Emory Corporate Governance and Accountability Review

Volume 8 | Issue 1

2021

Posted: No Phising

Lawrence J. Trautman

Mohammed T. Hussein

Emmanuel U. Opara

Mason J. Molesky

Shahedur Rahman

POSTED: NO PHISHING

Lawrence J. Trautman[*]
Mohammed T. Hussein[**]
Emmanuel U. Opara[***]
Mason J. Molesky[****]
Shahedur Rahman[*****]

ABSTRACT

Any engineering approach to cybersecurity must recognize that many breaches are the result of human behavior, rather than sophisticated malware. Effective cybersecurity defenses require a systematic engineering approach that recognizes the organizational, cultural and psychological barriers to effectively dealing with this problem. The U.S. Securities and Exchange Commission (SEC) defines "phishing" as, "the use of fraudulent emails and copy-cat websites to trick you into revealing valuable personal information—such as account numbers for banking, securities, mortgage, or credit accounts, your social security numbers, and the login IDs and passwords you use when accessing online financial service providers." Once this information is fraudulently obtained, it may be used to steal your identity, money, or both.

A review of the literature reveals an alarming lack of attention to the prevalent threat of low-technology, or low-complexity phishing attacks. Accordingly, here is a primer on the prominent exploit known as phishing, illustration of several cases, and the necessity for organizational and societal education of data users as to appropriate computer hygiene. Much of the

[*] BA, The American University; MBA, The George Washington University; J.D., Oklahoma City University School of Law. Mr. Trautman is Associate Professor of Business Law and Ethics at Prairie View A&M University. He is a past president of the New York and Washington/Baltimore Chapters of the National Association of Corporate Directors (NACD). He may be contacted at Lawrence.J.Trautman@gmail.com.

[**] BS, Prairie View A&M University; M.S. Texas A&M University-Kingsville (electrical engineering); Ph. D., Texas A&M University (electrical engineering). Dr. Hussein is Assistant Professor of Management Information Systems (MIS) at Prairie View A&M University. He may be contacted at mthussein@pvamu.edu.

[***] BS, University of South Alabama; MBA, University of Houston; DBA, Golden Gate University. Dr. Opara is Professor of Cyber Security-Network/Digital Forensics at Prairie View A&M University. He may be contacted at euopara@pvamu.edu.

[****] BS, Alma College (mathematics and Computer Science); M.S. (cybersecurity), Ph.D. Candidate (computer science), The George Washington University. Mr. Molesky is an adjunct professor at The George Washington University. He may be contacted at masonmolesky@gmail.com.

[*****] B. Com, University of Chittagong; M. Com, University of Chittagong; MBA, Texas A&M University. Mr. Rahman teaches Management Information Systems at Prairie View A&M University. He may be contacted at shrahman@pvamu.edu.

literature about cyberattack addresses technical aspects of computer code, encryption, and bad actor attribution. Yet human behavior remains a significant source responsible for successful cyber intrusions. Your authors believe this Article provides a valuable discussion about the human factors that very often comprise a back-door entryway into data systems.

OVERVIEW

Any engineering approach to cybersecurity must recognize that many breaches are the result of human behavior rather than sophisticated malware. Effective cybersecurity defenses require a systematic engineering approach that recognizes the organizational, cultural and psychological barriers to effectively dealing with this problem. The U.S. Securities and Exchange Commission (SEC) defines "phishing" as, "the use of fraudulent emails and copy-cat websites to trick you into revealing valuable personal information—such as account numbers for banking, securities, mortgage, or credit accounts, your social security numbers, and the login IDs and passwords you use when accessing online financial service providers."[1] Once this information is fraudulently obtained, it may be used to steal your identity, money, or both.[2]

A review of the literature reveals an alarming lack of attention to the prevalent threat of low-technology, or low-complexity, phishing attacks. Accordingly, here is a primer on the prominent exploit known as phishing, illustration of several cases, and the necessity for organizational and societal education of data users as to appropriate computer hygiene.

This Article proceeds as follows: First, we describe the escalating global cyber threat environment, and examine the high costs of data breaches. Second, we examine privacy issues. Third, we present an overview of the phishing exploit. Fourth, we discuss corporate responsibility for corrective action. Fifth, we provide a few thoughts about defensive tactics available to protect against phishing attacks. And last, we conclude. Much of the literature about cyberattack addresses technical aspects of computer code, encryption, and bad actor attribution. Yet human behavior remains a significant source responsible for successful cyber intrusions. Your authors believe this Article provides a valuable discussion about the human factors that very often comprise a back-door entryway into data systems.

I. ESCALATING GLOBAL CYBER THREAT ENVIRONMENT

> *Like their expanding user base, the data collected on Facebook users has also skyrocketed. They have moved on from schools, likes, and relationship status. Today, Facebook has access to dozens of data points, ranging from ads you've clicked on, events you've attended, and your location based on your mobile device.*

---

[1] *"Phishing" Fraud: How to Avoid Getting Fried by Phony Phishermen*, SEC (Sept. 5, 2013), https://www.sec.gov/reportspubs/investor-publications/investorpubsphishinghtm.html.

[2] *Id.*

> *It is no secret that Facebook makes money off this data through advertising revenue, although many seem confused by, or altogether unaware, of this fact. Facebook generated $40 billion in revenue in 2017, with about 98 percent coming from advertising across Facebook and Instagram.*
>
> —Senator Chuck Grassley
> Chairman, Senate Judiciary Committee
> April 10, 2018[3]

Cyber breaches and theft continue to grow at an alarming rate,[4] constituting a threat to business[5] and global stability and peace.[6] For perspective, during the most recent decade alone, RiskBased Security reports, "there were 986 reported breaches exposing 102,646,498 records in 2010. It only took two years to more than double the number of breaches—2012 jumped up to 3,335 reported breaches—and by 2016 the number of records exposed was consistently over the 5 billion mark."[7] RiskBased Security warns, "Looking ahead, we see little indication of improvement. In fact, it's quite the opposite. Low complexity phishing attacks show no sign of slowing, malware is as virulent as ever, and the black market for stolen data continues to thrive."[8] Recent key highlights for data breaches are depicted in Exhibit 1.

---

[3] *See Facebook, Social Media Privacy, and the Use and Abuse of Data: Hearing Before the S. Judiciary Comm. & the S. Com. Comm.,* 115th Cong. 1–2 (2018) (statement of Sen. Chuck Grassley, Chairman, S. Comm. on the Judiciary). *See also* Lawrence J. Trautman, *Governance of the Facebook Privacy Crisis,* 20 PITT. J. TECH. & POL'Y 41, 41–147 (2020).

[4] *See* Lawrence J. Trautman , *How Law Operates in a Wired Global Society: Cyber and E-Commerce Risk,* PROCEEDS OF THE KOREA LEGISLATION RESEARCH INSTITUTE (KLRI), 2017 LEGAL SCHOLAR ROUNDTABLE, Seoul, Korea, 21–22 Sept., 2017.

[5] *See* Lawrence J. Trautman & George P. Michaely, Jr., *The SEC and the Internet: Regulating the Web of Deceit*, 68 CONSUMER FIN. L. Q. REP. 262 (2014); Lawrence J. Trautman, *Congressional Cybersecurity Oversight: Who's Who and How It Works,* 5 J.L. & CYBER WARFARE 147 (2016).

[6] *See* Scott J. Shackelford, *The Law of Cyber Peace,* 18 CHI. J. INT'L L. 1 (2017); Scott J. Shackelford, Timothy L. Fort & Jamie D. Prenkert, *How Businesses Can Promote Cyber Peace*, 36 U. PA. J. INT'L L. 353 (2014); Scott J. Shackelford, *In Search of Cyber Peace: A Response to the Cybersecurity Act of 2012,* 64 STAN. L. REV. ONLINE 106 (2012).

[7] *2019 Year End Data Breach QuickView Report*, RISK BASED SECURITY 1, 22 (2020), https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf.

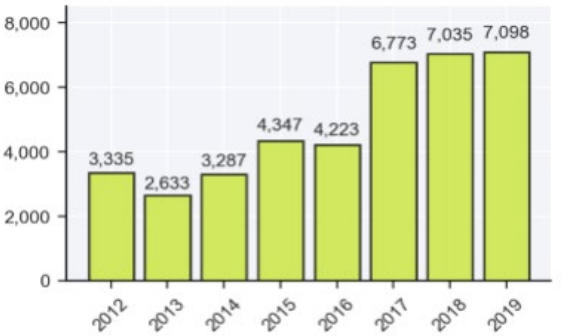
[8] *Id.*

Exhibit 1
Data Breach Key Highlights[9]

- In 2019, there were **7,098** breaches reported, exposing over **15.1 billion** records.
- The number of records exposed is [up] **284%** compared to 2018, [up] **91%** compared to 2017.
- Although the number of breaches in 2019 is only 1% higher compared to 2018, it is anticipated the gap will continue to grow throughout Q1 2020 as more 2019 incidents come to light.
- **Web** (inadvertent exposure of data online) compromised 13.5 billion records while hacking exposed 1.5 billion records. All other data types combined exposed approximately 120 million records.
- Breaches at technology providers pushed the **Information** sector to the top spot for number of breaches, followed by the **Healthcare** sector. . . .[10]

For additional perspective, RiskBased Security documents, "the number of breaches disclosed in 2019 once again hit an all-time high . . . . [while] the 2019 incident reports were still trickling in [when] this report was created. . . . Looking back at the patterns from the prior three years, we anticipate another 250–300 incidents will be added to 2019."[11] Exhibit 2 depicts the number of annual breaches reported.

