A Critical Study of Social Engineering vis-a-vis Phishing Attacks

Naresh Babu Andaluri[1], Dr Asha Srivastava[2], Dr Rupaali Andaluri[3]
[1]*Research Scholar, Singhania University. India, Ex-Head, Vulnerability Management for US corporate "Eagle View"*
[2]*Director, CFSL/DFSS/CBI, New Delhi*
[3]*Scientist C & Asst Director. CFSL/DFSS/CBI/New Delhi*

Abstract: The present study aims to present a Critical & Exploitable pattern used in Social Engineering attacks vis-a-vis Phishing attacks and different ways to counter measure those attacks. The current study also describes the ways to prevent the most widely used across the geographies which causes Financial and mental damage to human being. With the help of real time cases, we will now try to understand the present-day scenario and the remedies.

Keywords:; network security; phishing; Social Engineering; Cyber Crime

INTRODUCTION

We will first look into the basics of the Social engineering attacks (SEA) and types of SEA so that we can corroborate with the real cases and their impact on Human being and society as whole.

What is a social engineering attack?
Social engineering is the term used for a broad range of malicious activities accomplished through human interactions. Attacker uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
Social engineering attacks generally happen in one or more steps. The Attacker first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack. Then, the attacker moves to gain the victim's trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources
In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

What is a phishing attack?
Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.
Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as

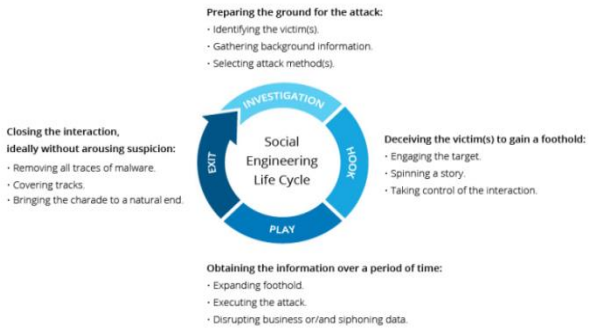
- Natural disasters (e.g., Hurricane Katrina, Indonesian tsunami)
- Epidemics and health scares (e.g., H1N1, COVID-19)
- Economic concerns (e.g., IRS scams)
- Major political elections
- Holidays

What are common indicators of phishing attempts?

- Suspicious sender's address. The sender's address may imitate a legitimate business. Cybercriminals often use an email address that closely resembles

one from a reputable company by altering or omitting a few characters.

- Generic greetings and signature. Both a generic greeting—such as “Dear Valued Customer” or “Sir/Ma’am”—and a lack of contact information in the signature block are strong indicators of a phishing email. A trusted organization will normally address you by name and provide their contact information.
- Spoofed hyperlinks and websites. If you hover your cursor over any links in the body of the email, and the links do not match the text that appears when hovering over them, the link may be spoofed. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net). Additionally, cybercriminals may use a URL shortening service to hide the true destination of the link.
- Spelling and layout. Poor grammar and sentence structure, misspellings, and inconsistent formatting are other indicators of a possible phishing attempt. Reputable institutions have dedicated personnel that produce, verify, and proofread customer correspondence.
- Suspicious attachments. An unsolicited email requesting a user download and open an attachment is a common delivery mechanism for malware. A cybercriminal may use a false sense of urgency or importance to help persuade a user to download or open an attachment without examining it first.



Social Engineering Attack Lifecycle (FIG-1)

Common Signs of Phishing Attempts

- Requests for personal data, login credentials, or credit card information
- Unreasonable threats
- Sense of urgency
- Offering big money/loans/prizes
- Spelling or grammatical errors
- Suspicious URLs
- Once-in-a-lifetime offers

Most Common Types of Phishing Attacks and How to Identify Them

1. Email Phishing

Phishing emails top this list as one of the oldest and most commonly used types of phishing attacks. Most attempts use emails to target individuals by pretending to come from a trustworthy sender. Dedicated hackers will copy the exact email format from a legitimate company and include a malicious link, document, or image file that can trick the user into "confirming" their personal information or automatically download malicious code.

