* and *Outlook* to be the most popular mobile, webmail and desktop email clients as of October 2018 (see Litmus Email Analytics. (2018) *Email Client Market Share*. Available from: <http://emailclientmarketshare.com/> [Accessed 20 November 2018]).

<sup>24</sup> Mobile devices are the most popular, followed by laptops, tablets and desktop computers. Fluent. (2017) *The Inbox Report 2017: Consumer Perceptions of Email*, p. 4.

represents the activity occurring over a one-month period in the final collection point for an individual who actively uses the email ecosystem. The inbox has also been used as a source of data to supplement the collection of emails for the analysis of specific scam types.<sup>25</sup> However, opting to collect emails over a certain time-period from a fixed source better represents actual events and potential crime commission “as-is” compared to focussing on specific types of emails the collection of which is not subject to a predetermined time-limit or source, e.g. openly accessible archives can be used.<sup>26</sup> The chosen data collection method has a direct impact on the subsequent application of criminal law provisions, as the raw material for any offence considered in the legal analysis was obtained from the fixed “end-of-route” collection point, i.e. legal analysis was performed on messages in fact received, not on the entire spectrum of possible variations and types available from external sources.

The total amount of emails received during the 30-day period was 297. Of these emails, 70 were automatically received in the spam folder of the email client and no emails with indications of phishing were detected in the primary folder. An initial indication of a phishing attempt includes elements such as unknown sender, grammatical errors, subject lines with upper-case letters throughout as well as ambiguous, generic or overtly out of place topics.<sup>27</sup> The indications were assessed for by quickly scanning, or “eye-balling”, the folders. From the 70 emails received in the spam folder, 28 were assessed to be advertisements from known senders and excluded from subsequent analysis. The remaining 42 emails presented clear initial indications of being a phishing attempt. Hence, the final sample (N=42) for subsequent qualitative text analysis was formed of emails with strong initial indications of being a phishing attempt that were collected over a one-month period in the “end-of-route” email client folders. The emails collected in the “end-of-route” client for the current research amounted to 9.9 emails received per day with the total unsolicited email ratio at 23 % and messages with strong initial indications of phishing at 14.1 %.

Qualitative text analysis was used for analysing the final (N=42) email sample. The analysis started with hierarchical coding as suggested

---

<sup>25</sup> Atkins, B. and Huang, W. (2013), op. cit., p. 27.

<sup>26</sup> See MillerSmiles. *Phishing scam archives*. [online] Available from: <http://www.millersmiles.co.uk/archives.php> [Accessed 20 November 2018].

<sup>27</sup> Jakobsson, M. (2007), op. cit., pp. 3–6.

by *Straus and Corbin*.<sup>28</sup> For the coding process, the guiding concept of “influence and impact on the will to act” was derived from a combination of influencing techniques described in extant literature<sup>29</sup> as well as how certain criminal offences against property are analysed in law. For instance, in extortion cases the offender “bends” the victim’s will to act,<sup>30</sup> while in robberies the victim’s will to act is “broken”, i.e. *vis absoluta* is used. Bending a victim’s will to act means applying significant pressure on the target to perform a specific action, which in extortion cases is expressed by the offender’s goal of ultimately receiving some proprietary gain through the use of threats or violence. The proprietary gain of the offender might be in the form of an object, e.g. smartphone or cash, or in the form of a proprietary right, i.e. a transfer of funds from the victim’s bank account to the offender. What differentiates extortion from robberies and bending the victim’s will to act from breaking it completely, is the presence or absence of the need for a victim to also perform some action. It is possible to assert that extortion-type interactions require an active victim, whilst in robbery type interactions the victim would remain largely inactive (see Figure 1).

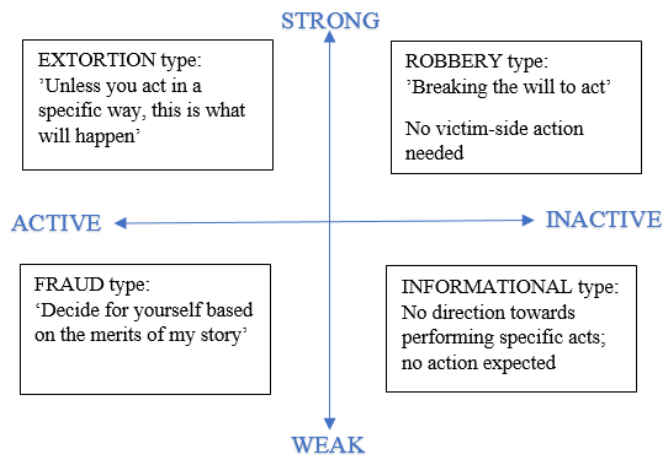


Figure 1: The RIFE (Robbery, Informational, Fraud, Extortion) scale of influence and impact on the will to act

<sup>28</sup> Strauss, A. and Corbin, J. (1998) *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks, CA: Sage Publications.

