International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 10 | Oct - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

Study of Phishing Attack and their Prevention Techniques

Rajesh Tanti [1]
Computer Science and Engineering
OP Jindal University,Raigarh , Chhattisgarh
Rajeshtanti20017@gmail.com

Abstract. The web has turned into a principal part of our conventional social and financial activities. The web isn't significant for singular clients just yet additionally for associations, since associations that offer web-based exchanging can accomplish an upper hand by serving overall customers. Webworks 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. .

Keyword: Phishing, scam,APWG,HTTP,Popup,EvilTwin, Man-in-The-Middle(MiTM),UniformResource locator(URL),SMS,Quarter1 (Q1),Quarter2 (Q2), Business e-Mail Compromise (BEC) Scam, Username, Password, Pin Number,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 much more aware about the security feature, the hackers are taking the benefit and performing the criminal activities . The one of the most dangerous criminal activity is phishing .

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. A phishing attack aims to trick the recipient into falling for the attacker's desired action, such as revealing financial information, system login credentials, or other sensitive information.

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.

Since the mid-1990s, the term "phishing" has been used to identify hackers who use fraudulent emails to "fish for" information from unsuspecting users. 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.

Phishing threats have reached unprecedented levels of sophistication in the past year, driven by the proliferation of generative AI tools. Transforming how cybercriminals operate, AI advancements are revolutionizing and reshaping the phishing threat landscape. Moreover, this technology has democratized the ability to orchestrate intricate phishing campaigns, making it easier than ever for even beginners to conduct complex and believable phishing attacks. Specifically, this observed shift is enabling novice cybercriminals to launch highly convincing, personalized scams with ease. As a result, organizations now face a myriad of new challenges in protecting their data and systems from the increasing onslaught of phishing attacks.

In response, the Zscaler ThreatLabz team has released the 2024 Phishing Report. This report analyzes over 2 billion phishing transactions from 2023, found within the Zscaler cloud, to equip organizations with a clear understanding of the rapidly evolving phishing landscape. Providing insights into the latest trends and tactics used by cybercriminals, the report highlights active phishing campaigns, exposes emerging schemes, and identifies top targets by region, industry, imitated brand, and more. Showcasing real-world examples, ThreatLabz phishing findings underscore the importance of applying constant vigilance and zero trust security strategies. The guidance offered aims to help organizations strengthen their defenses against these evolving phishing techniques.

Top phishing targets

The United State (US), United Kingdom (UK), India, Canada, and Germany were the top five countries targeted by phishing attacks.

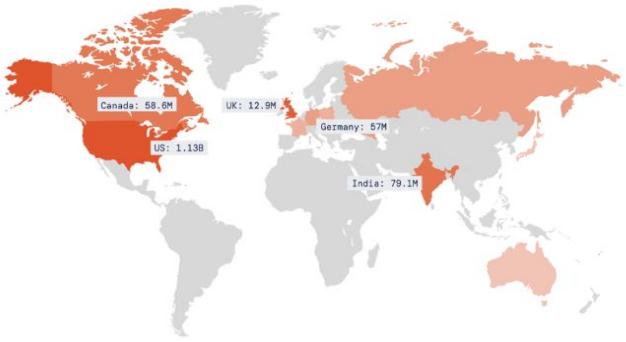


Figure 1 : Most targeted country in the world from phshing attack

II. The History of Phishing

Largely thanks to the pandemic forcing most employees to work from home, phishing has advanced leaps and bounds in the past couple of years.
However, phishing existed long before then.

Here's a quick timeline to help you see how phishing techniques That are changing over time.

1990s

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 really knew anything about phishing threats. However, phishing would only continue to be one of the most prevalent problems companies face today.

2000s-2010s

The 2000s and 2010s is when phishing has started evolving at a rapid pace.
In the early 2000s, people still didn't know much about phishing. It wasn't widespread knowledge that scammers pretend to be trusted authorities to score a jackpot.
During this period, phishers started to turn their attention to online payment gateways, such as Paypal and E-gold. For example, scammers sent an email to Paypal users—and at the time there were already a lot of users—telling them to update their credit card details but stole their details instead.
The late 2008 brought forth cryptocurrencies, untraceable payment methods that hackers use to collaborate with each other, extort their victims, or cash out on their most recent scams securely.

Ransomware, which are mainly sent through phishing emails, runs rampant starting from the Cryptolocker ransomware in 2013, to various other worms, such as WannaCry and Petra.

The loss caused by a ransomware attack isn't small either. Most lost millions of dollars, and that's only from the ransom. There are still fines, operational costs, and restoration costs to consider.

In the early 2010s, you also see a shift on how hackers use phishing attacks, with more of them using it for a larger purpose than the usual financial goals. For example, in 2016, a potentially politically-motivated phishing attack was launched on John Podesta, Hillary Clinton's campaign chairman.

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.

With the growth of social media like LinkedIn or Facebook, cybercriminals found a new treasure trove of information, where they can do research and make their phishing messages more specific and thus, convincing. Unrestricted access to sensitive information helps hackers build personalized spear phishing emails that rely on familiarity and make it harder for users to detect a phishing attempt.

The pandemic forced a lot of companies to go remote, improving the success rate of phishing campaigns over the past couple of years. While companies and employees are adapting to the new remote work security guidelines, hackers took this as an opportunity to attack more small businesses as they don't have much security as larger companies for a bigger payout. INTERPOL mentions that in March 2020, there were 589% more phishing attacks compared to February 2020. That's a nearly 600% increase over a month, which just shows how much hackers are capitalizing on the panic caused by the pandemic.

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.

The *APWG Phishing Activity Trends Report* analyses phishing attacks and other identity theft techniques, as reported to the APWG by its member companies the Q1 and Q2- 2024 having the following phishing activity -

Jan-Mar 2024

Phone-based phishing, directly engaging victims, proliferates unchecked. Phone numbers used for fraud comprised more than 20% of fraud-related assets identified by OpSec in Q1 2024.

Phishing using phone calls — so-called voice phishing or "vishing"— is increasing every quarter.

• In Q1 2024, APWG observed 963,994 phishing attacks, the lowest quarterly total since Q4 2021.

• Social media platforms were the most frequently attacked sector, targeted by 37.4% all phishing attacks in Q1 2024. Banking-segment phishing continued to decline, down to 9.8 percent.

• The average wire transfer amount requested in BEC attacks in Q1 2024 was $84,059, up nearly 50% from the prior quarter's average.

Apr-Jun 2024

In Q2 2024, APWG observed 877,536 phishing attacks while the number of reported phishing attacks has remained generally steady.

• Phishing via phone calls and text messages is being used with increasing frequency to attack bank customers and payment service users.

• Social media platforms were once again the most frequently attacked sector, representing 32.9 percent all phishing attacks.

• The average wire transfer amount requested in BEC attacks in Q1 2024 was $89,520, up from the prior quarter.

• 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.
Example of spear phishing
An attacker tried to target an employee of NTL World, which is a part of the Virgin Media company, using spear phishing. The attacker claimed that the victim needed to sign a new employee handbook. This was designed to lure them into clicking a link where they would have been asked to submit private information.

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.
Example of vishing
In 2019, there was a vishing campaign that targeted members of the UK's parliament and their staffers. The attack was part of an assault that involved at least 21 million spam emails targeting UK lawmakers.

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.

Example of email phishing
Hackers used LinkedIn to grab contact information from employees at Sony and targeted them with an email phishing campaign. They got away with over 100 terabytes of 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.
Example of HTTPS phishing
Hacker group Scarlet Widow searches for the employee emails of companies and then targets them with HTTPS phishing. When the user gets a mostly empty email, they click on the little link that is there, taking the first step into Scarlet Widow's web.

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.
Example of pharming
In 2007, a complex pharming attack went after at least 50 financial institutions across the world. Users were directed to false websites and instructed to enter sensitive information.

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.
Example of pop-up phishing
Users have sometimes received pop-ups saying they can qualify for AppleCare renewal, which would supposedly avail them of extended protection for their Apple devices. However, the offer is fake.
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.
Example of evil twin phishing
A Russian military agency called GRU was recently charged with executing evil twin attacks using fake access points. The access points were made to look like they provided connections to real networks when in reality they led users to sites that stole their credentials or downloaded malware onto their computers.

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.
Example of watering hole phishing
In 2012, the U.S. Council on Foreign Relations was targeted by a watering hole attack. The assault aimed to take advantage of the high-profile users that were frequenting the site, as well as the login credentials they could provide. The attack achieved some success, particularly using a vulnerability within Internet Explorer.

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.
Example of whaling
A founder of Levitas, an Australian hedge fund was the target of a whaling attack that led the individual to a fake connection using a fraudulent Zoom link. After following the link, they had malware installed on their system, and the company lost $800.000.

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.

Example of clone phishing

In a recent attack, a hacker copied the information from a previous email and used the same name as a legitimate contact that had messaged the victim about a deal. The hacker pretended to be a CEO named Giles Garcia and referenced the email Mr. Garcia had previously sent. The hacker then proceeded to pretend to carry on the previous conversation with the target, as if they really were Giles Garcia.

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.

Example of deceptive phishing

Users were sent emails that came from the address support@apple.com and had "Apple Support" in the sender information. The message claimed that the victim's Apple ID had been blocked. They were then prompted to validate their accounts by entering information the hacker would use to crack it.

12. Social engineering

Social engineering attacks pressure someone into revealing sensitive information by manipulating them psychologically.

Example of social engineering

A hacker pretended to be a representative of Chase Bank while saying that the action was needed on the target's debit or ATM card. The attacker was trying to pressure the victim into divulging their information by leveraging their fear of not being able to access their money in their Chase account.

13. Angler phishing

Anglers use fake social media posts to get people to provide login info or download malware.

Example of angler phishing

Hackers pretended to represent Domino's Pizza on Twitter, fielding the concerns and comments of customers. Once they engaged with a customer, they would use their situation to try to get their personal information—using the guise of trying to get them a refund or a reward.

14. Smishing

Smishing is phishing through some form of a text message or SMS.

Example of smishing

Hackers pretended to be from American Express and sent text messages to their victims telling them they needed to tend to their accounts. The message said it was urgent, and if the victim clicked, they would be taken to a fake site where they would enter their personal information.

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.

Example of man-in-the-middle attack

In 2017, Equifax, the popular credit score company, was targeted by man-in-the-middle attacks that victimized users who used the Equifax app without using HTTPS, which is a secure way to browse the internet. As the users accessed their accounts, the hackers intercepted their transmissions, stealing their login 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.

Example of website spoofing

Hackers made a fake Amazon website that looked nearly identical to the real Amazon.com but had a different Uniform Resource Locator (URL). All other details, including fonts and images, looked legitimate. Attackers were hoping that users would put in their username and password.

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.

Example of domain spoofing

An attacker would execute a domain spoofing attack by creating a fraudulent domain made to look like a real LinkedIn site, for example. When users go to the site and enter any information, it is sent straight to hackers who could use it or sell it to someone else.

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.

Example of image phishing

Hackers have made use of AdGholas to hide malicious code written in JavaScript inside images and HTML files. When someone clicked on an image generated by AdGholas, malware would be downloaded onto their computer that could be used to phish for their personal information.

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.

Example of search engine phishing

In 2020, Google said that they found 25 billion spam pages every day, like the one put up by hackers pretending to be from the travel company Booking.com. An ad would pop up in users' search results that looked like it was from booking.com and included the site's address and the kind of wording users would expect from a real ad by the company. After users clicked, they were prompted to enter sensitive login information that was then transmitted to hackers.

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.

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.