How to Identify Email Phishing:

- Requests for personal information - Legitimate companies will NEVER ask for your personal information through email.
- Urgent problem - Many scammers will disguise their phishing attempt with an urgent notice, such as an account breach, payment failure, login verification, or copyright infringement. Do NOT click on any links and go directly to the website to check.
- Shortened links - Shortened or condensed links are ways to mask malicious URLs. Services like Bitly or Tiny URL can hide the actual web address the link will take you.
- Non-domain email addresses - Fraudulent email addresses often use third-party providers or variations of legitimate email domains (ex. @upguardnow.com instead of @upguard.com). Always hover over the sender's email address to ensure it matches the user's or company's name.
- Spelling & grammar mistakes - Any misspellings or grammar issues in an email should trigger a red flag. Scammers often come from non-English speaking countries.
- Any file attachments - Unless the source is verified, a good rule of thumb is never to open any attachments, especially if they include .exe, .zip, and .scr extensions. Most companies will direct

you to their website to download files or documents.
- Single or blank image - If the email is a screenshot of an email or a blank box but with no real text, do NOT click on the image. Malware code may be tied to the image that can trigger an automatic download.

2. Spear Phishing

Spear phishing attacks are a more targeted approach to email phishing that focuses on specific individuals and organizations. Using open-source intelligence (OSINT), criminals can gather publicly available information and target entire businesses or sub-departments. They may trick users into believing the email is an internal communication or from a trustworthy source due to access to personal information.

How to Identify Spear Phishing:
- Unusual requests - If the requests come from within your company asking for credentials above their pay grade, message the individual directly using another communication channel for confirmation. Using direct messaging methods can also be helpful in the event of a hacked email.
- Links to shared drives - If the scammer pretends to be from an internal or other trustworthy source, there is no need to share links to a drive you should already have access to. The link is most likely corrupted and can redirect you to a fake website.
- Unsolicited emails - If the email provides an "important document" to download and view, but you didn't request it, it could be a fake email. ALWAYS verify the sender before opening.
- Specific mentions of personal details - Scammers may be trying to justify themselves as a trustworthy source by providing otherwise unnecessary information about you. Obvious attempts to gain your trust should be viewed with suspicion.

3. Whaling

If spear phishing emails target specific groups or individuals, whaling is the practice of targeting high-level executives. Also known as CEO fraud, whaling attacks are typically much more sophisticated, relying on OSINT, plenty of research into the company's business practices, and even a deep dive into social media accounts. Because the goal is to successfully dupe the executive, the emails are usually extremely fluent in business communications with near-perfect English.

How to Identify Whaling Attacks:
- Incorrect domain address - Unless an email has been hacked, scammers will attempt to use similar, but incorrect, domain addresses (ex. @rbi.co.in instead of @rbi.com). It's important to keep a detailed eye when viewing email communications.
- Use of personal email - Any communication from other executives or business partners should be done through work emails and NEVER through personal emails. Even if the individual asks for help outside of work, communicate with them directly through another offline channel to verify their identity.
- New contact requests - If you receive an email from a partner or supplier that has never contacted you for business dealings, it may signify a phishing attempt. Verify the communication through the proper channels or the individual responsible for the account.

4. Business Email Compromise (BEC)

A business email compromise is similar to whaling, but instead of attempting to trick the executive, it impersonates them. Criminals will impersonate or obtain access to an executive email account with decision-making authority and send internal requests to lower-level employees.

In 2014, Omaha-based agriculture company Scoular became a victim of a BEC attack. The corporate controller, Keith McMurtry, received an email from his CEO asking for an immediate wire transfer to acquire a Chinese-based company. The email detailed a lawyer who would be in charge of the transaction, and McMurtry wired in total $17.2 million to an offshore account. However, the email was ultimately fraudulent, containing fake phone numbers and email addresses.

How to Identify Business Email Compromise Attacks:
- Sense of urgency - Larger transactions and important business deals usually take time and pass through multiple sets of eyes before finalizing. It should raise red flags if the communication sounds especially urgent and does not have more than 2 or 3 people on the email and very authentic signage and discoloured

logos.(happens generally with manipulated logos & Screenshots)

- Unusual behaviours - Sophisticated BEC attacks will try to sound as professional as possible, but it may be possible to notice differences in tone or personality. If an executive talks or writes differently than usual, keep an eye out for other signs of a phishing attack.
- No legal correspondence - All business deals should involve a legal team or lawyer to ensure legitimacy and legality. If no lawyer is looped into the email, seek out the correct party through the company chain of command to verify the email's legitimacy.

