Contemporary Studies in Applied Sciences; Vol. 1, No. 1; 2024
ISSN 2810-9953
Published by July Press

A Pilot Study to Assess the Success Rate of Email Scams by Phishing: Case in Lebanon

Hasan Fayyad-Kazan[1], Hussin J. Hejase[2], Christy D. Darwish[3] & Ale J. Hejase[4]

[1] Computer Science & Engineering Department, Kuwait College of Science & Technology, Kuwait City, Kuwait

[2] IEEE Senior Member; Basic and Applied Sciences Research Center, Al Maaref University, Beirut, Lebanon

[3] Master's Student, Forensic Sciences, Faculty of Sciences I, Lebanese University, Beirut, Lebanon

[4] Adnan Kassar School of Business (AKSOB), Lebanese American University, Beirut, Lebanon

Correspondence: Hussin J. Hejase, Adnan Kassar School of Business (AKSOB), Lebanese American University, Beirut, Lebanon. E-mail: hussin.hejase@mu.edu.lb

Received: July 27, 2024 Accepted: September 2, 2024 Online Published: September 17, 2024

doi:10.20849/csas.v1i1.1453 URL: https://doi.org/10.20849/csas.v1i1.1453

Abstract

Nowadays, almost everyone with internet access has an email address. That has made it easier for individuals and companies to properly store data, buy and sell products, communicate with others, entertainment, and many more. Phishing is one of the highest cybersecurity risks; it is a process where an attacker poses as a legitimate individual or institution and contacts an individual or a group of individuals by phone calls, messages, or emails to lure them into performing specific actions such as sending their sensitive information; credit card information or log in details, by clicking on malicious links or attachments. This research aims to assess the success rate of email scams by phishing. The study uses targeted email phishing by applying the phishing tool Zphisher, creating fake phishing emails, and sending them to 15 Lebanese participants. Findings demonstrated that the likelihood of Lebanese users clicking on suspicious links found in emails is about 53%, and surprisingly 13.3% of the participants fell for the entire attack. This shows that Lebanese people are constantly aware of the harmful techniques that hackers are using to reach for and steal personal information. The findings benefit policymakers and practitioners in organizations to keep track of and mitigate cyber risks by phishing. Higher education institutions (HEIs) and other Lebanese institutions must offer specialized training to students and employees alike to raise cybersecurity knowledge that could affect business-sensitive information.

Keywords: Email, phishing, links, cyberattacks, victims, Lebanon, internet

1. Introduction

Nowadays, Internet users enjoy the benefits of significant advancements in technology. However, users are threatened, constantly and aggressively, by attackers attempting to steal their information (Li and Liu, 2021; Hejase, Fayyad-Kazan, Hejase, et al., 2021). A method facilitating the attacks is through email phishing which consists of designated and deceitful messages that plan to convince users to tap on malicious links or attachments or transfer their sensitive information (Vayansky and Kumar, 2018). Organizations are increasingly under threat from attackers attempting to infiltrate their computer systems by exploiting the behavior of human users (Sasse et al., 2001; Jang-Jaccard and Nepal, 2014; Hejase, Fayyad-Kazan, & Moukadem, 2020).

These kinds of attacks are characterized by being low cost, fast, and effective; making them more appealing to perform on citizens of different cultures and people of different ages. Therefore, phishing is a principal part of numerous digital assaults and is utilized as an initial step in different types of digital attacks (Alkhalil, Hewage, Nawaf, et al., 2021). Several factors affect the phishing results like age, occupation, and the amount of email checks daily. Some previous survey-based studies showed that many people all over the world are increasingly at risk of falling for email phishing and losing all their sensitive information (Pompon, Walkowski, Boddy, et al., 2018; Hewage, 2020; Karmakar and Bhatia, 2022).

Based on the above, this work was stimulated using a pilot study involving end-users to fill a significant research gap in the context of Lebanon and the continuous rise of phishing incidents among the diversity of institutions in

Lebanon. Therefore, this research is carried out to test the susceptibility of citizens in this developing country to email phishing, especially since Lebanon is going through current aggressive economic and financial difficulties (Rkein, Hejase, Rkein, et al., 2022a, b). In addition, the study uses targeted email phishing by applying the phishing tool Zphisher, creating fake phishing emails, and sending them to a sample of Lebanese participants.

This paper has five sections. The second section starts with a review related to work on phishing and focuses on phishing mediums, types of attacks, tools, and international scenarios. The literature review concludes with a highlight on phishing prevention. Section three outlines our study methodology and framework to assess the susceptibility of Lebanese participants to phishing emails. Section four reports the detailed results and findings. Concluding remarks followed by future perspectives are discussed in section five.

2. Literature Review

2.1 Phishing

Phishing is a significant threat to all users with an internet connection, especially today that everything is being stored online, and thus personal credentials are at risk of being stolen (Li and Liu, 2021; Hejase, Fayyad-Kazan, Hejase, et al., 2021). Phishing is one of the easiest and oldest ways of stealing information from people and is increasingly becoming one of the most dangerous cyberattacks or organized crimes of the 21st century (Alkhalil, Hewage, Nawaf, et al., 2021).

Phishing is the most common form of cybercrime, with an estimated 3.4 billion spam emails created every day. The usage of credentials that have been stolen is the most common cause of data breaches. In 2022, over 48% of emails sent were spam. Google screens over 100 million phishing emails per day. Millennials and Gen-Z internet users are particularly vulnerable to phishing attacks (Griffiths, 2024). Furthermore, according to Rushton (2023), phishing campaigns account for 36% of all data breaches that occur in the United States. 83% of firms experience a phishing assault annually. There were 345 percent more unique phishing websites in 2021 than there were in 2020. In 2022, the FBI was notified of 300,497 phishing attacks. A phishing attack on a firm typically costs $4.91 million (ibid).

According to Egress's (2024) "Email Security Risk Report 2024," based on 500 leaders, the three most popular phishing attack types are assaults delivered from trusted third-party accounts that have been compromised, malicious URLs, and malware or ransomware. In addition, the survey reports that phishing assaults affected 94% of firms and 96% of those affected negatively. For the attack to succeed, 83% of those attacks had multi-factor authentication (MFA) circumvented, and 79% of the attacks began with a phishing email. Out of the cybersecurity executives polled, 59% train staff members on security awareness on a weekly- or monthly basis.

Moreover, 83% of UK businesses that had a cyberattack in 2022 reported the assault type as phishing, according to UK AAG's (Griffiths, 2024) research on 1,400 organizations. In 2021, phishing was the most prevalent form of attack against Asian enterprises. An organization's average cost of a data breach is more than $4 million. A whale phishing assault can cost a company up to $47 million.

Phishing is one type of cyberattack that uses bogus emails as a weapon (Sibrian, 2020). By deceiving the recipient of the email into believing it is a bank request or a note from a colleague, for example, or something else entirely, these attacks use social engineering techniques to force them to click on a link or download an attachment (Karmakar and Bhatia, 2022; Fruhlinger, 2023). Fruhlinger (2020) states that "Phish" is pronounced exactly how it is spelled, that is, like the word "fish"; an angler may compare it to putting a baited hook out there and hoping to get a bit (para 10, para 10). PhishTank (2013) explains phishing as a "Dishonest email attempt to obtain personal information, such as a password, account number, credit card number, or social security number, and seem to be from a reputable company. Phishing efforts frequently look to be from websites, services, and businesses that one does not even have an account with. Cybercriminals need to trick the receiver into visiting a website via an email to "phish" personal data" (para 1-3). Almost invariably, phishing emails instruct the receiver to click on a link that leads to a website that requests personal information. Reputable companies would never email a person for this information (Sibrian, 2020).

2.2 Phishing Medium

The internet is the centerfield for phishing attacks. It is the playground that hackers or phishers to be exact, use to fish for prey online. With the ongoing use of the internet, social media, applications, and mobile access have been the most depended upon go-to mediums for phishing. Phishing mediums include weapons of influence and life domains (in the email subjects, for example), such as urgency and interest (Alkhalil, Hewage, Nawaf, et al., 2021).

2.2.1 Social Media Phishing

Social media has become as dependent as the air one breathes. People use Facebook, Instagram, Twitter, and a large number of various platforms to communicate with family and friends, keep steady over the most recent news, and dates, and interface with the world (Bashir, Hejase, Danash, et al, 2022; Bashir, Hejase, Yassin, et al., 2023), A study by Seymour and Tully (2016, p. 7) showed that social media phishing attacks are up to 66% effective.

“Today, phishing attacks span various platforms” (Seymour and Tully, 2016, p. 2). Social media phishing is any attack through social media platforms such as Instagram, LinkedIn, Facebook, or Twitter (Muir, 2021; Sabnis and Achar, 2022). "To steal personal data or gain control of one's social media account, to carry out further phishing attacks against one's friends, colleagues, or if one uses these platforms for business, one's customers too" is the common motivation behind social media assaults” (Muir, 2021, para 2). Many businesses are getting destroyed due to social media phishing through forms of loss of data, and possibly through reputation damage that leads to a significant loss in brand name and customer trust (CybSafe, 2023).

Graphus (2022) reports that “Average businesses these days experience up to 60 social media phishing attacks per month” (para 2). According to research by Duff in FL Computer Tech on social media email-linked phishing in 2019, nearly half of all social media-related phishing emails imitated LinkedIn messages followed by Facebook (Figure 1).

Every quarter, this pattern has continued, most likely due to the belief that the emails are authentically originating from a professional network. Because many LinkedIn users have their accounts linked to their work email addresses, this is a serious issue. Facebook subject lines are also becoming more popular, which is not surprising given the rise in brand emulation on the platform (Duff, 2019).

