iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** XII **Month of publication:** December 2024

DOI: https://doi.org/10.22214/ijraset.2024.66073

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XII Dec 2024- Available at www.ijraset.com

Phishing: History, Effects, Targeted Area and Countermeasure

Rajesh Tanti
Computer Science and Engineering, OP Jindal University, Raigarh, Chhattisgarh

Abstract. The web has turned into a principal part of our conventional social and financial activities. Web works arriving at clients all around the globe with no commercial center limitations and with successful utilization of internet business. Consequently, Internet customers may be defenceless against different kinds of web risks, that may cause financial damages, information forgery, brand reputation mischief, the sacrifice of private information, and loss of customers' confidence in online business and electronic banking. Thusly, the reasonableness of the Internet for business exchanges becomes dubious. Phishing is seen as a design of web peril which is classified as the forte of mimicking a website of a legitimate undertaking proposing to gain a client's private accreditations, for instance, usernames, passwords, and federal retirement aide numbers. In this paper, we present an survey on the phishing activity, their impact, causes prevention, threads , reports and Cyber Lab security concern . we also discuss about how we can establish a batter cyber security lab to protect from phishing and malware This paper also present an overview report of LACL Cyber Lab which establish in Los Angeles to protect from all cyber attack and how we can gain the knowledge about new threads. .

Keywords: Phishing attack, Phishing types ,Work strategy, Impact factor, Cost of Breach,Social media, Prevention, Man-in – middle (MiTM), SMS, MFA, CISCO, Los Angeles Cyber Lab ("LACL" or "Cyber Lab").

I. INTRODUCTION

Today is the era of digitalization , every individual is using the internet facility . Internet makes the life so much easy and predictable . every individual is using the social media , internet banking , online commerce etc. for their personal use and efficient process. People are sharing their information , uploading photos , live location and performing transactions of money and other things.

Because people are no awareness about the cyber-attack, the hackers are taking the benefit and performing the criminal activities .

Phishing is an act of attempting a victim for fraudulently acquires sensitive information by impersonating a trustworthy third party, which could be a person or a reputed business in an electronic communication. The objective of phishing attack is to trick receivers into divulging sensitive information such as bank account numbers, passwords and credit card details. For instance, a phisher may misrepresenting himself as a large banking corporation or popular on-line auction site will have a reasonable yield, despite knowing little to nothing about the recipient .Phishing is a common type of cyber-attack that targets individuals through email, text messages, phone calls, and other forms of communication. As a popular form of social engineering, phishing involves psychological manipulation and deception whereby threat actors masquerade as reputable entities to mislead users into performing specific actions. These actions often involve clicking links to fake websites, downloading and installing malicious files, and divulging private information, like bank account numbers or credit card information. However, phishing attacks have become increasingly sophisticated and are now broken down into different types, including email phishing, spear phishing, smishing, vishing, and whaling. Each type is characterized by specific channels and methods of execution – email, text, voice, social media, etc. – all with a similar underlying intention.

II. THE PHISHING HISTORY

The first time someone used the term 'phishing' can be traced back to January 2nd, 1996. During the 1990s, hackers would pretend to be AOL administrators and phish for login credentials so they can access the internet for free. A group called the Warez community, mainly composed of pirates and hackers, would steal user's credentials and generate random credit card numbers in order to get an AOL account. This scam, although very simple, was effective since no one. This scam, although very simple, was effective since no one really knew anything about phishing threats. However, phishing would only continue to be one of the most prevalent problems companies face today.

©IJRASET: All Rights are Reserved

The following table-1 shows the phishing attack scenario from 2005- 2019

Total number of unique phishing reports (campaigns) received, according to APWG[30]