<sup>29</sup> Williams, E. J., Beardmore, A. and Joinson, A. N. (2017), op. cit.

<sup>30</sup> Case no. 3-1-1-103-12. (2012) Estonian Supreme Court (Criminal Chamber), 23 November 2012.

However, robbery-type interactions are no longer possible in the email ecosystem,<sup>31</sup> i.e. a person cannot be victimised just by opening an email they have received. In terms of the intensity of impact on the victim's will to act, extortion and robbery type interactions populate the strong impact side of the intensity axis. The other side of the intensity axis, or the weak intensity of impact methods used in influencing a person's will to act, is inhabited by fraud type and purely informational type interactions. In cases of fraud, the victim performs an action freely but based on misconceptions caused by the offender, i.e. due to deception. Purely informational interactions merely convey a message from the sender and thus would not achieve the effects that criminal actors desire, e.g. forwarding sensitive personal information, credit card information, getting the recipient to transfer funds or open file attachments. As the intensity of impact can be considered weak in both fraud and purely informational types, distinguishing between the two derives from the presence or absence of cues directing the recipient to take action in a manner suggested by the sender. In fraud type messages, a bogus storyline is often presented to the recipient with the intention of getting the user to act in a specific way, e.g. visit a website or forward credit card information. Informational type messages do not direct the recipient towards taking specific action. It follows then that informational messages are also void of any guidance on how the recipient should go about performing an action, e.g. providing links to external websites or contact information in the form of email addresses and phone numbers. Therefore, the first order coding used the *RIFE scale* to assess emails received in the client. The initial coding resulted in 3 extortion type phishing emails and 39 fraud type emails. Hence, phishing emails are inherently actionable, i.e. the senders always have the goal of getting the recipient to act in a specific manner regardless of the intensity of impact present in the message or the methods of influence used in the interaction. The *RIFE scale* provides answers to the question "What, if anything, are the senders trying to get me to do?". As the second round of coding only concerns actionable phishing emails, it was designed to answer the question "How are the senders trying to get me to do it?". In the second round of coding, the extortion and fraud type emails were

---

<sup>31</sup> Hoffman, G. (2016) *Why You Can't Get Infected Just by Opening an Email (Anymore)*. [online] Available from: <https://www.howtogeek.com/135546/htg-explains-why-you-cant-get-infected-just-by-opening-an-email-and-when-you-can/> [Accessed 20 November 2018].



assessed based on four binary categories derived from the final sample of 42 emails (see Table 1).

	A	B
Relationship	Establishing	Assumed
Action	Implicit	Explicit
Influence	Persuasion-type	Threat-type
Dominance	Recipient Controlled	Sender Controlled

Table 1: The RAID (Relationship, Action, Influence, Dominance) categories present in phishing emails

The first category considered sender-recipient relationships, i.e. whether the email assumed an existing relationship between the two or tried to establish one. For example, a previous relationship would be assumed if the senders masquerade as employees of a company the services of which the recipient uses or might have used in the past. In contrast, establishing a relationship would be premised by an apologetic opening, e.g. *“You do not know me, but here is my story”*. The second category concerned whether the reference to the action desired by the recipient was explicit or implicit, e.g. *“pay the amount to this account”* versus *“the funds can only be released after your payment”*. The third category concerned the choice in influencing techniques, i.e. persuasion-influencing or presenting an enticing story based on bogus facts and threat-influencing or evoking the emotions of fear and urgency regarding the potential consequences of non-compliance. The fourth category pertained to the balance of control, or dominance, in sender-recipient interaction. In a sender-dominant communication, the interaction is controlled by the initiator, e.g. in extortion type interactions. In contrast, a recipient-dominant communication leaves it open for the recipient to choose whether to act or respond, e.g. in fraud type interactions. The RAID (*Relationship; Action, Influence, Dominance*) model was developed for a more in-depth analysis of the choices made by the senders in composing their phishing messages.