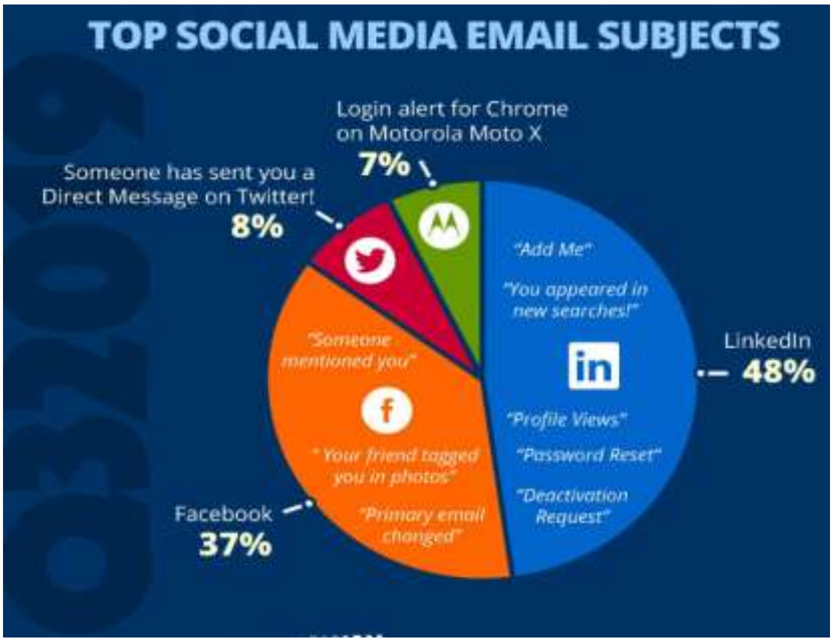


Figure 1. Top Social Media Email Subjects (Duff, 2019)

A. LinkedIn Phishing

LinkedIn is the world's most-utilized professional platform and the best phishing playground depicted in Figure 1. Hackers send their target victims LinkedIn messages, emails, and connections to force them into disclosing delicate data, credit card information, individual data, and login qualifications. Receiving messages directly from LinkedIn has become easy due to its many legitimate email domains, and this makes it hard for users to recognize real from fraudulent ones. Phishers could hack into the chosen victim’s LinkedIn account to impersonate him/her and send phishing messages to the victim’s connections to gather individual information.

B. Facebook Phishing

According to Dean (2023), Facebook had 3.049 billion monthly active users (MAUs) since its launching in 2004, making it the hero of all social media platforms in communication, even with all the new platforms. A typical Facebook phishing scam invites the victim to confirm or supply personal information through a message or link. It is frequently challenging to distinguish between a genuine message from a phishing effort when sent through Facebook Messenger or a post. Attackers can enter the victim's Facebook account using the information obtained from a Facebook phishing attempt. A notification alerting the victim about a problem with their Facebook account and requiring them to log in to fix it could be sent to them (Trend Micro, 2024). Following the embedded link in these messages to visit a Facebook imposter website similar to the real one, where victims are requested to log in; the hacker can then obtain their credentials from there.

C. Twitter and Instagram

Twitter and Instagram platforms are the comfort zone of most internet users as they use them to communicate with people worldwide, stay tuned about international matters, and update the world about their daily lives through images and other activities. They are now particularly vulnerable to phishing attempts, in which scammers send phony messages purporting to be from Instagram or Twitter. These texts entice recipients to provide private information, including credit card numbers, login credentials, and personal information (Trend Micro, 2024).

An example would be sending a “pay for followers, likes, or views” attack by informing victims that their profile will receive a rise in attention in return for a couple of dollars.

2.2.2 Application Phishing

These days, more and more application development is taking place online. All of the productivity suites that end users require in their daily lives are available on the Web, including Google Docs, calculators, email, storage, maps, weather, and news. Since most mobile applications link to the cloud and store files, usernames, passwords, and private information, mobile phones are useless without the Internet. (Ionescu, 2015, para 1).

Notwithstanding security measures like firewalls, applications are totally open to the outside world and so open to attacks. Hackers can penetrate programs and take in data without the network defense systems noticing or attacking them. Many individuals are downloading insecure apps and becoming victims of various distributed malware. According to Ceci (2023), “Installs of potentially hazardous applications (PHAs) through the Google Play Store accounted for more than 0.1 percent of all app installs on the platform between October and December 2022. Privilege escalation was seen in 72% of all PHA installations. Six (6) percent of the total contained Trojan malware, and another thirteen percent carried spyware" (para 1).

Since Google's Android market features open-source technology and does not need developers to go through a rigorous approval process as Apple does, it has a reputation for being developer-friendly. Altexsoft (2018) informs that “The released apps in the Apple App Store are renowned for being highly chosen. Although they have comparable policies, Google and Apple handle quality assurance in different ways. While the approval procedure on the App Store can be laborious and stringent, the Google review system is generally more lenient—that is, provided that you don't break any of its primary content restrictions” (para 15). However, malware occasionally infiltrates systems because of this openness and is utilized for malicious reasons (Goad, 2023). The first phishing attack on the Android Market occurred in January 2010, when certain apps impersonated bank websites using common techniques to trick users into entering their passwords (Smith, 2016).

Elgan (2019) provided another illustration, “The over 10 million times downloaded Weather Forecast app from TCL Corporation, the parent company of Alcatel, which is available on the Google Play Store. The weather app collected user information and transmitted it to a distant server, including location, email address, and International Mobile Equipment Identity (IMEI) numbers. Additionally, the app charged users' phone bills by subscribing them to phone number providers” (para 12).

In total, Apple (2023) protected users from more than $2.0 billion in potentially fraudulent transactions in 2022 (Apple, 2023).

2.2.3 Mobile Phishing

According to Bashir, Hejase, Danash, et al. (2022), internet users depend on smartphones and tablets for productivity and enjoyment, particularly during the pandemic and bad times in Lebanon. Email is still one of the main modes of communication for users in a business context, but a lot of companies are switching to other unified communication platforms like Microsoft Teams. These cloud services are among the most popular ways for customers to access business data from a mobile device because almost all of them provide online and mobile applications. They are one of the fastest-growing targets for phishing and other cybersecurity risks because of the easier access to company data on mobile devices (Goad, 2022, para 1). According to Verizon’s 2021 Data Breach Investigations Report (DBIR), cited in Goad (2022), "In 2021, ransomware and phishing attacks remained to be the most common type of data breaches, along with a significant increase in web application attacks. In this year's dataset, phishing attempts were detected in an astounding 36% of breaches, an increase of 11% from the previous year ” (para 10).

Goslin (2021) posits that “Given the significant move to digital during the pandemic, it is not unexpected that cloud-based web apps accounted for the majority of attacks (Figure 2). Brute force assaults or credentials theft were the main methods used in online application attacks. 95 percent of the firms that were the target of a credential management assault had between 637 and 3.3 billion unauthorized attempts to log in during the year” (para 5).

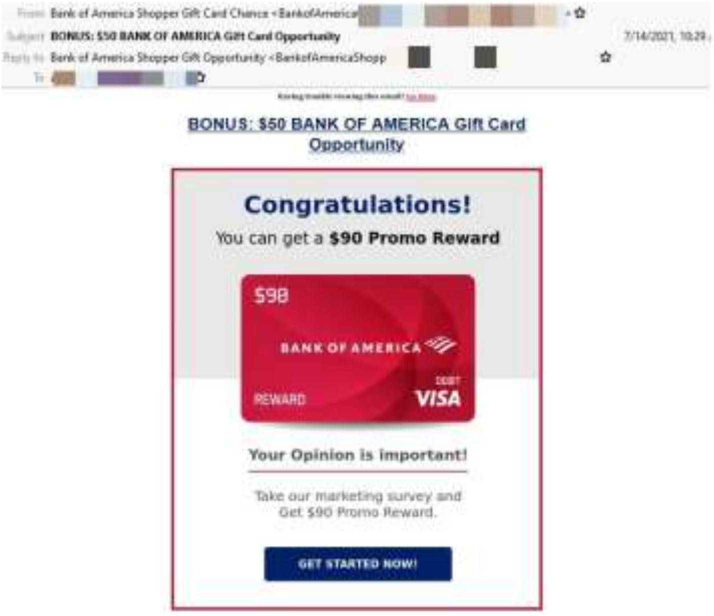
Zimperium (2023), the only mobile-first security platform purpose-built for enterprise environments, reports, “Phishing has been one of the most common types of cyberattacks on mobile devices and it still is. 80% of phishing sites today either target mobile devices directly or are designed to work on both desktop and mobile platforms, according to our study. An SMS phishing attempt has a 6–10 times higher chance of success for the average user than an email-based one” (p. 4). A rise in phishing attacks through different mediums is expected in the upcoming years.

2.3 Types of Phishing Attacks

Phishing attacks of different types commonly have a disguise but can be easily distinguished from each other by the way sent, and by who they target. Hawkins (2023) differentiated six types of attacks: Spear Phishing, Whaling, Vishing and Smishing, Email Phishing, and Search Engine Phishing.

2.3.1 Spear Phishing

Spear phishing is a type of cyberattack in which malevolent actors send targeted emails that seem to be from a reliable source in an attempt to fool recipients into downloading dangerous software or disclosing personal information. Attackers create the appearance of a legitimate email by using previously obtained personal information about the recipient (Hawkins, 2023). For example, someone in the finance division could be targeted by a perpetrator pretending to be the casualty's director mentioning the need for an immediate large bank transfer. Another example could be a company's system administrator. Figure 2 illustrates an example of a spear phishing email.



From: Bank of America Shopper Gift Card Chance <BankofAmerica[redacted]

Subject: BONUS: $50 BANK OF AMERICA Gift Card Opportunity 7/14/2021, 10:29

Reply to: Bank of America Shopper Gift Opportunity <BankofAmericaShopp[redacted]

To: [redacted]

Having trouble viewing this email? [illegible]

BONUS: $50 BANK OF AMERICA Gift Card Opportunity

Congratulations!

You can get a **$90 Promo Reward**

Your Opinion is important!

Take our marketing survey and Get $90 Promo Reward.

Figure 2. Spear Phishing Email Example focused on spear phishing

Source: BÎZGĂ, A. (2021, July 16).

A 2019 Europol EC3 report released in 2019 noted how “spear phishing is still one of the most common and most dangerous attack vectors.” (p. 10). Veltsos (2020) emphasizes that the report further “detailed how one organized criminal group caused over 1 billion dollars in losses to the financial services industry by leveraging spear phishing as part of their activities to move money via Automatic Teller Machines (ATMs) withdrawals and wire transfers” (para 5).

2.3.2 Whaling

Whale phishing, or whaling, is a “form of spear phishing aimed at the very big fish— Chief Executive Officers (CEOs), Chief Financial Officers (CFOs), project managers, or other high-value targets like company board members” (Fruhlinger, 2022; Hawkins, 2023).