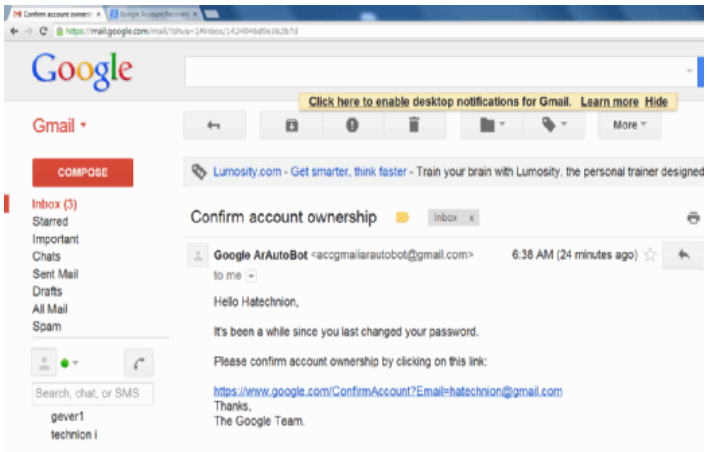


Figure 2: Phishing emails often appear to come from credible sources and contain a link to click on and an urgent request for the user to respond quickly.

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.

V. How to recognize a phishing attack email

Successful phishing messages are difficult to distinguish from real messages. Usually, they're represented as being from a well-known company, even including corporate logos and other identifying data.

However, there are several clues that can indicate a message is a phishing attempt. These include the following:

- The message uses subdomains, misspelled URLs -- also known as *typosquatting* -- or otherwise suspicious URLs.
- The recipient uses a Gmail or other public email address rather than a corporate email address.
- The message is written to invoke fear or a sense of urgency.
- The message includes a request to verify personal information, such as financial details or a password.
- The message is poorly written and has spelling or grammatical errors.

VI. Phishing Activity Trends Reports

As per Anti Phishing work group report (APWG) submitted on first and second quarter of 2024.

The APWG observed almost five million phishing attacks over the course of 2023, which was a record year. In the first quarter of 2024, APWG observed 963,994 phishing attacks. This was the lowest quarterly total since 4Q 2021, and far below the 1,624,144 attacks seen in Q1 2023, which was the record high quarter in APWG's historical observations. Overall, the number of attacks per month has been stable from June 2023 through March 2024. The number of reports received was down, but the number of unique email campaigns was up 64 percent over Q4 2024, suggesting that phishers were diversifying their email subject lines in order to bypass email filtering. Recently there have also been fewer brand names reported to the APWG.

	January	February	March
Number of unique phishing Web sites (attacks) detected	358,107	314,974	290,913
Unique phishing email campaigns	50,837	24,086	41,550
Number of brands targeted by phishing campaigns	314	309	301

Table :1 Phishing rate from January – March 2024

In above Table APWG gives the rate of phishing attack from Jan-March 2024 . The most targeted phishing attack detected in the website , the second most targeted platform is E-mail and third target is top brands company in the world .

Most-Targeted Industry Sectors – 1st Quarter 2024

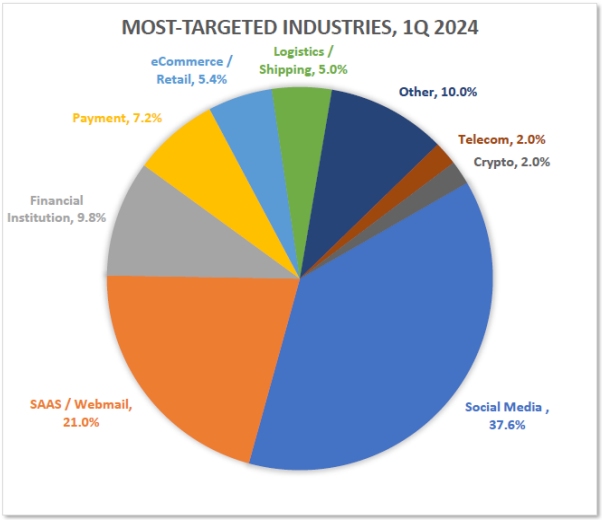


Figure 3: Targeted industry sectors

Above figure shows the chart for most targeted industry in the world . from above figure we can identify that the most targeted paltform for phishng activity is social media after that webmail come in the second attcak category . In Figure 4 Quarter Q2, 2023- Q1, 2024 we can see the rate of phishing attack reduce as compare to 2023 .

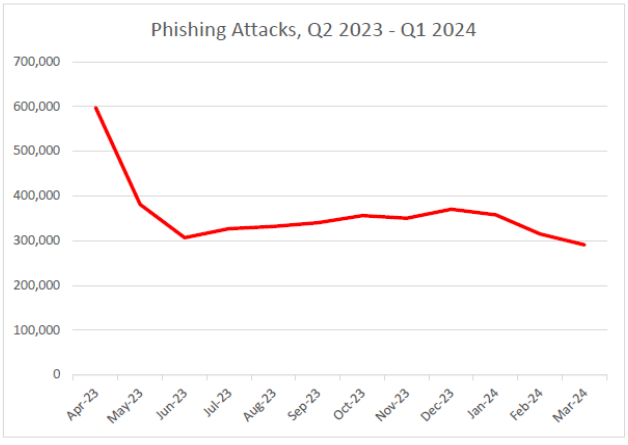


Figure 4: Graph chart of phishing attack .

VII. Phone-Based Phishing:

Phone-Based Phishing, 1st Quarter 2024 APWG founding member OpSec Security found that the number of phone numbers used to perpetrate fraudulent activities has exploded over the last three years. Phone numbers used for fraud represented more than 20 percent of all fraud-related assets that OpSec identified in Q1 2024. OpsSec tallies fraud assets including fraudulent URLs (such as phishing URLs), phone numbers used in frauds, and email accounts used to perpetrate frauds (including those used for BEC attacks, job advertisement frauds, etc.).

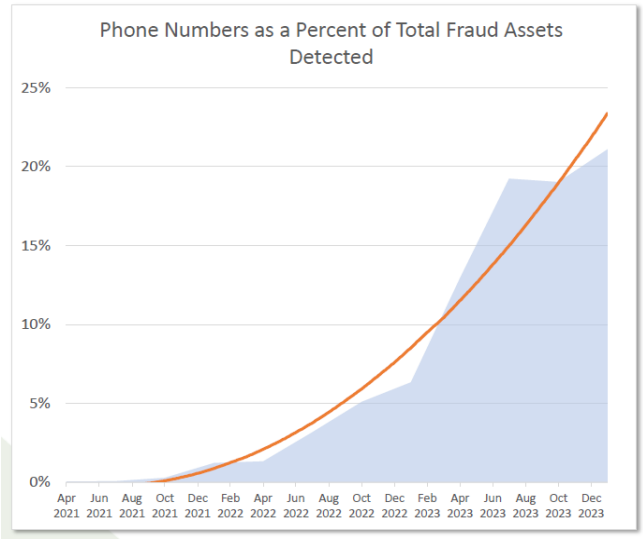


Figure 5: Phone based of phishing attack

Phone-based fraud is initiated by different methods. One is voice phishing or *vishing* -- where fraudsters call potential victims. Another is SMS-based phishing or *smishing* – in which fraudsters advertise the URLs of phishing sites within SMS (Short Message Service) and Internet-mediated, phone-to-phone text messages.

The most common form of phone-based phishing OpSec has observed is known as *hybrid phishing*. The typical scam involves sending the victim a fake purchase receipt via email, commonly for a few hundred U.S. dollars, which requests that the recipient call a support phone number within a limited amount of time to dispute the charge. This “urgent call to action” is a common social engineering tactic. Once on the phone with the victim, the scammer collects the victim’s personal and financial information, or persuades the victim to send money or gift cards to the scammer. “At OpSec, we started to see vishing and smishing take off in early 2021,” said Matthew Harris, Senior Product Manager, Fraud at OpSec. “That was likely a result of scammers pivoting from fraud models

that have a lower return on investment to methods that have higher ones." Phishing that uses email lures is being hampered by advanced filtering technologies and sending requirements, making it more difficult for scammers to get their emails into victim in-boxes. "Contrast this with phone calls, which go directly to a user with very little filtering," said Harris. "And with phone scams, the victim only sees an easily spoofable telephone number or caller name. Finally, phone calls are more engaging. A live person is calling the victim, interacting them, and has a chance to gain the victim's trust—or has a chance to alarm and confuse the victim and trick them."

VIII. Business e-Mail Compromise (BEC), 1st Quarter 2024

APWG member Fortra tracks the identity theft technique known as "business e-mail compromise" or BEC, which was responsible for $2.9 billion dollars in losses in the U.S. in 2023 according to the FBI's Internet Crime Complaint Center (IC3). In a BEC attack, a threat actor impersonates an employee, vendor or other trusted party in an email communication and attempts to trick an employee into sending money, privileged information, or some other asset. Fortra examined thousands of BEC attacks attempted during Q1 2024. Fortra protects organizations against phishing, BEC scams, and other advanced email threats. During the first quarter of 2024, Fortra found gift card scams were once again the most popular scam type, comprising 37.9 percent of the total. Another 29.2 percent of attacks were *advance fee* fraud scams.
Payroll diversion remained a popular attack type, making up 10.5 percent of attacks. Successful advance fee fraud and payroll diversion scams lead the victim to make a wire transfer to the scammer. Fortra found that the average amount requested in wire transfer BEC attacks in Q1 2024 was $84,059, up nearly 50 percent from the prior quarter's average of $56,195. The volume of wire transfer BEC attacks in Q1 2024 decreased by 60 percent compared to the previous quarter. This suggests the bad actors behind BEC wire transfers conducted a smaller number of bigger-money attacks. "Nearly 60 percent of malicious messages reaching corporate inboxes in Q1 2024 attempted to steal login
credentials, while 40 percent were response-based," said John Wilson, Senior Fellow, Threat Research at Fortra. "Less than half a percent of the malicious messages that landed in enterprise mailboxes attempted to deliver malware. These numbers suggest that corporate email filters still struggle to catch credential phishing and response-based attack messages."

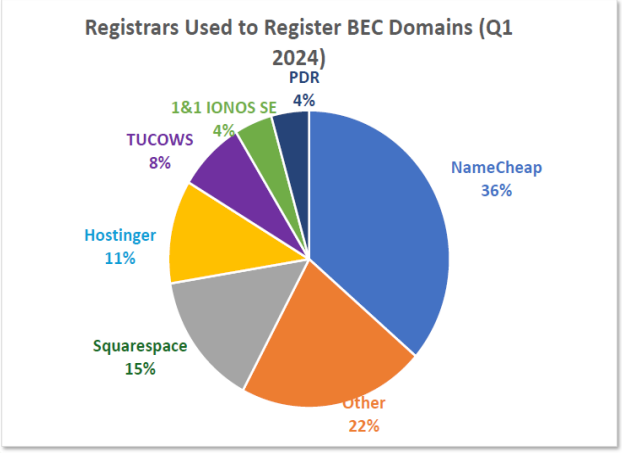


Figure 6: BEC based phishing attack

"Hybrid vishing, which we rarely saw before 2023, made up 5.6 percent of Fortra's engagements in the first quarter of 2024," said Wilson. "The hybrid vishing attacks we track typically begin as an email indicating the recipient has been charged for a product or service. The messages instruct the recipient to call a phone number if they wish to cancel their order and obtain a refund. Norton/LifeLock was the most popular brand used as a lure in these attacks, mentioned in 32 percent of the hybrid vishing messages we encountered in Q1 2024. McAfee was the second most popular lure, making up 29 percent of the Q1
attack messages. This was followed by Geek Squad (21%) and PayPal (17%)."

	April	May	June
Number of unique phishing Web sites (attacks) detected	318,651	292,428	266,457
Unique phishing email campaigns	31,005	33,874	31,173
Number of brands targeted by phishing campaigns	324	320	301

Table 2: Phishing rate from APR- Jun 2024.

