

# **COS30015 IT Security**

## **Practical Project**

**Topic: Attack & Security Tools  
(Phishing)**

**Name: Phang Xia Hui**

**Student ID: 102773508**

**Tutorial Group: Thursday**

**Submission Date / Time: 3/12/2023, Sunday,  
7:20pm.**

**Due Date / Time: 3/12/2023, Sunday, 11:59pm.**

## 1. Planning and Justification

Phishing refers to the act of seeking sensitive information, such as usernames, passwords, and credit card details, by masquerading as a trustworthy entity in electronic communications [4]. Deceptive messages claiming to originate from well-known social platforms, online auction sites, payment processors, or IT administrators are frequently employed to entice unsuspecting individuals. Phishing emails may include hyperlinks to websites that have been compromised with malware [4].

Phishing attacks encompass three primary stages: Initially, attacker sends a phishing email to the target victim [9]. Subsequently, the victim receive a phishing attempt and undertakes the recommended action in the message, commonly directing them to a counterfeit website or potentially involving actions like installing malware or disclosing sensitive information. Finally, the third phase involves criminals exploiting the stolen information for monetary gain [9].

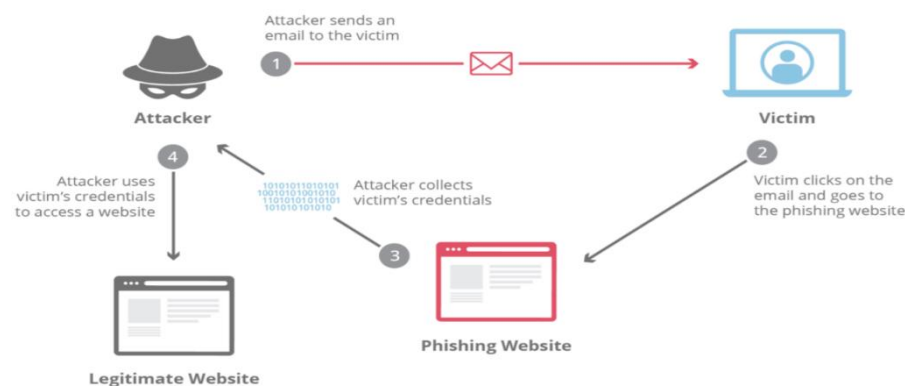


Figure 1: Phishing Process Diagram

Furthermore, the United States Computer Emergency Readiness Team (US-CERT) defines phishing as a type of social engineering that employs email or malicious websites, among other channels, to request personal information from an individual or organization by masquerading as a reliable entity or organization [3]. In this method, a cyber attacker employs email phishing, wherein a deceptive link is transmitted to the user, often disguising itself as a request for bank details or personal information [4]. Subsequently, the user, unsuspecting, accesses the provided link and inputs their details, unwittingly surrendering all pertinent information to the hacker [4]. This succinctly describes the modus operandi of phishing, as elucidated in Figure 1 [6].

Respondents in the United Kingdom indicated that they encountered deceptive solicitations through various channels, with email being the most common at 62%, followed by phone calls at 27%, text messages at 16%, mailed letters at 8%, and social media at 10% [3]. Furthermore, 17% confirmed falling victim to identity theft [3]. In 2013, phishing attacks emerged as the most significant threats. According to the Wombat Security's 2016 State of the Phish report, organizations not only face an increased frequency of phishing attacks but also contend with a rise in their sophistication levels [8]. Their study revealed that two-thirds of organizations experienced personalized or targeted phishing attacks. A report from Google Safe Browsing noted that between 2014 and 2015, the number of malicious web pages decreased from 18,454 to 14,977, while the number of phishing pages increased from around 24,864 to 33,571 [8].

Various forms of phishing have emerged in recent years, showcasing the adaptability of attackers who continually devise new methods to deceive users with innovative ideas. They

stay abreast of the latest technological advancements to enhance the authenticity of their sites, making them appear more convincing than ever before. Some examples include:

- **Clone Phishing** - Clone phishing involves a phishing strategy wherein a hacker endeavours to duplicate a website frequently visited by the victim [10]. The replicated site typically prompts the user to input login credentials, mirroring the appearance of legitimate websites. This tactic enables attackers to store the acquired credentials on their server, either within a text file or a database record [10]. Following this, the attacker guides the victim back to the genuine website, creating the illusion of an authenticated user [10]. Section 2.0 will showcase the execution of this phishing attack, illustrating the creation of a clone of the LinkedIn website. Notably, this demonstration excludes the step involving the transmission of an email.
- **Spear Phishing** - Spear phishing represents a precision-oriented approach to phishing, deviating from the conventional mass production of spam mail [2]. It is a targeted assault directed at an individual or organization, employing specifically crafted materials, often in the form of emails that seem to originate from familiar contacts of the victims [2]. This tailored approach increases the likelihood that the recipient, believing the communication to be trustworthy, will comply with the sender's intentions. To achieve this, the email content must not only appear harmless but also resonate with the recipient's interests, minimizing suspicion [2]. The email may even incorporate personalized details, referencing the target by name and including information that the target assumes to be private, alongside the service the phisher is impersonating. Platforms like LinkedIn or other social media outlets are commonly used by phishers for research, exploiting the ease of obtaining a target's professional and personal information [2]. While spear phishing demands additional time and effort during the planning phase, the increased likelihood of success makes it a favoured method for attackers seeking a higher payoff. As highlighted earlier, spear phishing remains the predominant infection vector for various attacks, with the nature of the attack contingent on the phisher's objectives, ranging from enticing the victim to click a link to downloading a malware-laden attachment [2].
- **Whaling** - Whaling, akin to spear phishing, is a targeted form of phishing that distinguishes itself by exclusively focusing on senior-level executives or other high-ranking employees possessing privileged access to their company's data [2]. Given its precise nature, phishers dedicate time to meticulously craft their scams, ensuring they are virtually indistinguishable from legitimate correspondence [2]. The primary vectors for this attack are typically either eFax or email. Similar to spear phishing, the attacker's objective is to convince the target to install malware, thereby granting unauthorized access to the target's system [2]. The malware is typically disseminated through infected attachments or links prompting malware downloads. Once installed, the malware serves to monitor keystrokes and/or provide the attacker with access to the compromised system, allowing them to perpetuate their attack by leveraging the acquired high-level privileges [2].
- **BEC** - BEC (business email compromise) is a sophisticated form of phishing, falling under the umbrella of spear phishing, exclusively targeting government bodies, non-profits, and commercial organizations to inflict negative consequences, often financial in nature [2]. The primary objective is to compromise corporate emails, utilizing the victim's access for activities like data mining and invoice scams. This method triggers a cascading effect, where compromising one account acts as a launchpad for manipulating or compromising another, known as a launchpad attack [2]. Notably,

phishers invest significant time within a company's networks, sometimes spanning weeks or months, analysing critical elements such as billing systems, vendors, or specific high-ranking executives [2]. Subsequently, an email is meticulously crafted to request fund transfers according to the attacker's goals. The distinctive feature of BEC lies in its indirect approach – instead of directly stealing money, the phisher engineers the theft using another party [2].

Based on earlier research, phishing constitutes an interdisciplinary field that integrates elements of social psychology, technical systems, security, and politics [3]. The prevalence of phishing attacks is on the rise, with a recent study by Proofpoint in 2020 revealing that almost 90% of organizations encountered targeted phishing attacks in 2019 [3]. The landscape of phishing attacks is dynamic, with spoofing methods constantly adapting to countermeasures. Exploiting system vulnerabilities with the aid of new toolkits and technologies, hackers employ social engineering techniques to deceive unsuspecting users [3]. As a result, phishing attacks persist as highly successful cybercrime tactics.

Within this landscape, Phishing kits serve as tools facilitating the creation of phishing websites, emails, and scripts, allowing individuals to gather user input without requiring advanced programming skills [5]. Available for purchase in the cybercriminal marketplace or distributed freely by developers within underground circles, these kits, while accessible, often come with a price [5]. It is noteworthy that some free phishing kits contain backdoors, enabling the leakage of harvested personal information back to the developer. While phishing kits themselves do not directly engage in extracting personal information from victims, they play a crucial role in facilitating phishing attacks [5]. This accessibility makes the initiation of phishing attacks feasible for individuals, regardless of their level of programming expertise [5]. In Section 2.0, we will illustrate how hackers leverage the Zphisher phishing tool.

Zphisher stands out as a potent open-source phishing tool, gaining substantial popularity for its efficacy in conducting phishing attacks on specific targets [12]. Renowned for its user-friendly interface compared to the Social Engineering Toolkit, Zphisher simplifies the phishing process. It encompasses various templates, generated through a tool named Zphisher, offering phishing templates for 33 prominent websites, including Facebook, Instagram, Google, Snapchat, GitHub, Yahoo, Proton mail, Spotify, Netflix, LinkedIn, WordPress, Origin, Steam, Microsoft, and more [12]. Additionally, users have the option to employ custom templates. This tool streamlines the execution of phishing attacks, making it convenient to obtain credentials such as usernames and passwords in a wide area network (WAN) [4]. Hence, the LinkedIn phishing scenario outlined later will comprehensively detail this tool, and Section 2 will delve deeper into its examination.

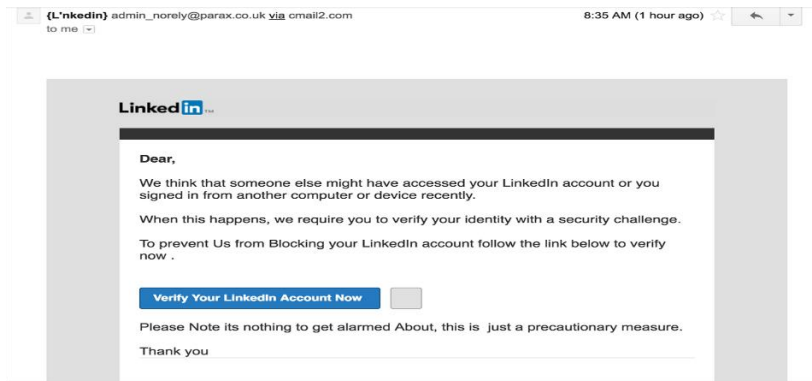


Figure 2: LinkedIn Phishing Email

As per the Brand Phishing Report for Q1 2022, there is a notable shift in the tactics of threat actors, with an increasing focus on exploiting social networks, surpassing traditional targets like shipping companies and prominent technology entities such as Google, Microsoft, and Apple [7]. Notably, LinkedIn stands out as the most targeted brand by a significant margin [7]. The report draws attention to a specific instance where LinkedIn users receive seemingly official emails, aiming to entice them into clicking on a deceptive link. Subsequently, users are directed to a fraudulent portal, urging them to log in, thereby facilitating the harvesting of their credentials [7]. **Error! Reference source not found.** [1] displays the LinkedIn phishing email that a user of LinkedIn received.