A whaling message might state that the company is passing through legal consequences and needs immediate attention. A link would be attached to it to fish out critical data about the company.

2.3.3 Vishing and Smishing

Phishing techniques that use text and voice messaging to target victims are called vishing and smishing. A vishing assault involves someone attempting to obtain a victim’s personal information over the phone. They often pose as representatives of reputable businesses (local or international). In contrast, smishing uses email or text messages to trick victims into visiting a malicious website where malware or information is installed or stolen (Hawkins, 2023, para 12-13).

2.3.4 Email Phishing

Phishing emails mainly mimic legitimate companies and send out generic emails to users hoping that victims will click on the link or download the file. They also often use panic or fear with words like ‘URGENT’ to lead users to click. It is the most common type of phishing. 96% of phishing attacks arrive by email with the top five subject lines being; Urgent, Request, Important, Payment, and Attention (Tessian, 2022).

Common features or red flags of phishing emails, according to KnowBe4, Inc., are the eye-catching offers and awards, the sense of urgencies that force the receiver to act fast, the hyperlinks, the attachments that could hold viruses, and the unusual users that seem to come out of nowhere suspiciously (Phishing.org, n.d.).

2.3.5 Clone Phishing

Phishing with a clone is cunning. Hawkins (2023) contends that to steal identities or disrupt entire networks, hackers replicate legitimate emails and insert harmful links or requests for critical information. For example, the majority of businesses regularly send invoices to their clientele. Usually, they would take reasonable steps to confirm email addresses and make sure the correct individual receives such invoices. Cybercriminals, however, may be able to access these emails. They, therefore, employ the doppelg änger (clone) for phishing after cloning the email. The distinction is that the malicious software will be used to replace the attachments and links. For this reason, clone phishing emails typically have a very authentic appearance (Globytė, 2023).

2.3.6 Social Engineering Attack

Cybercriminals use these attacks as a cunning strategy to take advantage of human error and obtain sensitive data (Hawkins, 2022). Psychological manipulation techniques including baiting, scareware, and pretexting are commonly employed in attacks. Baiting is the practice of an attacker luring a victim into a trap with an alluring offer or a persuasion cue (Valecha, Mandaokar, & Rao, 2022), such as reduced goods, free software, or a convincing argument. Scareware is the term for malicious software that tricks a victim into installing a phony or malicious alarm system through threats or false alerts. On the other hand, pretexting is the process by which an attacker gains the victim's trust by posing as a bank official or coworker and gathering information by telling a string of falsehoods.

In addition to the various phishing conventionally known, a seventh could be added as presented herein.

2.3.7 Search Engine Phishing

This is one of the newest types of phishing attacks that use legitimate search engines.

Cybercriminals utilize search engine optimization to position themselves as the top results on a search engine, a tactic known as "search engine phishing" or "Search Engine Optimization (SEO) poisoning," which aims to direct users to a fake website. The fake website is designed to appear authentic, allowing users who click on it to continue logging into their accounts as normal. They are unaware that if they reuse their passwords, hackers can obtain them and exploit them to breach their accounts or several accounts (Trevino, 2023).

2.4 Phishing Tools

Phishing tools are designed to give the capacity to rapidly and effectively set up and execute phishing engagements in the fastest ways possible.

According to Choudhary (2023), some Phishing Tools that have been used mostly in the past years are the following: EvilgenX2, SEToolkit, HiddenEye, King-Phisher, GoPhish, WifiPhisher, SocialFish, Blackeye, Shellphish, and Zphisher.

Blackeye and Zphisher, for example, can be entered from the GitHub (2024) portal, a developer platform to build codes and multiple types of software. A complete step-by-step guide with the installation processes for these phishing tools is provided to help ease the work of beginners and experts.

2.5 International Phishing Scenarios

An increase in phishing attacks internationally has been observed in recent years in various forms. According to Violino (2023), "In a report published in October 2022, messaging security vendor SlashNext discovered more than 255 million threats after analyzing billions of link-based URLs, attachments, and natural language communications sent across email, mobile, and browser channels during six months. When compared to 2021, that is a 61% increase in the frequency of phishing attempts" (para 6).

2.5.1 Account Takeovers

Hackers have been targeting a variety of social media accounts to fish out information used to cause harm. An example is the attack performed on the British Royal Army that included the takeover of their Twitter and YouTube accounts (Suciu, 2022). Similarly, according to CSIS (2022), many attacks were made on several accounts belonging to Italian, Ukrainian, and Russian corporations, companies, and networks (Barinka, Murphy, & Deutsch, 2023; Cybercrime Magazine, 2024).

2.5.2 Facebook and Google

According to a recent BBC investigation, Google and Facebook each sent over $100 million to a single hacker located in Lithuania. Even though these are large, international corporations, everyone can learn about cybersecurity in 2017 (BBC, 2020).

A man from Lithuania masterminded a fraudulent technique aimed at misleading these companies. He took advantage of the fact that Quanta was a client of both Google and Facebook by posing as a big Asian corporation. Executives signed bogus contracts and fake invoices that he sent (Phished, 2021).

2.5.3 Celebrities, Rappers, Athletes

In 2014, a hacker leaked and spread around 500 private and intimate pictures of celebrities online through spear phishing attacks made by hackers via Apple's iCloud Service (Cha and Christina Farr, 2014). In 2019, Rappers, National Basketball Association (NBA), and National Football League (NHL) athletes were targeted via email phishing by a hacker called Kwamaine Jerell Ford pretending to be the representative of Apple's customer support service (USAO, 2019; Jauniškis, 2022). He requested that the victims respond to security questions or reveal their usernames and passwords. Ford presented these as prerequisites for account resets and other tasks. Once the hacker accessed their accounts, they would alter their passwords and email addresses. Due to this, recovery was not feasible without speaking with Apple support directly. After that, Ford used his money to pay for furniture purchases, money transfers, and trip costs (Jauniškis, 2022).

2.5.4 Public Health Services and COVID-19

With the Coronavirus strike beginning in 2019, cybercriminals started focusing on the Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO) in the US, Asia, and worldwide. In his segment on phishing attacks in 2020, Patrick Mallory (2021), from Infosec, stated that during the start of the pandemic, attackers distributed malicious links and PDF documents purporting to be from the CDC or the WHO, which contained information on "how to protect yourself from the spread of the disease." The email included links that purported to be further security precautions. Then, either when the users downloaded the attachment or from the shoddy landing page, the attackers tried to infect their systems with malware (Mallory, 2021, para 17).

Many COVID-19-related and blood health tests have been played with in terms of results digitally by hacking into hospital systems and other health organizations (He Aliyu, Evans, et al., 2021).

2.5.5 Lebanon's Central Bank and Similar Cyberattacks

Several cyberattacks have surfaced recently in Lebanon without complete disclosure concerning matters such as the cyberattack attempt on the Central Bank in 2017 (Xinhuanet, 2017). "The central bank's online and electronic operations were unaffected, according to the Central Bank of Lebanon/Banque du Liban (BDL)'s Chief Information Officer Ali Nahle, because the bank is prepared to handle unanticipated emergencies (ibid, para 2).

Online frauds are expertly maneuvering their paths across social media platforms by phishing and performing devastatingly damaging moves like bullying, rape, murder, and theft through the digital world (CISO, 2024; Hamadi, 2024).

2.6 Phishing Prevention

Awareness should be raised concerning phishing. Prevention methods should be applied to prevent falling for these ongoing cyberattacks. Educating people of all ages about the matter through seminars, presentations, lectures, and many more techniques could help them properly comprehend the damage that phishing attacks could cause. For example, believing that "user education and deploying specialized software are the two main ways in which companies can develop an effective strategy for phishing protection," PhishProtection offers ideal phishing solutions, protection advice, and awareness training (Phish Protection, 2024).

2.6.1 Browser Anti-Phishing Protection

Various technology measures against phishing are available to provide protection, given that phishing causes significant losses and that attacks persist despite continuous, comprehensive, and continual user awareness information from several sources (Tittel, 2011, para 2).

A web browser is a popular software for accessing online pages and resources over the Internet. A browser can access files in file systems or information from web servers on private networks. Examples abound, including Firefox, Google Chrome, Microsoft Edge (which came before Internet Explorer), Safari, and Opera are the most widely used web browsers (Aboukir, 2017, para 1-2). Anti-phishing best practices include blocking pop-up ads, clearing cookies, not saving passwords, double-checking Uniform Resource Locators (URLs), and disabling automatic downloads and plugins (Aboukir, 2017).

2.6.2 Companies to Fight Phishing

Periods of uncertainty and risk are frequent. Persons and companies periodically necessitate support and need help being informed about what is right from wrong in the digital world. Phishing crimes shall continue and end-users need a hand in getting out of it. Maria Korolov thoroughly mentions several companies that are ready to assist in such occasions, some of which are PhishLabs, IronScales, MediaPro, KnowBe4, Wombat, Blackfin, InfoSec Institute, and PhishLine (Korolov, 2016).

2.6.3 Anti-Phishing Working Group (APWG)

A non-profit organization (NGO) called the Anti-Phishing Working Group (APWG) was established by grouping worldwide entities including forensic investigators, law enforcement agencies, technology companies, financial services firms, university researchers, non-governmental organizations, multilateral treaty organizations, and counter-cybercrime responders (APWG, 2024). This group offers cybersecurity awareness programs such as "APWG's STOP. THINK. CONNECT," as well as community-building conferences for cybercrime management professionals, government and law enforcement authorities, and cutting-edge cybercrime researchers. Furthermore, the APWG offers data standards, policy development, programs for the improvement of cybercrime research, and instruments for public education aimed at preventing cybercrime globally.

The current literature review provided a detailed account of the continuous phishing threats that any person is subject to. As illustrated with cases and statistics, reviewing the possible phishing methods, and observing that most of the cited work is based on reported empirical works, blogs, expert opinion, and anti-phishing tools providers, this threat is universal and affects individuals irrespective of location, culture, and demographics. Moreover, the experimental works on the subject were directed toward studying participants’ behavior and demographics (In Thailand, Chatchalermpun, Wuttidittachotti, & Daengsi, 2020; USA, Lawson, Pearson, Crowson, et al., 2020; Li, Lee, Purl, et al., 2020; Australia, Jayatilaka, Arachchilage, & Babar, 2021) rather than measuring success phishing rates. Therefore, capitalizing on the above besides the researchers’ knowledge that no pilot studies have been conducted in Lebanon on the subject, this paper uses an experimental research approach to target email phishing by applying the phishing tool Zphisher, creating fake phishing emails, and sending them to a sample of Lebanese participants. This work is a unique pilot experiment designed in the context of Lebanon. Notwithstanding that engaging with phishing emails by clicking on links, downloading files, or replying might be seen as dangerous response choices (Lawson et al., 2020), therefore, the aim is to assess the success rate of email scams by phishing based on a sample of participants’ willingness to engage with phishing emails.

