A Review on Phishing Attacks

Author: Mr. Prakash Amin  
*Master of Science in Information Technology (MSc-IT)*  
*SVKM’s Usha Pravin Gandhi College of Arts, Science and Commerce.*Mumbai, Maharashtra.  
aminprakash1@gmail.com

Author: Ms. Urvi Rathod   
*Master of Science in Information Technology (MSc-IT)*  
*SVKM’s Usha Pravin Gandhi College of Arts, Science and Commerce.*Mumbai, Maharashtra.  
urviirathod77@gmail.com

Guide: Prof. Prashant Chaudary  
*Master of Science in Information Technology (MSc-IT)*  
*SVKM’s Usha Pravin Gandhi College of Arts, Science and Commerce.*Mumbai, Maharashtra.  
prashantchaudary@gmail.com

*Abstract*— Phishing is a type of cyber-attack that involves the use of fraudulent emails, websites, or other digital communication channels to steal sensitive information from an unsuspecting victim. The objective of a phishing attack is to obtain personal information such as usernames, passwords, credit card numbers, and other confidential data from the victim. Phishing attacks are typically carried out by sending out malicious emails disguised as legitimate messages from trusted sources. These emails often contain malicious links or attachments, which when clicked on, will redirect the victim to a malicious website or open an application that will steal the victim’s information. Other methods of phishing include social engineering, where attackers use psychological manipulation in order to gain access to a victim’s system. This paper will discuss the various types of phishing attacks, the different anti-phishing techniques and how to identify different phishing types. It will also provide recommendations/tools on how individuals and organizations can protect themselves against phishing attacks.

Keywords—phishing, social engineering, cyber-attacks, anti-phishing techniques.

# Introduction

Phishing is a deceptive practice in which the attacker/phisher attempts to convince internet users to hand over their personal information or login credentials in exchange for money [1]. Phishing is compared to fishing, which has a different connotation; in phishing, the attacker exploits bait (sending an email with a hyperlink inserted that leads to a fake website) to get the login information of internet users. Before, the attackers were referred to as "Phreaks" (a Phreak is a person who unlawfully hacks into phone networks to place free long-distance calls or to tap phone lines), and they are all tied to one another. To connect phishing schemes with phreaks, "ph" has been used in place of "f" [2]. Phishing has evolved during the past 20 years into the most serious assault, and many attacks occur daily [3, 4]. On January 2, 1996, American Online (AOL), a provider of internet services, documented the first phishing fraud.

The fraudster creates credit card details at random, then they used that information to construct AOL profiles. Later, using AOL's instant messenger or email system, they send an email to clients requesting them to confirm their login information by clicking on an actual source. This data is immediately sent to the hacker, if the user clicks the hyperlink and provides their credentials, then the data is directly sent to the hacker. As a result, the attackers misuse such credentials for unethical means. Every time, an attacker develops a new method to deceive an individual user and steal their personal information (for instance, bank account details, social media profiles, email IDs, etc.). For the whole month of June 2021, the anti-phishing working group (APWG) 2nd quarter of 2021 recorded 2,22,127 distinct phishing assaults. The distinctive phishing sites created by the scammers in 2020–2021 are displayed in Figure 1. Pharming, often known as "phishing without bait," is an improved version of phishing [6, 7].

Thus, pharming is a DNS-based attack in which the attacker gets unauthorized access to the DNS and alters the host file entries, redirecting all users who obtain data from that DNS to the false website. It is difficult to identify and more hazardous since it affects a large number of people who have been affected by DNS poisoning. More recently, phishing has been discovered to be carried out via seizing control of access to user information via malware (ransomware) and blackmailing consumers into paying a ransom. In 2015, the internet crime report (ICR) received 2,453 ransomware-related complaints, totaling $1.6 million. The APWG study (1st quarter 2019) [8] found 1,80,768 distinct phishing websites. 36% of this phishing schemes target software-as-a-service (SaaS) and webmail providers. Various researchers and groups have created a plethora of anti-phishing technologies to protect users against phishing assaults. These anti-phishing solutions primarily function at the user level, with only a few exceptions working on the server. A comprehensive categorization of anti-phishing solutions is offered in our earlier study [9].