5. Voice Phishing

Voice phishing, also known as "vishing," is when a scammer calls your phone number in an attempt to steal information or money. New sophisticated technology allows criminals to spoof caller IDs and pretend to be from a trusted source. Typically, the caller will create a sense of urgency to appear authoritative and prevent the recipient from thinking clearly.

Some commonly used vishing attack tactics include:

- A family member is in trouble and needs monetary help
- IRS needs your social security number (SSN) to confirm tax returns
- Pay a small fee to redeem a fake prize or vacation that you didn't sign up for
- A warrant has been issued for your arrest
- Vehicle qualifies for extended warranty
- Your bank account has been flagged for suspicious activity
- Guaranteed returns on investment opportunities
- A large sum of debt that needs to be paid

How to Identify Voice Phishing:

- Blocked or unidentified number - Phishing calls tend to come from blocked numbers. If you answer and the caller sounds suspicious, asking you to press 1 & 2 etc in your dial pad, hang up immediately.
- Requests for sensitive information or money - Government organizations always conduct business through official mail and will NEVER ask for your personal information over a phone call.

6. HTTPS Phishing

HTTPS (hypertext transfer protocol secure) phishing is a URL-based attack that attempts to trick users into clicking a seemingly safe link. HTTPS is the standard protocol for traffic encryption between browsers and websites and requires TSL/SSL certificates to be enabled. In the past, browsers could detect sites that did not have HTTPS enabled as the first line of protection against cybercrime.

However, hackers now can obtain these certificates for free and add HTTPS to their phishing sites, making it harder to distinguish between what is safe and what is not.

How to Identify HTTPS Phishing:

- Shortened URLs - Shortened links can hide the link's true address and are a great way for scammers to hide phishing attempts. Links should be in their original format so you can verify their source.
- Hyperlinked text - Text with clickable links can also lead you to malicious websites. Make sure to hover over the link (without clicking on it) to see the source URL.
- URL misspellings - Any misspellings in the email domain are an immediate telltale sign that the email is fake & luring.

7. Clone Phishing

Instead of sending fake emails, clone phishing takes a real email sent by an individual or company, copies it to near-identical levels, and resends it to the target with a new corrupted attachment or link. The email will appear as a resend and display at the top of the victim's inbox. In some cases, the phisher will use a fake but similar email, but more sophisticated hackers will spoof the email address to appear as if sent by a legitimate domain.

How to Identify Clone Phishing:

- Duplicate emails - The best way to recognize clone phishing is to review your recent emails. If a duplicate appears, look for any new links in the more recent email that may be a sign of phishing. ALWAYS verify the correct link and compare it to previous email communications.
- Misspelled email addresses - Although minor, fake emails will usually always have a slight error that an untrained eye might miss.

- Hyperlinked text - When hovering over a link, browsers will show the real address in the bottom left of the screen. If the URL doesn't match the text that it's linked to, it could be a sign of phishing. Be watchful in the bottom left side of your browser for forwarding links.

8. SMS Phishing

SMS phishing or "smishing" is similar to vishing, but instead of calling, scammers will send SMS text messages with links or attachments. Because personal phone numbers are generally less accessible to the public, individuals tend to trust text messages more. However, with today's smart phones; it's just as easy for hackers to steal personal data through text message URLs.

How to Identify SMS Phishing:

- Unsolicited texts - Unless you signed up for SMS message alerts directly, phishing messages offering a free coupon or an amazing deal for a product you don't use are an obvious sign of phishing. Other tactics may ask for you to confirm account information, check on the status of an order, or verify medical information.
- Unknown numbers - Getting a request for information over text messaging should be a red flag. Use a free number lookup service to see if you can get any more information about the source of the text or contact related individuals to get verification. As a good rule of thumb, don't click on the link provided in the text and don't engage.
- Authentication request - If you receive an unauthorized authentication request, someone may be trying to access one of your accounts. You should change your password immediately if you receive one of these texts to prevent further access.
- Logoff the phone from Internet and run the security check and Anti Virus checks in your phone.