Year	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Total
2005	12,845	13,468	12,883	14,411	14,987	15,050	14,135	13,776	13,562	15,820	16,882	15,244	173,063
2006	17,877	17,163	18,480	17,490	20,109	28,571	23,670	26,150	22,136	26,877	25,816	23,787	268,126
2007	29,930	23,610	24,853	23,656	23,415	28,888	23,917	25,624	38,514	31,650	28,074	25,683	327,814
2008	29,284	30,716	25,630	24,924	23,762	28,151	24,007	33,928	33,261	34,758	24,357	23,187	335,965
2009	34,588	31,298	30,125	35,287	37,165	35,918	34,683	40,621	40,066	33,254	30,490	28,897	412,392
2010	29,499	26,909	30,577	24,664	26,781	33,617	26,353	25,273	22,188	23,619	23,017	21,020	313,517
2011	23,535	25,018	26,402	20,908	22,195	22,273	24,129	23,327	18,388	19,606	25,685	32,979	284,445
2012	25,444	30,237	29,762	25,850	33,464	24,811	30,955	21,751	21,684	23,365	24,563	28,195	320,081
2013	28,850	25,385	19,892	20,086	18,297	38,100	61,453	61,792	56,767	55,241	53,047	52,489	491,399
2014	53,984	56,883	60,925	57,733	60,809	53,259	55,282	54,390	53,661	68,270	66,217	62,765	704,178
2015	49,608	55,795	115,808	142,099	149,616	125,757	142,155	146,439	106,421	194,499	105,233	80,548	1,413,978
2016	99,384	229,315	229,265	121,028	96,490	98,006	93,160	66,166	69,925	51,153	64,324	95,555	1,313,771
2017	96,148	100,932	121,860	87,453	93,285	92,657	99,024	99,172	98,012	61,322	86,547	85,744	1,122,156
2018	89,250	89,010	84,444	91,054	82,547	90,882	93,078	89,323	88,156	87,619	64,905	87,386	1,040,654
2019	34,630	35,364	42,399	37,054	40,177	34,932	35,530	40,457	42,273	45,057	42,424	45,072	475,369

Table 1: Phishing report generated by APWG.

A. Today

While cybersecurity experts are catching up, it's far from enough. Both security researchers and hackers are stuck in a never ending battle where they constantly try to one-up the other using new technologies, scenarios, and attack methods.

INTERPOL mentions that in March 2020, there were more phishing attacks compared to February 2020. Additionally, while emails have been dominating in phishing the past decade, 2020 marked the rise in scams done through phone calls (vishing) and SMS or text messages (smishing).

In 2021 Tessian research found that employees receive an average of 14 malicious emails per year. Some industries were hit particularly hard, with retail workers receiving an average of 49. ESET's 2021 research found a 7.3% increase in email-based attacks between May and August 2021, the majority of which were part of phishing campaigns.

And 2021 research from IBM confirmed this trend, citing a 2 percentage-point rise in phishing attacks between 2019 and 2020, partly driven by COVID-19 and supply chain uncertainty. CISCO's 2021 Cybersecurity threat trends report suggests that at least one person clicked a phishing link in around 86% of organizations. The company's data suggests that phishing accounts for around 90% of data breaches.

There's an uneven distribution in phishing attacks throughout the year. Cisco found that phishing tends to peak around holiday times, finding that phishing attacks soared by 52% in December. We've written about a similar phenomenon that typically occurs around Black Friday.

B. Jan-Jun 2024

1) APWG observed total 18,41,530 phishing attacks, performed in first –Second quarter of 2024.

2) Social media platforms were the most frequently attacked sector, in 2024. Banking-segment phishing continued to decline, down to 9.8 percent.

3) Google Gmail accounts were used in 72.4 percent of all Business Email Compromise (BEC) scams.

III. DIFFERENT TYPES OF PHISHING ATTACKS

Phishing involves an attacker trying to trick someone into providing sensitive account or other login information online. All the different types of phishing are designed to take advantage of the fact that so many people do business over the internet. This makes phishing one of the most prevalent cybersecurity threats around, rivaling distributed denial-of-service (DDoS) attacks, data breaches, and many kinds of malware.

Knowing the different types of phishing attacks can equip you to protect your organization from each.