# Literature review

Ludl et al. (2007) [10] studied how successful phishing is, and sought for strategies to fix it, notably two prominent anti­phishing solutions. For three weeks, they examined the anti­phishing solutions included into Firefox 2 (i.e., Google blacklists) and Microsoft's Internet Explorer 7 by automatically testing them against a blacklisted of 10,000 false URLs maintained by Google and Microsoft. Furthermore, they investigated the existence of page properties that may be utilised to detect phishing pages by analysing a huge number of phishing sites. And how these characteristics (links, suspicious urls, forms, input fields) might be critical for users to be duped.

Tanvi Churi et al. [11] provided a prototype for determining whether a site is a phishing site or not. According to their report, existing phishing protection systems do not provide 100% accuracy code generating approaches that only authenticated individuals can breach. The proposed system produces a photo, which is then divided into two groups by the visual cryptographic techniques. These two parts of the image are then merged to create an image captcha, which is displayed and the user is asked to match the site with the image captcha to distinguish the site from phishing sites. In the following phase, a four-digit code is produced and authenticated by an authorised individual. The strategy is useful for identifying phishing sites and protecting passwords from unintended consequences.

Simono et al. [12] have briefly covered the inadequate security procedures in Android phone password managers, which are the source of phishing assaults. According to the research, there are a number of flaws in password manager designs that contribute to these assaults.

Rao et al. [13] developed a unique classification strategy based on heuristic feature extraction. They have divided the retrieved characteristics into three categories: URL obfuscation features, Third-Party-based features, and Hyperlink-based features. Furthermore, the proposed approach has a 99.55% accuracy. The disadvantage is that because this approach incorporates third-party characteristics, website classification is dependent on the speed of third-party services. This model is also entirely dependent on the quality and amount of the training data, and Broken links feature extraction includes lexical features, URL-based features, network-based features, and domain-based features.

Gupta et al. [14] developed a revolutionary anti-phishing technique that pulls characteristics just from the client-side. The proposed solution is quick and dependable since it does not rely on a third party and extracts features exclusively from URLs and source code. They got 99.09% total detection accuracy for phishing websites in their report. This article concluded that this technique has limitations because it can only recognise webpages written in HTML. This method cannot detect non-HTML websites.

Dhamija et al. [15] demonstrates that many internet users have difficulty detecting phishing assaults. Even when consumers are given the specific duty of identifying phishing schemes, many of them are unable to discern between a legal website and a faked website. The best phishing site in the survey deceived more than 90% of the subjects. Furthermore, people frequently do not understand certain security indicators, such as the padlock signifying secure transmission, signal the reliability of a website.

Fette et al. [16] introduced PILFER, an email filtering strategy that included ten characteristics, including URL and script-based elements, to identify phishing assaults. By screening phishing emails before they are seen by users, the percentage of fraudulent users can be reduced. Phishers can conceal the URL and utilise tools such as TinyUrl to make it look genuine. Phishers' methods are growing more complex, and they are adding ways to circumvent existing anti-phishing solutions.

# steps in phishing

A phisher is someone who engages in virus operations. Phishing attempts today generally deploy broad "lures", frightening victims and inciting panic - a frequent example is "we need you to confirm your account credentials or we must shut your account down". A more advanced strategy that is considered to be becoming more popular is context-aware attack: this is a more complex approach since it not only employs threat or inducement but also makes the target think of the communications as anticipated and therefore legitimate.

Phishers often create bogus websites that seem similar to legitimate websites by replicating the HTML code and using the same graphics, content, and sections. Some phishing websites register a domain name that is identical to the real website of a firm or bank. Forms are the most typical approach employed by phishers, such as the Internet Banking login page or a form for account verification. Many phishing efforts involve domain spoofing or homographic assaults to persuade victims to provide personal information (Gabrilovich & Gontmakher).