Exhibit 2
Number of Breaches Reported Each Year[12]



[9] *Id.* at 4.
[10] *Id.*
[11] *Id.* at 10 (alteration in original).
[12] *Id.*

Inga Goddijn, Executive Vice President at RiskBased Security, cautions, "as we look over the experience of 2019 what stands out is that we are often our own worst enemy."[13] Weak controls and human nature appear responsible for the severity and number of 2019 breaches, "whether it's a phishing campaign that ultimately provides malicious actors with a toehold into systems or misconfigured databases and services that leave millions of sensitive records freely available on the internet . . . ."[14] Growing interest in user credentials is observed during 2019 as "Troves of username and password combinations continue to become available on forums and file sharing sites while phishing for access credentials—a perennially popular method for gaining access to systems and services—has surged in recent months, proving . . . social engineering techniques still produce results for attackers."[15] RiskBased Security reports:

> The breach at Bodybuilding.com is a prime example of this trend. In July [2018], malicious actors gained access to the company's systems thanks to a successful phishing email. Hackers were able to move about the system for approximately eight months, potentially accessing data ranging from customer names and addresses to profile details and order history.
>
> Incidents like the breach at Bodybuilding.com also explain why the Miscellaneous data type is growing. Should something like order history and customer's interests be captured in the profile of a breach event? We think so. While not as sensitive as banking details or Social Security numbers, the data can be especially useful for creating targeted phishing campaigns—so much so that organizations are beginning to warn users of the risk. Bodybuilding.com did exactly this, stating in their FAQ's to customers, *Please note that the email from Bodybuilding.com does not ask you to click on any links or contain attachments and does not request your personal data. If the email you received about this issue prompts you to click on a link, suggests you download an attachment, or asks you for information, the email was not sent by Bodybuilding.com and may be an attempt to steal your personal data.*[16]

For perspective, Exhibit 3 provides information about the top 10 data breaches of all time.

---

[13] *Data Breach QuickView Report 2019 Q3 Trends*, RISK BASED SECURITY 1, 17 (2019), https://pages.riskbasedsecurity.com/hubfs/Reports/2019/Data%20Breach%20QuickView%20Report%202019%20Q3%20Trends.pdf.

[14] *Id.*

[15] *Cyber Risk Analytics 2019 MidYear QuickView Data Breach Report*, RISK BASED SECURITY 1, 4 (2019), https://pages.riskbasedsecurity.com/hubfs/Reports/2019/2019%20MidYear%20Data%20Breach%20QuickView%20Report.pdf.

[16] *Id.*

Exhibit 3
Top 10 Breaches of All Time[17]

1. **YAHOO.** Reported breach of 3 billion records on December 14, 2016.[18]

2. **FIRST AMERICAN FINANCIAL CORPORATION.** Breach of approximately 885,000,000 real estate closing transaction records containing names, Social Security numbers, phone numbers, email and physical addresses, driver's license images, banking details, and mortgage lender names and loan numbers exposed on the Internet due to IDOR flaw.[19]

3. **FACEBOOK.** Records about 540 million Facebook users were exposed publicly on Amazon's cloud computing service.[20]

4. **YAHOO.** 2014 Breach involving 500 million records: usernames; email addresses; phone numbers; dates of birth; hashed passwords and security questions and associated answers, not reported until 2016.[21]

5. **MARIOTT/STARWOOD HOTELS.** Personal information was breached including travel schedules and passport numbers of 500 million persons.[22]

6. **FRIEND FINDER NETWORKS.** The breach impacted 412 million people (over 15 million deleted accounts) that had not been deleted.[23]

7. **MYSPACE.** Affecting 360 million people, this substantially abandoned social network only discovered this breach when these data surfaced for sale during 2016.[24]

---

[17] *Top 10 Worst Data Breaches of All Time,* PURDUE UNIV. GLOB. (Oct. 4, 2019), https://www.purdueglobal.edu/blog/information-technology/worst-data-breaches-infographic/.

[18] *Id*.

[19] *Id.*; Dell Cameron, *855 Million Records Exposed Online: Bank Transactions, Social Security Numbers, and More*, GIZMODO (May 24, 2019, 5:35 PM), https://gizmodo.com/885-million-sensitive-records-leaked-online-bank-trans-1835016235.

[20] *Top 10 Worst Data Breaches of All Time, supra* note 17.

[21] *Id.*; Nicole Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, N.Y. TIMES (Sept. 22, 2016), https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html.

[22] *Top 10 Worst Data Breaches of All Time, supra* note 17.

[23] *Id.*

[24] *Top 10 Worst Data Breaches of All Time, supra* note 17.

8. **EQUIFAX.** During 2017, 143 million people were impacted by exposure of their personal information, including: credit card numbers and credit dispute documents.[25]

9. **CAPITAL ONE.** During 2019, information including names, addresses, phone numbers, credit scores and payment histories for the period 2005–2019 were exposed.[26]

10. **HEARTLAND PAYMENT SYSTEMS.** Impacting approximately 100 million persons, their information including magnetic strip data (allowing for credit card creation) went undetected for 8 months.[27]

A. Data Breach Costs

Based on interviews of more than 500 global companies having experienced a data breach between July 2018 and April 2019, the Ponemon Institute and IBM Security depict the average cost of a data breach for these companies at: $3.92 million; a cost per record of $150; average size of a data breach at 25,575 records; and average time to identify and contain a breach at 279 days.[28] An interesting aspect of data breaches is that costs of mitigation often extend over several years. The IBM/Ponemon study reveals, "[a]bout one-third of data breach costs occurred more than one year after a data breach incident in the 86 companies [studied] . . . . an average of 67 percent of breach costs came in the first year, 22 percent accrued in the second . . . and 11 percent . . . more than two years after . . . ."[29] In addition, "[t]he loss of customer trust had serious financial consequences for the companies studied."[30] The IBM / Ponemon study warns:

> While malicious breaches were most common, inadvertent breaches from human error and system glitches were still the root cause for nearly half (49 percent) of the data breaches studied in the report. Human error as a root cause of a breach includes "inadvertent insiders" who may be compromised by phishing attacks or have their devices infected or lost/stolen. These were responsible for about one-quarter of breaches. System glitches, or inadvertent failures that could not be tied to a human action, accounted for another quarter of breaches. While less expensive than malicious attacks, system glitches and

---

[25] *Id.*

[26] *Id*.

[27] *Id.*

[28] *See* PONEMON INSTITUTE & IBM SECURITY, COST OF DATA BREACH REPORT 3 (2019), https://www.ibm.com/security/data-breach.

[29] *Id.* at 5 (alteration in original).

[30] *Id.*

> human error breaches are still costly, with an average loss of $3.24 million and $3.5 million respectively.[31]

Another finding, of particular concern to entrepreneurs, is that "small businesses face disproportionately larger costs relative to larger organizations."[32] The Ponemon Institute and IBM Security study reports, "[t]he total cost for the largest organizations (more than 25,000 employees) averaged $5.11 million, which is $204 per employee. Smaller organizations with between 500 and 1,000 employees had an average cost of $2.65 million, or $3,533 per employee."[33] Therefore, underfunded smaller organizations may encounter costs from breaches that threaten their very survival. Now, we will look at phishing: what it is; and examine several examples of this gateway to cyber theft.

B. Social Engineering Attack

The U.S. Computer Emergency Readiness Team, an organization within the Department of Homeland Security's Cyber Security and Infrastructure Security Agency, in defining a social engineering attack, states, "an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity."[34] DHS warns, "by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network . . . gather enough information from one source . . . contact another source within the same organization and rely on the information from the first source to add to his or her credibility."[35]

---

[31] *Id.* at 7.

[32] *Id.*

[33] *Id.*

[34] *Avoiding Social Engineering and Phishing Attacks, Security Tip (ST04-014)*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Nov. 15, 2019), https://www.us-cert.gov/ncas/tips/ST04-014.

[35] *Id.*

II. GROWING CYBER PRIVACY RISK FACTORS

> *Something is awry. It is true that many capitalists, including surveillance capitalists, vigorously employ these century-old justifications for their freedom when they reject regulatory, legislative, judicial, societal, or any other form of public interference in their methods of operation.*
>
> —Soshana Zuboff
> The Charles Edward Wilson Professor emerita,
> Harvard Business School, 2019[36]

A. Security Breaches, Hacking and Phishing Attacks

Of particular relevance to our inquiry into privacy issues and Russia meddling into the 2016 and 2018 U.S. elections, Facebook warns, "Security breaches and improper access to or disclosure of our data or users data, or other hacking and phishing attacks on our systems, could harm our reputation and adversely affect our business."[37]

Accordingly:

> Our industry is prone to cyber-attacks by third parties seeking unauthorized access to our data or users' data or to disrupt our ability to provide service. Any failure to prevent or mitigate security breaches and improper access to or disclosure of our data or user data, including personal information, content or payment information from users, could result in the loss or misuse of such data, which could harm our business and reputation and diminish our competitive position. In addition, computer malware, viruses, social engineering (predominantly spear phishing attacks), and general hacking have become more prevalent in our industry, have occurred on our systems in the past, and will occur on our systems in the future. We also regularly encounter attempts to create false or undesirable user accounts, purchase ads, or take other actions on our platform for purposes such as spamming, spreading misinformation, or other objectionable ends. As a result of our prominence, the size of our user

---

[36] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 497 (2019).