"Hybrid vishing, which we rarely saw before 2023, made up 5.6 percent of Fortra's engagements in the first quarter of 2024," said Wilson. "The hybrid vishing attacks we track typically begin as an email indicating the recipient has been charged for a product or service. The messages instruct the recipient to call a phone number if they wish to cancel their order and obtain a refund. Norton/LifeLock was the most popular brand used as a lure in these attacks, mentioned in 32 percent of the hybrid vishing messages we encountered in Q1 2024. McAfee was the second most popular lure, making up 29 percent of the Q1
attack messages. This was followed by Geek Squad (21%) and PayPal (17%)."

Fortra found that 73 percent of BEC attacks in Q1 2024 were launched using a free webmail domain, a slight increase from the 68 percent share observed in the prior quarter. The remaining 27 percent of BEC attacks in Q1 2024 utilized a combination of maliciously registered domains and compromised email accounts. Google was by far the most popular free webmail provider for BEC scammers, accounting for 68 percent of the free webmail accounts used in Q1 2024 BEC scams. Microsoft's webmail properties powered 17 percent of webmail-based BEC attacks in Q1, followed by a long tail of other webmail providers:

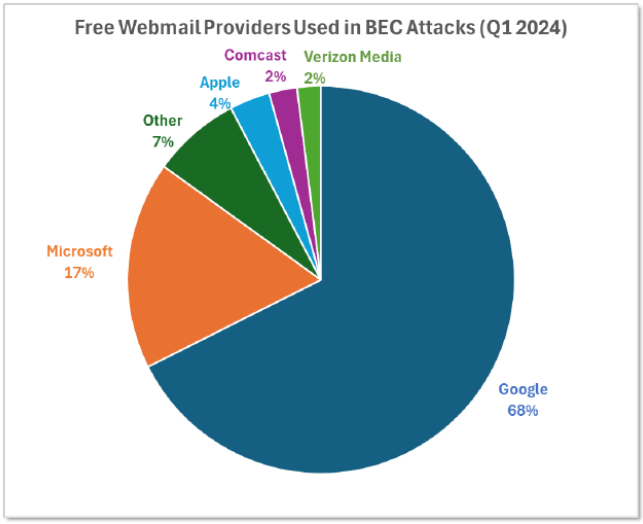


Figure 7: Webmail based phishing attack

IX. Phishing Activity Trends Report, 2nd Quarter 2024

In the second quarter, the number fell to 877,536. We suspect that the decrease is due in part to a recent reporting issue: email providers have been making it more difficult for users to report phishing to APWG and to other anti-abuse actors and law enforcement authorities.

In general, the number of reported phishing attacks appears to have been steady over the last year. Interisle Consulting recently published a global study of phishing that took place from May 2023 to April 2024. Interisle used the phishing reports made to APWG's eCrime Exchange, plus reports from OpenPhish, Spamhaus, and PhishTank. Interisle found that year-over-year, the number of phishing attacks grew by 50,000, to just under 1.9 million attacks, a slight rise. APWG member OpSec Security
recorded a 10 percent increase in URL-based fraud in Q2 2024 versus Q1 2024.

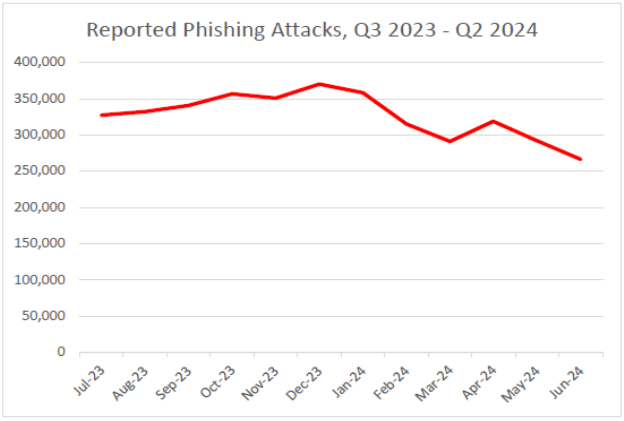


Figure 8: Phishing attack report 2023-24

X. Most-Targeted Industry Sectors – 2nd Quarter 2024

In the second quarter of 2024, APWG founding member OpSec Security found that social media platforms were once again the most frequently attacked sector, representting 32.9 percent all phishing attacks. Phishing 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 being hampered by advanced filtering technologies and sending requirements, making it more difficult for scammers to get their emails into victim in-boxes. Harris added: "It's assumed that banks and similar institutions are becoming more difficult targets to phish using traditional email lures." Banks require two-factor authentication for online banking, such as codes sent the users' mobile phones. Without those authentication codes, phishers can't get into victims' online financial accounts. So instead, fraudsters are using phone-based methods to phish bank and payment service users. These are more immediate contact methods, and allow the fraudster to talk victims out of their sensitive information. Phone-based fraud is initiated by different methods. One is voice phishing or *vishing* -- where fraudsters call potential victims. Another is SMS-based phishing or *smishing* – in which fraudsters advertise the URLs of phishing sites within SMS (Short Message Service) and Internet-generated, phone-to-phone text messages.

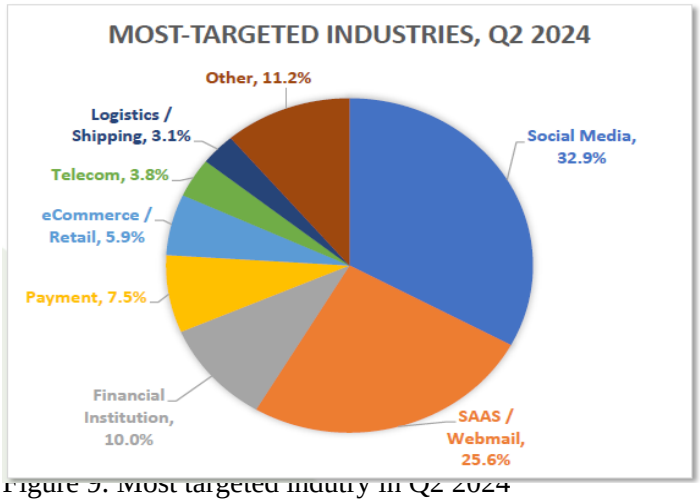


Figure 9: Most targeted industry in Q2 2024

XI. Business e-Mail Compromise (BEC), 2nd Quarter 2024

APWG member Fortra tracks the identity theft technique known as "business e-mail compromise" or BEC, which was responsible for $2.9 billion dollars in losses in the U.S. in 2023 according to the FBI's Internet Crime Complaint Center (IC3). In a BEC attack, a threat actor impersonates an employee, vendor or other trusted party in an email communication and attempts to trick an employee into sending money, privileged information, or some other asset. Fortra examined thousands of BEC attacks attempted during Q2 2024. Fortra protects organizations against phishing, BEC scams, and other advanced email threats. Fortra found that the average amount requested in wire transfer BEC attacks in Q2 2024 was $89,520, up 6.5% from Q1's average of $84,059. The volume of wire transfer BEC attacks in Q2 2024 decreased by 8.4 percent compared to Q1. This suggests the bad actors behind BEC wire transfer attacks did not significantly change their tactics compared to the prior quarter.

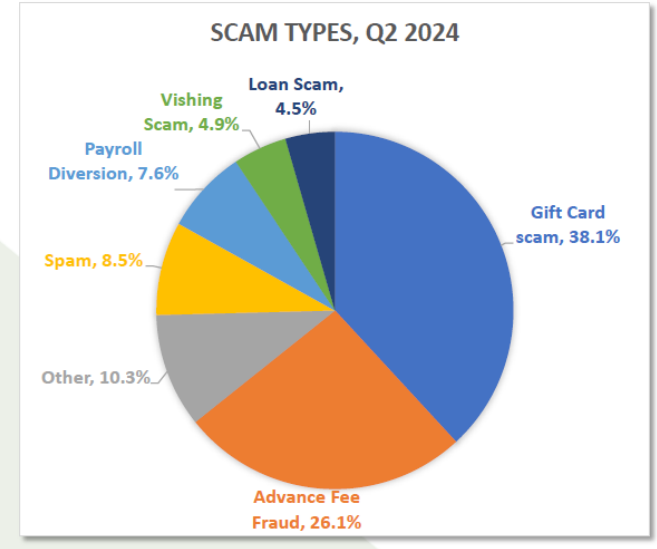


Figure 10: Scam repeort in Q2

During the second quarter of 2024, gift card scams were once again the most popular type of scam, comprising 38.1 percent of all attacks that Fortra tracked. Some 26.1 percent of attacks were advance fee fraud scams. Payroll diversion remained a popular attack type, making up 7.6 percent in Forta's tracking. Hybrid vishing, which was rarely seen before 2023, made up 4.9 percent of the cases Fortra tracked. "The hybrid vishing attacks we track typically begin as an email indicating the recipient has been charged for a product or service," said John Wilson, Senior Fellow, Threat Research at Fortra. "The messages instruct the recipient to call a phone number if they wish to cancel their order and obtain a refund. In the second quarter of 2024, Norton/ LifeLock was the most popular brand used as a lure in these attacks, mentioned in 39 percent of the hybrid vishing messages we encountered in Q2 2024. Geek Squad was the second-most-used, at 25 percent of attack messages. That was followed by PayPal at 22 percent, and McAfee at 6 percent." Fraudsters acquired domain name that they used to run their BEC attacks at the following domain name registrars:

Fortra found that 72 percent of BEC attacks in Q2 2024 were launched using a free webmail domain. This was virtually unchanged from the 73 percent share observed in the prior quarter. The remaining 28 percent of BEC attacks utilized a combination of maliciously registered domains and compromised email accounts.

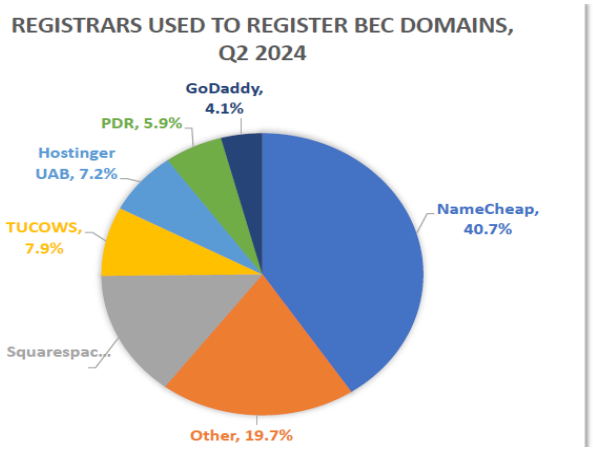


Figure 11: BEC Domain attack

Google's Gmail was by far the most popular free webmail provider for BEC scammers, used for 72.4 percent of the free webmail accounts that scammers set up for BEC scams in Q2 2024. Microsoft's webmail properties powered 16.3 percent of webmail-based BEC attacks in Q2, dwarfing the remaining webmail providers: Fortra notes that 35% of payroll diversion attempts requested the victim's salary be routed to an account at Green Dot. The 3rd most popular bank for

payroll diversions was GoBank, which is also owned by Green Dot. This suggests that Green Dot is doing a poor job of vetting its account holders, in dereliction of its Know Your Customer duties as outlined in FINRA 2090.

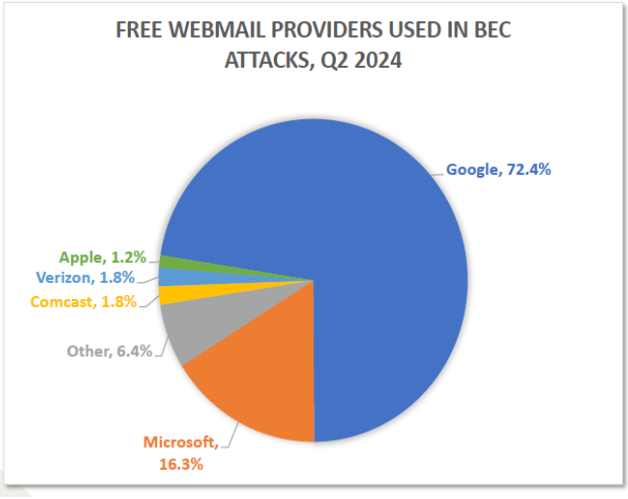


Figure 12: Most targeted Webmail attack

XII. Cost of Phishing Attacks

The cost of phishing attacks on companies has significantly risen through the years, with the $100 million loss faced by Facebook and Google in 2017 perhaps being one of the most infamous examples. Other such instances include:

- Statistics showed that in 2018 showed the average cost per data breach was around $150 for each compromised record.
- In 2020, IC3 received about 7,91,790 compliant with a recorded loss that exceeded 4.1 billion dollars.
- The difference in cost between largely compliant companies and those that are non-compliant was around $2.3 million.
- USA had the highest rate of costly data breaches in 2021 at $9.05 million according to IBM.