3. Materials and Method

This work uses a pilot study. That small-scale initiative gathers participants' data comparable to that of a larger population for future study. It looks into particular areas of the study to investigate the methods employed (Hejase and Hejase, 2013). In addition, this study is also experimental. Zikmund, Babin, Carr, et al. (2013) posit that "An experiment is a meticulously monitored study in which the researcher modifies a suggested cause and tracks any changes to the suggested result" (p. 58).

3.1 Materials and Setup

3.1.1 Sampling and Sample Size

Sampling was performed based on a convenient and non-statistical sampling approach based on the participant's willingness to undergo an experimental phishing exercise. Participants were instructed with a full explanation of the experiment details. They were informed that they could quit at any time with no questions asked. In addition, they were promised complete confidentiality of any personal information they provided during the experiment and carefully excluded from this study. Fifteen participants volunteered. The participants were diverse in their work and divided as follows: Participants were five students (3 seniors in the dentistry department, 20%, and two (2) master students in Forensic Science, 13.3%; all at the Lebanese University), two business professionals (2, 13.3%), two physiotherapists (13.3%), two psychomotor therapists (13.3%), one software engineer (6.7%), two academics (13.3%), and one medical sales representative (6.7%).

3.1.2 Experimental Material

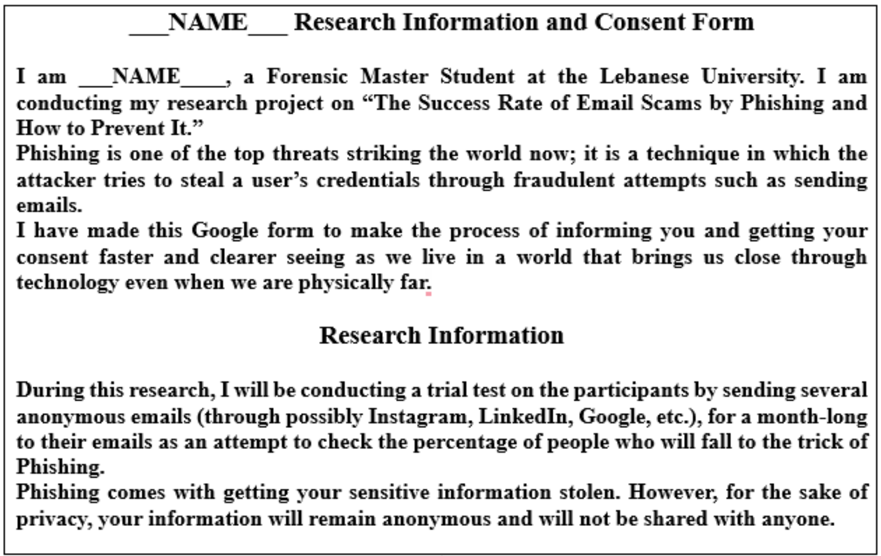
The experiment made use of the following software and websites installed to a laptop:

- Kali Linux as the virtual machine with the command line.
- Google for research and Google consent form.
- Gmail and WhatsApp.
- Bitly and Cuttly.
- Github Zphisher.

3.2 Experimental Process

3.2.1 Step 1: Google Consent Form

A Google Consent Form (Figure 3) was designed and prepared. It explains the email phishing process, what it demands, and the implementation period. It was shared with the 15 participants with reassurance of their privacy.



___NAME___ Research Information and Consent Form

I am ___NAME____, a Forensic Master Student at the Lebanese University. I am conducting my research project on "The Success Rate of Email Scams by Phishing and How to Prevent It."
Phishing is one of the top threats striking the world now; it is a technique in which the attacker tries to steal a user's credentials through fraudulent attempts such as sending emails.
I have made this Google form to make the process of informing you and getting your consent faster and clearer seeing as we live in a world that brings us close through technology even when we are physically far.

Research Information

During this research, I will be conducting a trial test on the participants by sending several anonymous emails (through possibly Instagram, LinkedIn, Google, etc.), for a month-long to their emails as an attempt to check the percentage of people who will fall to the trick of Phishing.
Phishing comes with getting your sensitive information stolen. However, for the sake of privacy, your information will remain anonymous and will not be shared with anyone.

Figure 3. Research Info and Consent form

The participants consent to go on with the research.

All 15 participants provided their full consent to participate in the research. They all agreed to allow the researchers access and use their emails. Again, participants were assured confidentiality throughout the experiment and beyond.

3.2.2 Step 2: Creating Fake Emails

Fake Gmail accounts related to Instagram, Netflix, and Google were created with different domains to trick the participants (Table 1).

Table 1. Fake Gmail Accounts

Instagram	**instaagramadmiin@gmail.com**
Netflix	netfliixadmiin@gmail.com
Google	admiin@gmail.com

3.2.3 Step 3: Kali Linux and Github Zphisher

Kali Linux virtual machine was powered on, and the application [https://github.com/htr-tech/zphisher] was opened on Google.

GitHub provided the necessary process to install the phishing tool Zphisher via the Command Line on Kali Linux as follows (Zphisher, 2024).

Exhibit 1. Installation

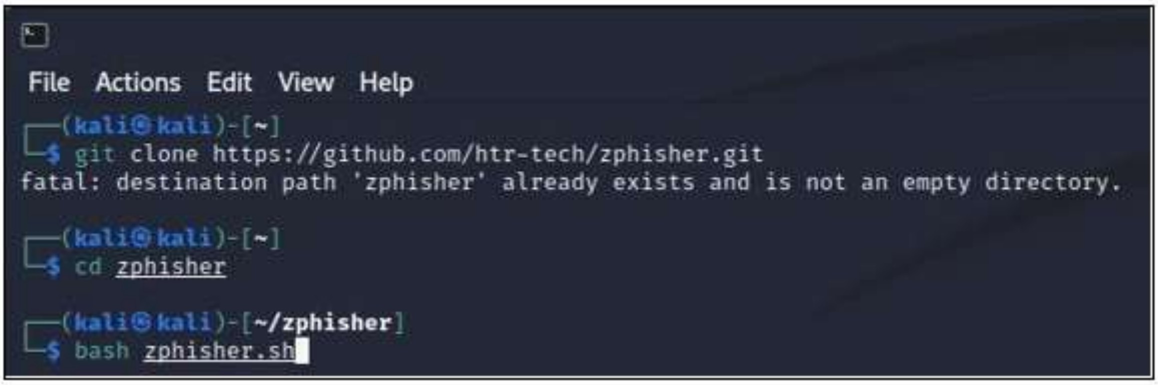
- Just, Clone this repository – git clone –depth=1 [https://github.com/htr-tech/zphisher]
- Now go to the cloned directory and run zphisher.sh -

```
$ cd zphisher
$ bash zphisher.sh
```

On the first launch, it will install the dependencies only. Zphisher is installed next.

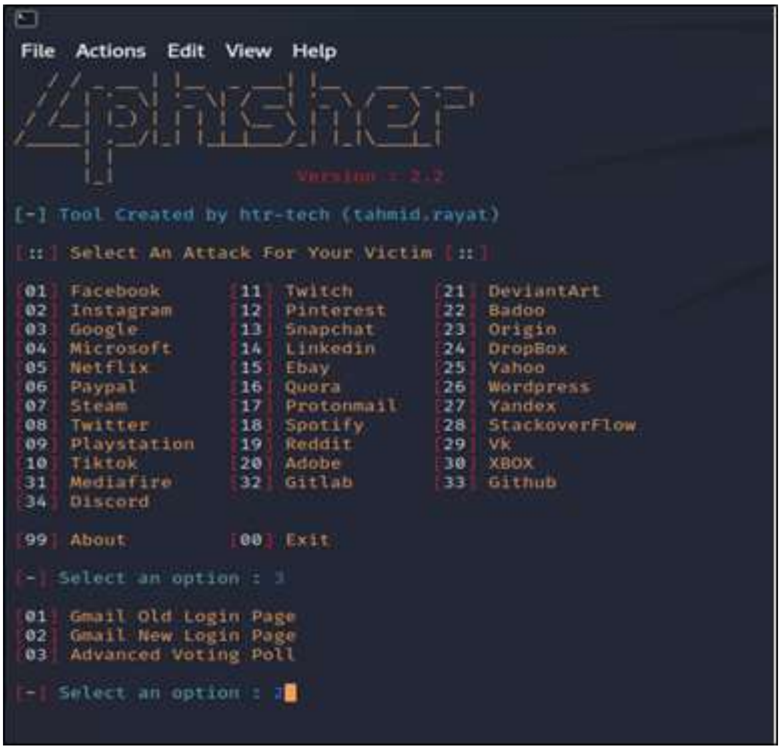
3.2.4 Command Line

The above process was copied onto the command line (Figure 4), then an attack based on the interest of the participant was picked (Figure 5), and a link was generated (Figure 6).