1) *Spear phishing:* Spear phishing involves targeting a specific individual in an organization to try to steal their login credentials. The attacker often first gathers information about the person before starting the attack, such as their name, position, and contact details.
2) *Vishing:* Vishing, which is short for "voice phishing," is when someone uses the phone to try to steal information. The attacker may pretend to be a trusted friend or relative or to represent them.
3) *Email phishing:* In an email phishing scam, the attacker sends an email that looks legitimate, designed to trick the recipient into entering information in reply or on a site that the hacker can use to steal or sell their data.
4) *HTTPS phishing:* An HTTPS phishing attack is carried out by sending the victim an email with a link to a fake website. The site may then be used to fool the victim into entering their private information.
5) *Pharming:* In a pharming attack, the victim gets malicious code installed on their computer. This code then sends the victim to a fake website designed to gather their login credentials.
6) *Pop-up phishing:* Pop-up phishing often uses a pop-up about a problem with your computer's security or some other issue to trick you into clicking. You are then directed to download a file, which ends up being malware, or to call what is supposed to be a support center.
7) *Evil twin phishing:* In an evil twin attack, the hacker sets up a false Wi-Fi network that looks real. If someone logs in to it and enters sensitive details, the hacker captures their info.
8) *Watering hole phishing:* In a watering hole phishing attack, a hacker figures out a site a group of users tends to visit. They then use it to infect the users' computers in an attempt to penetrate the network.
9) *Whaling:* A whaling attack is a phishing attack that targets a senior executive. These individuals often have deep access to sensitive areas of the network, so a successful attack can result in access to valuable info.
10) *Clone phishing:* A clone phishing attack involves a hacker making an identical copy of a message the recipient already received. They may include something like "resending this" and put a malicious link in the email.
11) *Deceptive phishing:* Deceptive phishers use deceptive technology to pretend they are with a real company to inform the targets they are already experiencing a cyberattack. The users then click on a malicious link, infecting their computer.
12) *Social engineering:* Social engineering attacks pressure someone into revealing sensitive information by manipulating them psychologically.
13) *Angler phishing:* Anglers use fake social media posts to get people to provide login info or download malware.
14) *Smishing:* Smishing is phishing through some form of a text message or SMS.
15) *Man-in-the-middle (MiTM) attacks:* With a man-in-the-middle attack, the hacker gets in "the middle" of two parties and tries to steal information exchanged between them, such as account credentials.
16) *Website spoofing:* With website spoofing, a hacker creates a fake website that looks legitimate. When you use the site to log in to an account, your info is collected by the attacker.
17) *Domain spoofing:* Domain spoofing, also referred to as DNS spoofing, is when a hacker imitates the domain of a company—either using email or a fake website—to lure people into entering sensitive information. To prevent domain spoofing, you should double-check the source of every link and email.
18) *Image Phishing:* Image phishing uses images with malicious files in them meant to help a hacker steal your account info or infect your computer.
19) *Search Engine Phishing:* A search engine phishing attack involves an attacker making fake products that look attractive. When these pop up in a search engine, the target is asked to enter sensitive information before purchasing, which then goes to a hacker.

IV. HOW PHISHING WORKS

Phishing is a type of social engineering and cybersecurity attack where the attacker impersonates someone else via email or other electronic communication methods, including social networks and Short Message Service (SMS) text messages, to reveal sensitive information.Phishers can use public sources of information, such as LinkedIn, Facebook and Twitter, to gather the victim's personal details, work history, interests and activities. These resources are often used to uncover information such as names, job titles and email addresses of potential victims. An attacker can then use information to craft a believable phishing email.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

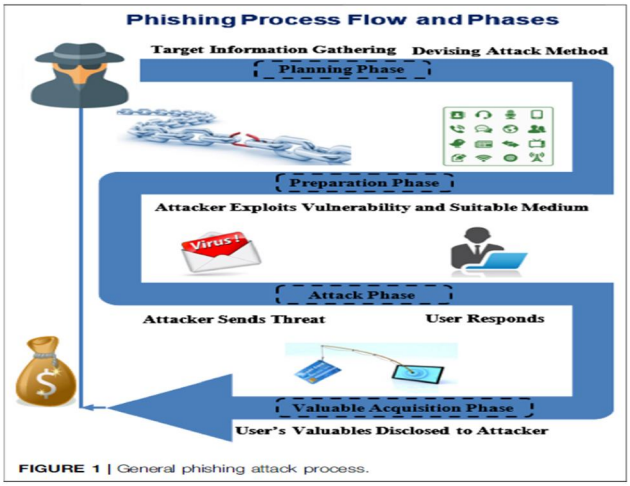


Figure 1 Showing the general method for phishing activity by hackers

Typically, a victim receives a message that appears to have been sent by a known contact or organization. The attack is then carried out either when the victim clicks on a malicious file attachment or clicks on a hyperlink connecting them to a malicious website. In either case, the attacker's objective is to install malware on the user's device or direct them to a fake website. Fake websites are set up to trick victims into divulging personal and financial information, such as passwords, account IDs or credit card details. Although many phishing emails are poorly written and clearly fake, cybercriminals are using artificial intelligence (AI) tools such as chatbots to make phishing attacks look more real.