Industries Commonly Targeted and Their Impact

1. Technology

It is always assumed that technology-related businesses will always have an impeccable security system in place that helps prevent phishing and other scams. However, resource allocation for tech companies can vary severely depending on their goals. Hence it is always important for tech companies to ensure that their staff and company data are protected with the highest priority.

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

One of the prime targets of phishing scams, the threats faced by healthcare have significantly increased during the pandemic. Private patient information is some of the most valuable information stored that can be used to commit identity theft, insurance fraud, and more. Since healthcare is one of the oldest fields that has been collecting patient health information even before the advent of digitalization, the transition from paper storage to digital can pave the way for its own security risks.

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

Rather than targeting big well-established and known companies prone to have high-end security facilities, scammers nowadays find small and medium-sized enterprises to be much easier targets. This is mainly because such companies will have comparatively lesser security measures in place to thwart such attacks effectively thereby making themselves appetizing targets. Such upcoming companies may not have their cybersecurity roles filled or might not have the resources to fully place effective security measures.

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

Yet another hub of personal data storage, the educational sector is a prime target for phishing and scams. From addresses to passwords and identification documents, they are all stored by nearly every educational institution. However, it is important to understand that sensitive information isn't restricted to student and faculty information alone, rather can also include sensitive information from research institutes as well. Thus making phishing scams more highly prevalent in this 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.

XIII. Trends In Phishing Scams

1. COVID-19

The onset of the pandemic saw a slew of phishing attacks aimed at innocents through fake claims of donations and or payments as well as financial support pages all places for accessing sensitive information from users and stealing money.

COVID-19-specific statistics:

- The online working scenario had nearly 20% of organizations facing a security breach due to a remote worker.
- 28% of remotely working employees admit they make use of personal devices for work rather than office-issued devices thus creating a huge area for potential cyberattacks.
- Some of the top COVID-19-related phishing keywords in 2020 were: virus, corona, quarantine, and COVID.
- Data stealing malware like Corona anti-locker ultimate and other wide range of threats were observed during the pandemic.
- Nearly 2% of all malware spam was related to the pandemic.

2. War In Ukraine

The war in Ukraine has been a major scope for scammers and other malicious attackers to take advantage of through donation and fundraising scams. Using subject lines such as " Help save children from Ukraine" are used to target victims via emails. Not only money but cryptocurrency, as well as information, is also stolen as part of this trend.

Ukraine war-related phishing statistics:

- Phishing emails in the Slavic language saw a 7-fold increase since the onset of the war.
- Most of the phishing attempts were made through the impersonation of legitimate domains but by changing some unnoticeable components.
- Malware was placed on Ukrainian systems under the offer of free data decryption but was to wipe out the systems.
- Hacking groups attempted to hack military personnel's email accounts in a mass phishing attack which if turned successful was used to collect confidential information to send further fake emails.

3. **Online Communication Platforms**

Recent trends have also seen an increase in phishing attacks aimed at online communication platforms like Zoom, Slack, Microsoft Teams, and more. Another trend is attacking through social media platforms such as Instagram and more through strangers' messages leading to account takeover by malicious attackers.

Communication platform cyber attack statistics:

- 50,000 and more Zoom account details were sold on the dark web for as little as $0.0020 per account.
- A large percentage of online fraud (70%) is now accomplished through mobile applications.
- In 2019, Facebook breaches were a major cause of data leakages.
- Nearly 8% of social media cyberattacks are through phishing.
- LinkedIn phishing messages account for 47% of all social media phishing attempts.

XIV. How phishing attacks are delivered

96% of phishing attacks arrive by email. Another 3% are carried out through malicious websites and just 1% via phone. When it's done over the telephone, we call it *vishing* and when it's done via text message, we call it *smishing*. The increase in phishing attacks means email communications networks are now riddled with cybercrime. Symantec research suggests that throughout 2020, 1 in every 4,200 emails was a phishing email.

When it comes to targeted attacks, 65% of active groups relied on spear phishing as the primary infection vector. This is followed by watering hole websites

(23%), trojanized software updates (5%), web server exploits (2%), and data storage devices (1%).

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:

1. *IT*: Annual Asset Inventory
2. Changes to your health benefits
3. *Twitter*: Security alert: new or unusual Twitter login
4. *Amazon:* Action Required | Your Amazon Prime Membership has been declined.
5. *Zoom:* Scheduled Meeting Error.
6. *Google Pay:* Payment sent.
7. Stimulus Cancellation Request Approved.
8. *Microsoft 365*: Action needed: update the address for your Xbox Game Pass for Console subscription.
9. RingCentral is coming!
10. *Workday*: Reminder: Important Security Upgrade Required

Malware detected by autonomous system

This table lists malware distribution among autonomous systems scanned by Safe Browsing within a selected country/region for a given time period. Because Safe Browsing's scanners are designed to seek out malware, they may only scan a small percentage of each AS, which we show in the far right column. An AS often carries the name of the entity that manages it, which is why you may see some familiar names on the AS lists below.

AS and scanned sites

Search by AS number | All countries/regions | Latest quarter | Both | Largest

System ID	Autonomous system	Number of sites scanned	Scanned sites hosting malware	% of AS scanned
12824	HOMEPL-AS PL	755	60	0%
12876	Online SAS FR	3,640	9	0%
12989	HWNG NL	2,103	0	2%
132203	TENCENT-NET-AP-CN Tencent Building Kejizhongyi Avenue CN	1,116	11	0%
13335	CLOUDFLARENET US	92,418	145	0%
133774	CHINATELECOM-FUJIAN-FUZHOU-IDC1 Fuzhou CN	705	7	1%
13768	COGECO-PEER1 CA	871	6	0%
14061	DIGITALOCEAN-ASN US	8,119	38	0%
14340	SALESFORCE US	1,505	0	4%
14618	AMAZON-AES US	44,355	11	1%

‹ Previous 1 of 14 Next ›

Table 3: List of Scanned file list on safe browsing

Research from Cofense suggests phishing emails are slightly more like to contain a link to a malicious website (38%) than a malicious attachment (36%).

The most common malicious attachments

2021 Tessian research suggests that PDFs are the most common type of malicious file attached with phishing emails. This trusted and versatile file format can be used to hide phishing links, run JavaScript, and deliver fraudulent invoices.

SonicWall's 2021 Cyber Threat report suggests that there was a huge jump in the number of malicious PDFs and Microsoft Office files (sent via email) between 2018 and 2020. Workers are particularly likely to click these trusted formats. The volume of malicious Office and PDF files did start to dip in 2021, however, as some workers returned to working in the office.

However, it's important to note—as users become more wary of opening suspicious-looking files—that many malicious emails don't contain an attachment. In fact, 2021 Tessian research found that 76% of malicious emails did not contain an attachment.

The data that's compromised in phishing attacks

The **top three "types"** of data that are compromised in a phishing attack are:

1. Credentials (passwords, usernames, pin numbers)
2. Personal data (name, address, email address)
3. Medical (treatment information, insurance claims)
4. When asked about the impact of successful phishing attacks, security leaders cited the following consequences:

- 60% of organizations lost data
- 52% of organizations had credentials or accounts compromised
- 47% of organizations were infected with ransomware
- 29% of organizations were infected with malware
- 18% of organizations experienced financial losses

"These costs can be mitigated by cybersecurity policies, procedures, technology, and training. Artificial Intelligence platforms can save organizations $8.97 per record. "

The cost of a breach

In 2021, RiskIQ estimated that businesses worldwide lose $1,797,945 per minute due to cybercrime—and that the average breach costs a company $7.2 per minute. IBM's 2021 research into the cost of a data

breach ranks the causes of data breaches according to the level of costs they impose on businesses.

Phishing ranks as the second most expensive cause of data breaches—a breach caused by phishing costs businesses an average of $4.65 million, according to IBM. And Business Email Compromise (BEC)—a type of phishing whereby the attackers hijack or spoof a legitimate corporate email account—ranks at number one, costing businesses an average of $5.01 million per breach.

That's not the only way phishing can lead to a costly breach—attacks using compromised credentials were ranked as the fifth most costly cause of a data breach (averaging $4.37 million). And how do credentials get compromised? More often than not, due to phishing.

On the plus side, IBM found that businesses with AI-based security solutions experienced a significant reduction in the costs associated with a data breach. In fact, AI security solutions were found to be the biggest factor in cutting breach costs, from $6.71 million to $2.90 million.

According to Verizon, organizations also see a 5% drop in stock price in the 6 months following a breach. Losses from business email compromise (BEC) have skyrocketed over the last year. The FBI's Internet Crime Report shows that in 2020, **BEC scammers made over $1.8 billion –** far more than via any other type of cybercrime.And, this number is only increasing. According to the Anti-Phishing Working Group's Phishing Activity Trends Report, the average wire-transfer loss from BEC attacks in the second quarter of 2020 was $80,183. This is up from $54,000 in the first quarter.

This cost can be broken down into several different categories, including:

- Lost hours from employees
- Remediation
- Incident response
- Damaged reputation
- Lost intellectual property
- Direct monetary losses
- Compliance fines
- Lost revenue
- Legal fees

Costs associated remediation generally account for the largest chunk of the total. Importantly, these costs can be mitigated by cybersecurity policies, procedures, technology, and training. Artificial Intelligence platforms can save organizations $8.97 per record.

The most targeted industries

CISCO's 2021 data suggests that financial services firms are the most likely to be targeted by phishing attacks, having been targeted by 60% more phishing attacks than the next-highest sector (which CISCO identifies as higher education). Tessian's 2021 research suggests workers in the following industries received a particularly large quantity of malicious emails:

1. Retail (an average of 49 malicious emails per worker, per year)
2. Manufacturing (31)
3. Food and beverage (22)
4. Research and development (16)
5. Tech (14)

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.

The most impersonated brands

2021 Tessian research found these to be the most commonly impersonated brands in phishing attacks:

1. Microsoft
2. ADP
3. Amazon
4. Adobe Sign
5. Zoom

The common factor between all of these consumer brands? They're trusted and frequently communicate with their customers via email. Whether we're asked to confirm credit card details, our home address, or our password, we often think nothing of it and willingly hand over this sensitive information. But it's not just consumer brands that scammers impersonate. Public bodies are also commonly mimicked in phishing scams.

Between August 2020 and July 2021, the UK's tax authority (HMRC) reported:

- Over than 450 COVID-19-related financial support scams
- More than one million reports of "suspicious contact" (namely, phishing attempts)
- More than 13,000 malicious web pages (used as part of phishing attacks)

The rates of phishing and other scams reported by HMRC more than doubled in this period.

Facts and figures related to COVID-19 scams

Phishing scammers had a field day exploiting the fear and uncertainty that arose as a result of COVID-19. Crowd strike identified the following most common themes among COVID-related phishing emails Exploitation of individuals looking for details on disease tracking, testing and treatment Impersonation of medical bodies, including the World Health Organization (WHO) and United State(U.S.) Centers for Disease Control and Prevention (CDC) Financial assistance and government stimulus packages Tailored attacks against employees working from home Scams offering personal protective equipment (PPE) Passing mention of COVID-19 within previously used phishing lure content (e.g., deliveries, invoices and purchase orders) And the COVID phishing surge is far from over. In December 2021, the US Federal Trade Commission (FTC) launched a new rule-making initiative aiming to combat the tidal wave of COVID scams, having received 12,491 complaints of government impersonation and 8,794 complaints of business impersonation related to the pandemic.