[37] Complaint at 7, Yuan v. Facebook, No. 3:18-cv-01725 (N.D. Cal. filed March 20, 2018). *See also* Lawrence J. Trautman & Peter C. Ormerod, *WannaCry, Ransomware, and the Emerging Threat to Corporations,* 86 TENN. L. REV. 503 (2019); Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things,* 72 U. MIAMI L. REV. 761 (2018); Lawrence J. Trautman, *Is Cyberattack the Next Pearl Harbor?,* 18 N.C. J.L. & TECH. 233 (2016); Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?,* 2015 J.L. TECH. & POL'Y 341 (2015); David D. Schein & Lawrence J. Trautman, *The Dark Web and Employer Liability,* 18 COLO. TECH. L.J. 49 (2020).

> base, and the types and volume of personal data on our systems, we believe that we are a particularly attractive target for such breaches and attacks. Such attacks may cause interruptions to the services we provide, degrade the user experience, cause users to lose confidence and trust in our products, impair our internal systems, or result in financial harm to us. . . . Cyber-attacks continue to evolve in sophistication and volume, and inherently may be difficult to detect for long periods of time. Although we have developed systems and processes that are designed to protect our data and user data, to prevent data loss, to disable undesirable accounts and activities on our platform, and to prevent or detect security breaches, we cannot assure you that such measures will provide absolute security, and we may incur significant costs in protecting against or remediating cyber-attacks.
>
> In addition, some of our developers or other partners, such as those that help us measure the effectiveness of ads, may receive or store information provided by us or by our users through mobile or web applications integrated with Facebook. . . .
>
> Affected users or government authorities could initiate legal or regulatory actions against us in connection with any security breaches or improper disclosure of data, which could cause us to incur significant expense and liability or result in orders or consent decrees forcing us to modify our business practices. Such incidents may also result in a decline in our active user base or engagement levels. Any of these events could have a material and adverse effect on our business, reputation, or financial results.[38]

B. Growth of Transnational Criminal Actors and Phishing

Transnational organized crime during recent years, "has added new lines of business, including industrial espionage and cyber theft to their long-standing lines of business staples such as blackmail, the drug trade, and prostitution."[39] Much of the growth in transnational organized crime during recent years has been attributed by former BBC journalist Misha Glenny, "to the downfall of the Soviet Union, which resulted in thousands of former KGB and Eastern European intelligence officers seeking new employment in rather unsavory occupations, primarily in the highly profitable illicit drug trade."[40] Consider the impact on political stability resulting from breaches of secrecy (think Snowden,[41] The

---

[38] Complaint at 7, *Yuan* (No. 3:18-cv-01725).

[39] Lawrence J. Trautman, *How Google Perceives Customer Privacy, Cyber, E-Commerce, Political and Regulatory Compliance Risks,* 10 WM. & MARY BUS. L. REV. 1, 12 (2018).

[40] *Id.*

[41] *See* Jonah Force Hill, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Business Leaders,* The Hague Inst. For Glob. Just. (2014).

Panama Papers,[42] and Russian hacking of elections in the United States and many other countries).[43]

A particular exploit that often results from phishing is "carding;" described by the FBI as, "criminal activities associated with stealing personal identification information and financial information belonging to other individuals—including the account information associated with credit cards, bank cards, debit cards, or other access devices—and using that information to obtain money, goods, or services without the victims' authorization or consent."[44]

III. THE PHISHING EXPLOIT

> *We assess Russian intelligence services will continue to develop capabilities to provide Putin with options to use against the United States, judging from past practice and current efforts. Immediately after Election Day, we assess Russian intelligence began a spearphishing campaign targeting US Government employees and individuals associated with US think tanks and NGOs in national security, defense, and foreign policy fields. This campaign could provide material for future influence efforts as well as foreign intelligence collection on the incoming administration's goals and plans.*
>
> —James Clapper
> Director of National Intelligence
> January 10, 2017[45]

A. What is Phishing?

DHS's Cybersecurity and Infrastructure Security Agency defines phishing as, "a form of social engineering. . . . [which often] use email or malicious

---

[42] *See* Lawrence J. Trautman, *How Google Perceives Customer Privacy, Cyber, E-Commerce, Political and Regulatory Compliance Risks,* 10 WM. & MARY BUS. L. REV. 1, 12 (2018) (citing Lawrence J. Trautman, *Following the Money: Lessons from the "Panama Papers," Part 1: Tip of the Iceberg*, 121 PENN ST. L. REV. 807 (2017)).

[43] *See* Lawrence J. Trautman, *Impeachment, Donald Trump and the Attempted Extortion of Ukraine,* 40 PACE L. REV. (2020); Lawrence J. Trautman, *Presidential Impeachment: A Contemporary Analysis*, 44 U. DAYTON L. REV. 529 (2019).

[44] Lawrence J. Trautman, *Managing Cyberthreat,* 33 SANTA CLARA HIGH TECH. L.J. 230, 245 (2017).

[45] *ODNI Statement on Declassified Intelligence Community Assessment of Russian Activities and Intentions in Recent U.S. Elections: Hearing Before the S. Intel. Comm.*, 115th Cong. (2017) (statement of James Clapper, Director of National Intelligence). *See also* OFF. DIR. NAT'L INTELL., BACKGROUND TO "ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS": THE ANALYTIC PROCESS AND CYBER INCIDENT ATTRIBUTION (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem."[46] Then, "[w]hen users respond with the requested information, attackers can use it to gain access to the accounts."[47] Unfortunately:

> Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as:
> - Natural disasters (e.g. Hurricane Katrina, Indonesian tsunami);
> - Epidemics and health scares (e.g., H1N1, COVID-19);
> - Economic concerns (e.g., IRS scams);
> - Major political elections; and
> - Holidays.[48]

Phishing can take many forms in an effort to deceive vulnerable users and gain access to sensitive information. One of the most common forms that most organizations and citizens are exposed to is phishing emails. Email attacks are usually composed of generic greetings, urgent phrases and some links that users are instructed to click on.[49] These emails are crafted in a way that appears to be from prominent and reliable resources such as Human Resources, which places users at a higher risk. Therefore, it is imperative for all online users to become more educated about the patterns of phishing emails and common features. Users are encouraged to disregard emails that ask for sensitive information such as date of birth, social security number, bank account number, etc.

Through data mining, companies can predict what products and services the user is most likely to purchase. If the user fails to check the web browser privacy settings, these companies can gain access to their internet search patterns, cookies, and email content from free email services. Users are encouraged to reach out to their technology department when these emails start to percolate in their inboxes.

In addition to alarming emails, phishing also takes place in many social media platforms as it often resides on one of the most used online platforms. The

---

[46] *Security Tip (ST04-014), Avoiding Social Engineering and Phishing Attacks*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Aug. 25, 2020), https://us-cert.cisa.gov/ncas/tips/ST04-014 (alteration in original).

[47] *Id.*

[48] *Id.*

[49] *Id.*

pattern of phishing through social media accounts are still very similar to the ones hackers use in emails. Hackers tend to send fake massages sourced from the user's friends' list, where they ask for sensitive information including bank accounts and financial matters. For users to dodge these phishing emails, they should always recognize suspicious patterns and never respond or provide any sensitive information through emails or texts. Another defense is available by installing anti-malware and anti-virus software to strengthen account protection and other data residing on a user's computer. These steps will contribute to flagging illegal hacking activities and preventing users from falling into such traps.

Kenneth D. Nguyen, Heather Rosoff and Richard S. John write, "Researchers are keenly aware that humans are the weakest link in the cyber security chain."[50] Although, "the security of any cyber infrastructure mostly depends on the participation of users to practice self-protective information security behavior. Nevertheless, getting users to participate in safe online behavior is a significant challenge."[51] As is reasonable, "studies have shown that internet users are very concerned about the privacy and security of their information, many users are willing to provide access to their private information in exchange for financial gain and convenience."[52] Nguyen, Rosoff and John contend, "This suggests that even though information security is an important priority, internet users are willing to make security compromises to achieve other goals."[53]

---

[50] Kenneth D. Nguyen, Heather Rosoff & Richard S. John, *Valuing Information Security from a Phishing Attack*, 3 J. CYBERSECURITY 159 (2017) (*citing* Iván Arce, *The Weakest Link Revisited* [information security], 1 IEEE SEC. & PRIV. 72-76 (2003)); M.A. Sasse, S. Brostoff & D. Weirich, *Transforming the 'Weakest Link' – A Human/Computer Interaction Approach to Usable and Effective Security,* 19 BT TECH. J. 122–31 (2001).

[51] Nguyen, et al., *supra* note 50 (*citing* S.M. Furnell, A. Jusoh & D. Katsabas, *The Challenges of Understanding and Using Security: A Survey of End-Users*, 25 COMPUTS. & SEC. 27 (2006)).

