UDC 621.3.049.77–048.24:537.2

EMAIL PHISHING: STRUCTURE AND DISTINGUISHING FEATURES

Bychek M.N.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Borbotko T.V. – Dr. Tech. Sc., full professor, head of the department of information security

Annotation. The term “phishing” is a type of cyber-attack where the attacker sends fraudulent emails, then asks the user to follow an embedded link, where the user is asked to enter private information. As a social engineering attack, a phishing attack causes huge financial losses to the recipients. A study of social engineering techniques that are used in email phishing has been conducted. Human feelings have been identified, which are used by cyberattackers to have a stronger impact on a person. Parts of emails containing the main signs of phishing have been identified.

Keywords. Phishing emails, social engineering, cyberattack.

Introduction. On the Internet, the term phishing is used to designate different types of cyberattacks, including social engineering, DNS phishing, content injection phishing, etc. It doesn’t matter which method of phishing is used, the objective is to steal user’s personal information or money. Technological advancements have led to more sophisticated phishing techniques being used. If attackers are unable to obtain additional data from a single source, they employ a new technique based on previous data to amass a sufficient amount of information from victims. According to a study conducted by the University of Maryland, an assault happens every 39 seconds on average.

An attacker employ social engineering techniques to entice a victim into clicking a link that is attached in the email that links to a fake website. It is common for attackers to pose as genuine companies or well-known individuals when sending phishing emails. The Federal Trade Commission defines phishing as online fraud that targets customers by sending them an email that looks to be from a well-known source. The attackers can be posing as an Internet service provider, financial institution, or mortgage agency.

Attackers have traditionally carried out phishing over email networks, but currently, attackers are exploiting a number of communication channels. These communications can be sent via email, phone, social media messaging (such as Facebook, Instagram or Twitter), or even text messages. Because of the increase in the number of digital platforms for online users, many attackers are updating their approaches and continually have new communication networks through which to interact with their victims.

Phishing has developed into a global danger that comes in many different shapes and sizes. When attackers mix phishing techniques with additional attack approaches, they create a unique sort of phishing attack. This “pseudo-phishing” has become more sophisticated in recent years, and it is now targeting a larger audience. As much as companies try to guard against them, phishing attempts are often successful because they target the weakest links in an organization, which are its employees. According to KnowBe4, phishing is the primary method behind 90 percent of cyberattacks, hacks, and data breaches [1].

Main part. Email is one of the most popular ways for phishing attacks to be distributed. In fact, email is thought to be the source of 96 percent of phishing attacks. However, phishing attacks have recently changed from basic phishing to spear phishing, as the success rate of spear- phishing attacks is higher than that of basic phishing, with 35 percent of people having encountered spear phishing and 65 percent having faced Business Email Compromise (BEC) attacks. BEC attacks use real or impersonated business email accounts to defraud employees. Malware distribution via phishing emails is a popular technique used by cybercriminals.

According to ESET’s Threat Survey, the most popular types of malicious files attached to phishing emails in the third quarter of 2020 were Windows executables (74 percent), script files (11 percent), and Office documents (5 percent). According to FAU experts, 78 percent of people are aware of the dangers of clicking unknown links in emails.

The most common channel for communication is email because many organizations or individuals prefer email to communicate with their customers or others. Emails are used to quickly transmit information to a large number of individuals, or even just one.

The most important advantage of email is that it allows users to keep a record of user correspondence. To date, more than half of the country such as United States uses email for communication, and that number is steadily increasing.

Usually, people are more vulnerable to social engineering tricks than technology attack. It is possible to fix technical weaknesses by adding extra security measures, but it is much more difficult to fix human flaws [2].

The following are a few examples of the most prevalent social engineering techniques used by attackers to conduct phishing attacks:

– Greed. It is possible for hackers to trick their victims into accepting monetary prizes by sending them emails or SMS messages that claim to reward them with prize. Here’s an example: “Congratulations! You’ve been chosen as the lucky winner of the year, and to collect your prize you must click a link or provide information for award shipment.” It is common for victims to feel that anything presented to them would be useful or reliable. As a result, the victim’s credentials are stolen by attackers, and the reward is never granted.