9. Pop-Up Phishing

Although most people have an ad or pop-up blocker installed on their web browsers, hackers can still embed malware on websites. They may come as notification boxes or look like legitimate ads on a web page. Anyone that clicks on these pop-ups or ads will become infected with malware.

How to Identify Pop-Up Phishing:

- Browser notifications - Many browsers, including Chrome and Safari, will prompt users to either "Allow" or "Decline" notifications when they visit a new site. Browsers don't filter out spam notifications, so if the user accidentally clicks "Allow," malicious code could be automatically downloaded.
- New tab or window - Web surfing without pop-up blockers can be dangerous, particularly for mobile devices. Visiting certain sites can trigger a new tab or window to open with links to download malware.
- Urgent messages - Pop-ups claiming that you need to update your antivirus or renew a subscription are clear indicators of phishing. You should resolve any updates, renewals, payments, or account issues on the main website and not through a pop-up on an unrelated website.

10. Social Media Phishing

Aside from email, social media has become a popular attack vector for phishing attacks. With so much personal information displayed through social media, attackers can easily use social engineering attacks to access sensitive data. Billions of people around the world use platforms like Facebook, Instagram, Snap chat, and LinkedIn to network, which also increases the risk of phishing attempts.

These attacks usually involve a link that can send you to malicious websites to steal important information. In some cases, a scammer will befriend you in an attempt to steal money from you by pretending to be in trouble.

The most commonly used tactics include:

- Offers or online discounts
- Surveys or contests
- Friend requests
- Fake videos
- Comments on videos or photos

How to Identify Social Media Phishing:

- Suspicious links - Even if you receive a link from your friend, it's possible that their account may have been hacked. If the link contains spelling

errors or includes a random assortment of numbers, letters, and symbols, it may be in your best interest to ignore the link.
- Suspicious account - If you receive a message or friend request from an unknown individual, do NOT accept. These accounts have little to no activity in nearly all cases because they are new accounts looking for phishing victims.

11. Angler Phishing

Attackers can take social media phishing to another level by posing as customer support staff in an angler phishing attack. The scammers will create a fake account and contact a disgruntled user they found through comments or posts on a social media account. During the interaction, the scammer offers assistance after verifying a few personal details and then provides a link to help resolve the issues. Of course, the link contains malware and the attacker has successfully exploited another victim.

How to Identify Angler Phishing:
- Non-verified account - An official support page or account for a company will typically be verified and be directly linked to the main page. If a large company such as Twitter or Facebook contacts you, make sure they have a blue checkmark next to their name. You can also check the company website for their official support page or contact information.
- Lack of profile history - For smaller businesses that may not be verified yet, they should still have an extensive history of other customer interactions. Accounts that have very few followers and no posts are most likely brand new accounts trying to take advantage of people that won't bother checking.

12. Evil Twin Phishing

An evil twin phishing attack creates an unsecured Wi-Fi hotspot access point that baits unsuspecting users into connecting. Once connected, all inbound and outbound data can be intercepted, including personal data or financial information. Hackers can also prompt the users to visit a fake website portal in hopes the user will provide valuable authentication details.

Evil twin phishing attacks are most common in public areas with free Wi-Fi, like coffee shops, libraries, airports, or hotels. The best way to prevent becoming an evil twin phishing target is to use a virtual private network (VPN) while using public Wi-Fi.

How to Identify Evil Twin Phishing:
- Duplicate Wi-Fi hotspots - If you notice multiple Wi-Fi access points with the same name, look for the one that is secured and requires a password (given by the establishment) to connect. If both access points are unsecured, it is highly discouraged to connect to be safe.
- Unsecure warnings - Some laptops or mobile devices will trigger a notification that the network you're connecting to is unsecured. If you receive this message, consider connecting to a secure network or not connecting at all.

13. Website Spoofing

Attackers will create an entirely fake website in a website spoofing attempt to steal your personal information. A well-made fake website will contain the same elements as the original, including logos, text, colours, and functionality. Finance, healthcare, and social media websites are commonly spoofed because they often contain your most important information.