[52] *Id*. (*citing* C. Papoutsi, J. Reed, C. Marston, R. Lewis, A. Majeed & D. Bell, *Patient and Public Views About the Security and Privacy of Electronic Health Records (EHRS) in the UK: Results from a Mixed Methods Study,* 15 BMC MED. INFORMATICS DECISION MAKING 86 (2015)); Oscar H. Gandy Jr., *Public Opinion Surveys and the Formation of Privacy Policy,* 59 J. SOC. ISSUES 283 (2003); R. Gross & A. Acquisti, *Information Revelation and Privacy in Online Social Networks, in* PROCEEDINGS OF 2005 ACM WORKSHOP ON PRIV. ELECT. SOC., 71 WPES (2005); TrustArc 2016, 2016 TRUSTe/NCSA Consumer Privacy Infographic – GB Edition (illustration); Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESAERCH CTR (2014), https://www.pewresearch.org/internet/2014/11/12/public-privacy-perceptions/; Bob Tedeschi, *E-Commerce Report; Everybody Talks About Online Privacy, But Few Do Anything About It,* N.Y. TIMES, June 3, 2002, at C6; M. Glassman, M. Vandenwauver & L. Tam, *The Psychology of Password Management: A Tradeoff Between Security and Convenience,* 29 BEHAV. & INFO. TECH. 233 (2010).

[53] *Id.*

Akamai warns, "phishing is a long-term, socially based problem, impacting multiple market segments and people from all walks of life each day."[54] Typically, "criminals use phishing to target the retail industry by masquerading as popular brands and retail outlets. The individuals who fall for phishing scams by submitting information, or those who inadvertently install malicious applications, are the same people who contribute to a billion-dollar retail economy worldwide."[55] The SEC explains it this way:

> When fraudsters go on "phishing" expeditions, they lure their targets into a false sense of security by hijacking the familiar, trusted logos of established, legitimate companies. A typical phishing scam starts with a fraudster sending out millions of emails that appear to come from a high-profile financial services provider or a respected Internet auction house.
>
> The email will usually ask you to provide valuable information about yourself or to "verify" information that you previously provided when you established your online account. To maximize the chances that a recipient will respond, the fraudster might employ any or all of the following tactics:
>
> > **Names of Real Companies**—Rather than create from scratch a phony company, the fraudster might use a legitimate company's name and incorporate the look and feel of its website (including the color scheme and graphics) into the phishy email.
> > **"From" an Actual Employee**—The "from" line or the text of the message (or both) might contain the names of real people who actually work for the company. That way, if you contacted the company to confirm whether "Jane Doe" truly is "VP of Client Services," you'd get a positive response and feel assured.
> > **URLs that "Look Right"**—The email might include a convenient link to a seemingly legitimate website where you can enter the information the fraudster wants to steal. But in reality the website will be a quickly cobbled copy-cat—a "spoofed" website that looks for all the world like the real thing. In some cases, the link might lead to select pages of a legitimate website—such as the real company's actual privacy policy or legal disclaimer.
> > **Urgent Messages**—Many fraudsters use fear to trigger a response, and phishers are no different. In common phishing scams, the emails warn that failure to respond will result in your no longer having access to your account. Other emails might claim that the company has detected suspicious activity in your account or that it is implementing new privacy software or identity theft solutions.[56]

---

[54] *Phishing –Baiting the Hook,* 5 State of the Internet / Security, Akamai 1, 2 (2019), https://www.akamai.com/fr/fr/multimedia/documents/state-of-the-internet/soti-security-phishing-baiting-the-hook-report-2019.pdf.

[55] *Id.*

[56] *"Phishing" Fraud: How to Avoid Getting Fried by Phony Phishermen,* U.S. SEC. AND EXCH. COMM'N

B. Spear Phishing

Sanchari Das et al. observe, "Spear phishing is the most common and effective type of phishing, as it focuses on specific individuals, using personal information about its victims. Spear phishing emails may address users by their real name(s) or reference uniquely identifiable information obtained through social engineering techniques."[57] Das et al. warn:

> Spear phishing is successful because attackers manipulate their targets, either by luring users by promising them specific benefits or by coercing users with specific threats. These manipulation techniques often lead to impulsive or quick decision making from the end users. One of the most common phishing motivations is the promise of financial benefits to the intended victim. Gao et al. found that many malicious websites attempt to attract users via money or product offers. Attackers often attempt to have users click on their website to earn a free product—such as an iPhone or video game system—or to obtain job prospects, such as working online.[58]

Inga Goddijn, Executive Vice President at RiskBased Security observes, "The practice of targeting employee email accounts hit new heights in 2019. It was a scenario that played out in a similar manner across different industries and organizations of all sizes. Attackers used phishing emails or click bait to lure users into giving up access to their email account."[59] According to Ms. Goddijn, "Once in, malicious actors were free to explore the content and contacts of the account holder. These events can be time-consuming, resource-intensive incidents to remediate. The breach at Children's Hope Alliance (CHA) illustrates just how challenging it can be to sort through the aftermath of this type of intrusion."[60] We have included the timeline for the Children's Hope Alliance (CHA) attack at Exhibit 4. In this one example, it took "134 days from discovery to finally being able to alert those that may have had their data accessed by attackers. Or in other words, Children's Hope Alliance spent one third of the year in response to 27 days of unauthorized access to emails."

(Sept. 5, 2013), https://www.sec.gov/reportspubs/investor-publications/investorpubsphishinghtm.html. *See also* Neal Newman & Lawrence J. Trautman, Securities Law: Overview and contemporary Issues, http://ssrn.com/abstract=3790804; Lawrence J. Trautman, Seletha Butler, Frederick Chang, Michele Hooper, Ron McCray & Ruth Simmons, Corporate Directors: Who They Are, What They Do, Cyber and Other Contemporary Challenges, http://ssrn.com/abstract=3792382.

[57] Sanchari Das, Andrew Kim, Zachary Tingle & Christena Nippert-Eng, *All About Phishing Exploring User Research Through a Systemic Literature Review, in* Proceedings of the Thirteenth Int'l Symp. on Human Aspects of Info. Sec. & Assurance (HA/SA 2019), http://ssrn.com/abstract=3438203.

[58] *Id.* (internal citations omitted).

[59] *RISK BASED SECURITY, supra* note 7.

[60] *Id.*

Exhibit 4
Timeline of Children's Hope Alliance Incident[61]

> April 23, 2019 – Unauthorized access to CHA email accounts begins;
> May 15, 2019 – CHA became aware of suspicious activity on one account and launches an investigation;
> May 20, 2019 – All compromised accounts secured; work gets underway on determining what information was contained in emails;
> July 20, 2019 – CHA confirmed that compromised accounts held sensitive data;
> August 1, 2019 – CHA begins notifying business partners who may have provided the sensitive data to Children's Hope; a list of potentially affected individuals is created, but it requires substantial de-duplication and is missing addresses for notification;
> September 10, 2019 – Contact list is clean and ready to use; [and]
> September 26, 2019 – CHA begins mailing notification letters to affected persons.[62]

C. Barbarians at the Gate Array

Exhibit 5 presents a contemporary example of a successful fraudulent phishing scheme that successfully resulted in more than $120 million being funneled to bank accounts located in vast parts of the globe.[63] Evaldas Rimasauskas was arrested in March 2017 for successfully targeting multinational internet companies from the other side of the globe. Rimasauskas targeted multinational internet companies and "tricked their agents and employees into wiring over $100 million to overseas bank accounts under his control."[64] The acting U.S. Attorney, Joon H. Kim, stated, "This case should serve as a wake-up call to all companies−even the most sophisticated−that they too can be victims of phishing attacks by cyber criminals."[65]

---

[61] *Id.*

[62] *Id.* (alteration in original).

[63] Press Release, U.S. Dep't of Just., Lithuanian Man Sentenced to 5 Years in Prison for Theft of over $120 Million in Fraudulent Business Email Compromise Scheme (Dec. 19, 2019), https://www.justice.gov/usao-sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business.

[64] Press Release, U.S. Dep't of Just., Lithuanian Man Arrested for Theft of over $100 Million in Fraudulent Email Compromise Scheme Against Multinational Internet Companies, (Mar. 21, 2017), https://www.justice.gov/usao-sdny/pr/lithuanian-man-arrested-theft-over-100-million-fraudulent-email-compromise-scheme.

[65] *Id*.

Exhibit 5
Lithuanian Man Sentenced to 5 Years in Prison for Theft of Over $120 Million in Fraudulent Business Email Compromise Scheme[66]


United States Department of Justice

THE UNITED STATES ATTORNEY'S OFFICE
SOUTHERN DISTRICT of NEW YORK

HOME ABOUT PRIORITIES NEWS RESOURCES PROGRAMS EMP

U.S. Attorneys » Southern District of New York » News » Press Releases

Department of Justice

U.S. Attorney's Office

Southern District of New York

SHARE

FOR IMMEDIATE RELEASE Thursday, December 19, 2019

Lithuanian Man Sentenced To 5 Years In Prison For Theft Of Over $120 Million In Fraudulent Business Email Compromise Scheme

Geoffrey S. Berman, the United States Attorney for the Southern District of New York, announced that EVALDAS RIMASAUSKAS, a Lithuanian citizen, was sentenced today to 60 months in prison for participating in a fraudulent business email compromise scheme that induced two U.S.-based Internet companies (the "Victim Companies") to wire a total of over $120 million to bank accounts he controlled. RIMASAUSKAS previously pled guilty to one count of wire fraud before U.S. District Judge George B. Daniels, who imposed today's sentence.