A phisher might target a variety of sensitive information, such as user names and passwords, credit card data, bank account details, and other personal information. According to Gartner research (Gartner Inc, 2004), around 19% of those polled claimed having clicked on a link in a phishing email, and 3% admitted to providing financial or personal information [17].

A common phishing attack is (for a phisher) to obtain a victim's authentication information corresponding to one website (that is corrupted by the attacker) and then use this at another site. This is a meaningful attack given that many computer users reuse passwords – whether verbatim or with only slight modifications. The phishing attack lifecycle can be decomposed in:

* Planning
* Setup
* Attack
* Collection
* Fraud
* Post-Attack Actions.

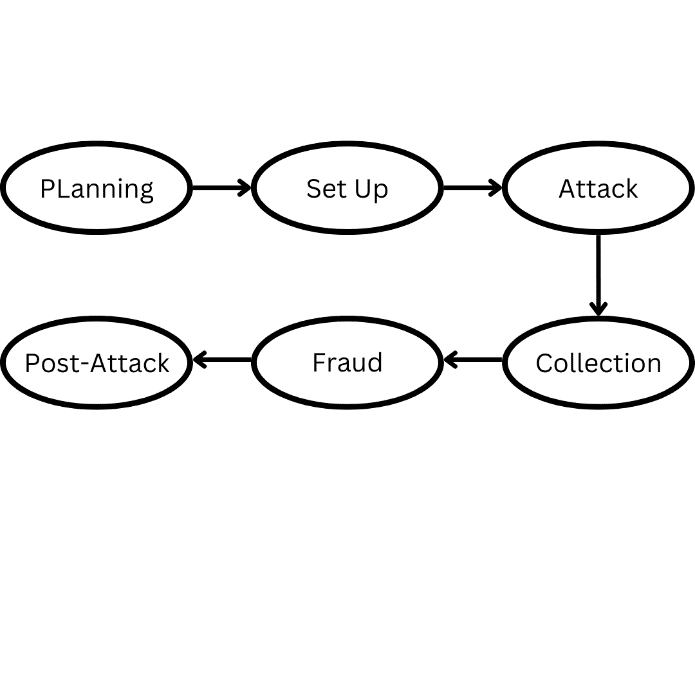


Figure 1. Steps in Phishing

The phisher produces the attack code/message and delivers it to the target user. A harmful message is delivered to the target site. The unaware target sees the message and does anything that exposes him or her to an information breach. The user is then solicited for sensitive information via a familiar and trustworthy online interface. The user divulges sensitive information. The phisher receives private information from a phishing server. The phisher commits fraud by impersonating the user using private information [18].

There is no single method for preventing all phishing. However, different approaches used at different phases of a phishing campaign can stop it, and correctly used technology can dramatically lower the danger of identity theft.

# types of phishing attacks

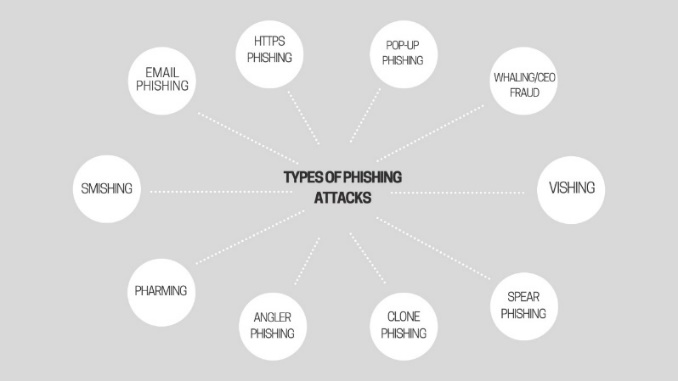


Figure 2. Types of Phishing Attacks

## Email phishing

Email phishing, often known as "deception phishing," is one of the most well-known attack methods. Malicious hackers send emails to consumers imitating a well-known company, then utilize social engineering strategies to create a false feeling of urgency, leading them to click on a link or download an item.