Other phishing attempts can be made via phone, where the attacker poses as an employee phishing for personal information. These messages can use an AI-generated voice of the victim's manager or other authority for the attacker to further deceive the victim. Figure 1 Showing the general method for phishing activity by hackers.

V. INDUSTRIES COMMONLY TARGETED AND THEIR IMPACT

1) Technology

Phishing statistics for Technology:

- Nearly 82% of CIOs believe that their software supply chain securities are weak.
- Cyber attacks were 50% more per week in 2021 on corporate networks globally.
- 65% increase in global losses between July 2019 to December 2021.
- Nearly 1.7 billion were lost businesses per minute in 2021.
- 80% of reported cyber crimes are generally attributed to phishing attacks in the technology sector.

2) Healthcare

Healthcare phishing statistics:

- 90% of healthcare institutions have experienced at least one security breach in the previous few years.
- Phishing and other forms of cyber attacks have seen a 75% increase in 2021.
- 30% of most data breaches occur in large hospitals with a record of exposing patients' private health information.

3) SMEs

Phishing statistics for SMEs:

- Only 14% of SMEs have a cyber security plan in place.
- The next five years are due to see a 15% increase in cybercrime costs reaching 10.5 trillion by 2025.
- Small businesses account for 43% of cyber attacks annually.
- An average of $25,000 is lost by SMEs.
- Besides phishing, other common cyber attacks on SMEs include credential theft and making use of stolen devices.

4) Educational Sector

- Educational institutions saw a 75% increase in cyber-attacks.
- Currently, most malware scams affect the educational sector largely making them an at-risk sector.

In terms of security against such phishing scams, educational institutions rank very last.

A. The Most Targeted Industries

In the second quarter of 2024, APWG founding member OpSec Security found that social media platformswere once again the most frequently attacked sector, representing 32.9 percent all phishing attacks. Phish- ing against the Financial Institution (banking) segment were mostly steady at 10 percent, down from 24.9 percent of all attacks in Q3 2023 and 14 percent in Q4 2023. Attacks against online payment services (such as PayPal, Venmo, Stripe, and similar companies) were also steady, with another 7.5 percent of all attacks.

Matthew Harris, Senior Product Manager, Fraud at OpSec, explained why banking and payment sites are being attacked less frequently. "We have observed an increased share of fraud being targeted towards sites that do not require high security, such as social media sites like Facebook and LinkedIn, and SAAS and Webmail accounts such as Microsoft Outlook and Netflix." Phishing that uses email lures is beinghampered by advanced filtering technologies and sending requirements, making it more difficult for scammers to get their emails into victim in-boxes. Figure 2 showing the graph of most targeted industries in the world by APWG 2024 report.



Figure 2 APWG 2024 report

B. The Most Impersonated Brands

Phishing attackers exploit popular enterprise applications by impersonating popular brands and themes. ThreatLabz researchers found that following enterprise brands a like Microsoft, OneDrive, Okta, Adobe, and SharePoint are prime targets for impersonation due to their widespread usage in enterprise environments and the value they hold in acquiring user credentials.

THE TOP 20 BRANDS MOST FREQUENTLY IMITATED IN PHISHING SCAMS WERE:			
S.no	Name	S.no	Name
01	Microsoft	11	WhatsApp
02	One drive	12	ANZ Banking Group
03	Okta	13	Amazon
04	Adobe	14	FBay
05	SharePoint	15	Instagram
06	Telegram	16	Google
07	pCloud	17	Sparkasse bank
08	FaceBook	18	Pay
09	DHL	19	Gucci
10	FedEx	20	Rakuten

Table 2 : List of Top Brands infected by phishing attack

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XII Dec 2024- Available at www.ijraset.com

C. Phishing by Country

Not all countries and regions are impacted by phishing to the same extent, or in the same way. Here are some statistics from another source showing the percentage of companies that experienced a successful phishing attack in 2020, by country:

- United States: 74%
- United Kingdom: 66%
- Australia: 60%
- Japan: 56%
- Spain: 51%
- France: 48%
- Germany: 47%

Phishing awareness also varies geographically. Here's the percentage of people who correctly answered the question: "What is phishing?", by country:

United Kingdom: 69% ,Australia: 66%,Japan: 66%,Germany: 64%
France: 63%,Spain: 63%,United States: 52%

As you can see, there's no direct correlation between phishing awareness and phishing susceptibility, which is why security training isn't enough to prevent cybercrime.