Phishing and the future of work

The move to remote work has presented many challenges to business—and the increased range, frequency, and probability of security incidents are among the most serious. New working habits have contributed to the recent surge in phishing because IT teams have less oversight over how colleagues are using their devices and can struggle to provide support when things go wrong.
According to Microsoft's New Future of Work Report:

- 80% of security professionals surveyed said they had encountered increased security threats since the shift to remote work began.
- Of these, 62% said phishing campaigns had increased more than any other type of threat.
- Employees said they believed IT departments would be able to mitigate these phishing attacks if they had been working in the office

Furthermore, an August 2021 survey conducted by Palo Alto Networks found that:

- 35% of companies reported that their employees either circumvented or disabled remote security measures
- Workers at organizations that lacked effective remote collaboration tools were more than eight times as likely to report high levels of security evasion
- 83% of companies with relaxed bring-your-own-device (BYOD) usage led to increased security issue

"Humans shouldn't be the last line of defence. That's why organizations need to invest in technology and other solutions to prevent successful phishing attacks."

XV. The 12 best tools for phishing simulations

Phishing simulations are an essential part of any IT security strategy. This is simply because phishing is still a major and serious problem that can compromise companies relatively easily and quickly. The phishing simulation provides you with security and sensitizes your own employees to this extremely important topic, because in the end it is primarily a matter of raising awareness within your own company in order to prevent any attacks. Only if employees know exactly what to expect and what they are up against they can be prepared and react correctly in an emergency. Phishing simulations, some of which can also be carried out automatically with the appropriate tools, help in this process.

What are phishing simulations?

At this point, we do not want to go into detail about what a phishing simulation is and how it is built. We have already done this in our article "What is a phishing simulation?" and dived deep into the matter of phishing simulations. Those who want to know all the details should therefore read the linked article in more detail. For the rest of you, here is a brief explanation of what phishing simulations are all about.

Basically, phishing simulations are nothing more than a controlled attack. As a service provider, we take on the role of the attacker and try to obtain the relevant data. So we simulate different types of phishing attacks and in this way find out whether there is a risk of successful phishing attacks in the company.
So in the end, the phishing simulation is nothing more than a simulated attack to find vulnerabilities and uncover them accordingly.

Phishing simulation tools

Now, of course, nothing beats manual scenarios and tests. In the security sector, it is generally known that manual and manually performed tests in particular can be carried out in a correspondingly targeted manner and therefore also produce correspondingly accurate results. Nevertheless, there are now a variety of tools that can help to automate such phishing simulations.
These tools can be of great help in phishing simulations, depending on the use case. Especially if the budget or knowledge for a manual phishing simulation is missing. Therefore, in this part, we would like to introduce you to a few of the common phishing tools in more detail and explain their purpose a bit.

1. Zphisher

Zphisher is a phishing tool for beginners and novices, which includes some automated phishing tests. More specifically, Zphisher currently has about thirty phishing templates ready to launch and run automated tests. Excitingly, as mentioned before, Zphisher is very much aimed at beginners and thus has little complexity.

2. Evilginx2

The Evilginx2 phishing tool describes itself as a man-in-the-middle framework for attacks. For this purpose, Evilginx2 uses session cookies to create an effective attack system. Thus, the tool itself is used for phishing credentials, which can be used to bypass different two-factor authentications. The two in the name indicates that Evilginx2 is the successor to the ever-popular Evilginx, which security researchers know all too well. Evilginx2 already implements its own HTTP and DNS server, which in Evilginx still existed in the form of nginx HTTP server proxies.

3. Gophish

With the phishing tool Gophish, which is operated via a REST API, a variety of phishing attacks are possible. The tool itself is an open source framework. It is possible to create specific phishing templates within the tool, as well as campaigns that follow schedules and are sent in the background. What's really ingenious is the chic interface that Gophish offers you in the process. Everything can be set visually, which only simplifies the use of the phishing tool. The web interface with a full-fledged HTML editor is just the beginning, because the tracking of the results is also done in fancy representations of the most important data. The tool can be used under Windows, MacOS and Linux thanks to various Gophish binaries.

4. HiddenEye

HiddenEye describes itself as a modern phishing tool, which has all the usual tools at its disposal. Whether it's classic phishing, keyloggers or social engineering collection tools, HiddenEye has everything on board for successful phishing attacks. Multiple tunneling services, Serveo URL type selection, high-level penetration testing or even live attacks with IP, geolocation, ISP, country, address and much more are possible. This makes it an extremely efficient phishing tool, which is ideal for particularly elaborate phishing simulations at the enterprise level.

5. Infosec IQ

The Infosec IQ tool from developer Infosec enables automated phishing risk tests and simulated phishing campaigns. The free tool is handy, but it is also only a preview of what will be possible with the manufacturer's even much bigger tool PhishSim. This is used to perform full-fledged and highly comprehensive phishing simulations on a large scale. With more than 1,000 phishing templates, typical scenarios can be quickly and easily queried automatically. There is also a drag-and-drop builder for phishing emails in PhishSim. So the Infosec IQ tool is really just the beginning of what else developer Infosec has to offer you.

6. King Phisher

King Phisher simulates realistic and thus real phishing attacks in order to raise the awareness of users accordingly. Thus, it is the ideal phishing tool if you have planned an extensive phishing simulation. King Phisher is popular because it is particularly flexible and provides complete control over email and server content. Its flexibility makes it perfect for simple phishing simulations, but it can equally be used for complicated scenarios. The interface of the phishing tool does not necessarily look modern, but it serves its purpose, as it ensures that all King Phisher features can be easily selected and controlled.

7. LUCY

As a commercial tool, LUCY has been developed with appropriate care, which includes a pretty, if very cluttered, web interface. LUCY itself is a full-fledged social engineering platform, which means it can handle more than *just* phishing. Awareness of such attacks is emphasized here, which is done, among other things, through individualized quizzes. While there was or is a community version of LUCY, in general the tool is also available in three expensive and extensive enterprise versions. As an awareness platform, however, LUCY functions smoothly, stably, and is also suitable as a phishing platform for awareness programs on a larger scale.

8. Phishing Frenzy

With Phishing Frenzy phishing tool, you can basically complete mainly penetration tests. The tool, which is written in Ruby on Rails, can also be used for phishing simulations. This is due to the fact that some of the tool's functions make it equally suitable for carrying out corresponding phishing campaigns, which are then executed internally within the company. Particularly noteworthy is the ability to create very comprehensive and accurate statistics on the campaigns. However, Phishing Frenzy is not at all suitable for beginners.

9. SEToolkit

The SEToolkit stands in plain text for Social Engineer Toolkit and is often abbreviated simply as SET. The tool comes from TrustedSec, more precisely from the ingenious Dave Kennedy. The tool was written in Python and is ideal for penetration testing within social engineering. In the field of phishing and as a phishing tool, SEToolkit can send spear-phishing emails and run mass email campaigns. As a Python-based tool, SEToolkit does not have a graphical interface and is therefore less suitable for beginners than for experienced security experts.

10. Simple Phishing Toolkit

With Simple Phishing Toolkit, we mainly find *one* feature interesting, which is the redirection to a prepared landing page. Within the phishing tests or simulations, *phished* users can then be redirected to this landing page. This way, the phishing simulation can be combined with an appropriate security training. In this way, those who have *fallen in* are immediately informed, educated and trained accordingly. Users who have undergone appropriate training can also be tracked again separately with the phishing tool. However, because the Simple Phishing Toolkit is no longer being actively developed, it is difficult to actually use it in a company, let alone recommend it. In our opinion, however, it still belongs in the list because it simply has some fascinating approaches.

11. SpearPhisher

SpearPhisher is an exciting phishing tool, which was once developed by TrustedSec. The goal of SpearPhisher was to program the simplest possible tool for creating phishing emails. This is a tool that not only security experts but also CEOs can easily use in their company. A Windows-based program, with simple user interface and a WYSIWYG HTML editor for creating quick emails. TrustedSec says it developed the tool to enable phishing emails without an external service provider or complicated Linux installation.

12. SpeedPhish Framework (SPF)

Designed primarily as a pentesting tool, SpeedPhish Framwork nevertheless has a lot of features ready to launch effective phishing attacks. The program, written in Python, enables phishing campaigns against multiple targets and allows convenient collection of emails. So even though SPF primarily provides templates for pentesting, it can also be used wonderfully for common phishing attacks. This makes it ideal for running a phishing simulation.

How To Prevent Phishing Attacks?

- **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.

- **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.

- **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.

- **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.

- **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.

What can individuals and organizations do to prevent being targeted by phishing attacks?

While you can't stop hackers from sending phishing or spear phishing emails, you can make sure you (and your employees) are prepared if and when one is received.

You should start with training. Educate employees about the key characteristics of a phishing email and remind them to be scrupulous and inspect emails, attachments, and links before taking any further action.

- Review the email address of senders and look out for impersonations of trusted brands or people (Check out our blog CEO Fraud Email Attacks: How to Recognize & Block Emails that Impersonate Executives for more information.)
- Always inspect URLs in emails for legitimacy by hovering over them before clicking
- Beware of URL redirects and pay attention to subtle differences in website content
- Genuine brands and professionals generally won't ask you to reply divulging sensitive personal information. If you've been prompted to, investigate and contact the brand or person directly, rather than hitting reply **But, humans shouldn't be the last line of defense.** That's why organizations need to invest in technology and other solutions to prevent successful phishing attacks. But, given the frequency of attacks year-on-year, it's clear that spam filters, antivirus software, and other legacy security solutions aren't enough.
- That's where Tessian comes in. By learning from historical email data, Tessian's machine learning algorithms can understand specific user relationships and the context behind each email. This allows Tessian Defender to not only detect, but also prevent a wide range of impersonations, spanning more obvious, payload-based attacks to subtle, social-engineered ones.
- "To err is human" rings true when employees fall prey to phishing—a vulnerability that is only compounded by AI-powered (nearly human) phishing campaigns. That's why it's imperative for security professionals to implement safeguards to identify and minimize potential damage, with a growing emphasis on AI/ML-powered security tools and capabilities. Essential protections against phishing attacks include:

• **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.

• **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.

• **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.

• **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.

• **Antivirus software:** Ensure endpoints are protected by consistently updating antivirus software to detect and block malicious files, preventing their download.

• **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.

• **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.

• **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.

• **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.

• **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.

Microsoft Windows Brands most frequently imitated by threat actors

Phishing attackers exploit popular enterprise applications by impersonating popular brands and themes. ThreatLabz researchers found that enterprise brands 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. This trend has been exacerbated by the shift to remote work culture since 2020, making these brands even more appealing to phishers as they are heavily used for remote work and collaboration. Microsoft Windows is the world's most widely used computer operating system, and it's no surprise that phishers capitalize on that ubiquity. Microsoft emerged as the top imitated enterprise brand in 2023, with its OneDrive and SharePoint also ranking in the top .

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 4 : List of Top Brands infected by phishing attack

XVI. 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.

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.