How to Identify Website Spoofing:
- URL misspellings - Attacks often take advantage of homograph attacks, which exploit the similarities between characters. For example, you might notice an "rn" in place of an "m" or "vv" (two v's) instead of a "w."
- Website errors - Very rarely are websites perfectly spoofed to match the original. Sometimes the site logos are slightly more pixelated or you might notice the text is misaligned. If anything looks off, stop using the website immediately, especially if you had accessed it from a link sent to you through email or messaging. It always helps to keep the original website bookmarked so you can easily access it.

14. Email Spoofing

Email spoofing is when a scammer creates an entirely fake email domain to try and fool users into believing they are legitimate. To avoid detection, the attackers can edit the header of the email to include the name of

a legitimate domain in hopes that the targeted user won't check the domain address where it was actually sent from. Because there is no domain verification under the Simple Mail Transfer Protocol (SMTP), so attackers can spoof emails easily.

Phishers can also choose to hide the sender's address to display only the name. They may try to use a real name that the targeted user will recognize so that they'll open the email. When the attacker combines both a real name and the legitimate domain name in the header, it can easily trick unsuspecting users.

Domain spoofing is different from DNS spoofing because it creates an entirely new domain rather than hacking the DNS server.

How to Identify Domain Spoofing:

- Unsolicited emails - Any unexpected emails, particularly ones that make requests, should be the first red flag of a phishing attempt. Take a closer look at the messaging and use another communication channel to verify the email.
- Emails address misspellings - Fake domains are supposed to look legitimate at first glance, but upon closer look, there could be homograph attacks involved. If you suspect the email might be from a fake domain, copy and paste the link into a notepad or Microsoft Word document to identify any misspellings.

15. DNS Spoofing

DNS spoofing attacks (also known as DNS server poisoning or pharming attacks) are a more technical process that requires cybercriminals to hack a Domain Name Server (DNS), a server that translates domain names into IP addresses. When a DNS server is hacked, it can automatically redirect a URL entry to a malicious website under an alternate IP address.

Once the user lands on the corrupted website, one of two things may happen - 1) Malware is automatically downloaded onto the device, or 2) A spoofed website may appear, prompting the user to enter their login information or ask to confirm personal information or credit card numbers.

How to Identify Pharming Attacks:

- Unsecure website - Typically, unsecured websites are a sign of phishing attempts or are at risk of becoming infected by malware. In most cases, the site will begin with HTTP instead of HTTPS.
- Website errors - A fake website usually contains errors, including misspellings, buttons that don't work, low-quality images, misaligned text, or wrong colours.

16. Image-Based Phishing

Image-based phishing usually finds itself in the content of a phishing email. In addition to hyperlinks and malicious URLs, images can also contain links to infected websites. In some cases, the image included may be the only thing in the email that has a phishing intention just to fool users into thinking the email is safe.

How to Identify Image-Based Phishing:

- Embedded image link - Hover over the image to check if there’s a link to a non-official, third-party website. Does the link have spelling errors? Generally, it’s safe to open and read an email to investigate, as long as you don’t click on anything.
- Spam email - Any email that was sent straight to the spam folder could be a sign of a phishing attempt, even if it seems like an official email from the company or individual. There are many ways to make an email seem legitimate, but if it has been flagged as spam, there may be phishing elements detected by the email server.
- Large CTA buttons - A popular phishing tactic is to include an inviting and eye-catching call-to-action (CTA) button, similar to sales promotional emails. Individuals that act mindlessly may not think twice and click on the button just because it told them to. Make sure that you verify the sender, URLs, and email content before clicking on the CTA image.