D. The Most Common Subject Lines

According to Symantec's 2019 Internet Security Threat Report (ISTR), the top five subject lines for business email compromise (BEC) attacks:

1) Urgent
2) Request
3) Important
4) Payment
5) Attention

Analysis of real-world phishing emails revealed these to be the most common subject lines in Q4, 2020:

a) *IT*: Annual Asset Inventory
b) Changes to your health benefits
c) *Twitter*: Security alert: new or unusual Twitter login
d) *Amazon:* Action Required | Your Amazon Prime Membership has been declined.
e) *Zoom:* Scheduled Meeting Error.
f) *Google Pay:* Payment sent.
g) Stimulus Cancellation Request Approved.
h) *Microsoft 365*: Action needed: update the address for your Xbox Game Pass for Console subscription.
i) RingCentral is coming!
j) *Workday*: Reminder: Important Security Upgrade Required

VI. THE COST OF A BREACH

IBM has released its annual Cost of a Data Breach report, which revealed that the average cost of a data breach in India has reached an all-time high of Rs. 19.5 crore ($2.35 million) during the financial year 2024. The numbers have jumped by 39% since 2020 and 9% from the previous year as data breaches become increasingly common.

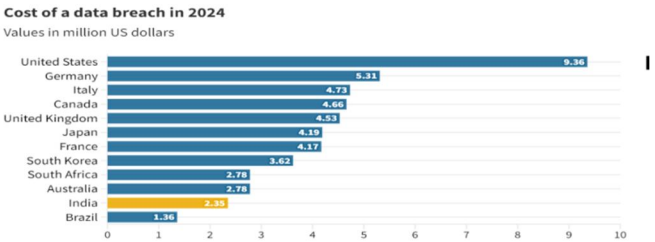


Figure 3: source – cost of data breach 2024 by IBM.

The 12 best tools for phishing simulations

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XII Dec 2024- Available at www.ijraset.com

VII. SOCIAL MEDIA PLATFORMS EXPLOITED BY THREAT ACTORS

In a world where social media reigns supreme, attackers are increasingly leveraging these platforms for phishing endeavors. This trend spans the globe, with the Asia-Pacific, Europe, the Middle East, and Africa experiencing similar patterns of exploitation. Figure 4 shows the most targeted social media platforms observed by ThreatLabz.

A. Most Exploited Social Media Platforms Worldwide

Phishing Attacks Observed in the Zscaler Cloud Platform

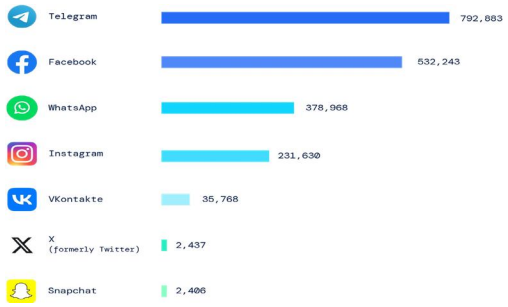


Figure 4:Top social media platforms used in phishing attacks

Above figure showing the phishing hits rate on social media platform , Such media uses more frequently by the world wide people. More details are as follows

Telegram, with 792,883 observed phishing hits, remains a popular target for malicious activities—a trend explored in our blog post on DuckTail. The platform's end-to-end encryption and emphasis on user privacy make it an attractive choice for secure communication. However, threat actors attempt to exploit vulnerabilities in Telegram's security measures to gain unauthorized access to user accounts or distribute malicious content.

Facebook, with 532,243 observed phishing hits, faces ongoing challenges in protecting user data and privacy. As one of the largest social media platforms globally, it attracts cybercriminals who aim to exploit security flaws, launch phishing campaigns, or engage in identity theft.

WhatsApp, with 378,968 observed phishing hits, encounters various security concerns due to its large user base and ubiquitous usage for messaging. While WhatsApp incorporates end-to-end encryption for secure conversations, attackers seek to exploit vulnerabilities to gain unauthorized access, distribute malware, or deceive users through social engineering techniques.