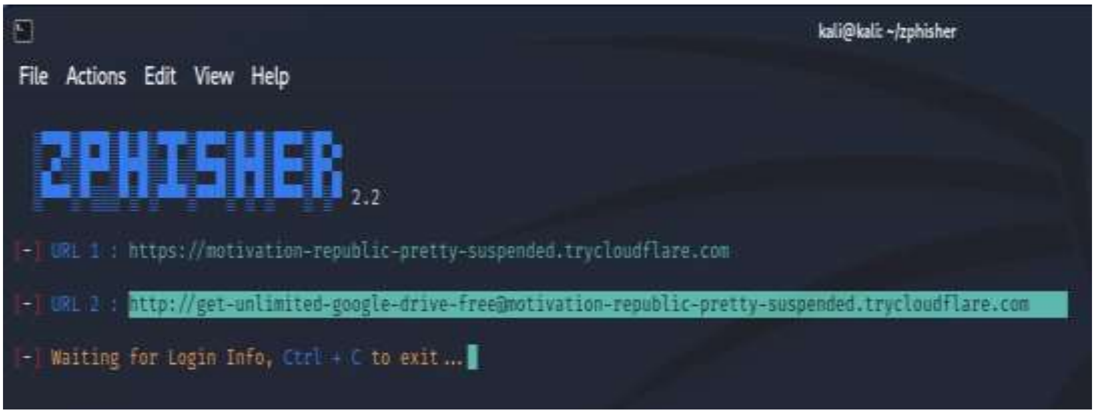
```
┌──(kali㉿kali)-[~]
└─$ git clone https://github.com/htr-tech/zphisher.git
fatal: destination path 'zphisher' already exists and is not an empty directory.

┌──(kali㉿kali)-[~]
└─$ cd zphisher

┌──(kali㉿kali)-[~/zphisher]
└─$ bash zphisher.sh
```

Figure 4. Zphisher Installation



```
                          Version : 2.2

[-] Tool Created by htr-tech (tahmid.rayat)

[::] Select An Attack For Your Victim [::]

[01] Facebook       [11] Twitch        [21] DeviantArt
[02] Instagram      [12] Pinterest     [22] Badoo
[03] Google         [13] Snapchat      [23] Origin
[04] Microsoft      [14] Linkedin      [24] DropBox
[05] Netflix        [15] Ebay          [25] Yahoo
[06] Paypal         [16] Quora         [26] Wordpress
[07] Steam          [17] Protonmail    [27] Yandex
[08] Twitter        [18] Spotify       [28] StackoverFlow
[09] Playstation    [19] Reddit        [29] Vk
[10] Tiktok         [20] Adobe         [30] XBOX
[31] Mediafire      [32] Gitlab        [33] Github
[34] Discord

[99] About          [00] Exit

[-] Select an option : 3

[01] Gmail Old Login Page
[02] Gmail New Login Page
[03] Advanced Voting Poll

[-] Select an option : 2
```

Figure 5. Attack Picking



```
[-] URL 1 : https://motivation-republic-pretty-suspended.trycloudflare.com

[-] URL 2 : http://get-unlimited-google-drive-free@motivation-republic-pretty-suspended.trycloudflare.com

[-] Waiting for Login Info, Ctrl + C to exit ...
```

Note that upon link generation, the "waiting for login info" of the participants was visible (seen).

Figure 6. Generated Links

3.2.5 Bitly/Cuttly

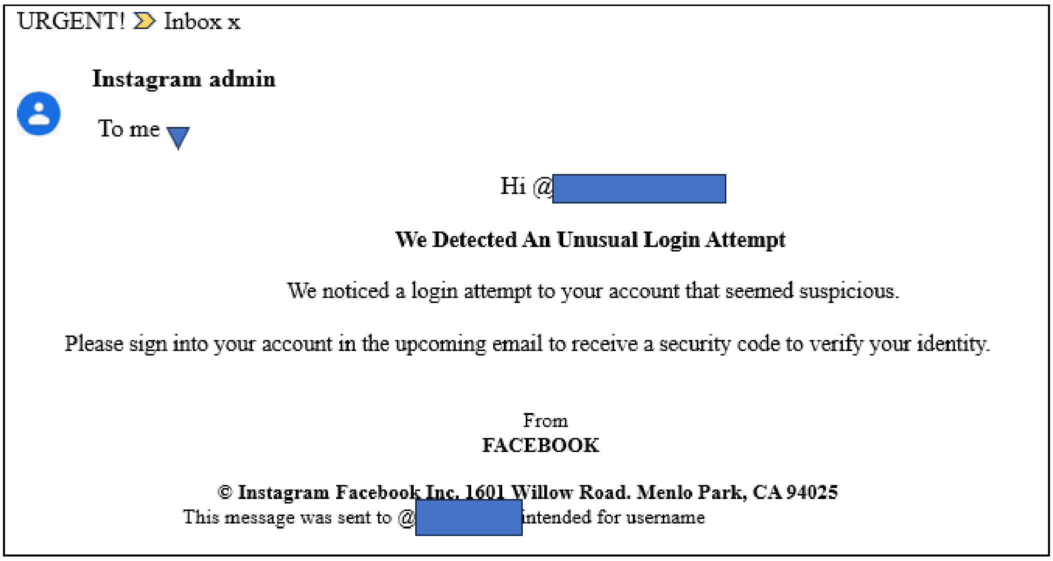
The generated links were copied and uploaded on Bitly/Cuttly, which are websites used to mask and shorten one's links to make participants more susceptible to attacks.

3.2.6 Emails

During June, the following happened to the 15 participants at different times and days:

A- Phishing Emails with "Urgent!", "Suspicious Login Attempt," "Password Reset Request," and "Membership Resubscribe" in the Subject were sent primarily without the attack links so that the emails were not thrown into spam and ignored but directly into inbox (Figure 7).

B- Following the first email, a secondary one was sent as a follow-up on the first one with the attack link copied from Bitly/Cuttly (Figures 8, 9, and 10).



URGENT! ⮞ Inbox x

Instagram admin

To me ▼

Hi @[redacted]

We Detected An Unusual Login Attempt

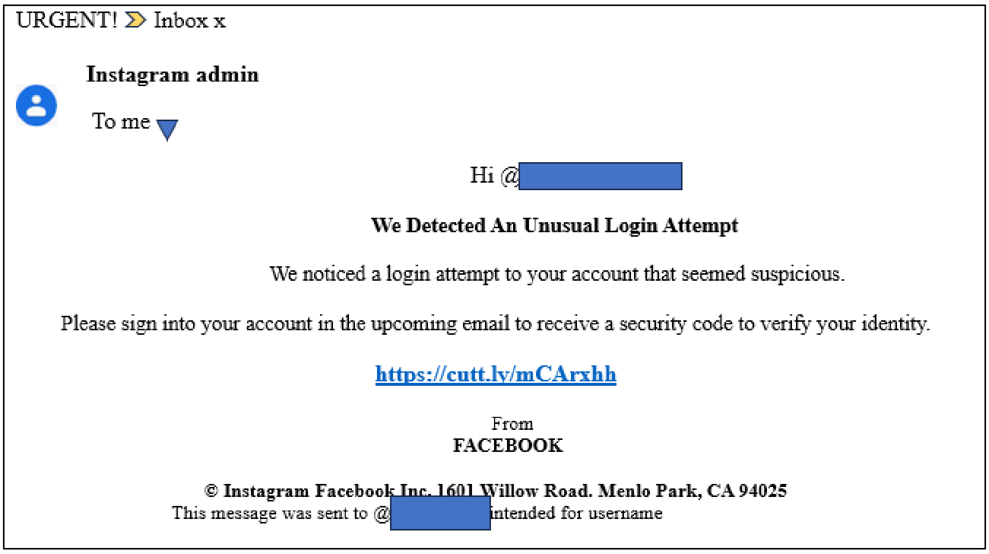
We noticed a login attempt to your account that seemed suspicious.

Please sign into your account in the upcoming email to receive a security code to verify your identity.

From
FACEBOOK

© Instagram Facebook Inc. 1601 Willow Road. Menlo Park, CA 94025
This message was sent to @[redacted] intended for username

Figure 7. Primary Phishing Email without Attack Link



URGENT! ⮞ Inbox x

Instagram admin

To me ▼

Hi @[redacted]

We Detected An Unusual Login Attempt

We noticed a login attempt to your account that seemed suspicious.

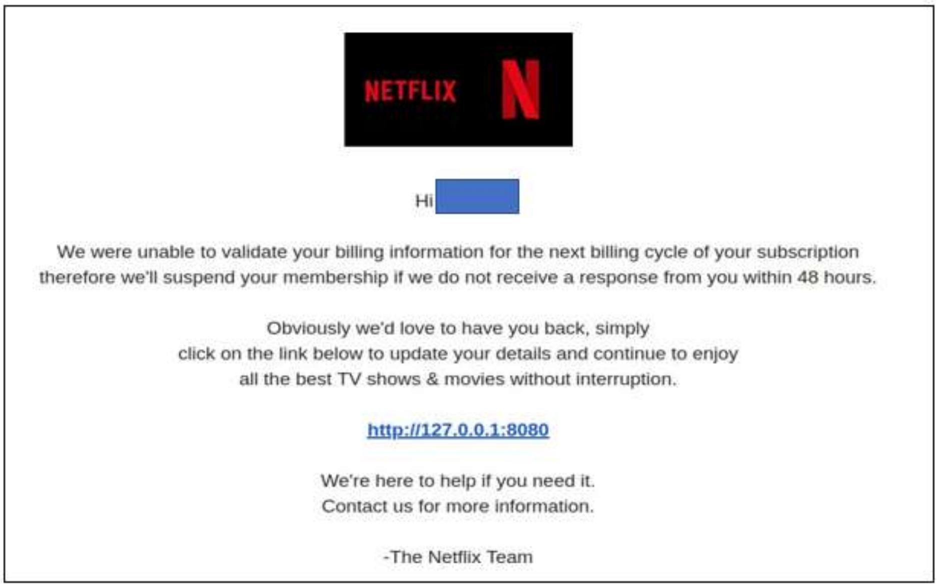
Please sign into your account in the upcoming email to receive a security code to verify your identity.

https://cutt.ly/mCArxhh

From
FACEBOOK

© Instagram Facebook Inc. 1601 Willow Road. Menlo Park, CA 94025
This message was sent to @[redacted] intended for username

Figure 8. Secondary Phishing Email with Attack Link on [Instagram]



Hi [redacted]

We were unable to validate your billing information for the next billing cycle of your subscription therefore we'll suspend your membership if we do not receive a response from you within 48 hours.