Traditionally, the links lead to malicious websites that either steal credentials or install harmful code, referred to as malware, on a user's device. The downloads, which are often PDFs, include harmful material that installs malware when the victim views the document.

How to identify email phishing:

The majority of individuals are aware of some of the basic indications of a phishing email. However, some conventional things to look for while attempting to manage risk include:

Genuine information: Search for contact information or other valid information about the faked company, then look for things like misspellings or a sender email address with the incorrect domain.

Code that is malicious and codes that is benign: Be on the lookout for anything, including code, that attempts to fool Exchange Online Protection (EOP), such as downloads or URLs with misspellings.

Abbreviated links: Avoid clicking on any shortened URLs since they are designed to deceive Secure Email Gateways.

## HTTPS phishing

Because it employs encrypting to strengthen security, the hypertext transfer protocol secure (HTTPS) is sometimes seen as a "safe" link to click. Because HTTPS provides authenticity, most reputable enterprises now utilize it instead of HTTP. However, fraudsters are increasing including HTTPS in the URLs they include in phishing emails.

How to identify HTTPS phishing:

While this is frequently used as part of an email phishing assault, it is a little more complex method. Take the following into account when determining if a link is authentic or not:

Link shortened: Check that the link is in its original, long-tail format and contains all of Check that the link is in its original, long-tail format and contains all of the URLs.

Hypertext: Hypertext links are "clickable" links contained in the text that mask the true URL.

## Spear phishing

Although spear phishing uses email, it is more targeted. Cybercriminals begin by gathering information from published or publicly available sources such as social media or a company site using open-source intelligence (OSINT). Then they target particular persons inside the business by utilizing legitimate names, work roles, or work phone numbers to fool the receiver into thinking the email came from someone else within the organization. Finally, because the receiver believes this is an authorized request, the individual does the activity specified in the email.

How to identify spear phishing:

Abnormal request: Be on the lookout for internal requests that originate from personnel in other departments or appear unusual given the job role.

Shared drive links: Links to documents kept on shared drives such as Google Suite, Office 365, and Dropbox should be avoided since they might redirect to a phony, malicious website.

Password-protected documents: Documents that demand a user login ID and password: Whatever documents need a user username and password could be an effort to steal data.

## Whaling/CEO fraud

Whale phishing, also known as whaling or CEO fraud, is another sort of corporate phishing that uses OSINT. Malicious hackers research the profile of the company's CEO or any senior management member via social media or the company website. They then use a similar email address to represent that individual. The email may demand a money transfer or that the correspondent evaluate a paper.

How to identify CEO fraud:

Abnormal request: If a top management member has never contacted you before, proceed with caution.

Recipient email: Because many individuals use email apps that connect all of their email accounts, make sure that any request that seems regular is made to a business email rather than a personal email account.

## Vishing

Voice phishing, often referred as "vishing," occurs when a computer hacker calls a phone number and instills a false sense of urgency, causing a person to act against their best interests. Generally, these calls are typically made during difficult periods. During tax season, for example, many people receive bogus phone calls from someone claiming to be from the Internal Revenue Service (IRS), saying that they want to conduct an audit and want a social security number. Because the call induces stress and urgency, the receiver may be duped into disclosing personal information.

How to identify vishing:

Caller ID: The number may be from an odd location or may be banned.

Timing: The call's timing corresponds with a stressful season or event.

Action requested: The caller seeks personal details that is strange given the sort of caller.

Unexpected call: When alternative, more established ways of communication are available, a call from even a recognized number or area code should be viewed with caution.

## Smishing

Cybercriminals frequently employ similar strategies across many sorts of technologies. Smishing is the practice of sending messages that request someone to do action. These are the next step in the progression of vishing. Frequently, the content will contain a link that, when visited, will install malware on the client’s device.