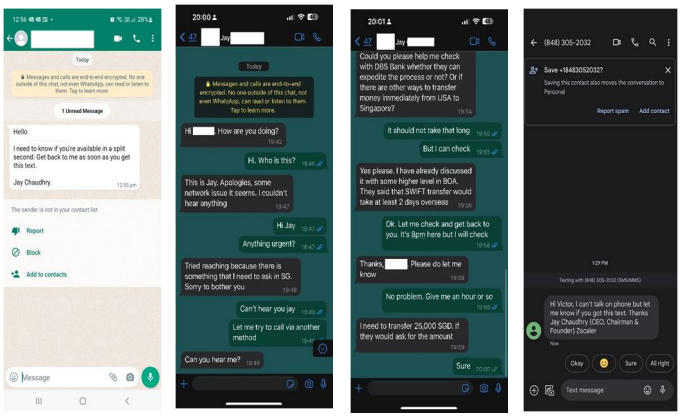


Figure 5: Phishing attack on Whatsapp plateform

Instagram: with 231,630 observed phishing hits, grapples with threats such as account hijacking, phishing attempts, and the spread of malicious links or content. As a leading photo and video sharing platform, it attracts cybercriminals who exploit weak passwords, social engineering tactics, or third-party app vulnerabilities to compromise user accounts.

VKontakte: with 35,768 observed phishing hits, encounters security challenges specific to its user base in Russia and neighboring countries. Cyberthreats targeting VKontakte, a social media and networking service based in Russia, include account breaches, phishing attacks, and the distribution of malicious content.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue XII Dec 2024- Available at www.ijraset.com

X (previously Twitter): with 2,437 observed phishing hits, encounters a range of security issues, including account breaches, impersonation attempts, and the dissemination of fake news or malicious links. X's real-time nature and large user base make it an attractive target for cybercriminals seeking to spread misinformation or compromise user accounts.

Snapchat: with 2,406 observed phishing hits, faces unique security concerns related to its multimedia messaging features and user- generated content. While Snapchat's self-destructing messages provide a level of privacy, attackers may attempt to exploit vulnerabilities to compromise accounts or engage in social engineering scams.

VIII. HOW TO PREVENT PHISHING ATTACKS?

1) *Enable Multifactor Authentication:* Enabling two or multi-Factor Authentication can drastically help reduce and avoid falling prey to phishing attacks. This is because the data obtained through phishing if successful becomes redundant due to the further authentication steps in place.
2) *Cybersecurity Software***:** Opting for a well-established and experienced cyber security software can help in the detection and blocking of such phishing attempts thereby keeping the company and its data secure.
3) *Employee Training:* Giving company employees regular training on secure data handling practices, tips to look out for in recognizing phishing emails, having a top-notch security system in place for their devices, and other similar measures can drastically reduce the chances of being a victim of a phishing scheme.
4) *Be Cautious About E-mails:* Always be cautious about e-mails received. Check for spelling mistakes, immediate requirement subject lines, company details, whether an email has previously been received from the same address, is it trustworthy, these are some of the questions and points that one should take note of when checking emails that look suspicious.
5) *IPv6 Email Infrastructure:* Adopting IPv6 email infrastructure can enhance the security of email systems. IPv6 offers better encryption and a more extensive range of IP addresses, reducing the risk of IP spoofing, a common tactic in phishing attacks. By transitioning to IPv6, organisations can leverage improved security features and more robust authentication mechanisms, making it harder for phishers to exploit vulnerabilities inherent in the older IPv4 systems.
6) *Email Scanning:* Filtering solutions that scan incoming emails for suspicious content, attachments, and links are essential as email remains a primary vector for such attacks. A cloud-based email scanning service is crucial, as it checks emails in real time before they reach a system to protect against malicious links and domain name spoofing.
7) *Awareness and Reporting:* Consider integrating a "report phishing" button directly into email clients, empowering users to report suspicious emails. Establish a comprehensive playbook for investigating and addressing phishing incidents, including reporting to relevant authorities to combat scammers and prevent attacks on other organizations.
8) *Multifactor Authentication (MFA):* MFA stands as a crucial defense against phishing, requiring more than just a password to compromise an account. However, MFA is not a foolproof solution. Instances where attackers target MFA users through SMS and voice phishing underscore the vulnerabilities inherent in MFA security measures.
9) *Encrypted Traffic Inspection:* According to another ThreatLabz report, almost 86% of attacks use encrypted channels across various stages of the kill chain, including initial phases like phishing. Encrypted phishing increased by almost 14% year-over-year in 2023, likely instigated by AI tools and plug-and-play (phishing as a service) offerings. Organizations must inspect all traffic, encrypted or not, to thwart phishing techniques.
10) *Antivirus Software:* Ensure endpoints are protected by consistently updating antivirus software to detect and block malicious files, preventing their download.
11) *Advanced Threat Protection:* Enhance your defenses against new, unknown malware variants that can bypass signature-based detection tools with an AI-powered inline sandbox that isolates and analyzes suspicious files. Additionally, implement browser isolation that creates an isolated browser session for potentially malicious web content, giving users access to a safe rendering while keeping malicious code at bay.
12) *URL Filtering:* Use policy-based controls to manage access to high-risk categories of web content, including newly registered domains. This proactive approach to URL filtering helps to reduce the likelihood of users encountering potentially malicious websites and enhances overall security posture.
13) *Regular Patching:* To minimize vulnerabilities and maintain the latest protections, it's essential to regularly update applications, operating systems, and security tools with the latest patches. Staying current with these updates will effectively reduce potential vulnerabilities and enhance the security of your systems.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