U.S. Attorney Geoffrey S. Berman said: "Evaldas Rimasauskas devised an audacious scheme to fleece U.S. companies out of more than $120 million, and then funneled those funds to bank accounts around the globe. Rimasauskas carried out his high-tech theft from halfway across the globe, but he got sentenced to prison right here in Manhattan federal court."

[66] Press Release, U.S. Dep't of Just., Lithuanian Man Sentenced to 5 Years in Prison for Theft of over $120 Million in Fraudulent Business Email Compromise Scheme (Dec. 19, 2019), https://www.justice.gov/usao-sdny/pr/lithuanian-man-sentenced-5-years-prison-theft-over-120-million-fraudulent-business.

According to the allegations in the Indictment to which RIMASAUSKAS pled guilty, court filings, and statements made in public court proceedings:

From at least in or around 2013 through in or about 2015, RIMASAUSKAS orchestrated a fraudulent scheme designed to deceive the Victim Companies, including a multinational technology company and a multinational online social media company, into wiring funds to bank accounts controlled by RIMASAUSKAS. Specifically, RIMASAUSKAS registered and incorporated a company in Latvia ("Company-2") that bore the same name as an Asian-based computer hardware manufacturer ("Company-1"), and opened, maintained, and controlled various accounts at banks located in Latvia and Cyprus in the name of Company-2. Thereafter, fraudulent phishing emails were sent to employees and agents of the Victim Companies, which regularly conducted multimillion-dollar transactions with Company-1, directing that money the Victim Companies owed Company-1 for legitimate goods and services be sent to Company-2's bank accounts in Latvia and Cyprus, which were controlled by RIMASAUSKAS. These emails purported to be from employees and agents of Company-1, and were sent from email accounts that were designed to create the false appearance that they were sent by employees and agents of Company-1, but in truth and in fact, were neither sent nor authorized by Company-1. This scheme succeeded in deceiving the Victim Companies into complying with the fraudulent wiring instructions.

After the Victim Companies wired funds intended for Company-1 to Company-2's bank accounts in Latvia and Cyprus, RIMASAUSKAS caused the stolen funds to be quickly wired into different bank accounts in various locations throughout the world, including Latvia, Cyprus, Slovakia, Lithuania, Hungary, and Hong Kong. RIMASAUSKAS also caused forged invoices, contracts, and letters that falsely appeared to have been executed and signed by executives and agents of the Victim Companies, and which bore false corporate stamps embossed with the Victim Companies' names, to be submitted to banks in support of the large volume of funds that were fraudulently transmitted via wire transfer.

Through these false and deceptive representations over the course of the scheme, RIMASAUSKAS, the defendant, caused the Victim Companies to transfer a total of over $120,000,000 in U.S. currency from the Victim Companies' bank accounts to Company-2's bank accounts.

RIMASAUSKAS was arrested by Lithuanian authorities in March 2017, pursuant to a provisional arrest warrant, and was extradited to the Southern District of New York in August 2017.

* * *

In addition to the prison term, Judge Daniels ordered RIMASAUSKAS to serve two years of supervised release, to forfeit $49,738,559.41, and to pay restitution in the amount of $26,479,079.24.

D. Romanian Online Organized Crime Ring

In another case, the U.S. Department of Justice (DOJ) reported, "according to court documents unsealed [on February 7, 2019], 20 people, including 16

foreign nationals, have been charged for their roles in an international organized crime group that defrauded American victims through online auction fraud causing millions of dollars in losses."[67] Assistant Attorney General Benczkowski states, "the defendants allegedly orchestrated a highly organized and sophisticated scheme to steal money from unsuspecting victims in America and then launder their funds using cryptocurrency."[68] In July 2018, a federal grand jury sitting in Lexington, Kentucky charged 15 foreign nationals with RICO conspiracy, wire fraud conspiracy, money laundering conspiracy, and aggravated identity theft in a 24-count indictment.[69] Just a few months later, a Lexington Kentucky grand jury, returned an 11-count indictment charging an additional foreign national and four Americans for their roles in the criminal enterprise. The DOJ reports:

> The indictment alleges that these defendants participated in a criminal conspiracy primarily located in Alexandria, Romania that engaged in a large-scale scheme of online auction fraud. Specifically, Romania-based members of the conspiracy and their associates posted false advertisements to popular online auction and sales websites—such as Craigslist and eBay—for high-cost goods (typically vehicles) that did not actually exist. According to the indictment, these members would convince American victims to send money for the advertised goods by crafting persuasive narratives, for example, by impersonating a military member who needed to sell the advertised item before deployment. The members of the conspiracy are alleged to have created fictitious online accounts to post these advertisements and communicate with victims, often using the stolen identities of Americans to do so. They are alleged to have delivered invoices to the victims bearing trademarks of reputable companies in order to make the transactions appear legitimate. Once victims were convinced to send payment, the indictment alleges that the conspiracy engaged in a complicated money laundering scheme wherein domestic associates would accept victim funds, convert these funds to cryptocurrency, and transfer proceeds in the form of cryptocurrency to foreign-based associates. The indictment alleges that these foreign-based money launderers . . . exchanged cryptocurrency into local fiat currency on

---

[67] Press Release, U.S. Dep't of Just., United States and International Law Enforcement Dismantle Online Organized Crime Ring Operating out of Romania that Victimized Thousands of U.S. Residents (Feb. 7, 2019) (alteration in original), https://www.justice.gov/opa/pr/united-states-and-international-law-enforcement-dismantle-online-organized-crime-ring.

[68] *Id. See also* Lawrence J. Trautman, *Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J.L. & TECH. 13 (2014) (discussing the use of virtual currencies for money laundering and payment from illicit activities).

[69] U.S. Dep't of Just., *supra* note 67.

> behalf of the Romania-based members of the conspiracy, knowing that they were exchanging bitcoin that represented the proceeds of fraud.[70]

The DOJ stated that, "[Defendant] Adrian Mitan, who was charged in the July 5, 2018 indictment, was also charged in a separate indictment unsealed [February 7, 2019] with money laundering offenses arising from a credit card phishing and brute-force attack scheme, likewise designed to steal money from Americans."[71] As explained in the indictment, "phishing is an attempt to acquire personal information by masquerading as a trustworthy entity through electronic communications, and a brute force is a cryptological trial-and-error methodology used to obtain information such as personal identification numbers for credit cards."[72] The DOJ reports:

> [The defendant] allegedly phished for credit/debit card information of U.S. customers, hacked into the electronic systems of American businesses, and then conducted a brute force attack on their point-of-sale systems for the purpose of stealing the remaining credit/debit card information. According to the indictment, [the defendant] then directed American money launderers to create "dummy" credit/debit cards with the stolen information, which were used to extract money from the customers' accounts. These fraudulent proceeds were then returned to [the defendant] in the form of bitcoin.[73]

While each defendant maintains a presumption of innocence until proven guilty beyond a reasonable doubt in a court of law, the DOJ provides the following discussion and analysis of potential sentencing ramifications if found guilty:

> For the RICO conspiracy and wire fraud conspiracy charges, each defendant faces up to 20 years in prison, a fine of $250,000, and three years of supervised release. The same penalties apply to the money laundering conspiracy charges, except that the fine may be up to $500,000. Additionally, if convicted of identity theft, Brown faces a term of 15 years in prison, a fine of $250,000, and three years of supervised release, and if convicted of aggravated identity theft, those charged face a mandatory-minimum sentence of two years in prison, to be served consecutive to any term of imprisonment ordered for the

---

[70] *Id. See also* Lawrence J. Trautman & Alvin C. Harrell, *Bitcoin Versus Regulated Payment Systems: What Gives?*, 38 CARDOZO L. REV. 1041 (2017); Lawrence J. Trautman & Mason J. Molesky, *A Primer for Blockchain*, 88 UMKC L. REV. 239 (2019); Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?*, 69 CONSUMER FIN. L. Q. REP. 232 (2016) (discussing blockchain and virtual currencies).

[71] U.S. Dep't of Just., *supra* note 67 (alteration in original).

[72] *Id.*

[73] *Id.* (alteration in original).

> other counts of conviction. However, any sentence following a conviction would be imposed by the Court, after its consideration of the U.S. Sentencing Guidelines and the federal statutes.[74]

Next, we discuss another 2019 example of a transnational online criminal enterprise employing phishing emails, the GozNym network.

E. GozNym Cyber-Criminal Network

On May 16, 2019, the DOJ announced that "A complex transnational organized cybercrime network that used GozNym malware in an attempt to steal an estimated $100 million from unsuspecting victims in the United States and around the world has been dismantled as part of an international law enforcement operation."[75] According to the DOJ, "The spamming operations involved the mass distribution of GozNym malware through 'phishing' emails. The phishing emails were designed to appear legitimate to entice the victim recipients into operating the emails and clicking on a malicious link or attachment, which facilitated the downloading of GozNym onto the victims' computers."[76] In a cooperative effort by law enforcement agencies in Bulgaria, Georgia, Germany, Moldova, Ukraine, along with Europol and Eurojust, numerous criminal prosecutions have been brought. The DOJ reports, "GozNym infected tens of thousands of victim computers worldwide, primarily in the United States and Europe."[77] According to the Indictment, the defendants conspired to:

> - infect victims' computers with GozNym malware designed to capture victims' online banking login credentials;
> - use the captured login credentials to fraudulently gain unauthorized access to victims' online bank accounts; and,
> - steal money from victims' bank accounts and launder those funds using U.S. and foreign beneficiary bank accounts controlled by the defendants.
>
> The defendants reside in Russia, Georgia, Ukraine, Moldova and Bulgaria. The operation was an unprecedented international effort to share evidence and initiate criminal prosecutions against members of the same criminal network in multiple countries. . .