How to identify smishing:

Change in delivery status: A text message demanding that the receiver take action to alter a delivery will contain a link, so always check emails or the delivery service site to monitor the status.

Unusual area code: Before replying to a text or executing a suggested action, check the area code and match it to your contacts list.

## Angler phishing

As criminal actors shift between attack channels, social media has emerged as a new hotspot for phishing assaults. Angler phishing, like vishing and smishing, occurs when a malicious attack exploits the notifications or online messaging functions of a social networking program to urge someone to take action.

How to identify angler phishing:

Notifications: Be aware of notifications indicating that you have been added to a post since they may contain links that take recipients to malicious websites.

Direct communications from users who infrequently use the function should be avoided since the account might be faked or fraudulently constructed.

Website links: Never follow a link in a direct message, no matter how credible it appears, unless the sender routinely sends relevant links in this manner.

## Pharming

Pharming is more sophisticated and frequently harder to detect. The malicious actors compromise a Domain Name Service (DNS), which is the server that converts URLs from natural language to IP addresses. When a user fills in the website address, the DNS server sends the user to the IP address of a malicious website that may appear legitimate.

How to identify pharming:

Unsafe website: Look for a website that is HTTP rather than HTTPS.

Website inconsistencies: Be wary of any inconsistencies that suggest a false website, such as mismatched colors, misspellings, or unusual typefaces.

## Pop-up phishing

Despite the fact that most individuals use pop-up blockers, pop-up phishing is still a concern. Harmful actors can insert malicious malware into the little notice windows known as pop-ups that appear when visitors visit websites. The most recent variant of pop-up phishing makes use of the web browser's "notifications" feature. When a person browses a website, for example, the browser asks them "www.thisisabadlifechoice.com wishes to show alerts." When the user selects "Allow," harmful malware is installed.

How to identify pop-up phishing:

Irregularities: Check for spelling mistakes or unusual color schemes.

Malicious pop-ups can cause a browser to switch to full-screen mode, thus any automatic change in screen size could be a warning.

## Clone phishing

Another type of targeted email phishing assault, clone phishing, uses services that someone has already used to initiate the negative action. Most business systems that need individuals to click links as part of their regular activity are known to be malicious attackers. They will frequently do research to determine what sorts of services a firm utilizes on a regular basis, then deliver specific targeting emails that look to be from these services. Because many businesses use DocuSign to issue and receive electronic contracts, unscrupulous actors may create fabricated emails for this service.

How to identify clone phishing:

Abnormal timing: Be suspicious of any unanticipated email from a network operator, even if it is part of your routine daily work function.

Personal information: Be wary of emails that want personal and sensitive information that the network operator never requests.

# anti-phishing techniques

In [19] a method was developed in which the Automated Individual White-List (AIWL), an automated list, aims to maintain a white list of the user's familiar Login User Interfaces (LUI). When a user submits login credentials or sensitive information to a LUI that is not on the white-list, AIWL warns the user of the potential trap and warns him/her of the ensuing assault.

In [20] the authors presented a method to fight against phishing assaults by combining visual similarity-based approaches with a white list. The Speed up Robust Features (SURF) detector is a Computer Vision (CV) tool. This detector extracts discriminative key point characteristics using square-shaped filters. These characteristics are taken from both questionable and legitimate websites. The retrieved characteristics from the websites are then compared to determine the degree of resemblance. The degree of resemblance thus aids in deciding whether or not the website is credible. If the degree of similarity was great, it was considered harmful since the real website was attempting to be mimicked.

In [21], a new approach was presented, using the use of Support Vector Machines (SVM) to determine whether or not the email is malicious. The SVM extracted common properties of the email, such as language, layout, and structure. It then compares the retrieved details with the details in the system to determine the correctness of the similarity. If the accuracy surpasses a particular level, the email is classified as malicious.