– Urgency. This type of phishing email contains a strict deadline, implying that the victim must act quickly before it is too late. As a result, it generates a sense of urgency, and many victims believe that the situation is temporary, so they act without thinking about it. Here’s an example: “Your account is about to expire, and you must sign in immediately to avoid losing all of your data.” Taking action without thinking about it is the most common human error.

– Fear. In phishing emails, scaring recipients is a common tactic. An attacker threatens a victim with negative consequences or punishment, or the victims are treated suspiciously. Here’s an example: “Your insurance has been denied due to insufficient information. To submit your information, please click here.”

– Helpfulness. Everyone has a natural desire to help others, but attackers take advantage of this and send out an email asking for assistance while displaying a tragic tale. Here’s an example: “As you may be aware, many people are dying of starvation as a result of the COVIC-19 pandemic, and we are forming a charitable organization to help them. So, if you’re willing to help, please send XYZ to this account. It would be beneficial to them, and God will assist you.” The victim’s contribution does not benefit those in need, and it allows criminals to engage in more cybercrime.

– Curiosity. Typically, attackers gather some important or interesting news online and seduce victims by providing only a portion of the information. Here’s an example: “Greetings, I’m sure you’ve heard about the plane crash that killed all of the passengers and crew members. As a result, to learn more about this information, click the link below.” Many victims are interested in learning more about the accident and follow the link to learn more. The link directs victims to a fake news site where they must enter their credentials, or it may install malware on their computers.

– Trust. Social engineers build a trust relationship with the target primarily because people can only be deceived when they trust social engineers otherwise they not share sensitive information with them. Once the trust is developed the collection of information is easier and faster. They information can be collected directly or indirectly. This type is not so popular, because it needs time and close contact between phisher and victim [3].

Figure 1 shows some of the common emotions tapped by social techniques attackers.

According to Statista, the worldwide user base for email reached 3.9 billion in 2019 and is expected to reach 4.3 billion by 2023. According to a report from PhishMe research, 91 percent of cyberattacks rise with a phishing emails, with the top reasons people are tricked by phishing emails being curiosity (13.7 percent), fear (13.4 percent), and urgency (13.2 percent), supported by the prize, social, entertainment, and opportunity [4].

Despite that phishing emails resemble legitimate emails, they have some distinct characteristics that can be called typical.