---

[74] *Id.*

[75] Press Release, U.S. Dep't of Just., *GozNym Cyber-Criminal Network Operating out of Europe Targeting American Entities Dismantled in International Operation* (May 16, 2019), https://www.justice.gov/opa/pr/goznym-cyber-criminal-network-operating-out-europe-targeting-american-entities-dismantled.

[76] *Id.*

[77] *Id.*

> Five of the named defendants reside in Russia and remain fugitives from justice. However, to overcome the inability to extradite the remaining defendants to the United States for prosecution, an unprecedented effort was undertaken to share evidence and build prosecutions against defendants in the remaining countries where they reside, including Georgia, Ukraine and Moldova. The prosecutions are based on shared evidence acquired through coordinated searches for evidence in Georgia, Ukraine, Moldova and Bulgaria, as well as from evidence shared by the United States and Germany from their respective investigations.
>
> The GozNym network exemplified the concept of "cybercrime as a service." According to the Indictment, the defendants advertised their specialized technical skills and services on underground, Russian-language, online criminal forums. The GozNym network was formed when these individuals were recruited from the online forums and came together to use their specialized technical skills and services in furtherance of the conspiracy. . .
>
> Victims of the GozNym malware attacks include:
>
> An asphalt and paving business located in New Castle, Pennsylvania;
> A law firm located in Washington, DC;
> A church located in Southlake, Texas;
> An association dedicated to providing recreation programs and other services to persons with disabilities located in Downers Grove, Illinois;
> A distributor of neurosurgical and medical equipment headquartered in Freiburg, Germany, with a U.S. subsidiary in Cape Coral, Florida;
> A furniture business located in Chula Vista, California;
> A provider of electrical safety devices located in Cumberland, Rhode Island;
> A contracting business located in Warren, Michigan;
> A casino located in Gulfport, Mississippi;
> A stud farm located in Midway, Kentucky; and
> A law office located in Wellesley, Massachusetts.[78]

F. Common Indicators of Phishing Attempts

The CISA provides the following description about some of the common indicators of phishing attempts:

- **Suspicious senders address.** The sender's address may imitate a legitimate business. Cybercriminals often use an

---

[78] *Id.*

email address that closely resembles one from a reputable company by altering or omitting a few characters.

- **Generic greetings and signature.** Both a generic greeting—such as "Dear Valued Customer" or "Sir/Ma'am"—and a lack of contact information in the signature block are strong indicators of a phishing email. A trusted organization will normally address you by name and provide their contact information.
- **Spoofed hyperlinks.** If you hover your cursor over any links in the body of the email, and the links do not match the text that appears when hovering over them, the link may be spoofed. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). Additionally, cybercriminals may use a URL shortening service to hide the true destination of the link.
- **Spelling and layout.** Poor grammar and sentence structure, misspelling, and inconsistent formatting are other indicators of a possible phishing attempt. Reputable institutions have dedicated personnel that produce, verify, and proofread customer correspondence.
- **Suspicious attachments.** An unsolicited email requesting a user download and open an attachment is a common delivery mechanism for malware. A cybercriminal may use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first.[79]

G. Frauds Against Senior Citizens

Phishing emails targeting the elderly are among the greatest threats to online information security for their ability to exploit the trust and naivety of senior citizens. Studies shows that senior citizens fall prey to the breaches and attacks because the bad actors consider the group as soft targets.[80] As much as we understand that all age groups are equally vulnerable to on-line frauds, it can be assumed that the elderly are more prone to these attacks. The reason might be that most of the senior citizen group, retirees, widows, and lonely grandparents, have their online data unprotected and are easily accessible by bad actors.[81]

---

[79] *See Avoiding Social Engineering and Phishing Attacks*, *supra* note 34.

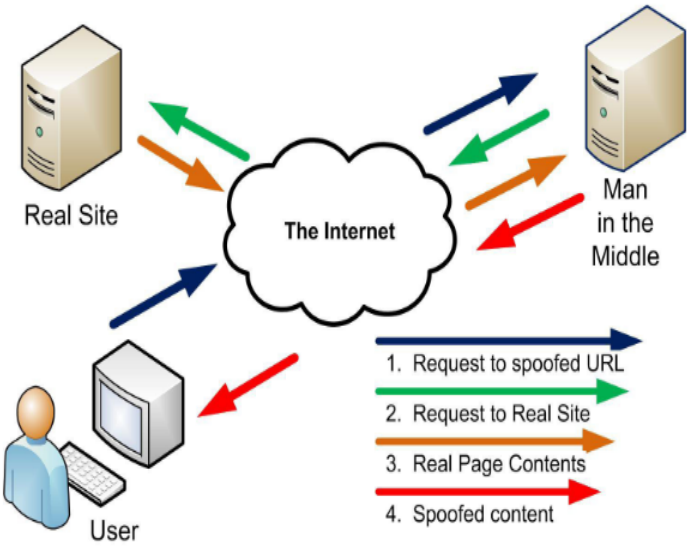
[80] Rui Zhao, Samantha John, Stacy Karas, Cara Bussell, Jennifer Roberts, Daniel Six, Brandon Gavett & Chuan Yue, *The Highly Insidious Extreme Phishing Attacks, in* 25th International Conference on Computer Communications and Networks (2016), https://ieeexplore.ieee.org/document/7568582; *see also* Ibrahim Alseadoon, M.F.I. Othman & Taizan Chan, *What Is the Influence of Users' Characteristics on Their Ability to Detect Phishing Emails?*, *in* ADVANCED COMPUT. & COMMC'N ENG'G TECH. 949, 962 (2015).

[81] *See* Stacey Wood, Benjamin Rakela, Pi-Ju Liu, Adria E. Navaro, Susan Bernatz, Kathleen H. Wilber,

When the elderly are hacked through phishing and spear-phishing activities, adverse financial and emotional loss often results.

The constantly changing accessibility of technology results in more successful phishing attacks.[82] Most of the elderly are unwilling to use complex passwords or learn how to strengthen them, perhaps because they feel it is too much of a hassle to remember long and difficult passwords. Those age 65 and older are more likely to report a tech scam, and less likely to report retail-related scams, especially when financial loss is involved.[83] Senior citizens can be exploited thru Man-in-the-middle / Man-in-the-Browser attack. This is a technical network attack where the spoofed web site is a part of a man-in-the-middle / man-in-the browser attack. When seniors visit a site, they are redirected to a false wireless access point or Domain Name System [DNS] posing as shown in Exhibit 6.

Exhibit 6
Man-in-the-Middle Attack on Elderly-Senior Citizens[84]



Robin Allen & Diana Homeier, *Neuropsychological Profiles of Victims of Financial Elder Exploitation at the Los Angeles County Elder Abuse Forensic Center*, 26 J. ELDER ABUSE & NEGLECT 414 (2014).

[82] Brandon E. Gavett, Rui Zhao, Samantha E. John, Cara A. Bussell, Jennifer R. Roberts & Chuan Yue, *Phishing Suspiciousness in Older and Younger Adults: The Role of Executive Functioning*, 2017 PLoS ONE 1.

[83] *See* Zhao et. al., *supra* note 80.

[84] *Phishing: A Primer on What Phishing is and How it Works,* DIGICERT (2009), https://www.digicert.com/news/DigiCert_Phishing_White_Paper.pdf.

Research suggests that bad actors may target the elderly because they are often naïve, inexperienced with computers, and potentially more willing to listen to others.[85] Most of the attacks are conducted thru spear-phishing activities.[86] In other situations, the bad actors attack the vulnerable senior citizen thru fraudulent bank transfers. The bad actors accomplish this by picking disposed deposit slips that were erroneously thrown away at the bank's dustbin. The elderly also leave acknowledgement slips around. This has been a potential gold mine for the bad actors.

Exhibit 7
Example of a Phishing Home Page[87]

Exhibit 7 illustrates a phishing generating homepage on the Amazon phishing website that presents the same content that is displayed on a legitimate Amazon website.[88] Another example of a Deep-Level Phishing Web Page is presented as Exhibit 8.[89] These sites look real and are very deceiving to senior citizens because they can be generated and presented to the elderly in real time.

---

85 *See* Gavett, et al., *supra* note 72.
86 *See* Das, et al., *supra* note 57 (defining spear-phishing).
87 Gavett, et al., *supra* note 82, fig.1.
88 *Id.*
89 *See* Gavett, et al., *supra* note 82, fig.2.

Exhibit 8
Another Example of a Phishing Home Page[90]

H. Protecting Senior Citizens

Senior citizens can reduce the chance of falling victim to phishing attacks by being sensitive and smart while browsing the net and checking their emails. They should question and avoid unnecessary clicking on links, download files or opening attachments in email or social media, even if it appears legitimate from a known trusted source. Seniors should also be sensitive to emails requesting confidential information such as personal information and banking details. The Bad actors use "Fake" sites to steal personal data or perform a drive-by-download attack. Hackers employ these drive-by-download attacks by targeting unsuspecting networks or computers and downloading malicious codes to such computers or networks. The bad actors compromise breached websites and embed malicious elements inside the sites. Unsuspecting Senior citizens while browsing a web page that has been infected can activate the exploit, which happens in the background and without the user's knowledge or consent.