## 4. FINDINGS

### 4.1. PHISHING EMAILS: TEXT ANALYSIS

With most messages, the sender information displayed in the mandatory email headers (From; Date) did not match the information available from the full email header. For example, an email apparently originating from

*Shauna*, sent from *admin@localuniversity.ee*, in fact, has a return-path, or the address where non-delivery receipts – also called bounce messages – are sent, of *admin@alisonparkerg.com*. This instance is made problematic for email recipients who are less informed about the technological underpinnings of the email ecosystem. Judging by the mandatory email headers displayed, the message seems to originate from *Shauna* and the local university. However, without looking at the full email header, the rest of the information remains hidden to the recipient. The malicious practice of sending communication from an unknown source disguised as a source known to the sender is called “spoofing” and email spoofing is one of the most common versions of it. Central to the issue here is whether an end-user possesses the know-how to scrutinise the available information further or obtain additional information. *Shauna* working for the administration of an international university is certainly possible. Due to the name, however, local users’ attention is likely to become activated based on the discrepancy between what is observed and what is expected.<sup>32</sup> In other instances, the claimed sender and the email address were visibly mismatched. For example, different senders claimed to be from the U.S. Department of Homeland Security, the U.S. Federal Reserve Bank as well as from JPMorgan Chase Bank, but all messages were sent via mail-servers in Japan with reply-to addresses registered in *Gmail*. Within the context of processing an email, sender information spoofing is usually the first attempt at social engineering. The above examples used the perceived authority of the sender to elicit compliance from the recipient.<sup>33</sup> Additionally, senders tried to establish legitimacy by describing their reputable business (“EVANS THOMAS LAW FIRM SOLICITORS & ADVOCATES”) or position (“I’m Mohamed Usman, a delegate from the united nation office”).

In an email message, greetings can be considered a separate group of recipient activators. Common openings can range from generic (“Hi”) to out-of-place ones (“Dearly Beloved,”) but also include overtly shrill examples like “GOOD DAY LUCKY ONES, DEAR EMAIL OWNER”. When no suspicions arose regarding sender information, then generic greetings

---

<sup>32</sup> Grazioli, S. (2004) Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception over the Internet. *Group Decision and Negotiation*, 13, pp. 149–172.

<sup>33</sup> Office of Fair Trading. (2009) *The Psychology of Scams: Provoking and Committing Errors of Judgement*.

direct the recipient to continue on to the body of the message. Conversely, markedly out-of-place or overemphasised openings seem counterproductive to the sender's intentions as it draws all attention to the discrepancy in the greeting, even if nothing about sender information was particularly alarming. The major difference between less sophisticated *phishing* emails and *spear phishing* emails seems to be based on the understanding that everything up to the body of the email is about maintaining neutrality about the legitimacy of the message, not actively establishing it. This notion was abided by in the *Shauna* example, as the email had no alarming qualities in the sender information, skipped the opening entirely and started with the text body. Legitimate "cold emails", or emails sent without prior contact between the sender and recipient, are a common occurrence in business environments.<sup>34</sup> For this reason, it's not always possible for people to outright disregard emails they were not expecting to receive, unless they are put off by a non-sensical subject line or a shrill greeting.

An additional category of openings, which at times also simultaneously feature on the email's subject line, are the senders who explicitly require attention from the recipients ("*ATTENTION CARD HOLDER*"; "*Attention Dear Esteemed Beneficiary*"; "*Attention my old friend*"). However, expressions of influencing techniques do not necessarily have to be explicit in the messages to still be effective. In well-timed *spear phishing*<sup>35</sup> emails used in *Business Email Compromise (BEC)* scams – sometimes also called *whale phishing* because of the high-value target – perpetrators collect more background information about the person they will be impersonating as well as the one to be victimised prior to submitting the email. A message with spoofed sender information, legitimacy derived from the employment relationship between the perceived sender and recipient, an excuse for spelling mistakes in the form of "*sent from a mobile device*" as well as stating that they cannot be currently reached are all a build-up to the persuasion. Requiring the recipient to make a wire transfer the same day and given that such emails are often sent an hour or less before the close of business, creates a sense of urgency from context. The choices left to the recipient are

---

<sup>34</sup> Krause, M. and Kulkarni, A. (2015) Predicting Sales E-Mail Responders Using a Natural Language Model. In: *Conference on Human Computation & Crowdsourcing 2015*, San Diego, USA.