Moreover, LinkedIn-themed phishing is on the rise, with a notable 45% of email phishing attempts in Q2 2022 adopting the guise of LinkedIn's communication style, enticing users to interact with a deceptive login page and unwittingly disclose their account credentials, as reported by Check Point [11]. Exploiting tactics like notifications about the target's visibility in searches or pending messages, cybercriminals take advantage of the job market's dynamics. This surge marks a significant jump from Q4 2021 when LinkedIn-themed phishing constituted only 8% of total brand phishing attacks [11]. With over 810 million users, LinkedIn becomes an attractive hub for cybercriminals seeking personal data and a strategic platform for tailored scams. In addition to mimicry, common phishing approaches include fake notifications of unusual account activity, temporary restrictions, and enticing offers or threats regarding account upgrades [11].

By leveraging the capabilities of ZPhisher empowers us to meticulously craft a sophisticated LinkedIn webpage, meticulously replicating the authentic platform's appearance. Subsequently, this meticulously constructed fraudulent webpage is strategically disseminated to designated targets through malicious emails. The objective is to deceive the recipients into interacting with the counterfeit LinkedIn page, unknowingly divulging their login credentials and sensitive information. Section 2 will intricately illustrate the operational aspects of these phishing techniques.

There are several strategies to stop phishing attacks. This part examines the variety of technical techniques available for preventing phishing attempts.

- Black and White Listing - Blacklisting maintains an extensive list of suspicious or harmful domain names or URLs, reducing site traffic by up to 95% and causing severe financial harm to phishing sites [2]. Public blacklists vary in effectiveness, considering update speed and detection accuracy. Integration into browser-based security tools

automates detection, preventing users from entering credentials into illegitimate sites. Some anti-phishing tools actively search for clones of official websites online [2]. In contrast, whitelisting, a database of legitimate sites, is impractical due to the challenge of predicting user destinations, classifying new sites as suspicious, even if legitimate [2].

- **Heuristic Detection** - Heuristic Detection involves extracting features from phishing sites for the purpose of detecting and preventing phishing attacks [2]. However, its current limitations stem from the potential absence of heuristic features in some phishing sites. Additionally, if the phisher is aware of the detection features or algorithms being used, they can easily bypass detection [2].
- **Visual Similarity Detection** - Visual Similarity Detection involves computing the similarity between a suspicious site and a database of legitimate website features, encompassing logos, icons, screenshots, and document-oriented models [2]. If the similarity score surpasses a predefined threshold, it suggests the suspicious site is being mimicked. This method proves valuable in detecting attackers who often replicate legitimate sites to deceive users into divulging their credentials [2]. However, its reliability is not infallible, as phishers can easily circumvent detection by making slight adjustments to visual elements without altering the overall appearance or content of their mimicked page.
- **Machine Learning** - Machine learning plays a pivotal role in detecting phishing emails, messages, and websites, focusing on classification. Various techniques, including decision trees, neural networks, and support vector machines, have been researched for anti-phishing applications, such as email detection and identifying structural discrepancies in websites [2]. Machine learning offers versatility, capable of detecting changes in phishing sites that might evade other detection methods [2]. It has the potential to prevent even zero-day phishing attacks with sufficient training data. However, its effectiveness relies heavily on the size and quality of the training dataset and the precise tuning of hyperparameters for optimal accuracy [2].

In the realm of cybersecurity, robust tools are essential for protecting users from various online threats. Phishing attacks, in particular, pose a significant risk to personal and organizational security. One noteworthy security tool addressing this concern is SafeSurf. Developed in Python, SafeSurf is a cutting-edge phishing domain detection tool that not only identifies suspicious websites but also allows users to safely preview them without direct visits. Its user-friendly interface, coupled with features like trust scores, checks against PhishTank's database, and provision of critical domain details, makes SafeSurf an invaluable resource in defending against phishing attempts. In section 2, SafeSurf will be showcased as a security tool demonstrating its effectiveness.

## **2. Application and Documentation**

### **Attack Tool: ZPhisher**

ZPhisher GitHub: <https://github.com/htr-tech/zphisher>

### **ZPhisher Installation:**

Step 1: To keep your Kali Linux system secure and up-to-date, run the commands '**sudo apt update**' and '**sudo apt upgrade**' in the terminal. The first command updates the package lists,