The study done in [22] employed a novel Natural Language Processing (NLP) approach to identify whether or not the email was malicious. In this research, they used NLP methods to extract and compare common traits. PhishNet-NLP used natural language approaches in conjunction with the information contained in an email, including the header, links, and body content. PhishSnag detected phishing by using information retrieved from emails. Phish-Sem employed natural language processing (NLP) and statistical analysis on the body of the email to determine if it was phishing or not.

In [23] a more advanced filtering and classification approach was applied. The authors of this research checked the URLs to see if they were malicious. They employed an automated way to detect phishing. It was divided into two phases: pre-filtering and classification. During the pre-filtering step, the URL was compared to a black list utilising the domain portion of the URL. If the URL was on that list, it was classed as malicious and would not progress to the Classification Phase. The randomness of the URL (RU) and the position of the domain token were tested for consistency in the next phase. Based on the findings of the Classification Phase, the URL was classed as malicious or non-malicious.

In [24] the authors of employed text mining to extract different characteristics from emails. For improved identification of the assault, the emails might be phishing or real. Following an initial translation of the email to a vector form, feature selection approaches for classification were used. The study was performed using data sets gathered from the SpamAssassin project's HamCorpus (legitimate e-mail) and the publically accessible PhishingCorpus (phishing e-mail).

# anti-phishing tools

A number of solutions are available to assist defend your business from the sorts of hazards that phishing assaults bring. Knowing what solutions are available and how they may assist safeguard your organisation, and consequently your staff and customers, is half the battle.

## Avanan

Avanan provides anti-phishing software for cloud-hosted email, utilising APIs to train their AI using historical email. The service considers existing relationships between senders and recipients to create a level of confidence, in addition to message contents, formatting, and header information.

## Barracuda Sentinel

Another product that uses mail provider APIs to guard against phishing and corporate email intrusion is Barracuda Sentinel (BEC). Because compromised email accounts frequently lead to other phishing efforts or account-based assaults, Barracuda's emphasis on mitigating subsequent harm as a result of a successful phishing attempt is more valuable than depending exclusively on prevention. Through DMARC research and reporting, Barracuda additionally provides brand protection and domain fraud prevention.

## BrandShield

BrandShield is only dedicated to defending your company's and executives' brands. Detecting phishing attempts (through email, social media, or other channels) that use your company's name or the names of your executives is only one aspect of BrandShield's portfolio. BrandShield also searches the internet for rogue websites that use your brand, as well as marketplaces like Amazon where actual counterfeits of your items may be for sale.

## Cofense PDR

Cofense PDR (Phishing Detection and Response) is a managed service that use both AI-based tools and security specialists to detect and neutralise phishing assaults as they occur. If you need to increase the degree of security, managed services can be more effective than even hiring a full-time team to handle phishing prevention since the managed services team can assess threat data from all of the enterprise systems they safeguard.

## RSA FraudAction

The RSA FraudAction anti-phishing service is definitely from one of the top brands in network security, and the feature set is what you'd expect from a strong hitter. The anti-phishing facility is a managed service, similar to what Cofense provides, and RSA adds capabilities such as site shutdown, forensics, and optional countermeasures such as strategically responding to phishing attempts with planted credentials to track the attack chain and respond appropriately.

## IRONSCALES

IRONSCALES is an email security platform that aims to augment your current email system by dynamic detection and analysis, such as blocking, flagging, or simply putting a banner to potentially suspect messages. IRONSCALES also provides end-user training, with an emphasis on email security and general awareness, to assist reinforce your defence against the heart of phishing: the social engineering assault.

## Mimecast

Mimecast provides many anti-phishing technologies, including capabilities that identify dangerous URLs and attachments and remove or render them safe using sophisticated approaches such as sandboxing. Mimecast's ability to prevent code-based assaults begun via phishing emails or more complex means such as QR codes by opening links within the Mimecast cloud, simplifying deployment and guaranteeing preventative measures are constantly up to date.