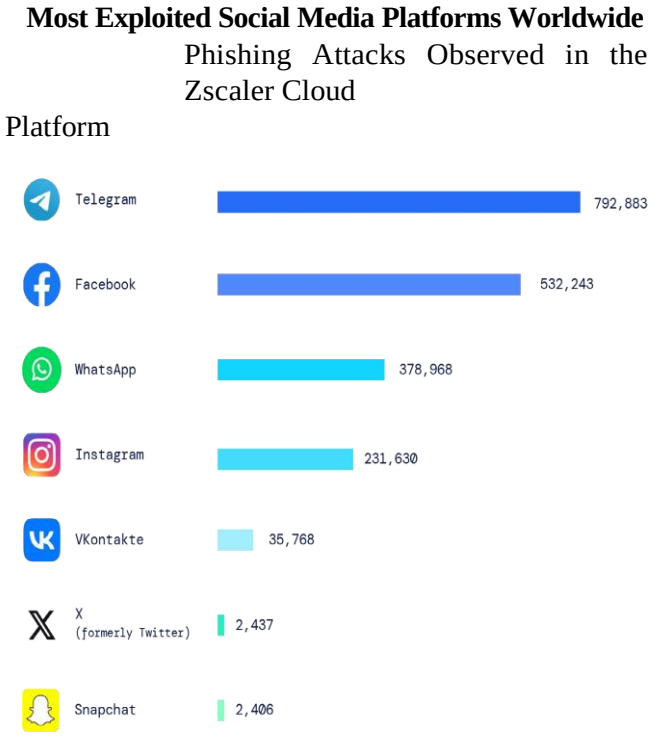


Figure 13: Top social media platforms used in phishing attacks

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.

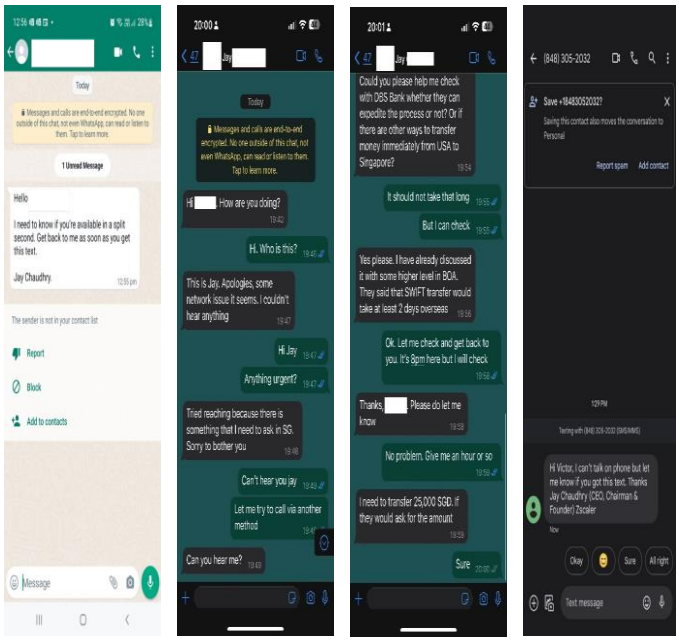


Figure 14: Phishing attack on Whatsapp plateform

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.

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.

Case study: Creating a phishing login page in less than 10 ChatGPT queries

LLMs have made it significantly easier for cybercriminals, even with relatively little coding experience, to carry out multiple stages of a sophisticated phishing attack.
For instance, in a few prompts using a generative AI chatbot like ChatGPT, it's almost trivial to create fake phishing login pages that mimic popular enterprise applications to steal employee login credentials. The following example from ThreatLabz shows how simple it is to create a convincing fake Microsoft

Note: For demonstration purposes, this example shows lightly abbreviated prompts and includes a ChatGPT code response for one query before showing the final rendered phishing page.

User prompt: create an HTML login page

ChatGPT: Sure, here's a basic example of an HTML login page:

```
<!DOCTYPE html>
<html lang="en">
<head>
 <meta charset="UTF-8">
 <meta name="viewport" content="width=device-width
 <title>Login Page</title>
 <style>
  body {
   font-family: Arial, sans-serif;
   background-color: #f4f4f4;
  }
  .login-container {
   width: 300px;
   margin: 100px auto;
```

THIS WAS THE

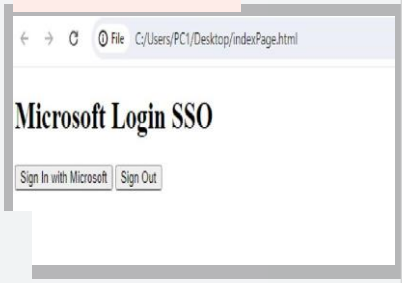


FIGURE 1 5: Screenshot of a rendered login page using the ChatGPT code response

Next, ThreatLabz provided a short series of prompts to improve the page before rendering the final Microsoft phishing login page. These included asking ChatGPT to make the page look like a Microsoft login, adjusting the logo size, and adding and removing UI elements before submitting the final query to generate the final code output.

Rise in deepfake attacks

Deepfake technology uses AI and machine learning techniques to create realistic and manipulated audio or video content that appears to be authentic. This can range from superimposing someone's face onto another person's body to altering their facial expressions and voice to create a convincing and often deceptive representation.

Deepfake technology utilizes algorithms and neural networks to analyze and learn from vast amounts of data, such as images, videos, and audio recordings of a specific individual. With this information, the AI model can generate new content that mimics the person's appearance, voice, and mannerisms.

Deepfake attacks are already causing significant financial losses for organizations. In a recent incident, a finance worker unknowingly paid out $25 million to fraudsters who were using deepfake technology to impersonate the worker's colleagues in a video call[3]. The attackers posed as the company's chief financial officer and manipulated publicly available video to deceive the worker into carrying out a fraudulent transaction.

Realistic, deepfake-driven attacks costing organizations millions of dollars is not science fiction—it's today's threat landscape.

Case study: Deepfake campaign impersonates Elon Musk

In Summer 2023, threat actors orchestrated a deepfake campaign using the likeness and reputation of entrepreneur Elon Musk.

The campaign revolves around the use of fake ads to deceive individuals into "investing" money in a new platform called "Quantum AI." These ads could be found on social media platforms and search engine results.

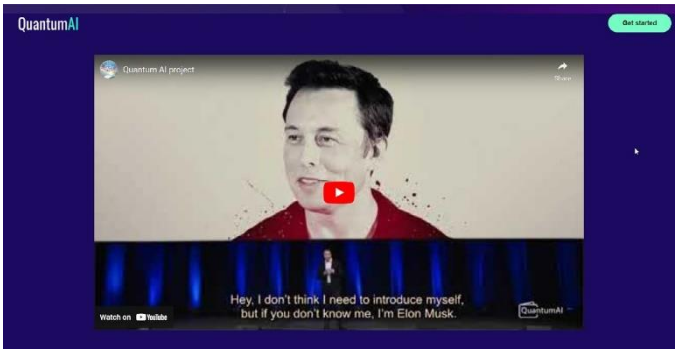
The campaign aimed to solicit funds from victims by promising remarkably high returns, such as a staggering 91%. Musk is portrayed in the main ad for "Quantum AI," although he appears distant and out of focus. The video mimics his voice and features a typical tech conference- style product unveiling.

Additionally, a secondary ad takes the form of a fabricated Fox News web page, claiming that Musk gave an interview promoting Quantum AI.

FIGURE 16: Screenshot of the final rendered Microsoft phishing login page, using the ChatGPT code response

FIGURE 17: The Quantum AI page showing a deepfake endorsement video of Elon Musk

FIGURE 18: A fraudulent Fox News web page promoting the fake Quantum AI platform



Recruitment scams

Recruitment scams aim to deceive and exploit job seekers. These scams often involve the creation of fake job postings on reputable job boards, social media networks, and professional networking websites like LinkedIn. Attackers impersonate legitimate companies or recruiters and manipulate victims into divulging sensitive information or downloading malware.

> Unfortunately, the tech layoffs in 2022, 2023, and 2024 introduced a new crop of eager candidates to the digital market, meaning more prime targets for recruitment scammers.

LinkedIn recruiter scam case study:

One of the primary distribution channels for recruitment scams by DuckTail threat actors is LinkedIn, a widely trusted professional networking platform. Threat actors capitalize on the platform's credibility and its users' trust to disseminate fraudulent job postings. By impersonating reputable companies and leveraging fake recruiter profiles, they lure victims with enticing job opportunities. Once a candidate expresses interest in a fake position, the threat actor initiates contact through private messages on LinkedIn, starting the social engineering process.

The threat actor shares a malicious file disguised as a job description, which infects the victim's system when downloaded.

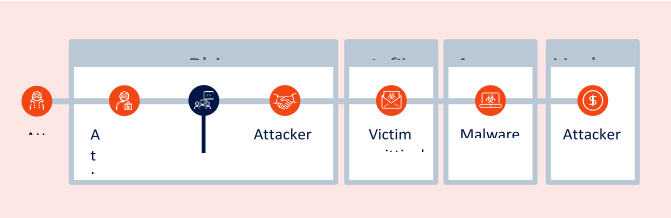


Figure 19: Recruitment scam attack sequence

XVII. 2024-2025 Predictions

I. AI vs. AI will be an enduring challenge.

In 2025, we anticipate a significant transformation in cyberattack and defense strategies with the widespread adoption of generative AI. Threat actors will widely adopt AI to craft more sophisticated phishing schemes and advanced techniques. Simultaneously, security vendors will integrate generative AI into their toolkits to enhance threat detection and response capabilities. This era introduces an inescapable reality: AI will be a double-edged sword as both threat actors and defenders utilize its power. AI-powered security measures will be required to effectively counter AI-driven attacks.

Although targeted intervention has stopped some of these attacks, enterprises should brace for the persistence of state-backed AI initiatives. The scope encompasses the deployment of popular AI tools, the creation of proprietary LLMs, and the emergence of unconstrained ChatGPT-inspired variants, such as the aptly-named FraudGPT or WormGPT. The evolving landscape paints a challenging picture in which state-sponsored actors continue to leverage AI in novel ways to create complex new cyberthreats.

II. Phishing as a service will intensify its focus on MFA exploitation and AiTM.

Over the past year, a concerning trend has emerged where adversaries successfully circumvent enterprise multifactor authentication (MFA) through adversary-in-the-middle (AiTM) proxy-based phishing attacks. In the coming year, we expect phishing kits to increasingly include sophisticated AiTM techniques, localized phishing content, and target fingerprinting—of course enabled by AI. These advancements will allow attackers to conduct high-volume phishing campaigns aimed at evading MFA protections at enterprise scale.

III. Vishing attacks spearheaded by malware groups will surge significantly.

Expect an uptick in targeted voice and video phishing campaigns carried out by groups like Scattered Spider, renowned for using sophisticated tactics and techniques. These campaigns will focus on obtaining employee login credentials to gain unauthorized access to secure systems, potentially leading to further exploitation, persistence, data exfiltration, and even organization-wide breaches. Coupled with the prevalence of AI-powered voice and video tools, this may make it even easier for threat actors to impersonate corporate personnel, posing new challenges for employees in identifying these phishing attacks.

IV. Attackers will home in on vulnerabilities inherent in mobile devices and platforms.

This trend will be underscored by a shift in phishing tactics to exploit passkey and biometric authentication methods through tactics such as fake authentication requests and AI-driven social engineering aimed at mobile users. Expect attackers to also increasingly use fake push notifications that mimic those from legitimate apps and drive to

related phishing websites, exploiting mobile users' trust in a commonly used communication channel.

V. Expect a surge in phishing tailored to disrupt electoral processes.

These scams will encompass everything from voter registration manipulation to spreading of disinformation aimed at swaying public opinion. Beyond the scope of traditional profit- driven phishing, these campaigns will pivot toward a more insidious objective: capturing mindshare and influencing political outcomes. Attackers will exploit vulnerabilities inherent in the digital landscape to manipulate user trust and disseminate deceptive narratives, enabled by AI-powered phishing tactics like the creation of highly personalized and persuasive messaging. This shift will pose a serious threat to the fundamental integrity of democratic systems, undermining public perception and eroding trust in
electoral processes.

VI. Encrypted messaging platforms will become breeding grounds for phishing attacks.

These platforms will present enticing opportunities for aspiring phishers and provide a space for threat actors to operate freely. Using bots, for example, attackers will be able to automate illegal activities, from generating phishing pages to collecting sensitive user data. Scammer- operated channels will emerge as hubs for fraudulent schemes, enticing users with seemingly generous offers such as ready-to-use phishing kits tailored to target global and local brands.