fetching the latest information from repositories, while the second command upgrades installed packages to their latest versions. These steps are crucial before installing tools like Zphisher, ensuring your system has the latest package data and security patches.

```
kali@kali: ~  
File Actions Edit View Help  
~  
(kali@kali)-[~]  
└─$ sudo apt update  
[sudo] password for kali:  
Hit:1 http://mirror.aktkn.sg/kali kali-rolling InRelease  
Reading package lists ... Done  
Building dependency tree ... Done  
Reading state information ... Done  
11 packages can be upgraded. Run 'apt list --upgradable' to see them.  
  
~  
(kali@kali)-[~]  
└─$ sudo apt upgrade  
Reading package lists ... Done  
Building dependency tree ... Done  
Reading state information ... Done  
Calculating upgrade ... Done  
The following packages were automatically installed and are no longer required:  
gcc-12-base libarmadillo11 libcanberra-gtk-module libcanberra-gtk0 libcbor0.8 libcurl3-nss libgcc-12-dev libgdal33 libgeos3.12.0 libgumbo1  
libgupp-igd-1.0-4 libjim0.81 libnfs13 libobjc-12-dev libstdc++-12-dev libtexluaajit2 libutf8proc2 lua-lpeg nss-plugin-pem python3-aioredis  
python3-apscheduler python3-jdcal python3-pyminifier python3-quamash python3-tzlocal  
Use 'sudo apt autoremove' to remove them.  
The following packages have been kept back:  
libavcodec60 libavfilter9 libavformat60 libgd3 libjavascriptcoregtk-4.0-18 libjavascriptcoregtk-4.1-0 libwebkit2gtk-4.0-37 libwebkit2gtk-4.1-0 tshark  
wireshark wireshark-common  
0 upgraded, 0 newly installed, 0 to remove and 11 not upgraded.
```

Step 2: Install Git within the Kali Linux virtual machine with the command ‘**sudo apt install git**’ to clone the Zphisher repository

```
kali@kali: ~  
File Actions Edit View Help  
~  
(kali@kali)-[~]  
└─$ sudo apt install git  
Reading package lists ... Done  
Building dependency tree ... Done  
Reading state information ... Done  
git is already the newest version (1:2.42.0-1).  
The following packages were automatically installed and are no longer required:  
gcc-12-base libarmadillo11 libcanberra-gtk-module libcanberra-gtk0 libcbor0.8 libcurl3-nss libgcc-12-dev libgdal33 libgeos3.12.0 libgumbo1 libgupp-igd-1.0-4 libjim0.81 libnfs13 libobjc-12-dev libstdc++-12-dev libtexluaajit2  
libutf8proc2 lua-lpeg nss-plugin-pem python3-aioredis python3-apscheduler python3-jdcal python3-pyminifier python3-quamash python3-tzlocal  
Use 'sudo apt autoremove' to remove them.  
0 upgraded, 0 newly installed, 0 to remove and 11 not upgraded.
```

Step 3: Clone the Zphisher repository from GitHub into the desired directory with the command ‘**git clone https://github.com/htr-tech/zphisher**’

```
(kali@kali)-[~]  
└─$ git clone https://github.com/htr-tech/zphisher  
Cloning into 'zphisher' ...  
remote: Enumerating objects: 1794, done.  
remote: Counting objects: 100% (8/8), done.  
remote: Compressing objects: 100% (6/6), done.  
remote: Total 1794 (delta 2), reused 6 (delta 2), pack-reused 1786  
Receiving objects: 100% (1794/1794), 28.69 MiB | 8.15 MiB/s, done.  
Resolving deltas: 100% (804/804), done.
```

Step 4: Navigate to Zphisher Directory using command ‘**cd zphisher**’

```
(kali@kali)-[~]  
└─$ cd  
  
(kali@kali)-[~]  
└─$ ls  
Desktop Documents Downloads Music Pictures Public Templates Videos zphisher  
  
(kali@kali)-[~]  
└─$ cd zphisher
```

Step 5: Run the 'zphisher.sh' command to start the installation process

```
kali@kali:~/zphisher$ ls
Dockerfile LICENSE make-deb.sh README.md run-docker.sh scripts zphisher.sh
kali@kali:~/zphisher$ ./zphisher.sh
[*] Installing required packages...
[*] Packages already installed.
[*] Internet Status : Online
[*] Checking for update : up to date
[*] Installing Cloudflared...
[*] Installing LocalXpose...
```

Step 6: Upon initiation, the tool will present the main menu, featuring a range of options for user selection. The primary objective of this investigation is to gain unauthorized access to the LinkedIn account of a targeted individual. Specifically, selecting option "14" will trigger the creation of a replica of the authentic LinkedIn login screen. Consequently, a link to this deceptive webpage will be generated. While users can opt for various choices based on their specific objectives, our illustration here focuses on the utilization of LinkedIn as an example.

```
File Actions Edit View Help
Zphisher
Version : 2.3.5
[-] 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 Vx
10 Tiktok        20 Adobe        30 XBOX
11 Mediastore    22 Gitlab       33 Github
14 Discord       35 Hubot
99 About        00 Exit
[-] Select an option : 14
```

Step 7: After entering their preferred keywords, Zphisher users can proceed to select a port forwarding service from three available options: Localhost, Cloudflared, or LocalXpose. For the purpose of this illustration, we will use Cloudflared as an example.

```
File Actions Edit View Help
ZPHISHER
Version : 2.3.5
01 Localhost
02 CloudFlared   Auto Detects
03 LocalXpose   NEW! Max 15Min
[-] Select a port forwarding service : 02
7) Do You Want A Custom Port [y/N] : N
[-] Using Default Port 8080 ...
[-] Initializing... ( http://127.0.0.1:8080 )
[-] Setting up server...
[-] Starting PHP server...
[-] Launching CloudFlared...
```