---

90 *Id.*

The FBI's common scheme webpage reports that senior citizens are one of the most likely groups in society to get hacked or scammed.[91] Formerly known as the American Association of Retired Persons, the AARP reports that older Americans are scammed out of billions of dollars each year.[92] Many senior citizens who grew-up during the 1930s, 1940s, or 1950s were raised to trust people. During that time, technology was not as abundant or ubiquitous as it is now. Thus, many senior citizens are not properly and adequately trained to this generation's reliance on technology. Con artists are also attracted to seniors because they often have near perfect credit scores.

Furthermore, when seniors are targeted, they are less likely to realize quickly, nor report the theft accurately to officials. Con artists take advantage of elders' often poor health conditions, since these elderly victims are likely not able to report fraud incidents or advocate for themselves passionately and vigorously because, "Con artists know the effects of age on memory, and they are counting on elderly victims not being able to supply enough detailed information to investigators."[93] The FBI's website reports:

> Older Americans are less likely to report a fraud because they don't know who to report it to, are too ashamed at having been scammed, or don't know they have been scammed. Elderly victims may not report crimes, for example, because they are concerned that relatives may think the victims no longer have the mental capacity to take care of their own financial affairs.[94]

Seniors should be aware of suspicious emails especially those with typos, words in capital and exclamation marks. Examples are 'Dear Customer' or Dear Sir/Madam' salutations. Threats and urgent deadlines are suspicious and should be investigated. Awareness to browse securely with HTTPs is very important. This can be indicated by https:// and a security "lock" icon in the browser's address bar. Before sending credit information, ensure that the above protocol is in the address bar.[95] The following are signs that a phishing attack is underway: when an email has unofficial "From" address, when an urgent action is required, when linked to a fake web site on a browser, and when the Web address looks

---

[91] *See Elder Fraud*, FBI, https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/seniors (last visited Jan. 5, 2021) [hereinafter Scams and Safety].

[92] Katherine Skiba, *Older Americans Hit Hard by Financial Fraud,* AARP (Feb. 28, 2019), https://www.aarp.org/money/scams-fraud/info-2019/cfpb-report-financial-elder-abuse.html.

[93] *Senior Citizens: Fraud Targets*, NATIONAL CAREGIVERS LIBRARY, http://www.caregiverslibrary.org/Featured/Consumer-Protection/Fraud-Target-Senior-Citizens (last visited Jan. 5, 2021) (*citing* Scams and Safety, *supra* note 91).

[94] *See* Scams and Safety*, supra* note 91.

[95] *See* Wood, et al., *supra* note 81.

suspicious.[96] Experts recommend preventing against phishing attacks by using a web browser with anti-phishing detection.[97]

IV. CORPORATE RESPONSIBILITY FOR CORRECTIVE ACTION

> *Undoubtedly, the decision to notify law enforcement of a cyber-attack and to cooperate fully in an investigation involves a certain risk-reward calculation weighing the anticipated benefits of a pro-active approach against potential legal, reputational, and other costs.*
>
> —Rod Rosenstein
> Deputy Attorney General
> October 30, 2017[98]

A. Corporate Duties of Loyalty and Care

In a corporate setting, "officers and directors have two primary duties to shareholders: a duty of loyalty (no self-dealing); and a duty of care (a duty to behave reasonably). We now present a brief discussion of the corporate director's primary duties of loyalty and care.

B. Duty of Loyalty

In sum, the duty of loyalty, under Delaware law, requires, "that there shall be no conflict between duty and self-interest."[99] Breaches of the duty of loyalty do not result per se from conflicts of interest. It is the manner in which directors handle conflicts (full disclosure to the board, and solicitation of board determination whether the conflict disqualifies the director from proceeding to vote on related matters) that is required, "to ensure fairness to the corporation and its stockholders that will determine the propriety of the director's conduct . . . ."[100]

---

[96] Mathias J. Klenk, Phishing Attack Prevention: Best 10 Ways to Prevent Email Phishing Attacks, GBHACKERS (Sept. 9, 2019), https://gbhackers.com/phishing-attacks-prevention/.

[97] *Id.*

[98] Rod J. Rosenstein, Deputy Att'y Gen., U.S. Dep't of Just., Remarks at the 2017 North American International Cyber Summit (Oct. 30, 2017).

[99] *See* Lawrence J. Trautman, Mohammed T. Hussein, Louis Ngamassi & Mason J. Molesky, *Governance of the Internet of Things (IoT)*, 60 JURIMETRICS 319 (2020) (citing Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 28 J. MARSHALL J. COMPUT. & INFO. L. 313 (2011).

[100] *Id.* (citing Byron Egan, *Director Duties: Process and Proof*, TEXASBARCLE WEBCAST: CORPORATE MINUTES/DIRECTOR DUTIES (Oct. 23, 2008)).

C. Duty of Care

One of your authors has observed elsewhere, every director's legal duty of care requires "a careful, diligent approach to the effective discharge of their individual duties and responsibilities."[101] In a corporate setting, phishing exploits may be characterized as a foreseeable risk, potentially resulting in catastrophic crisis for the organization.[102] Perceived by bad actors as easy targets, recent examples of phishing exploits leading to data systems being held hostage over ransomware demands have reached crisis levels for hospitals, municipalities and educational institutions.[103] Fiduciary duties and the duty of care are also applicable to the governance requirements of directors in a nonprofit setting.[104] Effective corporate governance requires that the Nominating and Governance Committees recruit directors who have experience, and understand both information technology and matters related to cybersecurity risk.[105] In addition, board audit committees are well advised to have cyber expertise on the committee to enable better committee comprehension of cyber vulnerabilities.[106] A good example of how corporate boards struggle to keep pace with rapid technological change may be found in the experience of PayPal.[107]

D. Ormerod-Trautman Cybersecurity Model

Elsewhere Professors Ormerod and Trautman present a way to think about the management of cybersecurity, The Profit-Maximizating Model of Security, in Exhibit 9.[108]

---

[101] *See* Lawrence J. Trautman, *The Board's Responsibility for Crisis Governance,* 13 HASTINGS BUS. L.J. 275, 282 (2017).

[102] *Id.* at 287.

[103] Trautman & Ormerod, *supra* note 37, at 510 (depicting numerous examples of ransomware attacks).

[104] *See* Lawrence J. Trautman & Janet Ford, *Nonprofit Governance: The Basics*, 52 AKRON L. REV. 971 (2018).

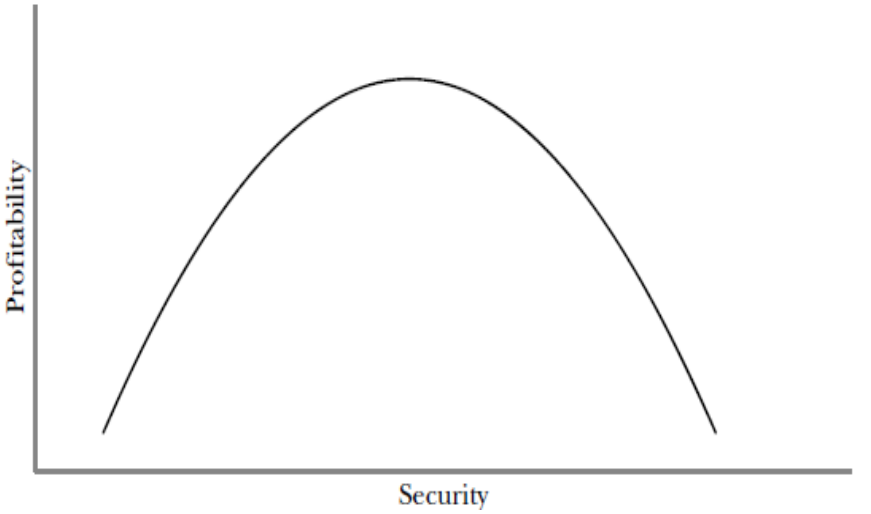
[105] Lawrence J. Trautman, *The Matrix: The Board's Responsibility for Director Selection and Recruitment,* 11 FLA. ST. U. BUS. REV. 75 (2012).

[106] Lawrence J. Trautman, *Who Qualifies as an Audit Committee Financial Expert Under SEC Regulations and NYSE Rules?*, 11 DEPAUL BUS. & COMM. L.J. 205 (2013).

[107] Lawrence J. Trautman, *E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from PayPal,* 16 U.C. DAVIS BUS. L.J. 261 (2016)*; see also* Lawrence J. Trautman, *Bitcoin, Virtual Currencies, and the Struggle of Law and Regulation to Keep Pace*, 102 MARQ. L. REV. 447 (2018).

[108] Lawrence J. Trautman & Janet Ford*, supra* note 104, at 1033.