17. Search Engine Phishing

In search engine phishing, scammers create legitimate pages based on high-value keywords and searches to get them ranked on popular search engines, such as Google or Bing. These pages often feature an eye-catching offer to lure unsuspecting users. Once the users land on these pages, they're asked to enter banking information or their SSN. These fake pages often include:

- Sanctioned Credit cards

- Free products
- Lottery results
- Free vacation
- Investment opportunities
- Discount codes
- Job offers
- Dating matches
- Infected by computer virus

How to Identify Search Engine Phishing:

- Once-in-a-lifetime offers - Nothing is truly free, and if it sounds too good to be true, it probably is. Criminals are looking to take advantage of people trying to make a quick buck or cut corners on spending. Do your due diligence and properly research a website or offer before you accept and start entering your personal information.
- Poorly made websites - Many of these websites are made extremely quickly because they tend to get shut down once they get reported. If it looks like a low-quality site with minimal functionality and excess links, avoid it at all costs.

18. Watering Hole Phishing

Watering hole phishing is a tactic that targets one particular company or group of people by infecting a third-party website they frequently visit. The attackers find and exploit vulnerability on the website, infect the site with malware, and then bait users by sending emails directing them to the site.

Although this type of attack is less common than the others, once the hackers infect a single user, they can gain access to the entire network and system. Additional site visitors can also become victims, even if they have no relation to the main targeted group.

How to Identify Watering Hole Phishing:

- Security alerts - One of the first signs of a phishing attack is when your antivirus or anti-malware software detects an attack. That's why it's important to keep your security solutions updated so the software can detect phishing attempts automatically.
- Security testing - Because it's hard to control third-party risk, the best way to identify potential cyber threats is to continually test your security defenses and install security patches. If the third-party site is frequently visited, installing endpoint protection software can protect against watering hole phishing attacks.

19. Man-in-the-Middle (MITM) Phishing

A man-in-the-middle phishing attack is when an attacker intercepts and alters a communication chain, effectively becoming the "middleman." The attacker then controls the communication flow and is responsible for sending and receiving all messages. While the attacker is intercepting the data, he can manipulate it to gain personal information from both parties.

How to Identify MITM attacks:

Generally, MITM attacks are hard to detect, as URL errors are more likely the result of another phishing method. Network administrators must constantly monitor traffic to detect altered communication. Some signs that should raise red flags are:

- Unsecured websites - If you are web browsing, always give a quick look for the padlock next to the URL in the search bar in the browser. Typically, a locked padlock shows that the website has a valid SSL certificate and HTTPS protocol (instead of HTTP).
- URL misspellings - If the URL is misspelled or has random numbers inserted in between, double-check the website with a different device.
- Noticeably slower messaging - Instant messaging platforms typically have little to no delay when sending messages. However, platforms that don’t use end-to-end encryption can fall victim to a MITM attack. Messages that take noticeably longer to send could be a sign of an attack.

Why phishing is successful

- Most phishing attacks are less about the technology and more about social engineering. It’s amazing how easily humans are manipulated when emotions are triggered.
- Many modern phishing emails play on empathy or fear, or even make hostile accusations in order to trigger an angry response.
- Nowadays many internet users / online payment users are illiterates in terms of minimal awareness about what is happening in the present day world.
- Little or lesser propaganda on victims of these attacks by concerned organisation.

- Failure to educate the users by financial & Federal agencies.
- Digital payments at very ground level, forcing uneducated to be victimised by attackers.

Top anti-phishing tools

1. Avanan

Avanan offers anti-phishing software for cloud-hosted email, tying into your email provider using APIs to train their AI using historical email. The service analyzes not just message contents, formatting, and header information, but evaluates existing relationships between senders and receivers to establish a level of trust.

2. Barracuda Sentinel

Barracuda Sentinel is another tool that leverages mail provider APIs to protect against phishing as well as business email compromise (BEC). Because compromised email accounts tend to lead to more phishing attempts or further account-based attacks, Barracuda's focus on minimizing further damage as a result of a successful phishing attempt has more value than relying solely on prevention. Barracuda also provides brand protection and domain fraud prevention through DMARC analysis and reporting.

3. Brand Shield

Brand Shield focuses exclusively on protecting your corporate brand and that of your executives. Identifying phishing attacks (through email, social media, or other mediums) which leverage your brand or the names of your executives is just one component of Brand Shield's portfolio. Brand Shield also monitors the internet for rogue websites using your brand as well as marketplaces like Amazon where physical counterfeits of your products could pop up for sale.