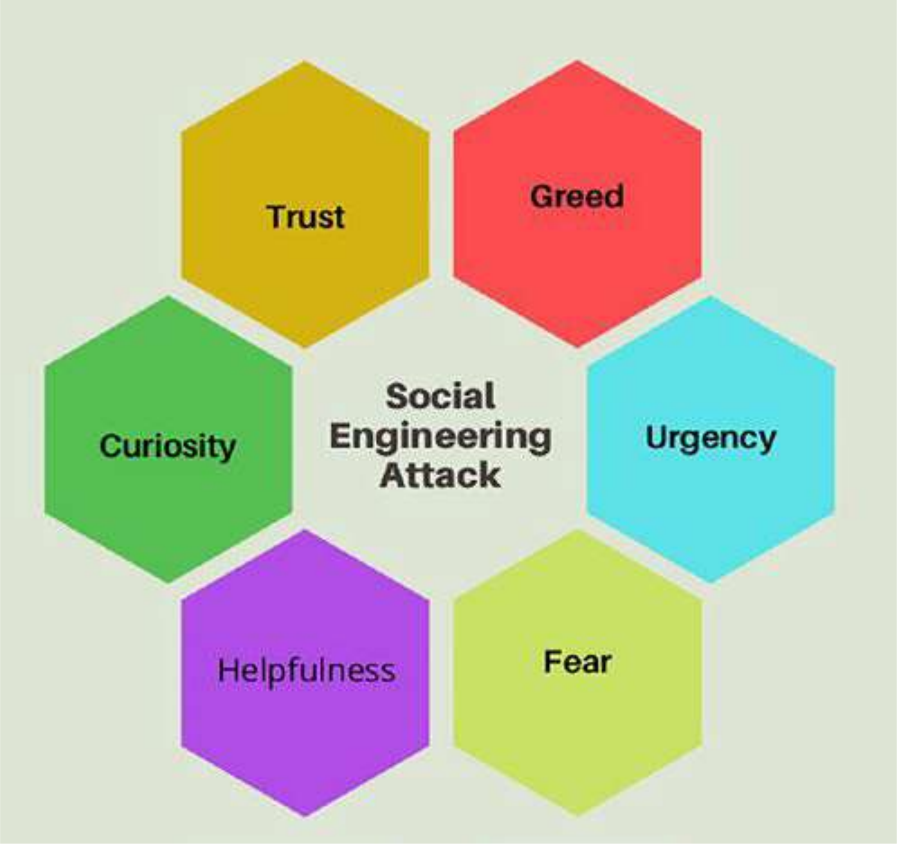


Figure 1 – Social engineering attack emotions

1. Domain Spoofing. The email domain is the part of the email address after the @ symbol. It enables a company or individual to create an email address with a company name that incorporates their company or brand name. For sending and receiving emails, most legitimate organizations and businesses have their own domain. Domain spoofing is a common type of phishing in which attackers impersonate a company or one of its employees by using the company's domain.

2. Social Engineering Statements. Phishing email is a type of social engineering statement that includes things such as lucrative offers or eye-catching or attention-getting statements. The purpose of using social engineering statements in phishing emails is to gain the victim's trust and request personal information such as credit card numbers, account numbers, or passwords.

3. Hyperlink Attachments. Initially, the attacker targets legitimate websites and impersonates them to create a phishing site. If the attacker pastes the phishing URL directly into the email, the victims will quickly recognize it. As a result, attackers use a hyperlink to hide the phishing link within the email.

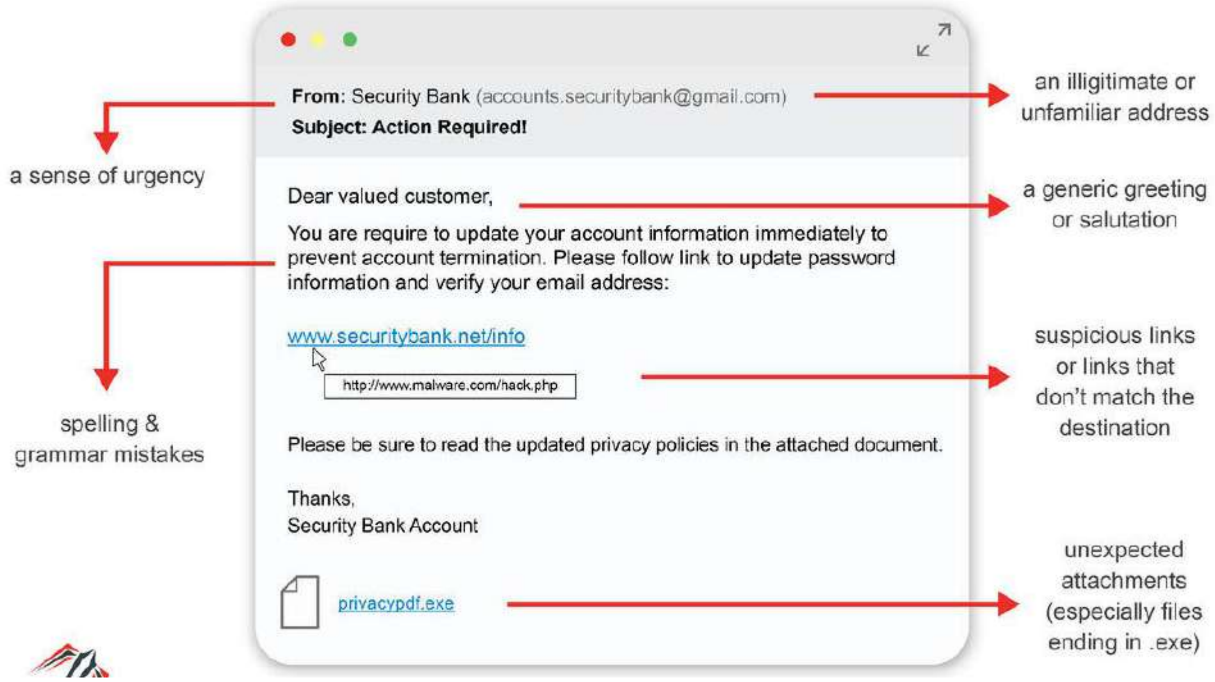
4. Unexpected Attachments. A malware attachment sent via a phishing email is a common technique for attackers. An example of this type of attachment is a keylogger that monitors keyboard strokes through pattern recognition and other techniques. In other words, whatever is typed by the user is sent to the attacker's server. Some extremely dangerous file types have the extensions .bat, .exe, .vbs, .com, .ade, .adp, .cpl, .wsc, and many more.