Exhibit 9
The Ormerod-Trautman Profit-Maximizing Model of Security[109]



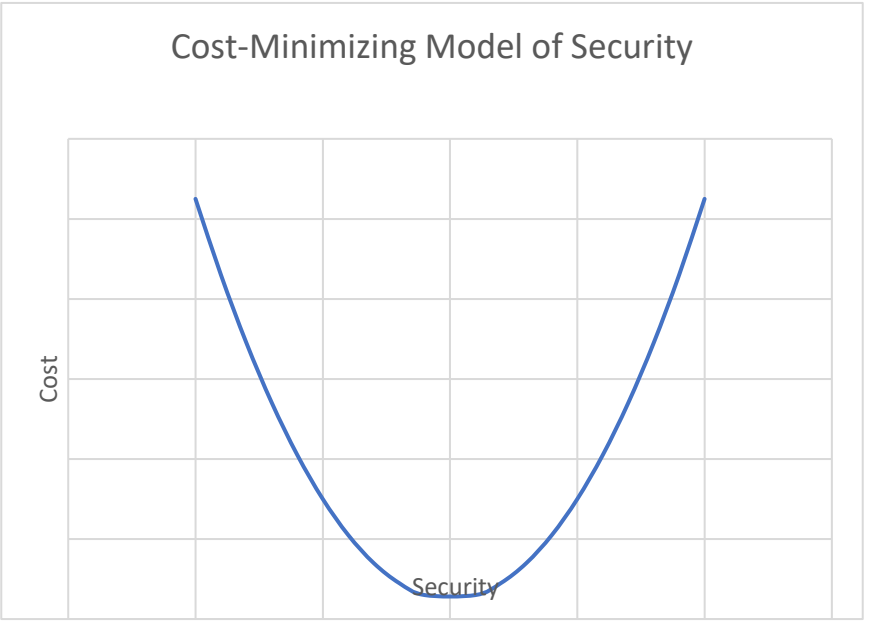
Note that at the leftmost point on the curve, enterprise data security is so abysmal that few, if any, users trust the enterprise with their Personally Identifiable Information (PII), therefore rendering the profitability or efficiency of the enterprise's data security function a nullity. To paraphrase, zero security measures, as shown at the bottom left-hand side of the graph, result in zero users and, therefore zero profitability (efficiency). But, as the enterprise security improves an increasing number of users trust the enterprise with their PII, and the risk of data breach and loss of users' PII decreases, both of which contribute to increased profitability (efficiency). At a point where the number of users is maximized, increased security measures (spending on cybersecurity) result in limiting the usability of the data/website and thus decrease profitability (efficiency). Thus, taken to an extreme, excessive security measures may theoretically drive usability to the point of futility, achieving no additional benefit from the next dollar spent on cybersecurity and decreasing utility of additional spend. For nonprofits, the Ormerod-Trautman Model can be rephrased to illustrate the "cost-minimizing" level of security, as shown in Exhibit 10.[110]

---

[109] *Id.*

[110] Lawrence J. Trautman & Janet Ford, *supra* note 104, at 1034.

Exhibit 10
Ormerod-Trautman
Cost-Minimizing Model of Security



On the left, as Professor Ormerod explains, "[C]yber services are costly due to the threat of litigation and penalties; on the right, cyber services are costly because they are prohibitively difficult to use and cost money to generate / host. This re-conception allows nonprofits and governments to express security within the confines of a dollar amount."[111] The critical takeaway is that little or no digital security may be just as damaging to an enterprise's financial health as implementing overly excessive security. Professors Trautman and Ormerod further observe:

> As this area of the law develops and matures in the coming years, courts, regulators, shareholders, and commentators will increasingly view the relationship between data security and [enterprise efficiency] as described in [Exhibits 5 and 6 herein]. Perhaps the most important implication of embracing the relationship depicted in the [Ormerod-Trautman model] is that there is a profit-maximization [or cost effective] amount of security. And, as this view of the relationship between security and profitability is embraced, there can be little doubt

[111] *Id.*

> that the various constituencies of stakeholders will increasingly expect corporate officers and directors to actively seek their company's profit-maximizing level of data security.[112]

V. PROTECTING YOURSELF FROM PHISHING

How can you best protect yourself from fraudulent and phony phishers? The SEC suggests that the best approach "is to understand what legitimate financial service providers and respectable online auction houses will and will not do. Most importantly, legitimate entities will not ask you to provide or verify sensitive information through a non-secure means, such as email."[113]

A. Recommended Action Steps

Here is a list of five simple steps that individuals can take to protect against phishing exploits. Organizations should seek to educate all their employees to the dangers posed by this problem. Accordingly, the SEC recommends:

1. **Pick Up the Phone to Verify**—Do not respond to any emails that request personal or financial information, especially ones that use pressure tactics or prey on fear. If you have reason to believe that a financial institution actually does need personal information from you, pick up the phone and call the company yourself—using the number in your rolodex, not the one the email provides!
2. **Do Your Own Typing**—Rather than merely clicking on the link provided in the email, type the URL into your web browser yourself (or use a bookmark you previously created). Even though a URL in an email may look like the real deal, fraudsters can mask the true destination.
3. **Beef Up Your Security**—Personal firewalls and security software packages (with anti-virus, anti-spam, and spyware detection features) are a must-have for those who engage in online financial transactions. Make sure your computer has the latest security patches, and make sure that you conduct your financial transactions only on a secure web page using encryption. You can tell if a page is secure in a couple of ways. Look for a closed padlock in the status bar and see that the URL starts with "https" instead of just "http."
4. **Read Your Statements**—Don't toss aside your monthly account statements! Read them thoroughly as soon as they arrive to make sure that all transactions shown are ones that

---

112 Lawrence J. Trautman & Janet Ford, *supra* note 104, at 1034–35.

113 *See* "Phishing," *supra* note 1.

> you actually made, and check to see whether all of the transactions that you thought you made appear as well. Be sure that the company has current contact information for you, including your mailing address and email address.
> 5. **Spot the Sharks**—Visit the website of the Anti-Phishing Working Group at www.antiphishing.org for a list of current phishing attacks and the latest news in the fight to prevent phishing. There you'll find more information about phishing and links to helpful resources.[114]

The SEC recommends that you "always act quickly when you come face to face with a potential fraud, especially when if you've lost money or believe your identity has been stolen."[115] In particular:

> - **Phishy Emails**—If a phishing scam rolls into your email box, be sure to tell the company right away. You can also report the scam to the FBI's Internet Fraud Complaint Center at www.ic3.gov. If the email purports to come from the Securities and Exchange Commission, alert the SEC by submitting a tip online at https://denebleo.sec.gov/TCRExternal/disclaimer.xhtml.
> - **Identity Theft**—If you think that your personal information has been stolen, visit the Federal Trade Commission's feature on Identity Theft at www.consumer.ftc.gov/features/feature-0014-identity-theft for information on how to control the damage.
> - **Securities Scams**—Before you do business with any investment-related firm or individual, do your own independent research to check out their background and confirm whether they are legitimate. For step-by-step tips and links to helpful websites, please read Check Out Brokers and Advisers and SIPC Exposes Phony "Look-Alike" Web Site. Report investment-related scams to the SEC using our online Complaint Center.[116]

B. Ease of Usernames and Passwords Access

While on the subject of organizational and self-protection of access credentials, we believe that all should learn lessons from the following valuable insights. While observing that the top data types compromised are email addresses, usernames and passwords, RiskBased Security discusses the

---

114 *Id.*
115 *Id.*
116 *Id.*

September 12, 2019 disclosure, "that Zynga, the company behind Words with Friends had been hacked. The attack exposed data on millions of players including names, phone numbers and login information. Much had been said and written about the need to strengthen passwords in recent years."[117] What did the Zynga data reveal? Unfortunately, as disclosed in Exhibit 11, an analysis of the breach's top 10 passwords:

> shows that there has been very little movement away from weak, easy to guess passwords. In fact, 'password' came in at the top spot, followed by ubiquitous number sequences. The presence of 'words' in the #6 spot is disheartening. Not only is it a weak choice, it is taken directly from the name of the service.[118]

Exhibit 11
Top 10 Passwords in the Zynga Breach[119]

10. changeme
9. 12345
8. qwerty
7. 12345678
6. words
5. 123123123
4. 123456
3. 1234567
2. 123456789
1. password

117 *See* RISK BASED SECURITY, *supra* note 7.
118 *Id.*
119 *Id.*

CONCLUSION

Phishing has become a rising phenomenon in the current era, especially with the advent of modern technology. It can take many forms such as suspicious links and fraudulent emails that potentially lead to theft of valuable personal information such as bank accounts, social security, and important passwords used to access personal items. It is rather alarming that reviewed literature reveals a lack of attention to the prominent threat of phishing attacks. Hence, some steps have been recommended to prevent the exploits of phishing attacks, such as identity verification, increasing security, and thoroughly reading statements. It is the goal of this review to shed some light on the threat of phishing attacks and grant it some of the attention that it deserves.

Keywords: computer hygiene, congressional oversight, constitutional law, consumer surplus, corporate governance, crisis, cyber security, data mining, Definers, duties of loyalty and care, ethics, Facebook, fake news, FTC, Google, GozNym attack, hacking, Internet, national security, Ormerod-Trautman Cybersecurity Model, phishing, privacy, risk management, Russian election meddling, security breaches, social engineering attack, social media, spear phishing, surveillance capitalism, terrorism

JEL Classifications: D72, D74, G32, G34, J15, K00, K10, K11, K12, K13, K20, K36, K49, L82, L86, M3, M31, M37, M38, N32, N34, O34, O35, Z10