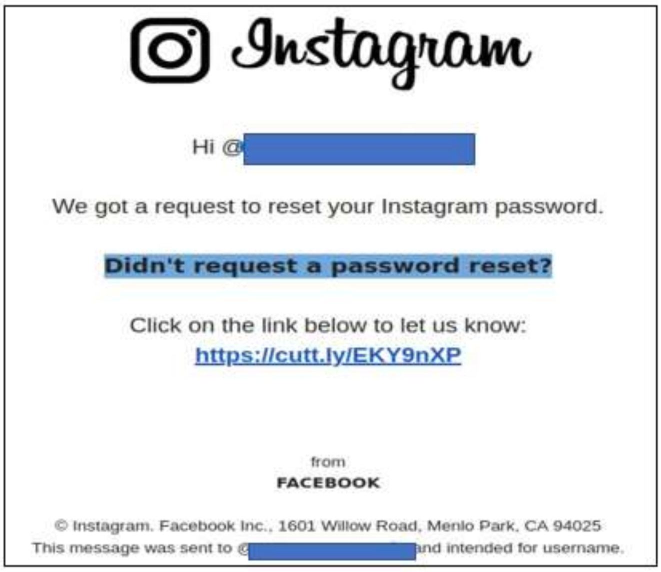
Obviously we'd love to have you back, simply
click on the link below to update your details and continue to enjoy
all the best TV shows & movies without interruption.

http://127.0.0.1:8080

We're here to help if you need it.
Contact us for more information.

-The Netflix Team

Figure 9. Secondary Phishing Email with Attack Link on [NETFLIX]



Hi @[redacted]

We got a request to reset your Instagram password.

Didn't request a password reset?

Click on the link below to let us know:
https://cutt.ly/EKY9nXP

from
FACEBOOK

© Instagram. Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025
This message was sent to @[redacted] and intended for username.

Figure 10. Secondary Phishing Email with Attack Link on [Instagram]

That was performed on all 15 participants based on their interests and mostly used Social Media Applications (Table 2).

Table 2. Participants' Information

Participants with Ages	Number of Emails Sent	Type of Email
No. 1 (21)	2	Urgent
No. 2 (22)	2	Urgent
No. 3 (23)	2	Urgent
No. 4 (23)	2	Urgent
No. 5 (22)	2	Password / Reset Request
No. 6 (22)	2	Password / Reset Request
No. 7 (24)	2	Password / Reset Request
No. 8 (23)	2	Password / Reset Request
No. 9 (22)	2	Netflix / Resubscription
No. 10 (47)	2	Suspicious / Log-in Attempt
No. 11 (22)	2	Suspicious / Log-in Attempt
No. 12 (22)	2	Suspicious / Log-in Attempt
No. 13 (27)	2	Suspicious / Log-in Attempt
No. 14 (22)	2	LinkedIn Message / Request
No. 15 (23)	2	LinkedIn Message / Request

4. Results and Discussion

This section depicts the results of the email phishing experiment and provides a clear discussion explaining what led to such findings. After sending a variety of phishing emails to the 15 participants to get their personal information such as login credentials, the following were the results:

4.1 Results

4.1.1 Demographics

Occupations

Participants include five students (3 seniors in the dentistry department, 20%, and two (2) master students in Forensic Science, 13.3%; all at the Lebanese University), two business professionals (2, 13.3%), two physiotherapists (13.3%), two psychomotor therapists (13.3%), one software engineer (6.7%), two academics (13.3%), and one medical sales representative (6.7%).

Age

Participants' age constituted seven (46.7%) aged 22, four (26.7%) aged 23, and one of each (6.7%) of the following age 21, 24, 27, and 47, respectively.

Frequency of checking emails

Participants check on their emails as follows: 46.7% check their emails very often, 40% of them said not as often as should, and 13.3% barely check their emails.

Social Media Applications they use the most

Participants used multiple social media platforms as depicted in Table 3.

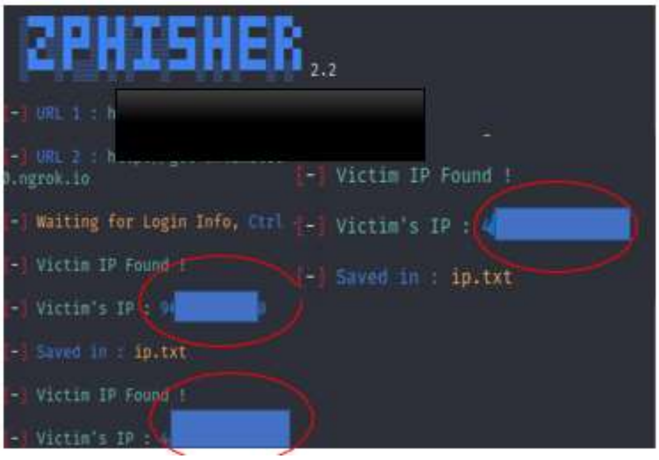
Table 3. Social media used Most

	Frequency		Frequency
Instagram	7	**Twitter**	1
Facebook	4	**LinkedIn**	1
Whatts App	5	**Tik Tok**	1

4.1.2 Number of Participants Who Clicked

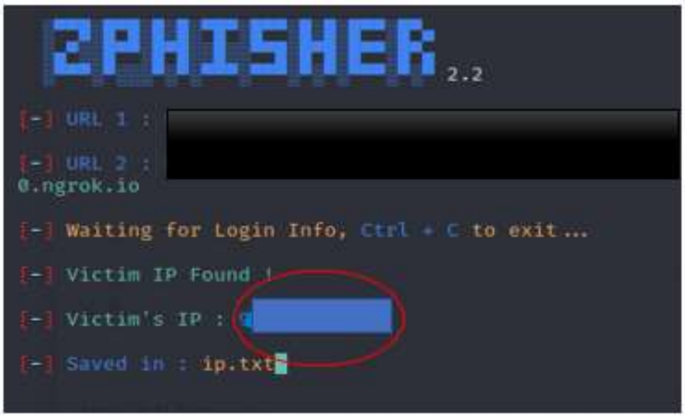
Out of the 15 participants, 8 of them clicked on the links attached to the emails but not all logged in their details.

IP Addresses of the 8 participants who clicked on the links attached to the emails were collected (Figures 11 to 13).



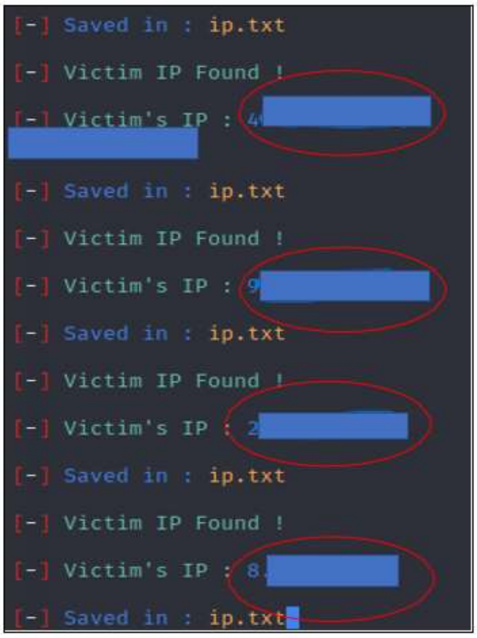
```
ZPHISHER 2.2

[-] URL 1 : h[redacted]

[-] URL 2 : h
0.ngrok.io                       [-] Victim IP Found !

[-] Waiting for Login Info, Ctrl [-] Victim's IP : [redacted]

[-] Victim IP Found !            [-] Saved in : ip.txt

[-] Victim's IP : [redacted]

[-] Saved in : ip.txt

[-] Victim IP Found !

[-] Victim's IP : [redacted]
```

Figure 11. Participants 10, 11, and 12’s IP Addresses Recorded in Correspondence to Opening Links in “Suspicious Log-in Attempt” Phishing Emails



```
ZPHISHER 2.2

[-] URL 1 : [redacted]

[-] URL 2 :
0.ngrok.io

[-] Waiting for Login Info, Ctrl + C to exit...

[-] Victim IP Found !

[-] Victim's IP : [redacted]

[-] Saved in : ip.txt
```

Figure 12. Participant 14’s IP Address Recorded in Correspondence to Opening the Link in “LinkedIn Message Request” Phishing Emails



```
[-] Saved in : ip.txt

[-] Victim IP Found !

[-] Victim's IP : [redacted]

[-] Saved in : ip.txt

[-] Victim IP Found !

[-] Victim's IP : [redacted]

[-] Saved in : ip.txt

[-] Victim IP Found !

[-] Victim's IP : [redacted]

[-] Saved in : ip.txt

[-] Victim IP Found !

[-] Victim's IP : [redacted]

[-] Saved in : ip.txt
```

Figure 13. The first 4 Participants' IP Addresses were Recorded in Correspondence to Opening Links in "Urgent" Phishing Emails

IP Addresses are digital locations of people connected to the internet. These can be used to geolocate the participant upon crime. Example: 12.345.678.90

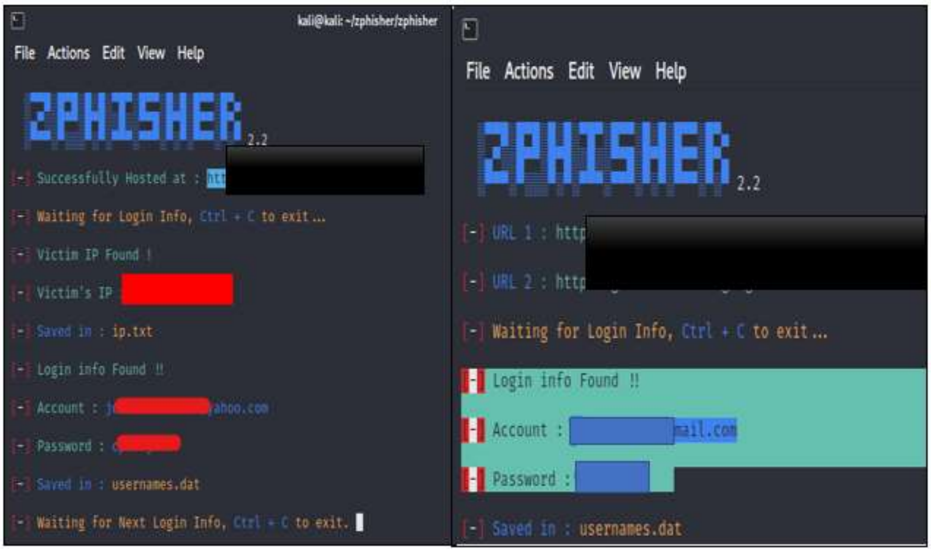
Table 4, in the second column, properly shows how the links in the emails were opened in correspondence to the 8 participants:

Table 4. Participants with Ages, Who Opened Link Attachments in Emails, and Who Logged in their Details