4. Cofense PDR

Cofense PDR (Phishing Detection and Response) is a managed service where both AI-based tools and security professionals are leveraged in concert to identify and mitigate phishing attacks as they happen. Managed services can be a good option if you need to maximize the level of protection, as they can be more effective than even hiring a full-time team to handle phishing prevention since the managed services team is able to evaluate threat data from all of the enterprise systems they protect.

5. RSA Fraud Action

RSA Fraud Action anti-phishing service obviously comes from one of the big names in network security, and the list of features offered is what you'd expect from a heavy hitter. The anti-phishing service is a managed service like what Cofense offers and RSA brings capabilities like site shutdown, forensics, and optional countermeasures such as strategically responding to phishing attempts with planted credentials in order to track the attack chain and respond accordingly.

6. IRONSCALES

IRONSCALES is an email security platform that seeks to strengthen your existing email system through dynamic detection and analysis: blocking, flagging, or simply adding a banner to potentially suspicious email. IRONSCALES also offers end user training, focused on email security and general awareness, which helps strengthen your defense against the core of phishing: the social engineering attack.

7. KnowBe4

KnowBe4 boasts one of the biggest names in hacking (Kevin Mitnick) as their Chief Hacking Officer. Many of Mitnick's exploits were centred around social engineering, and their business reflects that by focusing on enabling employees to make better decisions through education. In addition to their top-rated awareness training KnowBe4 also offers Phisher, which is a Security Orchestration, Automation, and Response (SOAR) platform centered on phishing attempts: enabling your security team to more efficiently respond to email-based threats to your organization.

8. Mimecast

Mimecast offers several tools for protecting against phishing attempts, including features which detect malicious links and attachments removing them or rendering them safe using advanced methods like sandboxing. Mime cast's ability to prevent code-based attacks initiated through phishing emails or more sophisticated methods like QR codes by opening links within the Mime cast cloud, simplifying the

deployment process and ensuring prevention tools are always updated to the bleeding age.

9. Microsoft Defender for Office 365

Microsoft Defender for Office 365 brings similar capabilities as some of the other tools on this list: user training, phishing detection and prevention, forensic and root-cause analysis, and even threat hunting. Because Defender is simply an add-on for Office 365, it's integrated tightly without having to configure the initial integration. Microsoft also offers preset security policies that you can adjust to your needs; supporting enforcement, the option for users to override, and tracking policy changes over time. This service has special advantages for Office 365 customers and special disadvantages for everyone else.

10. Valimail

Valimail should be of interest even to IT shops with little-to-no budget. Valimail DMARC offering walks you through configuring DMARC for your email domains, and then aggregates and generates daily DMARC reports. Gaining this visibility into email authentication can help you rapidly identify additional senders that may be legitimate, potentially add them to your DMARC configuration, and then ramp up enforcement in order to prevent unauthorized email forging your domain. The best part is that Valimail offers several of their DMARC tools for free. The other service Valimail offers is Amplify, which facilitates implementation of the BIMI standard (Brand Indicators for Message Identification), which adds a corporate logo to email originating from your organization, showing that the sender is authenticated and valid. BIMI not only adds a layer of sophistication to your email config, it enhances trust in emails coming from your domain both for receiving servers and ultimately the recipient.

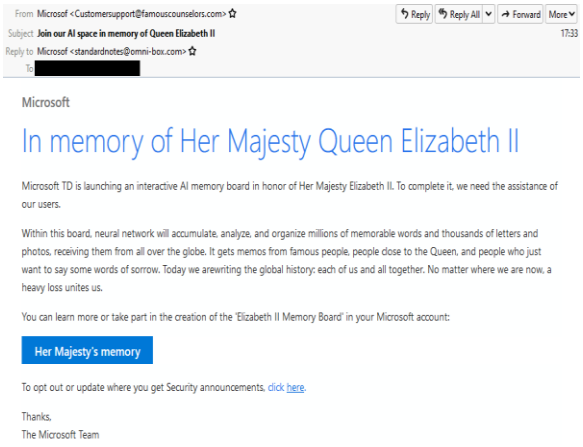
Case Studies

1. Threat actors are exploiting the death of Queen Elizabeth II in phishing attacks to lure their targets to sites that steal their Microsoft account credentials. Besides Microsoft account details, the attackers also attempt to steal their victims' multi-factor authentication (MFA) codes to take over their accounts.