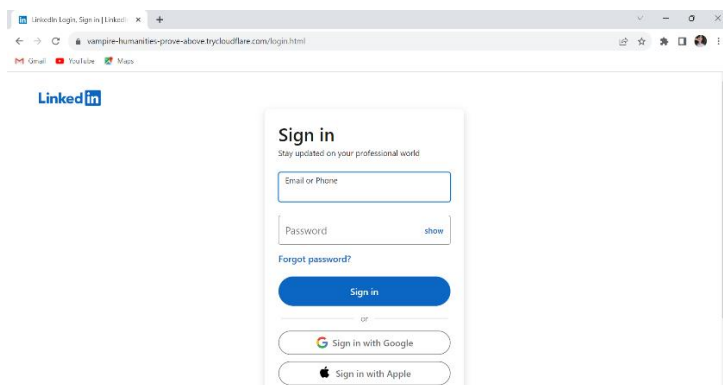
Step 8: No custom link

```
ZPHISHER 2.3.5
[?] Do you want to change Host URL? [y/N] : n
```

Step 9: Now that the website link has been properly constructed, users can use it for the intended purpose.

```
2PHISHER 2.3.5
[~] URL_1 : https://vampire-humanities-prove-above.trycloudflare.com
[~] URL_2 : https://
[~] URL_3 : https://get-a-premium-plan-for-linkedin-free@
[~] Waiting for Login Info, Ctrl + C to exit ...
```

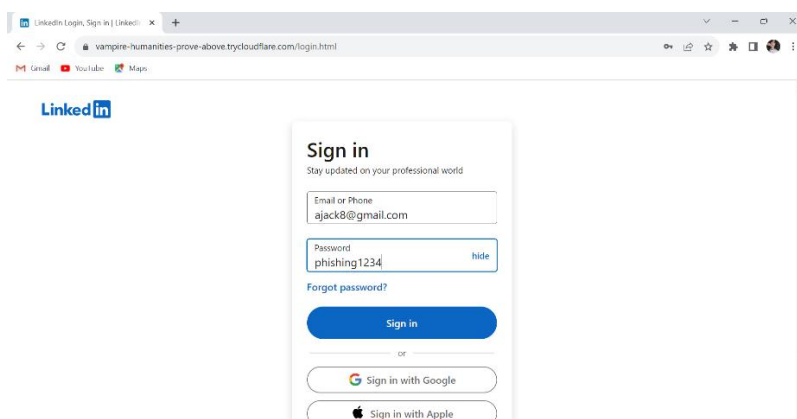
Step 10: Next, we will copy the generated Cloudflare URL: <https://vampire-humanities-prove-above.trycloudflare.com> and paste it into a web browser, such as Google Chrome. Upon doing so, the browser will display a counterfeit website that strikingly resembles the login page of LinkedIn.



Step 11: When the URL is pasted into Firefox, ZPhisher adeptly captures the victim's credentials, including their IP address.

```
kali@kali: ~$ zphisher
File Actions Edit View Help
2PHISHER 2.3.5
[~] URL_1 : https://vampire-humanities-prove-above.trycloudflare.com
[~] URL_2 : https://
[~] URL_3 : https://get-a-premium-plan-for-linkedin-free@
[~] Waiting for Login Info, Ctrl + C to exit ...
[~] Victim IP Found !
[~] Victim's IP : 175.136.143.253
[~] Saved in : auth/ip.txt
```

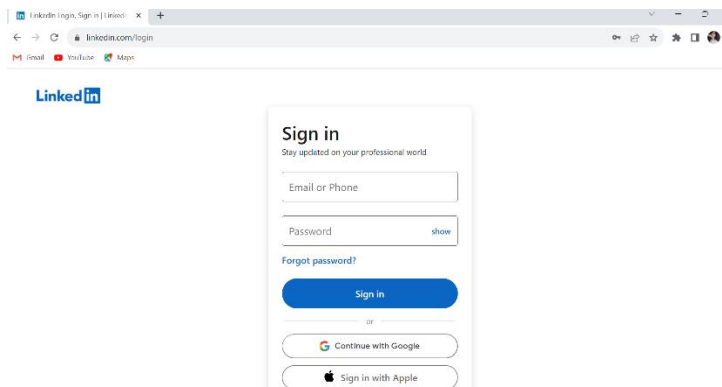
Step 12: As a demonstration, we'll input "[ajack8@gmail.com](mailto:ajack8@gmail.com)" as the email and "phishing1234" as the password. Subsequently, we'll click on "Sign In."



Step 13: Subsequently, ZPhisher shows the username and password entered by the victim on the fake website.

```
[*] Login Info Found !!  
[*] Account : ajack@gmail.com  
[*] Password : phishing1234  
[*] Saved in : auth/usernames.dat  
[*] Waiting for Next Login Info, Ctrl + C to exit.
```

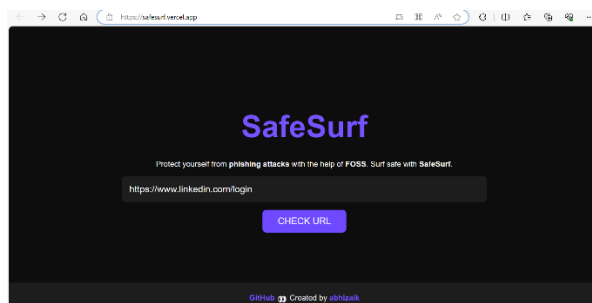
Step 14: Upon returning to Google Chrome, the website's URL transitions to the official LinkedIn website.