## Microsoft Defender for Office 365

Microsoft Defender for Office 365 has many of the same features as the other solutions on our list, including user training, phishing detection and prevention, forensic and root-cause analysis, and threat hunting. Defender is tightly integrated without the need for configuration because it is merely an add-on for Office 365. Microsoft also provides pre-configured security rules that you can customise to meet your needs, as well as support for enforcement, the possibility for users to override, and tracking policy changes over time. This service provides unique benefits for Office 365 users and unique drawbacks for everyone else.

# Case Study

## Case No. 1 – Twitter Phishing Case 2020

Everyone should be thinking about the July 2020 Twitter Phishing incident. The employees' passwords were compromised by threat actors in a textbook instance of illegal access.

In July 2020, spear phishing assaults targeted a number of Twitter workers, giving the malicious attackers access to the admin tools. Malicious attackers pretended to be Twitter IT managers and contacted remote workers by phone or email and requested login credentials. The cybercriminals were able to use these hacked accounts to access the administrator's tools. In order to tweet scam messages requesting Bitcoin donations, they were able to reset the Twitter accounts of famous people such as Elon Musk, Barack Obama, Jeff Bezos, Apple, Uber, and many more.

Given the enormous fan bases of these celebrity accounts, at least $180,000 worth of Bitcoin was sent to phishing accounts by several Twitter users. Fortunately, the press reported on the hoax communications and found them. It compelled Twitter to act right away.

Lessons Learned from The Case

Because the affected employees' devices lacked the necessary email phishing prevention software, Twitter failed to implement suitable cybersecurity tactics. Solutions for managing privileged access and keeping an eye on user and object behavior may have prevented this fraud.

Due to its inability to identify and stop the fraud in time, Twitter saw a 4% decline in its share price. In order to upgrade security standards, Twitter has to halt the rollout of its new API. It is essential to educate staff members about social engineering scams to stop such frauds from happening. Even though the financial loss was minimal, Twitter's status as one of the most secure social media networks was damaged.

## Case No. 2: Upsher - Smith Laboratories Case 2014

Over $39 Million Loss. Even though this event occurred in 2014, it is essential since it is one of the primary email cases of CEO Fraud. CEO fraud is a cyber-attack done by criminal actors in which they send phishing emails to workers of an enterprise while impersonating the CEO.

In this case, cyber attackers posing as the organization's CEO contacted the Accounts Payable Coordinator at Upsher-Smith Laboratories, a Maple Grove-based medicine store, instructing her to obey the CEO's and the organization's lawyer's instructions. The commands were to make nine wire payments totaling more than $50 million to the scammer's accounts. Despite successfully halting one of the bank transfers, the group suffered a $39 million loss.

Factor of Employee Negligence

The employee in this situation was careless in taking the emails at face value. He or she may have called the CEO's office to check the origin of such communications, particularly if they were not following established protocols. The bank managing the transfer is also irresponsible in failing to notice the numerous red flags, namely the quantity and frequency of transfers, questionable recipients, and failure to include a second signature to the requests.

Lessons Learned from The Case

In general, CEOs do not actively request that workers make urgent transfers. Even if they do, the staff may have sent an email confirming the request. A simple phone call may have prevented this crime from occurring.

Most phishing emails have a sense of urgency. They also demand secrecy. In general, such requests are deviations from the organization's standard operating procedures.

The main takeaway from this attack is to never take an email at its value. It is not expensive to confirm.

# Conclusion

Phishing attacks have become a major issue in today’s digital world. They are an attempt to acquire sensitive information such as usernames, passwords, and credit card details through deceptive emails and websites. As more and more people become increasingly reliant on technology, the risk of falling victim to a phishing attack continues to rise.

In order to protect against phishing attacks, it is important to understand the tactics used by attackers. Be aware of any emails or websites that look suspicious or ask for personal information. Always double-check the URL of any website before providing any sensitive information. Additionally, practice good password hygiene and use two-factor authentication when available.

Finally, it is important to stay informed of the latest phishing tactics and be aware of the potential risks associated with phishing. Organizations should also invest in security solutions that can detect and block phishing attempts. By following these simple precautions, users and organizations can avoid falling victim to a phishing attack.