<sup>35</sup> A more advanced form of phishing emails that can be highly sophisticated, targeted and personalised.

to either go against the direct instructions of their superior or, using pre-existing knowledge about BEC scams, still try and verify the transaction through channels other than the one used to send instructions.

Based on the body text of the emails in the sample, two distinct ways of eliciting compliance from the recipients can be brought out: persuasions and threats. There were three instances of threatening emails that followed an almost identical *modus operandi*, so these will be analysed collectively based on one example. The message started with priming the recipient with a suggestion to prepare oneself and establishing relevancy without a greeting (“*Take a deep breath and read very carefully do not ignore this e-mail !!*”). The next line of the email was a failed attempt at legitimising the subsequent threat by exhibiting that the sender knows something about the sender (“*It appears that, (), is your password. Will possibly not know me and you are probably wondering why you are getting this e-mail, right?*”). The closed brackets in the message are a placeholder for a password related to the email address or account that the message was received on. In preparation for sending these emails, the perpetrators often scrape online resources to find data dumps or published lists of accounts and respective passwords for the purposes of adding perceived legitimacy to their threats.<sup>36</sup> After presenting what was intended to be a real password for an account, the email continued to describe specific ways the sender had gained access to the recipient’s personal device that leads to:

*“my computer software obtained all your contacts from the Messenger, Microsoft outlook, FB, in addition to emails it created a backdoor so i accessed and downloaded all of the data which includes all videos, photographs and records in it”.*

Instructions are then provided to the recipient on how to avoid the ensuing embarrassment by paying the sender in *Bitcoin* cryptocurrency:

*“Important: You have 1 day to make the payment. (I have a completely unique pixel within this e mail, and at this moment I am aware that you’ve read through this email message). If I do not get the BitCoins, I will certainly send your video recording to all of your contacts including relatives, co-workers, and so forth”.*

---

<sup>36</sup> Jaeger, D. et al. (2016) Analysis of Publicly Leaked Credentials and the Long Story of Password (Re-)use. In: *11th International Conference on Passwords (PASS-WORDS2016)*, Germany: Springer.

The email concludes by attempting to evoke a feeling of helplessness in the recipient by stating:

*"It is a non-negotiable offer, that being said don't waste my personal time and yours by responding to this message".*

The same scenario with slight differences in wording was played out in three separate emails. Aside from trying to coerce the target into following specific payment instructions, there was an evident attempt on the part of the sender to confuse the recipient by adding as many technical terms to their activity description as possible. For example, the sender included both an abbreviation of a term and its explanation in the message:

*"During the time you were watching videos, your internet browser began operating as a RDP (Remote Access) which gave me accessibility of your computer screen".*

Thus, the *modus operandi* in these three cases was first to assert legitimacy by trying to display a real password and confuse the recipient with an overload of technical terms. This was followed by evoking a feeling of fear and embarrassment in the user by claiming to possess images and videos of a sensitive nature. The email was concluded by presenting a demand and threatening the recipient.

In contrast to the threatening emails, most of the messages in the sample employed persuasive tactics to get the recipient to follow instructions. The main actions suggested to the user were to forward their personal information so that a large payment could be released to them, or alternatively to pay a small amount of money to obtain access to outrageous riches. To establish rapport with the recipient, a common opening was detailed regarding the sender's person and described the hard times they had fallen on:

*"I am Mrs. Iris J. Stobbs from Sao Tome and Principe, I was married to late Mr. Patrick Stobbs the CEO of PATCAT Oil Mining & Exploration, I am 58 years old, I am suffering from a long time cancer of the breast which has affected my talking & hearing lately".*

By referring to the impaired speaking and hearing abilities, the sender is trying to persuade the user that the received email was perhaps the only viable way for them to establish contact. The story continues to describe the sender and their late husband as “*true Christians*” who unfortunately were not able to have a child, which is why the sender

*“sold all my inherited belongings and deposited all the sum of USD10,300,000.00 with a Bank”.*

Claiming a religious affiliation is intended to provide a motivational basis for what the sender would like to see happen to the money once the recipient has received it:

*“It is my last wish to see that this money is invested in any Charitable Organization of your choice and distributed each year among the Charity organizations and Orphanages, so I want a good humanitarian to use this money to fund Churches, Needy and Widows in São Tomé and Príncipe or in your Country but preferably in São Tomé and Príncipe”.*

The message concludes with the sender reasserting previous claims about her failing health and expects a reply to an email address that does not match the sender’s. The reply would be considered an indication that the recipient is willing to carry out the sender’s final wish. In a final attempt to describe her conditions, the sender adds:

*“As soon as I receive your reply I shall use the little money I have for my drugs and Medi-care to procure and issue you a letter of authority which will prove that you are the new beneficiary of my funds and I shall release the contact of the Bank to you”.*

Thus, if the recipient is willing, they would ultimately receive an outrageous sum of money while the sender languishes with next to nothing. Should the recipient then engage in communication with the sender, it’s likely that somewhere along the way the poor sender would need some financial assistance in releasing the funds. Other variants of the final request included a specific list of personal information required from the recipient upfront, or the request for a small sum of money was indeed already included in the initial email.

#### 4.2. PHISHING EMAILS: LEGAL ANALYSIS

Considering the results presented in the previous section, the following offences will be discussed in the legal analysis: attempt to commit fraud (§ 209 I, § 25 II), extortion (§ 214) as criminal offences under the Estonian Penal Code<sup>37</sup> (hereinafter PC), as well as the violation of personal data processing requirements, which constitutes a misdemeanour under § 42 I of the Personal Data Protection Act<sup>38</sup> (hereinafter PDPA). As provided for in § 209 I of the PC, the *corpus delicti* of general fraud is

*“the causing of proprietary damage to another person by knowingly causing a misconception of the existing facts”*

and the perpetrator must act with the aim of gaining proprietary benefit himself or herself. Causing a misconception or deceiving the potential victim is a necessary element for an offence to be considered under § 209 I. Fraud is a consequence-offence, i.e. the commission of fraud has not fully concluded unless proprietary damage has occurred to the victim. In the sample emails, the senders claimed that

*“You have \$5000 waiting for you at MONEY GRAM now to pick it”*

and followed it by:

*“but before you can pick up the \$5000 you have to pay sum of \$27 for ACTIVATION”.*

The misconception of the existing facts, in this case, would be the fraudulent claim that a fairly large sum of money is waiting for the recipient in a payment system. Yet, to gain access to this money, the recipients would have to pay something first themselves – a sum of USD27 that is small relative to the promised gain. The likelihood of ever receiving the promised sum after payment is non-existent. Therefore, the senders are acting with the aim of gaining proprietary benefit and have also engaged in deceiving or trying to deceive the recipient. Fraud under § 209 I must be an intentional act according to § 15 I of the PC, it cannot be

<sup>37</sup> *Penal Code (Karistusseadustik) 2001*. SI 2001/61, 364. Estonia: Riigi Teataja (State Gazette). In Estonian. English translation available from: <https://www.riigiteataja.ee/en/eli/509072018004/consolide> [Accessed 19 November 2018].

<sup>38</sup> *Personal Data Protection Act (Isikuandmete kaitse seadus) 2007*. SI 2007/24, 127. Estonia: Riigi Teataja (State Gazette). In Estonian. English translation available from: <https://www.riigiteataja.ee/en/eli/507032016001/consolide> [Accessed 19 November 2018].

committed with negligence. In the current case, it would be difficult to claim that the senders submitted the email by being negligent in wording their message or choosing the recipient. Since the recipient never engaged the senders and, more importantly, did not pay the small activation sum, no proprietary damage has occurred. In other words, the necessary consequence has not occurred, and the senders of the email have not committed fraud. However, § 25 I of the PC also establishes the definition of an attempt, which is an intentional act the purpose for which is to commit an offence. We established the intent in the email but were unable to consider the commission of fraud as completed. § 25 II of the PC states that an attempt is deemed to have commenced at the moment when the person, according to the person's understanding of the act, directly commences the commission of an offence. In the example, the senders had submitted the email as-is but had gained no benefit, because the recipient did not fall for the deception. It is characteristic of an attempt to involve all the subjective injustice of an offence but have certain shortcomings in the objective elements,<sup>39</sup> which in the chosen example was both the lack of proprietary benefit gained by the senders and proprietary damage inflicted on the recipient. Based on the facts, the senders might be accountable for an attempt to commit fraud according to § 209 I, § 25 II of the PC.