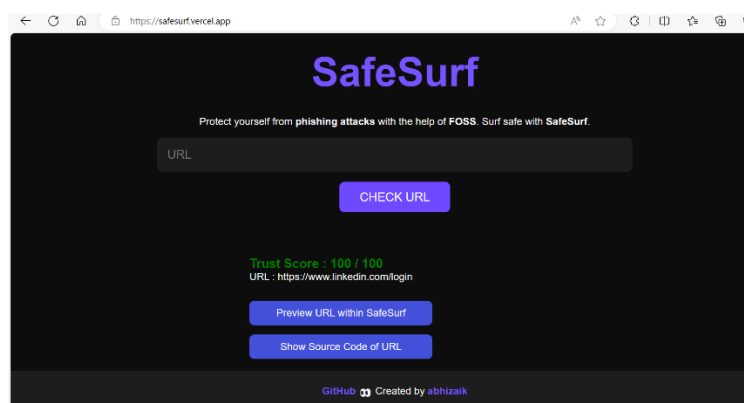
Security Tool: SafeSurf - <https://safesurf.vercel.app/>

SafeSurf GitHub: <https://github.com/abhizaik/SafeSurf>

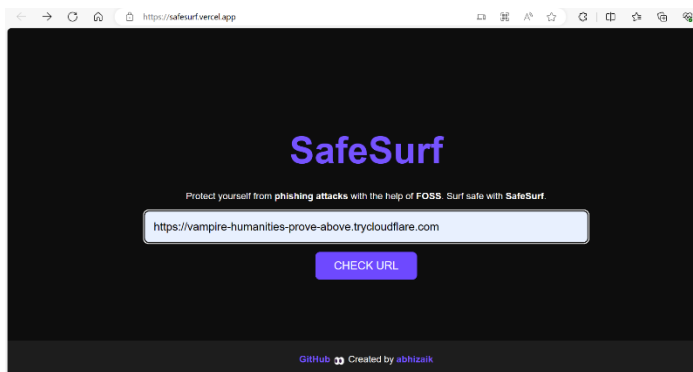
Step 1: Paste the LinkedIn official website link “<https://www.linkedin.com/login>”



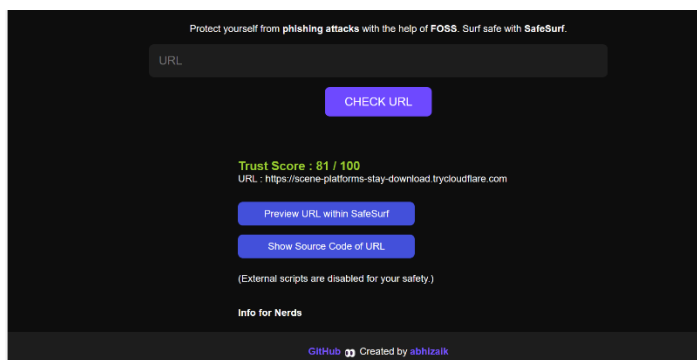
Step 2: This indicates that the official website link can be trusted with a 100% assurance, affirming its status as a secure site.



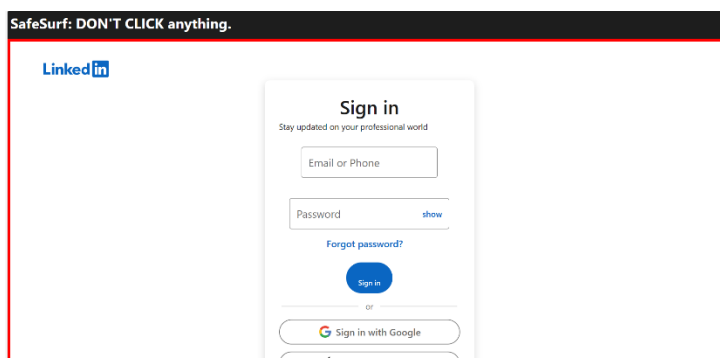
Step 3: Then, we can paste the Cloudflare URL “<https://vampire-humanities-prove-above.trycloudflare.com>” or the other same used Cloudflare URL but different with different name “<https://scene-platform-stay-download.trycloudflare.com>”



Step 4: The displayed trust score for this website is 81%, signifying that it cannot be fully trusted with 100% certainty.



Step 5: Therefore, to ensure safety, we can click on the "Preview URL with SafeSurf" option to view the website without encountering potential dangers. This action will reveal the fabricated LinkedIn website.



### 3. Analysis

The conducted analysis reveals a comprehensive understanding of the phishing landscape, particularly in the context of the ZPhisher tool and the SafeSurf security tool. Here are key insights and considerations:

#### 3.1 Phishing Lanscape

- **Sophistication and Diversity:** Phishing attacks have evolved significantly, adopting varied strategies such as clone phishing, spear phishing, whaling, and BEC. The attackers showcase adaptability, staying ahead of countermeasures by leveraging new technologies and social engineering techniques.
- **Targeting LinkedIn:** The Brand Phishing Report highlights a shift towards exploiting social networks, with LinkedIn emerging as a prime target. The report details instances where users receive seemingly official emails, leading them to deceptive portals for harvesting credentials.