Participants with Ages	The link in the Email Opened	Log-In Details Entered
No. 1 (21)	**Yes**	No
No. 2 (22)	**Yes**	No
No. 3 (23)	**Yes**	No
No. 4 (23)	**Yes**	No
No. 5 (22)	No	-
No. 6 (22)	No	-
No. 7 (24)	No	-
No. 8 (23)	No	-
No. 9 (22)	No	-
No. 10 (47)	**Yes**	Yes
No. 11 (22)	**Yes**	No
No. 12 (22)	**Yes**	No
No. 13 (27)	No	-
No. 14 (22)	**Yes**	Yes
No. 15 (23)	No	-

4.1.3 Number of Participants Who Entered Their Information

Results show (Table 4) that out of the eight (8**)** participants who clicked on the links attached to the emails**,** two **(**2**)** of them provided their log-in details (Figure 14).


kali@kali: ~/zphisher/zphisher
File Actions Edit View Help
ZPHISHER 2.2
File Actions Edit View Help
ZPHISHER 2.2

```
[-] Successfully Hosted at : htt[redacted]
[-] Waiting for Login Info, Ctrl + C to exit...
[-] Victim IP Found !
[-] Victim's IP [redacted]
[-] Saved in : ip.txt
[-] Login info Found !!
[-] Account : j[redacted]ahoo.com
[-] Password : [redacted]
[-] Saved in : usernames.dat
[-] Waiting for Next Login Info, Ctrl + C to exit.
```

```
[-] URL 1 : http[redacted]
[-] URL 2 : http
[-] Waiting for Login Info, Ctrl + C to exit...
[-] Login info Found !!
[-] Account : [redacted]mail.com
[-] Password : [redacted]
[-] Saved in : usernames.dat
```

Figure 14. The log-in details of Participants 10 and 14 were Received

4.2 Discussion

This study aimed to investigate the success rate of email phishing attacks on a sample of Lebanese citizens, especially since technology is constantly updating and harmful cybercrimes are increasing in Lebanon. According to the Office of the Prime Minister (2019), "Cybercrime, espionage, sabotage, blackmail, and the fraudulent or excessive use of personal data are only a few of the risks that Lebanon, like all other States, must deal with to maintain confidence and security in cyberspace" (p. 6). As with other studies, this one focused on a single phishing experiment and aggregated survey and phishing data, rather than doing in-depth research according to locales, jobs, and age groups. Although the results may not be directly comparable, this study shows that the Lebanese sample was successfully attacked, as evidenced by the fact that eight out of fifteen participants clicked on a link in the phishing emails, increasing their likelihood of being victims of email phishing. This amounts to almost 53%. However, when it came to entering personal information into a fraudulent website that was activated by clicking the phishing link, an interesting result was noted: 75% of the participants who clicked on the links and gave us their IP Addresses never provided any personal information on a simulated phishing website. Only 25% of the eight (8) Lebanese participants (2/8) fell into the trap of providing their sensitive information as seen in the Results Section. This shows that people might truly be checking their emails quite frequently with carefulness.

After sending the phishing emails to the 15 participants, regardless of their ages and occupations, with different subject messages as seen in Table 2, eight (8) of them opened the link attachments in the emails as their IP Addresses were received without log-in details as seen in the Results. Out of the eight participants, four (4) opened the Links in the "Urgent" emails, three (3) in the "Suspicious Log-in Attempt" emails, and one (1) in the "LinkedIn Message Request" email showing us that people are more at risk of falling for weapons of influence (subjects) that show authority and legality.

The above eight (8) participants' ages were as follows: One participant aged 21, four participants aged 22, two participants aged 23, and one participant aged 47.

Two participants out of the eight, namely one who is 47 years old, and the other 22 years old, entered their log-in details following the step of clicking on the link found in the "Suspicious Log-in Attempt" email and "LinkedIn Message Request" email, respectively. This led to their personal information directly being sent straight to the command line as seen in Figure 14 in the Results section.

Two out of fifteen participants (13.33%) fell for the entire attack. That shows that Lebanese people are constantly aware of the harmful techniques that hackers are using to destroy their identities and steal personal information such as log-in credentials, bank accounts, and possibly medical results. All ages and occupations are susceptible to email phishing attacks.

Moving forward, it would be interesting to research the appropriate techniques to raise awareness among different members of the Lebanese community. For example, offering seminars and workshops in schools and universities, especially for young adults and children as they are mostly at risk of falling for such cybercrimes without knowing the consequences.

It would also be relevant in future research to address and assess the extent of past exposure to phishing and total phishing emails received daily. In addition, to characterize the susceptibility to possible future attacks among Lebanese citizens of different ages.

4.3 Limitations

This study is a pilot study with a small sample that leads to not generalizing the findings; nevertheless, the results are beneficial for further investigation and serve as a current insight into what future research expects. Moreover, this study is the first of its kind, adding to the theoretical and practical knowledge of phishing in the context of Lebanon. Researchers and experts in cybersecurity may benefit from such findings for their future explorative endeavors.

5. Conclusion and Recommendations

Hejase et al. (2015) posit that “The Lebanese-educated community is still not prepared to deal with one of the most serious threats of the century” (p. 496). Their research included 635 educated adults explored shortcomings of what is going on globally concerning cyber-attacks and cybersecurity besides the poor awareness level that encompasses Lebanon. Considering the previously described information, companies can proactively reduce risks to their cybersecurity (Hejase, Fayyad-Kazan, & Moukadem, 2020). On the other hand, this paper generated experimental findings regarding participants’ susceptibility to email phishing. There was about 53% risk of falling for such a cybercrime regardless of the age and occupation of the person. Therefore, all persons were susceptible to such attacks. This research also has shown that 13.33% of the participants provided private personal information not knowing or being aware of the consequences.

5.1 Recommendations

1. Cultivating national awareness

   Robust adoption of security "best practices" and providing ongoing education to the different organizations’ most vulnerable users are essential for efficient Advanced Persistent Threats (APT) prevention, detection, and response. Nonetheless, companies and institutions must have a strong awareness culture and top management that is knowledgeable about information and technology (Hejase, Fayyad-Kazan, Hejase, et al., 2021, p. 20).

2. Based on our findings, we propose that all national Lebanese stakeholders, like businesses of all sorts from the private sector and governmental institutions from the public sector take user awareness of cyberbullying and cyber-safety measures in email content into consideration, among other functions. Worth mentioning that the Office of the Prime Minister launched 2019 the Lebanon National Security Strategy (Office of the Prime Minister, 2019). Among the measures adopted was institutionalizing The National Cyber Security and Information System Agency (NCISA).

3. Higher education institutions must actively involve students of all majors in a series of seminars, workshops, and training sessions about all sorts of cyber-security threats besides the more advanced courses in information and network security.

4. Professional information and communications technology (ICT) organizations need to offer periodic Infographics about the status of cyber-security in Lebanon in collaboration with the Lebanese specialized armed forces, and the NCISA agency.

References

Aboukir, Y. (2017, November 23). Best practices for web browser security. *INFOSEC*. Retrieved June 8, 2024, from https://resources.infosecinstitute.com/topics/application-security/best-practices-web-browser-security/

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Front. Comput. Sci., 3*, 563060 (pp. 1-23). https://doi.org/10.3389/fcomp.2021.563060

APWG. (2024). *About the APWG*. Retrieved June 8, 2024, from https://apwg.org/about-us/

Barinka, A., Murphy, M., & Deutsch, J. (2023, February 9). TikTok Reveals Russian Disinformation Network Targeting European Users. *Bloomberg*. Retrieved May 31, 2024, from https://www.bloomberg.com/news/articles/2023-02-09/tiktok-reveals-russian-disinfo-network-targeting-european-users

Bashir, E., Hejase, H. J., Danash, K., Fayyad-Kazan, H., & Hejase, A. J. (2022). An Assessment of Students' Preferences Using Social Media Platforms on Their Selection of Private Universities in Lebanon. *Journal of Business Theory and Practice*, *10*(3), 1-39. https://doi.org/10.22158/jbtp.v10n3p1

Bashir, E., Hejase, H.J., Yassin, W., & Hejase, A. J. (2023). An Assessment of the University Usage of Social Media Platforms: Case from Lebanon – A Theoretical Foundations – Part 1. *Journal of Business Theory and Practice, 11*(4), 60-104. https://doi.org/10.22158/jbtp.v11n4p60

BBC. (2020, January 21). 3 Lessons from the Facebook and Google Loss of $100M to a Spear Phishing Attack. *Graphus*. Retrieved May 31, 2024, from https://www.graphus.ai/blog/3-lessons-from-the-facebook-and-google-loss-of-100m-to-a-spear-phishing-attack/

Chan, E., & Christina Farr, C. (2014, September 3). Apple says its systems are not to blame for celebrity photo breach. *Reuters*. Retrieved June 8, 2024, from https://www.reuters.com/article/idUSKBN0GX29F/

Chatchalermpun, S., Wuttidittachotti, P., & Daengsi, T. (2020). Cybersecurity Drill Test Using Phishing Attack: A Pilot Study of a Large Financial Services Firm in Thailand. *Proceedings of the 2020 IEEE 10th Symposium on Computer Applications & Industrial Electronics (ISCAIE)*, (283-286), Malaysia, 2020. https://doi.org/10.1109/ISCAIE47305.2020.9108832

Choudhary, A. (2023, November 7). Top 10 Phishing Tools [Blog] *Medium*. Retrieved May 30, 2024, from https://medium.com/@Rad1antC0d3/top-10-phishing-tools-7c6e5a8be0d7

CISO. (2024). *Lebanese hacker group targets Beirut airport with anti-Iran messages: Report*. Retrieved June 8, 2024, from https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/lebanese-hacker-group-targets-beirut-airport-with-anti-iran-messages-report/106657241

Cybercrime Magazine. (2024, February 1). *Who's Hacked? Latest Data Breaches and Cyberattacks*. Retrieved May 31, 2024, from https://cybersecurityventures.com/intrusion-daily-cyber-threat-alert/

CybSafe. (2023, July 3). *The ripple effect: How one phishing attack can cause disaster across your organization* [Blog]. Retrieved June 17, 2024, from https://www.cybsafe.com/blog/how-can-phishing-affect-a-business/

Duff, M. (2019). The Top Clicked Phishing Email Subjects for the 3rd Quarter 2019. *FL Computer Tech*. Retrieved June 17, 2024, from https://flcomputer.tech/tag/phishing/

Egress. (2024, January 19). Must-know phishing statistics for 2024. *Egress Software Technologies*. Retrieved May 15, 2024, from https://www.egress.com/blog/phishing/phishing-statistics-round-up

Fruhlinger, J. (2023, November 2). What is phishing? Examples, types, and techniques. *CSO*. Retrieved June 17, 2024, from https://www.csoonline.com/article/514515/what-is-phishing-examples-types-and-techniques.html

Github. (2024). *Phishing.* Retrieved May 30, 2024, from https://github.com/topics/phishing?l=html

Griffiths, C. (2024, February). The Latest 2024 Phishing Statistics (updated February 2024). *AAG IT Services*. Retrieved May 15, 2024, from https://aag-it.com/the-latest-phishing-statistics/

Hamadi, G. (2024, January 22). After the hacking of the Parliament and Social Affairs ministry websites 'more attacks' are expected in Lebanon, expert says. *L'Orient Today*. Retrieved June 8, 2024, from https://today.lorientlejour.com/article/1365266/lebanons-ministry-of-social-affairs-website-hacked.html

He, Y., Aliyu, A., Evans, M., & Luo, C. (2021, April 20). Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *J Med Internet Res*., *23*(4), e21747. https://doi.org/10.2196/21747. Erratum in: *J Med Internet Res*., 2021 Apr 28, *23*(4), e29877.