##### References

1. Kirda E, Kruegel C. Protecting users against phishing attacks with antiphishing techniques. In annual international computer software and applications conference 2005 (pp. 517-24). IEEE.
2. Mei Y. Anti-phishing system: detecting phishing e-mail. School of Mathematics and Systems Engineering. 2008.
3. Yadav S, Bohra B. A review of recent phishing attacks on the internet. In international conference on green computing and internet of things 2015 (pp. 1312-5). IEEE.
4. IRONSCALES. How modern email phishing attacks have organizations on the hook. 2017.
5. APWG. APWG phishing trends report 2nd quarter 2021. 2021.
6. Alfayoumi IS, Barhoom TS. Client â [euro]" Side pharming attacks detection using authoritative domain name servers. International Journal of Computer Applications. 2015; 113(10):26-31.
7. Ollmann G. The vishing guide. IBM Global Technology Services. 2007:1-16.
8. Anti-phishing working group. APWG Phishing activity trends report 2nd quarter 2012.
9. Chanti S, Chithralekha T. Classification of anti-phishing solutions. SN Computer Science. 2020; 1(1):1-8.
10. Ludl, Christian et al. “On the Effectiveness of Techniques to Detect Phishing Sites”. In: (2007). Ed. by Bernhard M. Hämmerli and Robin Sommer, pp. 20–39.
11. T. Churi, P. Sawardekar, A. Pardeshi, and P. Vartak, “A secured methodology for anti-phishing,” Proc. 2017 Int. Conf. Innov. Information, Embed. Commun. Syst. ICIIECS 2017, vol. 2018- Janua, pp. 1–4, 2018.
12. S. Aonzo, A. Merlo, G. Tavella, and Y. Fratantonio, “Phishing attacks on modern android,” Proc. ACM Conf. Comput. Commun. Secur., pp. 1788–1801, 2018.
13. Routhu Srinivasa Rao1 , Alwyn Roshan Pais : Detection of phishing websites using an efficient feature-based machine learning framework :In Springer 2018.
14. Ankit Kumar Jain, B. B. Gupta : Towards detection of phishing websites on client-side using machine learning based approach :In Springer Science+Business Media, LLC, part of Springer Nature 2017.
15. R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in Computing Systems, pages 581–590, 2006.
16. Fette, I., Sadeh, N., Tomasic, A.: Learning to detect phishing emails. In: Proceedings of the 16th international conference on World Wide Web, pp. 649–656 (2007)
17. Kirk J. (2011). Phishing Tool Constructs New Sites in Two Seconds.
18. Camp LJ, Goodman S, House CH, Jack WB, Ramer R and Stella M. Chapter 6: Offshoring: Risks and Exposures.
19. Ye Cao, Weili Han and Yueran Le - Anti-phishing based on automated individual white-list, Proceed- ings of the 4th ACM workshop on Digital Identity Management, pp. 51-60, October 2008.
20. Routhu Srinivasa Rao and Syed Taqi Ali - A Com- puter Vision Technique to Detect Phishing Attacks, 5th International Conference on Communication Systems and Network Technologies, IEEE, October 2015.
21. Madhusudhanan Chandrasekaran, Krishnan Narayanan and Shambhu Upadhyaya - Phishing E- mail Detection based on Structural Properties, IEEE, November 2015.
22. Rakesh Verma, Narasimha Karpoor, Nabil Hossain and Nirmala Rai - Automatic Phishing Email De- tection based on Natural Language Processing Techniques, Research Gate, 2016.
23. Yi-Shin Chen, Huei-Sin Liu, Yi-Hsuan Yu and Pang-Chieh Wang, Detect Phishing by Checking Content Consistency, IEEE, 2017.
24. Masoumeh Zareapoor, K.R. Seeja, Text Mining for Phishing E-mail Detection, Intelligent Computing, Communication and Devices: Advances in Intelli- gent Systems and Computing, vol. 308, pp. 65-71, August 2016.