However, the majority of persuasive emails did not prompt the recipient to pay a certain sum but instead crafted a fraudulent story to obtain personal information. In the following example, the preceding story was similar to the one described previously:

*"We have deposited the check of your fund (\$4.500,000 Million USD) through MONEY",*

which was followed by asking the recipient to forward their name, country, phone number and address to the senders. Alternatively, the recipient could also call the number provided in the email. Since the basis for the collection of personal data from the recipients in the example is fraudulent, the senders might be accountable for the misdemeanour offence of violating other requirements for the processing of personal data under § 42 I of the PDPA. The other requirements that are violated in the cases

---

<sup>39</sup> Sootak, J. (2010) *Karistusõigus. Üldosa*. Tallinn: Juura, p. 474.



of fraudulent emails come mainly from the first and second sentences of § 12 I of the PDPA. Namely, the subject whose personal data would be processed must provide, of their free will, consent for any processing activities. Furthermore, the processor of personal data must also clearly state the purpose for which the subject's personal data is collected. In the example email, the purpose for collecting personal data from the recipient is connected to the release of outrageous sums of money. The likelihood of that basis being legitimate is of course non-existent. If the recipient decides to release their information to the senders based on the bogus premise, the senders would be accountable for the misdemeanour offence. When recipients are asked for personal information and the perpetrators, in fact, manage to obtain it, the most common subsequent course of action on the part of the perpetrators has been to illegally use the identity of the unsuspecting victim to order goods or sign up for services in their name.

Three phishing emails in the sample constituted the commission of extortion according to § 214 I of the PC. Extortion is defined as the coercion of another person to transfer proprietary benefits by the use of threat to restrict the liberty of the person, disclose embarrassing information or destroy or damage property, or by use of violence. The sender threatened to disclose embarrassing videos and pictures of the recipient, unless the recipient paid USD1,200 in Bitcoin cryptocurrency within one day of having received the email. Extortion as a criminal offence has a truncated body of constituent elements, meaning that the criminal act need not, in fact, be entirely completed to hold a person accountable for its commission.<sup>40</sup> Put differently, the necessary elements of extortion were fulfilled once the sender levied the threat accompanied by a demand for proprietary value. Whether the sender ever receives the *Bitcoins* or any other proprietary benefit in relation to the specific case, is irrelevant for prosecution. Similarly, whether the sender of the email really possessed any embarrassing videos or images of the recipient bears no relevance.

Considering that the emails in the sample were collected over a period of just 30 days on two personal email accounts, the total of 3 cases of extortion, 29 attempts to commit fraud as well as ten attempts to obtain

---

<sup>40</sup> Sootak, J. (2010), *op. cit.*, p. 235.

personal information from the recipient is extensive. By comparison, there were only 74 registered cases of extortion nation-wide according to the Estonian crime statistics for 2017.<sup>41</sup> The way modern electronic communications have enabled the convergence of perpetrators and potential victims has created a startling ballooning of the number of offences committed in the course of daily life. The ease with which crimes can be committed by sending a specifically crafted email raises the age-old issue regarding the trustworthiness of registered crime statistics as the reflection of social reality. From an international perspective, when cybercrimes were first included into the crime statistics published by the *Office for National Statistics* for England and Wales in 2016, the numbers nearly doubled compared to the previous year.<sup>42</sup> The experimental statistics on fraud and computer misuse offences have mostly retained their rates since, with some decrease in the commission of computer misuse offences.<sup>43</sup> Derived from the results of the current analysis, a similar spike in crime reporting would take place in Estonia. In terms of their *modus operandi*, criminal offences are no longer in the process of moving from the physical to the digital but have already found a very comfortable home. Yet, these offences are still poorly reported by people and thus also in national statistics, which ultimately results in the obfuscation and to an extent even the downplaying of the ongoing situation. Anti-crime efforts in this specific area must turn the focus to providing people with the necessary know-how of detecting and reporting instances of email-based commission of offences. Traditional law enforcement efforts are severely hindered when it comes to cybercrime due to the speed with which these offences are committed, i.e. it only takes an email and its submission to fulfil the necessary elements of the offences analysed in the sample. With no reasonable way of interjecting traditional protective measures between the offender and victim, the latter need better tools and knowledge to protect themselves – these can be facilitated

---

<sup>41</sup> Ministry of Justice. (2017) *Kuritegevus Eestis 2017*, p.146. In Estonian. Available from: [http://www.kriminaalpolitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/kuritegevu\\_seestis\\_2017\\_veebi01.pdf](http://www.kriminaalpolitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/kuritegevu_seestis_2017_veebi01.pdf) [Accessed 5 November 2018].