### 3.2 ZPhisher Tool

- **Ease of Use:** ZPhisher is recognized for its user-friendly interface, simplifying the phishing process. It offers templates for a range of popular websites, including LinkedIn, streamlining the execution of phishing attacks even for individuals with limited programming expertise.
- **LinkedIn Phishing Demonstration:** The detailed step-by-step demonstration of a LinkedIn phishing scenario using ZPhisher provides practical insights. It illustrates how attackers can create a convincing replica of the LinkedIn login page to trick users into divulging their credentials.

### 3.3 SafeSurf Security Tool

- **Phishing Domain Detection:** SafeSurf emerges as a valuable tool for detecting phishing domains. Its features, including trust scores and checks against PhishTank's database, enhance user protection against phishing attacks.
- **Safe Website Preview:** The tool's ability to provide a preview of websites without direct visits, especially for URLs with lower trust scores, adds an extra layer of security. This is crucial in mitigating the risks associated with potentially harmful sites.

### 3.4 Analysis of Preventive Techniques

- **Black and White Listing:** The analysis emphasizes the effectiveness of blacklisting, reducing site traffic to phishing sites significantly. However, whitelisting is deemed impractical due to challenges in predicting user destinations.
- **Heuristic Detection and Visual Similarity Detection:** Limitations in heuristic detection, where some phishing sites may lack heuristic features, and the potential for visual similarity detection to be bypassed if the attacker is aware of the detection features, are highlighted.
- **Machine Learning:** The versatility of machine learning in detecting phishing attacks is acknowledged, with an emphasis on its dependence on the quality and size of the training dataset for optimal accuracy.

### 3.5 Future Challenges and Considerations

- **Evolution of Phishing:** The analysis recognizes the dynamic nature of phishing attacks, continually adapting to countermeasures. The use of phishing kits and the rise of LinkedIn-themed phishing attacks underscore the challenges faced by defenders.
- **Role of ZPhisher:** While ZPhisher simplifies the execution of phishing attacks, its prevalence poses challenges for defenders. The ease of access to such tools, including free phishing kits with potential backdoors, raises concerns about their misuse.

- **SafeSurf and User Awareness:** SafeSurf's role in enhancing user awareness and safety is highlighted. However, the analysis underscores the importance of user education and awareness in recognizing and avoiding phishing attempts.

In conclusion, the analysis provides a holistic view of the phishing landscape, the functionalities of ZPhisher and SafeSurf, and the challenges faced by defenders. The comparison of preventive techniques and the exploration of future challenges contribute to a well-rounded understanding of the cybersecurity landscape.

#### 4. Evaluation

The comprehensive analysis of phishing, ZPhisher, and SafeSurf sheds light on various aspects within the security landscape, encompassing results, challenges, usage, and threats/needs.

The analysis effectively reveals the evolving landscape of phishing attacks, highlighting their sophistication and diversity. The focus on LinkedIn as a prime target, as indicated by the Brand Phishing Report, and the rise of LinkedIn-themed phishing attacks provide actionable insights. The step-by-step demonstration of a LinkedIn phishing scenario using ZPhisher adds a practical dimension to the results, showcasing the ease with which attackers can replicate legitimate login pages. SafeSurf's role in detecting phishing domains and providing trust scores contributes positively to the security landscape.

The analysis brings attention to significant challenges within the security landscape. A persistent challenge lies in the dynamic nature of phishing attacks, requiring continuous adaptation of countermeasures to effectively thwart evolving cyber threats. The prevalence of accessible tools such as ZPhisher and freely available phishing kits introduces concerns about potential misuse, amplifying the ease with which individuals lacking advanced programming skills can engage in cyberattacks. The identified challenges related to whitelisting impracticality, limitations in heuristic detection, and the potential for attackers to circumvent visual similarity detection emphasize the necessity for nuanced and multifaceted preventive strategies. Addressing these challenges is crucial for fortifying cybersecurity measures and staying ahead of the ever-changing tactics employed by cyber adversaries.

The usage of ZPhisher as a potent open-source phishing tool is effectively illustrated in the analysis. Renowned for its user-friendly interface and extensive template options, ZPhisher simplifies the phishing process, making it accessible even for users with limited technical skills. The stepwise demonstration of a LinkedIn phishing attack provides practical insights into how the tool can be utilized to replicate legitimate login pages, emphasizing its potential risks in the hands of attackers. This portrayal underscores the need for heightened awareness and preventive strategies to mitigate the misuse of such tools.

Similarly, SafeSurf's usage as a phishing domain detection tool is highlighted, showcasing its relevance in enhancing user protection against phishing attempts. The tool's features, including trust scores and the ability to preview websites without direct visits, contribute to a safer online experience. SafeSurf's application in verifying the legitimacy of website links, such as the official LinkedIn login page, adds an extra layer of security. The portrayal of SafeSurf's usage underscores its significance in the cybersecurity landscape, particularly in a context where phishing attacks continue to evolve and pose persistent threats. Overall, the analysis effectively communicates the practical applications of both ZPhisher and

SafeSurf, offering insights into their functionalities and emphasizing the importance of responsible use and user awareness.