5. Poor Spelling and Grammar. People nowadays use software spell-checkers to prevent spelling and grammar errors. In addition, businesses hire experts to edit the contents of emails so that recipients can understand them. This means that legitimate emails will usually not contain any errors. Grammar errors and spelling mistakes are two of the most common features of phishing emails. Because the attackers are not accomplished authors, they likely will write emails that contain minor errors.

6. Generic Greeting or Salutation. Because phishing emails are sent to random consumers, the attackers do not address the recipients by name—especially if the email contains account information

or other sensitive information. Although phrases like dear client and user may appear honest, a nonpersonalized greeting is usually an indication of trouble [5].

Figure 2 shows an example of a phishing email, with the different parts explained.



From: Security Bank (accounts.securitybank@gmail.com)
Subject: Action Required!

Dear valued customer,

You are require to update your account information immediately to prevent account termination. Please follow link to update password information and verify your email address:

www.securitybank.net/info

http://www.malware.com/hack.php

Please be sure to read the updated privacy policies in the attached document.

Thanks,
Security Bank Account

privacypdf.exe

a sense of urgency
spelling & grammar mistakes
an illigitimate or unfamiliar address
a generic greeting or salutation
suspicious links or links that don't match the destination
unexpected attachments (especially files ending in .exe)

Figure 2 – Phishing email example

Today, the market offers many different anti-phishing applications and filters. But, nevertheless, a certain number of phishers find their victims. And the most successful solution to this problem is still the awareness and suspicion of electronic mail users.

Conclusion. Phishing emails have been found to contain social engineering statements, hyperlinks, and unexpected attachments in order to trick users into clicking the phishing link. It was revealed that the main feelings influenced by phishers are greed, urgency, fear, helpfulness, curiosity and trust. Also different parts of the email were also examined to identify signs of phishing. They are: illegitimate addresses, generic greetings, grammar mistakes, links that don't match the destination, suspicious attachments and so on.

References

1. Fette, I. Learning to Detect Phishing Emails / I. Fette, N. Sadeh, A. Tomasic // World Wide Web Conference Committee (IW3C2). 2007, May 8–12, 2007, Banff, Alberta, Canada.

2. Phishing and Communication Channels. A Guide to Identifying and Mitigating Phishing Attacks / Gunikhan Sonowal – Apress, 2022. – 230 p. – ISBN-13: 978-1-4842-7744-7

3. Stojnic, T. Phishing email strategies: Understanding cybercriminals' strategies of crafting phishing emails. / T. Stojnic, D. Vatsalan, NAG. Arachchilage // Security and Privacy. – 2021 – Vol. 4, Issue 5. – DOI: https://doi.org/10.1002/spy2.165

4. Analysis of phishing emails / L. Burita, P. Matoulek, K. Halouzka and P. Kozak // AIMS Electronics and Electrical Engineering – 2021. – Vol. 5, Issue 1. – Pp. 93–116.

5. Drake, Ch. Anatomy of a Phishing Email / Ch. Drake, J. Oliver, E. Koontz // CEAS 2004 - First Conference on Email and Anti-Spam, July 30-31, 2004.