<sup>42</sup> Office for National Statistics. (2017) *Crime in England and Wales: Year Ending in Dec 2016*. Available from: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingdec2016> [Accessed 5 November 2018].

<sup>43</sup> Office for National Statistics. (2018) *Crime in England and Wales: Year Ending in March 2018*. Available from: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018> [Accessed 5 November 2018].

in the form of systematic public campaigns and educational undertakings, e.g. massive open online courses (MOOCs).

## 5. CONCLUSION

This article discussed the current prevalence of email-based commission of crimes and how these offences remain largely hidden, both from the victims and thus also from national statistics. To illustrate the situation, qualitative text analysis was performed on emails (N=42) received from two email accounts as collected in a single "end-of-route" email client. The results of the criminal law analysis showed that over the course of only one month there were 3 cases of extortion, 29 attempts of fraud and 10 personal data processing related misdemeanour offences committed. Contrary to officially available national statistics, the analysis in the current article clearly showed that the real situation in cybercrime commission is much more severe and in need of immediate attention by criminal policy decision-makers. Traditional law enforcement efforts have largely failed due to the speed of crime commission in online environments. The difference between having to bear the negative consequences of email-based extortion, fraud and issues concerning personal data and securely using important modern communications environments lies with the potential victims themselves. By analysing the rates of offending as well as providing an in-depth analysis of how criminals craft their messages, the article has practical implications for decision-makers in their future crime prevention efforts. Specifically, as such efforts approach the dissemination of relevant knowledge necessary for preventing victimisation via email.

## LIST OF REFERENCES

- [1] Atkins, B. and Huang, W. (2013) A Study of Social Engineering in Online Frauds. *Open Journal of Social Sciences*, 1 (3).
- [2] Burgoon, J. K. et al. (1994) Interpersonal Deception: Accuracy in Deception Detection. *Communication Monographs*, 61.
- [3] Burgoon, J. K. et al. (2003) Detecting Deception Through Linguistic Analysis. In: Hsinchun Chen et al. (eds.). *Intelligence and Security Informatics*, Springer.
- [4] Button, M. et al. (2014) Online Frauds: Learning from Victims Why They Fall for These Scams. *Australian & New Zealand Journal of Criminology*, 47 (3).

- [5] Case no. 3-1-1-103-12. (2012) Estonian Supreme Court (Criminal Chamber), 23 November 2012.
- [6] Cromwell, C. R., Narvaez, D. and Gomberg, A. (2005) Moral Psychology and Information Ethics: The Effects of Psychological Distance on the Components of Moral Behavior in a Digital World. In: Lee Freeman and A. Graham Peace (eds.). *Information Ethics: Privacy and Intellectual Property*, Hershey, PA: IdeaGroup.
- [7] European Commission. (2017) *Special Eurobarometer 464a: Europeans' Attitudes Towards Cyber Security*.
- [8] Fluent. (2017) *The Inbox Report 2017: Consumer Perceptions of Email*.
- [9] Grazioli, S. (2004) Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception over the Internet. *Group Decision and Negotiation*, 13.
- [10] Hutchings, A. and Hayes, H. (2009) Routine Activity Theory and Phishing Victimization: Who Gets Caught in the 'Net'?. *Current Issues in Criminal Justice*, 20 (3).
- [11] Jakobsson, M. (2007) The Human Factor in Phishing. *Privacy & Security of Consumer Information*.
- [12] Jaeger, D. et al. (2016) Analysis of Publicly Leaked Credentials and the Long Story of Password (Re-)use. In: *11th International Conference on Passwords (PASS-WORDS2016)*. Germany: Springer.
- [13] Krause, M. and Kulkarni, A. (2015) Predicting Sales E-Mail Responders Using a Natural Language Model. In: *Conference on Human Computation & Crowdsourcing 2015*, San Diego, USA.
- [14] Langenderfer, J. and Shimp, T. A. (2001) Consumer Vulnerability to Scams, Swindles, and Fraud: A New Theory of Visceral Influences on Persuasion. *Psychology and Marketing*, 18.
- [15] Litmus Email Analytics. (2018) *Email Client Market Share*. Available from: <http://emailclientmarketshare.com/> [Accessed 20 November 2018].
- [16] MillerSmiles. *Phishing scam archives*. [online] Available from: <http://www.millersmiles.co.uk/archives.php> [Accessed 20 November 2018].
- [17] Ministry of Justice. (2017) *Kuritegevus Eestis 2017*. In Estonian. Available from: [http://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumentid/kuritegevuseestis\\_2017\\_veebi01.pdf](http://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumentid/kuritegevuseestis_2017_veebi01.pdf) [Accessed 5 November 2018].
- [18] Office for National Statistics. (2017) *Crime in England and Wales: Year Ending in Dec 2016*. Available from: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeand>