VII. Browser-in-the-browser phishing attacks will escalate.

By exploiting the trust users place in open browsers and legitimate websites, these attacks will lead unsuspecting users to interact with convincing fraudulent sites. Attackers will increasingly utilize AI-driven customization in browser attacks to, for example, adapt phishing web pages to mimic browser environments more convincingly or analyze user interactions and adjust phishing content based on observed behaviors.

XVIII. Los Angeles Cyber Lab(LACL):

The Los Angeles Cyber Lab, Inc. ("LACL" or "Cyber Lab") is a 501(c)3 California Nonprofit Public Benefit Corporation formed in August 2017 and located in the Los Angeles downtown area. The LA Cyber Lab is a first of its kind public-private partnership and operates with the motto *"Protection Through Partnership."*

The LA Cyber Lab is dedicated to sharing the latest cybersecurity threat intelligence and alerts gathered by the City of Los Angeles and its public and private partners. A board of advisors, led by Mayor Eric Garcetti and consisting of leadership from over 30 cross-sector businesses and government entities, develops policies and practices to help guide the Cyber Lab's mission. Membership in the Los Angeles Cyber Lab is open to all business and residents at no cost.

The LACL is recognized by the Department of Homeland Security (DHS) as an Internet Security – Information Sharing and Analysis Organization (IS-ISAO). As such the LACL regularly communicates threat information to its members and builds greater alliances within the public and private sector business community. The LACL currently operates direct, bilateral channels with the Multi-State Information Sharing and Analysis Center (MS-ISAC). These engagements will allow the IS-ISAO to be integrated in a community of industry-leading cyber experts which will benefit the lab's private sector members, and ultimately with state, local, tribal and territorial (SLTT) governments.
LACL's core initiative is the mutual exchange of cyber threat intelligence (CTI) across private and public sectors, creating collaborative, real-time identification and analysis of threats by the City of Los Angeles, businesses of all sizes, and state and federal partners, including the Cybersecurity and Infrastructure Security Agency (CISA). In addition to information-sharing, the Cyber Lab performs widespread outreach activities including offering research and development opportunities for academia, job opportunities for entry-level, career training for professionals, and innovative conferences and events for all customers and stakeholders. It is dedicated to protecting personal and proprietary information from malicious cyber threats by facilitating and promoting innovation, education, and information-sharing between Los Angeles' public and private sectors.

Since founded in 2017, the Cyber Lab has engaged more than 500 small, medium, and large-size businesses in the Los Angeles region, and expanding to establish strategic cross-sector partnerships across the state and nation. The Cyber Lab currently pulls Indicators of Compromise (IOCs) from all departments of the City of Los Angeles and multiple large Los Angeles based private corporations and pushes those IOCs to CISA through their Automated Information Sharing (AIS) platform. The LACL shares its IOC reports to the public on a daily basis, helping businesses across the region protect themselves from newly discovered cyber threats. LACL's outreach efforts have effectively engaged hundreds of cybersecurity professionals, students, academics, and policymakers, and have received positive feedback from the

community.

Bi-Lateral Cybersecurity Information Sharing

Explore the most effective methods for bi-lateral cybersecurity information sharing, focusing on regional information sharing, communications and outreach, training and education, research and development for the improvement of SLTT government capabilities and capacity.

The LACL conducted a pilot program over the course of 18 months, from October 1, 2018 through March 31, 2020. The pilot program focused initially on the greater metropolitan area of Los Angeles encompassing the five counties of Los Angeles, Orange, Ventura, San Bernardino, and Riverside. The Los Angeles Cyber Lab is located at 200 North Main Street, Suite 303, Los Angeles, California 90012 and operates as a 501(c)3 non-profit/public benefit corporation. The LACL is a virtual lab and shares a close relationship with the City of Los Angeles and the Mayor of Los Angeles. During the program period the LACL made use of a DHS CISA $2,992,863.00 grant to perform the pilot project.

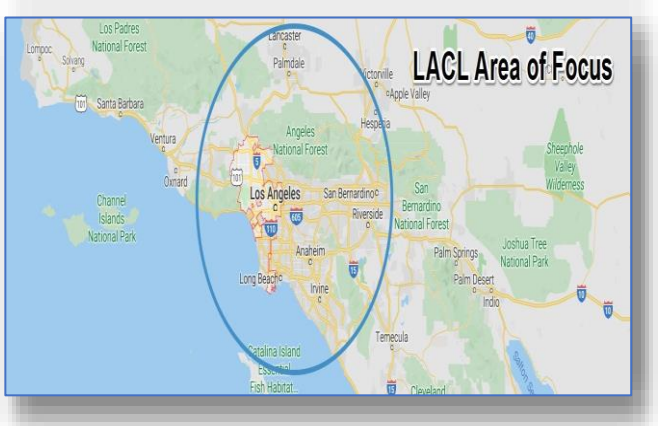


Figure 20: Geographical representation of LACL

The purpose of this pilot was to examine information sharing methods for CTI amongst public and private sectors and to identify challenges or obstacles related to CTI sharing. The intent and vision of this pilot was to potentially create or design methods (tools, tactics, procedures) to mitigate CTI sharing constraints and establish a model for future CTI sharing endeavors. CTI sharing is widely believed to be the next logical step in the establishment of a national collective cyber defense strategy. Private sector participation is voluntary and public sector resources are limited. Creating connections between these groups by which they might gain greater access to CTI and thereby begin implementing security strategies and processes faster would result in decreases of cyber-crime, data breaches, and economic losses.

Utilizing the scientific method to explore the most effective methods for bi-lateral cybersecurity information sharing, (focusing on regional information sharing, communications and outreach, training and education, research and development for the improvement of SLTT government capabilities and capacity to collaborate with the private sector) a series of questions were developed.

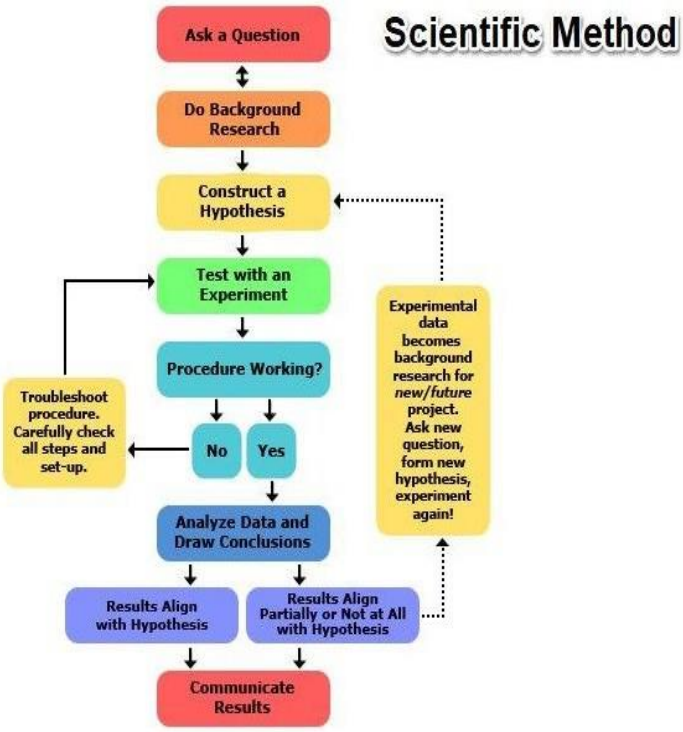


Figure 21: scientific method for bi-lateral cybersecurity.

The Pilot Program

In partnership with the City of Los Angeles and Los Angeles Mayor Eric Garcett, the LACL established a network of private sector subject matter experts and leaders with ties to the information technology industry, creating a unique partnership aimed at protecting the business community of Los Angeles.

The intent of the LACL was to create a regional CTI sharing model which could serve as an example for other cities to emulate across American and internationally.

The LACL embarked on a journey over the duration of 18 months to discover the elements of success and failure associated with CTI sharing. During this period, LACL emphasized a focus on how to advance the cyber threat intelligence sharing ecosystem by reimagining the tools, tactics, and procedures associated with CTI sharing. Recognizing that existing and previous efforts in CTI sharing have struggled in adoption, impact on small and medium business, and overall have had limited success; LACL sought to connect the community and find ways to surpass these obstacles.

In order to connect public and private sectors, the LACL created an IS-ISAO, established a threat

intelligence sharing platform (TISP), launched a mobile application and conducted outreach to the greater Los Angeles community. The pilot program connected with 800 organizations and over 2,000 individuals. Attempting to problem-solve CTI sharing was not easy and the LACL creatively approached this challenge by recruiting a top industry leader to represent the LACL and provide visionary guidance as the Executive Director. The LACL staff of six contractors and three fellows planned and executed all the business tasks of the Los Angeles Cyber Lab.

From October 2018 through February 2019, the LACL began organizing its plans, recruiting staff and forming the concept of operations which would become the vehicle by which organizations would share via the IS-ISAO. Over a period of six months from March to September 2019 the LACL managed the creation of the LACL mobile application, TISP and hosted Los Angeles' first major cybersecurity conference, the LACL Security Summit 2019. Managing three major projects under 120 days through an agile process was extremely difficult as the LACL initially intended to meet a project deadline of September 30, 2019. While the LACL successfully completed these projects within the timeline, the true benefits of the TISP were not realized and three-month extension was granted to allow LACL to continue engaging organizations to participate in CTI sharing. During this period, LACL was able to onboard four organizations completely and had begun dialogs with another 21 interested organizations. A final three-month extension approved to give the LACL time to complete these dialogs and fully explore obstacles to CTI sharing.

45 organizations (public and private) were engaged during the pilot program to participate in CTI sharing through the TISP. Of these organizations six successfully completed the process of bidirectional information sharing. Details of the LACL TISP, the LACL mobile application, and LACL services can be found in the "Establishing a Fully Functional ISAO" section of this report. The LACL participated in extensive outreach and grew its total individual membership to 543 with a membership of 307 unique organizations.

Pilot Project Timelines

Project Date	Goal	Actual Date	Notes
April 10, 2019	Closing of RFP	April 10, 2019	
April 19, 2019	Complete internal review of the vendor proposals	April 19, 2019	
May 10, 2019	Interview vendors	May 10, 2019	
May 15, 2019	Award contract	May 20, 2019	Formal notice to non-selected vendors took longer than expected.
May 2019	Execute Contract with Vendor	August 26, 2019	IBM took 89 days to finalize the contract which greatly impacted the timeline of the partner onboarding.
June 6, 2019	Project Kickoff Meeting	June 6, 2019	
July 3, 2019	Kickoff +30 days – Complete Use Cases,	July 3, 2019	

Table 5 : Project Timeline

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 that effect of phishing . Building on our analysis of the research literature, we outlined how an effective anti-phishing program should be designed and implemented.

Based on the weak coherence between our empirical findings and currently used anti-phishing solutions, we believe that this contribution addresses a crucial technical gap. In our discussion, we outlined several implications of our findings concerning the design and capabilities of anti-phishing tools. Significant design aspects and capabilities in this regard are automated

operation and individualization with continuous assessment/ optimization of the configuration of training parameters. 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. Moreover, an effective anti-phishing tool should have community functions to facilitate cooperation and load-balancing among disparate anti-phishing efforts (e.g., shared email templates or co-designed training curricula.) Based on our survey and analysis of relevant sources in the technical literature, we found that, despite the various advanced capabilities that tools currently available in the anti-phishing domain offer, such tools only support a limited subset of the potential factors identified as necessary to yield the desired training effects. Therefore, we believe that our work does have a high practical value in terms of contributing to the development of more complete training solutions with a more significant impact to reduce phishing susceptibility on the part of users. In this paper we also seen that how we can create the technical Cyber Lab for better anti phishing detection technique and their solution . Los Angeles Cyber Lab report 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.