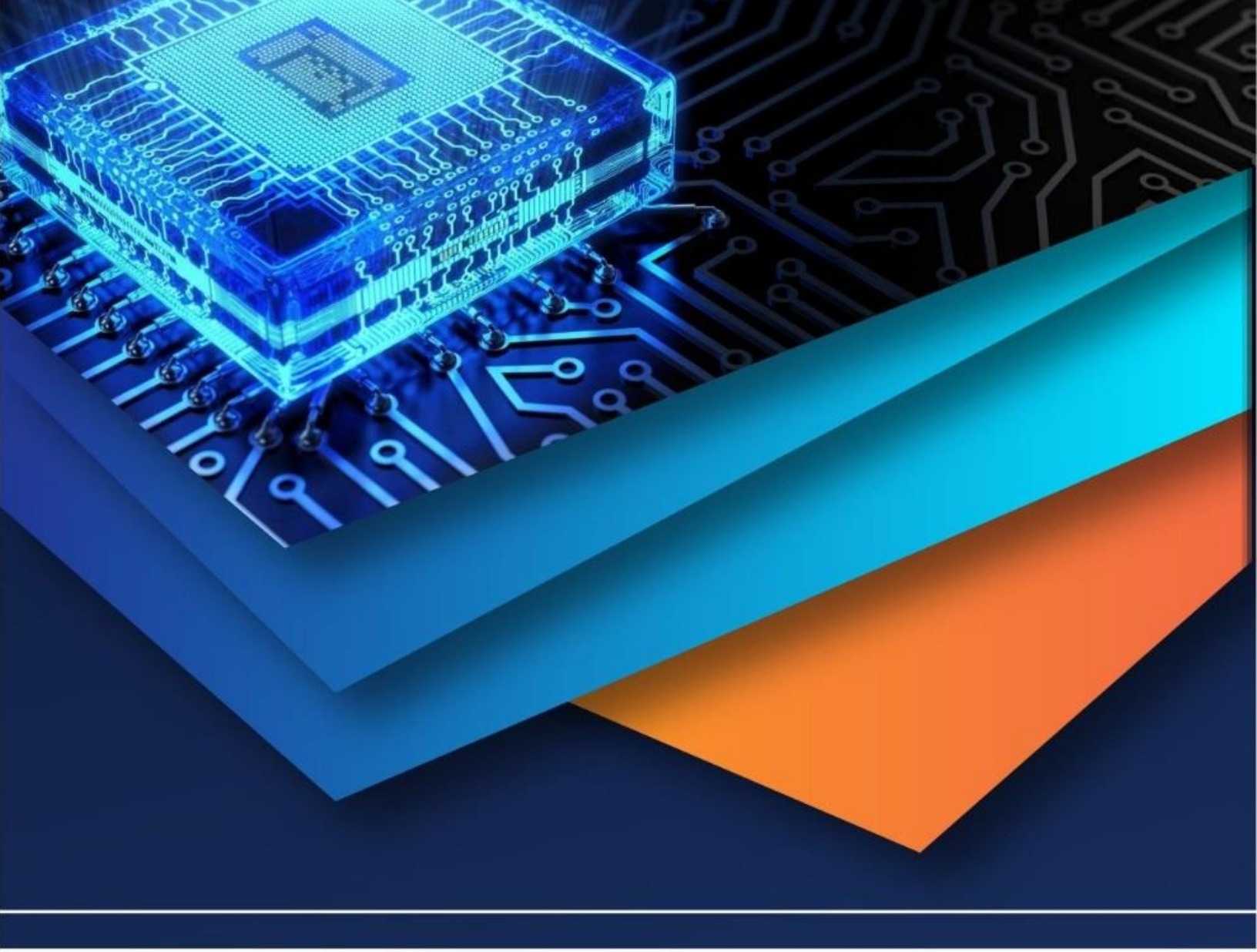
14) *Zero Trust Architecture:* Establishing preventive measures against phishing attacks is key, but it's equally vital to implement a zero trust architecture that reduces your attack surface, prevents lateral movement, and lowers the risk of a breach. Employ granular segmentation to compartmentalize your network, enforce least-privileged access to restrict user permissions, and maintain continuous traffic monitoring. These proactive measures will enable you to identify and respond to threat actors, minimizing potential damage and impact.
15) *Threat intel feeds:* Integrate threat intelligence feeds that continuously monitor for phishing threats with your current security tools to enhance detection capabilities and expedite the resolution of threats. Stay updated with the latest context on reported URLs, extracted indicators of compromise (IOCs), and tactics, techniques, and procedures (TTPs) to facilitate decision-making and prioritization.