The analysis brings attention to the inherent threats within the cybersecurity landscape, highlighting the dynamic evolution of phishing attacks and the concerning potential for the misuse of readily available tools, such as ZPhisher and phishing kits. The notable rise of LinkedIn-themed phishing attacks serves as a poignant example of the shifting tactics employed by threat actors, underscoring the need for adaptive and robust security measures. The analysis advocates for a multifaceted approach to cybersecurity, outlining the necessity for preventive techniques like blacklisting, heuristic detection, visual similarity detection, and machine learning to effectively combat the sophisticated nature of modern phishing attempts. In response to these threats, SafeSurf emerges as a solution that addresses the growing need for tools capable of detecting phishing domains and providing users with safe previews of websites, contributing to a comprehensive defense against evolving cyber threats. The portrayal of these threats and corresponding needs reinforces the imperative for continuous innovation and vigilance in the development and implementation of security measures to safeguard against the ever-changing landscape of cyber threats.

In conclusion, this research provides a comprehensive assessment of cybersecurity, navigating through the complexities of evolving phishing attacks and emphasizing LinkedIn as a prime target. The identification of challenges, such as the dynamic nature of phishing and the accessibility of tools like ZPhisher, highlights the need for continuous adaptation and innovative countermeasures. Practical illustrations of ZPhisher's risks and SafeSurf's usage underscore the importance of user awareness and enhanced protection measures. The outlined preventive techniques, including blacklisting and machine learning, emphasize the ongoing demand for effective security measures in the face of a dynamic cyber threat landscape. In essence, this research calls for sustained innovation, vigilance, and user education to fortify cybersecurity defenses against ever-evolving cyber threats.

## List of References:

1. 360totalsecurity.com. 2017 [cited 2023 Nov 24]. Available from: <https://blog.360totalsecurity.com/wp-content/uploads/2017/03/Screen-Shot-2017-03-06-at-10.07.13-1.png>
2. Alabdan R. Phishing Attacks Survey: Types, Vectors, and Technical Approaches. Future Internet [Internet]. 2020 Sep 30 [cited 2023 Nov 23];12(10):168. Available from: <https://doi.org/10.3390/fi12100168>
3. Alkhalil Z, Hewage C, Nawaf L, Khan I. Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science [Internet]. 2021 Mar 9 [cited 2023 Nov 20];3(1). Available from: <https://www.frontiersin.org/articles/10.3389/fcomp.2021.563060/full>
4. Bhavsar V, Kadlak A, Sharma S. Study on Phishing Attacks. International Journal of Computer Applications [Internet]. 2018 Dec 17 [cited 2023 Nov 15];182(33):27–9. Available from: [https://www.researchgate.net/profile/Shabnam-Sharma-/publication/329716781\\_Study\\_on\\_Phishing\\_Attacks/links/5ef9867a92851c52d6069bf2/Study-on-Phishing-Attacks.pdf](https://www.researchgate.net/profile/Shabnam-Sharma-/publication/329716781_Study_on_Phishing_Attacks/links/5ef9867a92851c52d6069bf2/Study-on-Phishing-Attacks.pdf)
5. Chiew KL, Yong KSC, Tan CL. A survey of phishing attacks: Their types, vectors and technical approaches. Expert Systems with Applications [Internet]. 2018 Sep [cited 2023 Nov 19];106:1–20. Available from: <https://doi.org/10.1016/j.eswa.2018.03.050>
6. Cyberhoot.com. 2023 [cited 2023 Nov 28]. Available from: <https://cyberhoot.com/wp-content/uploads/2019/12/diagram-phishing-attack-1024x534.png>
7. Brand Phishing Report Q1 2022 [Internet]. Check Point Blog. 2022 [cited 2023 Dec 1]. Available from: <https://blog.checkpoint.com/security/social-networks-most-likely-to-be-imitated-by-criminal-groups-with-linkedin-now-accounting-for-half-of-all-phishing-attempts-worldwide/>
8. Gupta BB, Arachchilage NAG, Psannis KE. Defending against phishing attacks: taxonomy of methods, current issues and future directions. Telecommunication Systems [Internet]. 2017 May 23 [cited 2023 Nov 27];67(2):247–67. Available from: <https://link.springer.com/content/pdf/10.1007/s00521-016-2275-y.pdf>
9. Hong J. The state of phishing attacks. Communications of the ACM [Internet]. 2012 Jan 1 [cited 2023 Nov 18];55(1):74. Available from: <https://dl.acm.org/doi/pdf/10.1145/2063176.2063197>
10. Nazreen M, Munawara Banu B. A Comprehensive Study of Phishing Attacks [Internet]. 2018 Dec [cited 2023 Nov 22]. Available from: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=2bf12ff75150903efee426f23035c94d599597ae>
11. Zorz Z. The rise and continuing popularity of LinkedIn-themed phishing [Internet]. Help Net Security. 2022 [cited 2023 Nov 26]. Available from: <https://www.helpnetsecurity.com/2022/07/21/linkedin-phishing/>

12. Zphisher - Automated Phishing Tool in Kali Linux [Internet]. GeeksforGeeks. 2021 [cited 2023 Nov 25]. Available from: <https://www.geeksforgeeks.org/zphisher-automated-phishing-tool-in-kali-linux/>