Reference:

[1]. https://www.zscaler.com/campaign/threatlabz-phishing-report
[2]. https://inspiredelearning.com/blog/history-of-phishing/
[3]. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.zscaler.com/resources/industry-reports/threatlabz-phishing-report-2024.pdf
[4]. https://jumpcloud.com/blog/phishing-attack-statistics
[5]. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://info.greathorn.com/hubfs/Reports/2021-Business-Email-Compromise-Report-GreatHorn.pdf
[6]. https://info.perception-point.io/pdf-h1-report-2024?submissionGuid=f8161522-7672-430d-9132-cdcd3b137287
[7]. https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks
[8]. https://www.tessian.com/blog/phishing-statistics-2020
[9]. https://www.statista.com/statistics/266155/number-of-phishing-domain-names-worldwide/
[10]. https://www.getastra.com/blog/security-audit/phishing-attack-statistics/
[11]. https://www.proofpoint.com/us/threat-reference/phishing
[12]. Ransomware Report | ThreatLabz (zscaler.com)
[13]. https://www.globenewswire.com/news-release/2020/10/19/2110233/0/en/Microsoft-is-Most-Imitated-Brand-for-Phishing-Attempts-in-Q3-2020.html
[14]. Infosec: phishing definition, prevention, and examples (2019). https ://resou rces.infos ecins titut e.com/categ ory/
[15]. enter prise /phish ing/
[16]. 2. Bissell K, LaSalle RM, Cin PD (2019) Accenture's ninth annual cost of cybercrime study: unlocking the value of
[17]. improved cybersecurity protection. https ://www.accen ture.com/us-en/insights/secur ity/cost-cyber crime -study
[18]. 3. Nero PJ, Wardman B, Copes H, Warner G (2011) Phishing: crime that pays. In: 2011 eCrime researchers summit, pp
[19]. 1–10
[20]. 4. Bisson D (2015) Sony hackers used phishing emails to breach company networks. https ://www.tripw ire.com/state
[21]. -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
[22]. Dec 2017
[23]. 5. Sanger DE, Benner K (2018) U.S. accuses North Korea of plot to hurt economy as spy is charged in Sony hack. The
[24]. New York Times, Chap, U.S. Accessed 29 Oct 2018
[25]. 6. Franceschi-Bicchierai L (2016) Russian hackers launch targeted cyberattacks hours after trump's win. https ://
[26]. mothe rboar d.vice.com/en_us/article/nz79g b/russi an-hacke rs-launc h-targe ted-cyber attac ks-hours -after -trump
[27]. s-win. Accessed 26 Dec 2017
[28]. 7. Aaron G (2020) APWG phishing activity trends 4th quarter report 2019. https ://docs.apwg.org/repor ts/apwg_

[29]. trend s_repor t_q4_2019.pdf. Accessed 04 Jan 2020
[30]. 8. Aaron G (2019) APWG phishing activity trends 4th quarter report 2018. https ://docs.apwg.org//repor ts/apwg_
[31]. trend s_repor t_q4_2018.pdf. Accessed 04 Jan 2020
[32]. 9. Aaron G (2018) APWG phishing activity trends 4th quarter report 2017. https ://docs.apwg.org//repor ts/apwg_
[33]. trend s_repor t_q4_2017.pdf. Accessed 04 Jan 2020
[34]. 10. Aaron G (2017) APWG phishing activity trends 4th quarter report 2016. https ://docs.apwg.org//repor ts/apwg_
[35]. trend s_repor t_q4_2016.pdf. Accessed 04 Jan 2020
[36]. 11. Hong J (2012) The state of phishing attacks. Commun ACM 55(1):74–81
[37]. 12. Gorman S (2013) Annual U.S. cybercrime costs estimated at \$100 billion. Wall Street J. Accessed 22 Mar 2017
[38]. 13. Morrow S (2019) Juniper research—the future of cybercrime & security research report. https ://www.junip erres
[39]. earch .com/docum ent-libra ry/white - paper s/the-futur e-of-cyber crime -white - paper
[40]. 14. Cybersecurity ventures: 2019 official annual cybercrime report (2019). https ://www.herja vecgr oup.com/the-
[41]. 2019-offic ial-annua l-cyber crime - repor t/
[42]. 15. CNBC: Xoom says $30.8 mln transferred fraudulently to overseas accounts (2015). https ://www.cnbc.
[43]. com/2015/01/06/xoom-says-308-mln- trans ferre d-fraud ulent ly-to-overs eas-accou nts.html
[44]. 16. Dou Z, Khalil I, Khreishah A, Al-Fuqaha A, Guizani M (2017) Systematization of knowledge (SoK): a systematic
[45]. review of software-based web phishing detection. IEEE Commun Surv Tutor 19(4):2797–2819
[46]. 17. Gupta BB, Tewari A, Jain AK, Agrawal DP (2017) Fighting against phishing attacks: state of the art and future challenges.
[47]. Neural Comput Appl 28(12):3629–3654
[48]. Nadeem M, Arshad A, Riaz S, Zahra SW, Dutta AK, Almotairi S. Preventing the Cloud Networks through Semi-Supervised Clustering from Both Sides Attacks. Appl Sci. 2022; 12(15): 7701.
[49]. 2. Rashid A, Chaturvedi A. Cloud computing characteristics and services: a brief review. Int J Comput Sci Eng. 2019; 7(2): 421–426.
[50]. 3. Nadeem M, Arshad A, Riaz S, Band SS, Mosavi A. Intercept the Cloud Network from Brute Force and DDoS Attacks via Intrusion Detection and Prevention System. IEEE Access. 2021; 9: 152300–152309.
[51]. 4. Jangjou M, Sohrabi MK. A comprehensive survey on security challenges in different network layers in cloud computing. Arch Comput Methods Eng. 2022; 29(6): 3587–3608.
[52]. 5. Alam A. Cloud-Based E-learning: Scaffolding the Environment for Adaptive E-learning Ecosystem Based on Cloud Computing Infrastructure. In Computer Communication, Networking and IoT: Proceedings of 5th ICICC 2021. 2022; 2: 1–9. Singapore: Springer Nature Singapore.
[53]. 6. Seifert M, Kuehnel S, Sackmann S. Hybrid Clouds Arising from Software as a Service Adoption: Challenges, Solutions, and Future Research Directions. ACM Comput Surv. 2023; 55(11): 1–35.
[54]. 7. Nadeem F. Evaluating and Ranking Cloud IaaS, PaaS and SaaS Models Based on Functional and Non-Functional Key Performance Indicators. IEEE Access. 2022; 10: 63245–63257.
[55]. 8. Parast FK, Sindhav C, Nikam S, Yekta HI, Kent KB, Hakak S. Cloud computing security: A survey of service-based models. Comput Secur. 2022; 114: 102580.
[56]. Mohammed CM, Zeebaree SR. Sufficient comparison among cloud computing services: IaaS, PaaS, and SaaS: A review. Int J Sci Bus. 2021; 5(2): 17–30.
[57]. 11. Ali M, Jung LT, Sodhro AH, Laghari AA, Belhaouari SB, Gillani Z. A Confidentiality-based data Classification-as-a-Service (C2aaS) for cloud security. Alex Eng J. 2023; 64(2): 749–760.
[58]. 12. Butt UA, Amin R, Mehmood M, Aldabbas H, Alharbi MT, Albaqami N. Cloud Security Threats and Solutions: A Survey. Wirel Pers Commun. 2023; 128(1): 387–413.
[59]. 13. Aoudni Y, Donald C, Farouk A, Sahay KB, Babu DV, Tripathi V, Dhabliya D. Cloud security based attack detection using transductive learning integrated with Hidden Markov Model. Pattern Recognit Lett. 2022; 157: 16–26.

[60]. 14. Nadeem M, Arshad A, Riaz S, Zahra SW, Dutta AK, Al Moteri M, Almotairi S. An Efficient Technique to Prevent Data Misuse with Matrix Cipher Encryption Algorithms. Comput Mater Contin. 2022; 74(2): 4059–4079.

[61]. 15. Upadhyay D, Zaman M, Joshi R, Sampalli S. An efficient key management and multi-layered security framework for SCADA systems. IEEE Trans Netw Service Manag. 2021; 19(1): 642–660.

[62]. 16. Zahra SW, Arshad A, Nadeem M, Riaz S, Dutta AK, Alzaid Z, Almotairi S, *et al*. Development of Security Rules and Mechanisms to Protect Data from Assaults. Appl Sci. 2022; 12(24): 12578.

[63]. 17. Al-Shabi MA. A survey on symmetric and asymmetric cryptography algorithms in information security. Int J Sci Res Publ (IJSRP). 2019; 9(3): 576–589.

[64]. 18. Musa A, Mahmood A. Client-side cryptography based security for cloud computing system. In 2021 Int Conf on Artificial Intelligence and Smart Systems (ICAIS), Coimbatore, India. 2021; 594–600.

[65]. 19. Hossain ME. Enhancing the security of caesar cipher algorithm by designing a hybrid cryptography system. Int J Comput Appl. 2021; 183(21): 55–57.

[66]. Adewole, K. S., Akintola, A. G., Salihu, S. A., Faruk, N., and Jimoh, R. G. (2019). Hybrid rule-based model for phishing URLs detection. *Lecture Notes Inst. Comput. Sci. Soc. Inf. Telecommun. Eng.* 12, 119–135. doi: 10.1007/978-3-030-23943-5_9

[67]. Alabdan, R. (2020). Phishing attacks survey: types, vectors, and technical approaches. *Fut. Int.* 12:168. doi: 10.3390/fi12100168

[68]. Aljofey, A., Jiang, Q., Rasool, A., Chen, H., Liu,W., Qu, Q., et al. (2022). An effective detection approach for phishing websites using URL and HTML features. *Sci. Rep.*12:10841. doi: 10.1038/s41598-022-10841-5

[69]. Jain, A. K., and Gupta, B. B. (2017). Phishing detection: analysis of visual similarity based approaches. *Secur. Commun. Netw.* 2017, 1–20. doi: 10.1155/2017/5421046

[70]. Anti-Phishing Working Group (APWG) (2024). *Phishing Activity Trends Report, 3rd Quarter 2022.* Available online at:https://docs.apwg.org/reports/apwg_trends_report_q3_2024.pdf (accessed october, 2024).

[71]. APWG and Phishing Activity Trends Reports (2024). Apwg.org. Available: https://apwg.org/trendsreports. (accessed October , 2024).

[72]. S. Loftesness, Responding to "Phishing" Attacks, Glenbrook Partners, 2004.

[73]. Gupta, B. B., Tewari, A., Jain, A. K., & Agrawal, D. P. (2017). Fighting against phishing attacks: state of the art and future challenges. *Neural Computing and Applications*, *28*(12), 3629-3654.

[74]. Huang, H., Zhong, S., & Tan, J. (2009, August). Browser-side countermeasures for deceptive phishing attack. In *2009 Fifth International Conference on Information Assurance and Security* (pp. 352-355). IEEE.

[75]. https://www.techtarget.com/searchsecurity/tip/How-to-detect-deepfakes-manually-and-using-AI

[76]. https://ironscales.com/glossary/deepfake-phishing

[77]. U.S. Secret Service. 2020. *Secret Service issues COVID-19 (Coronavirus)phishing alert* [Press release]. https:// www. secre tserv ice. gov/ press/ releases/ 2020/ 03/ secret- servi ce- issues- covid-19- coron avirusphishing- alert. Accessed 7 Apr 2020.

[78]. https://www.ncsc.gov.uk/guidance/phishing

[79]. https://transparencyreport.google.com/safe-browsing/search?hl=en

[80]. A. Aleroud and L. Zhou, "Phishing environments, techniques, and countermeasures: A survey," Comput. Secur., vol. 68, pp. 160–196, 2017, doi: 10.1016/j.cose.2017.04.006