Hejase, A. J., & Hejase, H. J. (2013). *Research Methods: A Practical Approach for Business Students* (2nd ed.). Philadelphia, PA, USA: Masadir Incorporated.

Hejase, A. J., Hejase, H. J., & Hejase, J. A. (2015, September). Cyber Warfare Awareness in Lebanon: Exploratory Research. *International Journal of Cyber-Security and Digital Forensics 4*(4), 482-497. https://doi.org/10.17781/P001892

Hejase, H. J., Fayyad-Kazan, H. F., & Moukadem, I. (2020). Advanced Persistent Threats (APT): An Awareness Review. *Journal of Economics and Economic Education Research (JEEER), 21*(6), 1-8. https://doi.org/10.13140/RG.2.2.31300.65927

Hejase, H. J., Fayyad-Kazan, H., Hejase, A. J., & Moukadem, I. (2021). Cyber Security amid COVID-19. *Computer and Information Science, 14*(2), 10-25. https://doi.org/10.5539/cis.v14n2p10

Hewage, C. (2020). The coronavirus pandemic has unleashed a wave of cyberattacks – here's how to protect yourself. *Conversat*. Retrieved January 16, 2024, from https://theconversation.com/coronavirus-pandemic-has-unleashed-a-wave-ofcyber-attacks-heres-how-to-protect-yourself-135057

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences, 80*(5), 973-993. https://doi.org/10.1016/j.jcss.2014.02.005

Jauniškis, P. (2022, March 7). 10 famous phishing attacks that targeted people and corporations. *Surfshark*. Retrieved June 8, 2024, from https://surfshark.com/blog/biggest-phishing-attacks

Jayatilaka, A., Arachchilage, N. A. G., & Babar, M. A. (2021). Falling for Phishing: An Empirical Investigation into People's Email Response Behaviors. *Forty-Second International Conference on Information Systems*, Austin 2021. Retrieved August 30, 2024, from https://arxiv.org/pdf/2108.04766

Karmakar, S., & Bhatia, M. (2022). Phishing Attacks and Its Working Methodology and How Spear Phishing Is Happening in Modern IT Hubs. *International Journal of Mechanical Engineering, 7*(4), 1793-1801.

Korolov, M. (2016, May 05). 10 companies that can help you fight phishing. *CSO*. Retrieved June 21, 2024, from https://www.csoonline.com/article/556025/10-companies-that-can-help-you-fight-phishing.html

Lawson, P., Pearson, C. J., Crowson, A., & Mayhorn, C. B. (2020). Email Phishing and Signal Detection: How Persuasion Principles and Personality Influence Response Patterns and Accuracy. *Applied ergonomics*, (86), 103084. https://doi.org/10.1016/j.apergo.2020.103084

Li, W., Lee, J., Purl, J., Greitzer, F., Yousefi, B., & Laskey, K. 2020. Experimental Investigation of Demographic Factors Related to Phishing Susceptibility. *Proceedings of the 53rd Hawaii International Conference on System Sciences (HICSS' 2020)*. https://doi.org/10.24251/HICSS.2020.274

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports, 7*, 8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126

Mallory, P. (2021, April 27). 6 most sophisticated phishing attacks of 2020. *INFOSEC*. Retrieved June 21, 2024, from https://resources.infosecinstitute.com/topics/phishing/most-sophisticated-phishing-attacks/

Muir, M. (2021, December). What is Social Media Phishing and How Can It Affect You and Your Business?. Retrieved June 16, 2024, from https://www.waterstons.com/insights/articles/what-social-media-phishing-and-how-can-it-affect-you-and-your-business

Office of the Prime Minister. (2019, June). *Lebanon National Cybersecurity Strategy*. Retrieved June 9, 2024, from http://pcm.gov.lb/Library/Files/LRF/tamim/Strategie_Liban_Cyber_EN_V20_Lg.pdf

Phish Protection. (2024). *17 Phishing Prevention Tips – Prevent Phishing Attacks, Scams and Email Threats*. Retrieved May 30, 2024, from https://www.phishprotection.com/content/phishing-prevention

Phished. (2021, August 26). 5 biggest phishing attacks in world history [Blog]. Retrieved May 30, 2024, from https://phished.io/blog/5-biggest-phishing-attacks-in-world-history

PhishTank. (2013). *What is phishing?*. Retrieved June 17, 2024, from https://phishtank.org/what_is_phishing.php#:~:text=Phishing%20emails%20usually%20appear%20to,not%20even%20have%20an%20account

Pompon, R., Walkowski, D., Boddy, S., & Levin, M. (2018, November 8). Phishing and Fraud Report: Attacks Peak During the Holidays. *F5*. Retrieved January 16, 2024, from https://www.f5.com/labs/articles/threat-intelligence/2018-phishing-and-fraud-report--attacks-peak-during-the-holidays

Rkein, A., Hejase, H. J., Rkein, H., & Fayyad-Kazan, H. (2022b). Bank's Financial Statements as a Source for Investors' Decision-making: A Case from Lebanon. *Academy of Accounting and Financial Studies Journal, 26*(6), 1-14.

Rkein, H. I., Hejase, H. J., Rkein, A., Hejase, A. J., & Fayyad-Kazan, H. (2022a). The Use of Banks' Financial Statements by Depositors and the Impact on Their Decision-Making: A Case from Lebanon. *International Journal of Business and Social Science, 13*(3), 1-11. https://doi.org/10.30845/ijbss.v13n3p1

Rushton, J. (2023, July 3). 50+ Phishing Statistics You Need to Know – Where Who & What is Targeted. *Techopedia*. Retrieved February 15, 2024, from https://www.techopedia.com/phishing-statistics

Sabnis, H., & Achar, C. (2022). Research Paper on Social Media Phishing. *International Research Journal of Modernization in Engineering Technology and Science, 4*(6), 4034-4038. Retrieved January 16, 2024, from https://www.irjmets.com/uploadedfiles/paper//issue_6_june_2022/26869/final/fin_irjmets1656308641.pdf

Seymour, J., & Tully, P. (2016). Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter. *Blackhat*. Retrieved June 22, 2024, from https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter-wp.pdf

Sibrian, J. (2020). *Sensitive Data? Now That's a Catch! the Psychology of Phishing*. (Bachelor's Thesis), Harvard University John A. Paulson School of Engineering and Applied Sciences. Retrieved June 22, 2024, from https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37364686

Suciu, P. (2022, July 5). Not On Guard – British Army's Twitter and YouTube Accounts Were Hacked. Forbes. Retrieved May 31, 2024, from https://www.forbes.com/sites/petersuciu/2022/07/05/not-on-guard--british-armys-twitter-and-youtube-accounts-were-hacked/?sh=d0b639f4e249

Tittel, E. (2011, July 31). A Review of Browser Anti-Phishing Protection. Retrieved June 22, 2024, from https://readwrite.com/a-review-of-browser-anti-phish/

Trevino, A. (2023, April 12). What is Search Engine Phishing?. [Blog] *Keeper*. Retrieved June 22, 2024, from https://www.keepersecurity.com/blog/2023/04/12/what-is-search-engine-phishing/

USAO. (2019, July 18). Georgia man who hacked professional athletes and musicians sentenced to prison. *U.S. Attorney's Office, Northern District of Georgia.* Retrieved June 8, 2024, from https://www.justice.gov/usao-ndga/pr/georgia-man-who-hacked-professional-athletes-and-musicians-sentenced-prison#:~:text=ATLANTA%20%2D%20Kwamaine%20Jerell%20Ford%20has,from%20several%20of%20these%20victims

Valecha, R., Mandaokar, P., & Rao, H. (2022). Phishing Email Detection Using Persuasion Cues. *IEEE Transactions on Dependable and Secure Computing, 19*(02), 747-756. https://doi.org/10.1109/TDSC.2021.3118931

Vayansky, I., & Kumar, S. (2018). Phishing – challenges and solutions. *Computer Fraud & Security, 2018*(1), 15-20. https://doi.org/10.1016/S1361-3723(18)30007-1

Violino, B. (2023, January 10). Phishing attacks are increasing and getting more sophisticated. Here's how to avoid them. *CNBC: Cyber Report*. Retrieved June 23, 2024, from https://www.cnbc.com/2023/01/07/phishing-attacks-are-increasing-and-getting-more-sophisticated.html

Xinhuanet. (2017, May 15). *Lebanon central bank foils a cyber-attack on its email system*. Retrieved June 23, 2024, from http://www.xinhuanet.com/english/2017-05/16/c_136286520.htm

Zikmund, W.G., Babin, B.J., Carr, J.C., & Mitch Griffin, M. (2013). *Business Research Methods* (9th ed.) Mason, Ohio: South-Western, Cengage Learning.

Zphisher. (2024). htr-tech / zphisher. *GitHub*. Retrieved June 23, 2024, from https://github.com/topics/zphisher

Copyrights