IX. CONCLUSION

Phishing is a growing security issue for both institutions and individuals. Although there are various mitigation techniques, proactive anti-phishing training is an important building block of any multi-level phishing defence strategy. In this paper, we discuss about the various factors of phishing, phishing trends and prevention technique , effect of phishing , cost of breach. This is crucial, as our literature analysis showed that research results concerning some of the parameters are inconclusive or even contradictory, indicating that these parameters require further investigation. In this paper we include the report generated by APWG and ThreadLabz with the accurate facts . By the study of research literature we observe that there is no proper Lab or exact method to find and protect from phishing attack because of its upgradation technique ,high technology and lack of knowledge . Because phishing activity developing continuously with high technology , so there is a requirement of high-tech laboratory as a Los Angeles Cyber Lab (LACL) , which provide us a better platform to support the anti phishing program, and courage us to develop such group of specialist to identify new threads and their solution. We are convinced that greater awareness of phishing techniques and means of addressing them increases overall security and peace of mind.

REFERENCES

[1] https://www.zscaler.com/campaign/threatlabz-phishing-report
[2] https://inspiredelearning.com/blog/history-of-phishing/
[3] https://www.zscaler.com/resources/industry-reports/threatlabz-phishing-report-2024.pdf
[4] https://jumpcloud.com/blog/phishing-attack-statistics
[5] https://info.perception-point.io/pdf-h1-report-2024?submissionGuid=f8161522-7672-430d-9132-cdcd3b1 37287
[6] https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks
[7] https://www.tessian.com/blog/phishing-statistics-2020
[8] https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide/
[9] https://www.getastra.com/blog/security-audit/phishing-attack-statistics/
[10] Infosec: phishing definition, prevention, and examples (2019). https ://resou rces.infos ecins titut e.com/categ ory/ enter prise /phish ing/
[11] Bissell K, LaSalle RM, Cin PD (2019) Accenture's ninth annual cost of cybercrime study: unlocking the value of improved cybersecurity protection.
[12] Nero PJ, Wardman B, Copes H, Warner G (2011) Phishing: crime that pays. In: 2011 eCrime researchers summit, pp
[13] 1–10 4. Bisson D (2015) Sony hackers used phishing emails to breach company networks. https ://www.tripw ire.com/state-of-secur ity/lates t-secur ity-news/sony-hacke rs-used-phish ing-email s-to-breac h-compa ny-netwo rks/. Accessed 26
[14] https ://www.accen ture.com/us-en/insig hts/secur ity/cost-cyber crime –study
[15] https://www.globenewswire.com/news- Phishing-Attempts-in-Q3-2020.html



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)