- justice/bulletins/crimeinenglandandwales/yearendingdec2016 [Accessed 5 November 2018].
- [19] Office for National Statistics. (2018) *Crime in England and Wales: Year Ending in March 2018*. Available from: <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2018> [Accessed 5 November 2018].
- [20] Office of Fair Trading. (2009) *The Psychology of Scams: Provoking and Committing Errors of Judgement*.
- [21] Osula, A.-M. (2015) Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data. *Masaryk University Journal of Law and Technology*, 9 (1).
- [22] *Penal Code (Karistusseadustik) 2001*. SI 2001/61, 364. Estonia: Riigi Teataja (State Gazette). In Estonian. English translation available from: <https://www.riigiteataja.ee/en/eli/509072018004/consolide> [Accessed 19 November 2018].
- [23] *Personal Data Protection Act (Isikuandmete kaitse seadus) 2007*. SI 2007/24, 127. Estonia: Riigi Teataja (State Gazette). In Estonian. English translation available from: <https://www.riigiteataja.ee/en/eli/507032016001/consolide> [Accessed 19 November 2018].
- [24] Proposal for a Directive of the European Parliament and of the Council on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA. (2017/0226) 13 September. Available from: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0489:FIN> [Accessed 20 November 2018].
- [25] Radicati Group. (2018) *Executive Summary*. Available from: <https://www.radicati.com/wp/wp-content/uploads/2018/05/Email-Market-2018-2022-Executive-Summary.pdf> [Accessed 20 November 2018].
- [26] Rajivan, P. and Gonzalez, C. (2018) Creative Persuasion: A Study on Adversarial Behaviors and Strategies in Phishing Attacks. *Frontiers in Psychology*, 135 (9).
- [27] Reyns, B. W. (2015) A Routine Activity Perspective on Online Victimization: Results from the Canadian General Social Survey. *Journal of Financial Crime*, 42 (4).
- [28] Sootak, J. (2010) *Karistusõigus. Üldosa*. Tallinn: Juura.
- [29] Strauss, A. and Corbin, J. (1998) *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks, CA: Sage Publications.
- [30] Symantec. (2018) *Internet Security Threat Report*. Available from: <https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf> [Accessed 20 November 2018].

- [31] United Nations Office on Drugs and Crime. (2013) *Draft Comprehensive Study on Cybercrime*. Available from: [https://www.unodc.org/documents/organized-crime/UNODC\\_CCPCJ\\_EG.4\\_2013/CYBERCRIME\\_STUDY\\_210213.pdf](https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf) [Accessed 20 November 2018].
- [32] Verizon. (2017) *Data Breach Investigations Report, 10th Ed.*
- [33] Vishwanath, A. et al. (2011) Why Do People Get Phished? Testing Individual Differences in Phishing Vulnerability within an Integrated, Information Processing Model. *Decision Support Systems*, 51 (3).
- [34] Williams, E. J., Beardmore, A. and Joinson, A. N. (2017) Individual Differences in Susceptibility to Online Influence: A Theoretical Review. *Computers in Human Behavior*, 72.
- [35] Williams, E. J., Hinds, J. and Joinson, A. N. (2018) Exploring Susceptibility to Phishing in the Workplace. *International Journal of Human-Computer Studies*.
- [36] Workman, M. (2008) Wisecrackers: A Theory-grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security. *Journal of the American Society for Information Science and Technology*, 59 (4).