In the campaign spotted by Proof point, the phishing actors impersonate "the Microsoft team" and try to bait the recipients into adding their memo onto an online memory board "in memory of Her Majesty Queen Elizabeth II."

After clicking a button embedded within the phishing email, the targets are instead sent to a phishing landing page where they're asked first to enter their Microsoft credentials.

"Messages contained links to a URL redirecting credential harvesting page targeting Microsoft email credentials including MFA collection," Proof point added.



The attackers use a new reverse-proxy Phishing-as-a-Service (PaaS) platform known as EvilProxy promoted on clearnet and dark web hacking forums, which allows low-skill threat actors to steal authentication tokens to bypass MFA

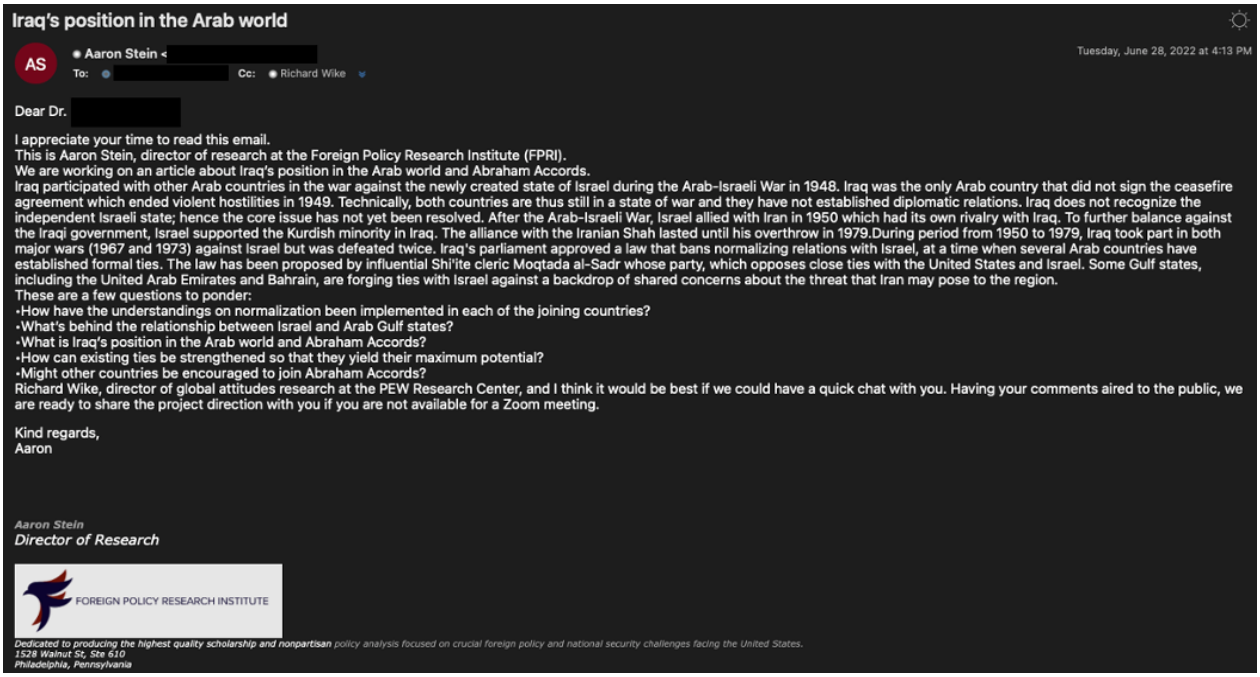
2. TA453 is an Iranian threat group believed to be operating from within the IRGC (Islamic Revolutionary Guard Corps), previously seen impersonating journalists to target academics and policy experts in the Middle East.

Multiple persona impersonation

TA453's new tactic requires far more effort from their side to carry out the phishing attacks, as each target needs to be entrapped in an elaborate realistic conversation held by fake personas, or sock puppets.

However, the extra effort pays off, as it creates a realistic-looking exchange of emails, which makes the conversation look legitimate.

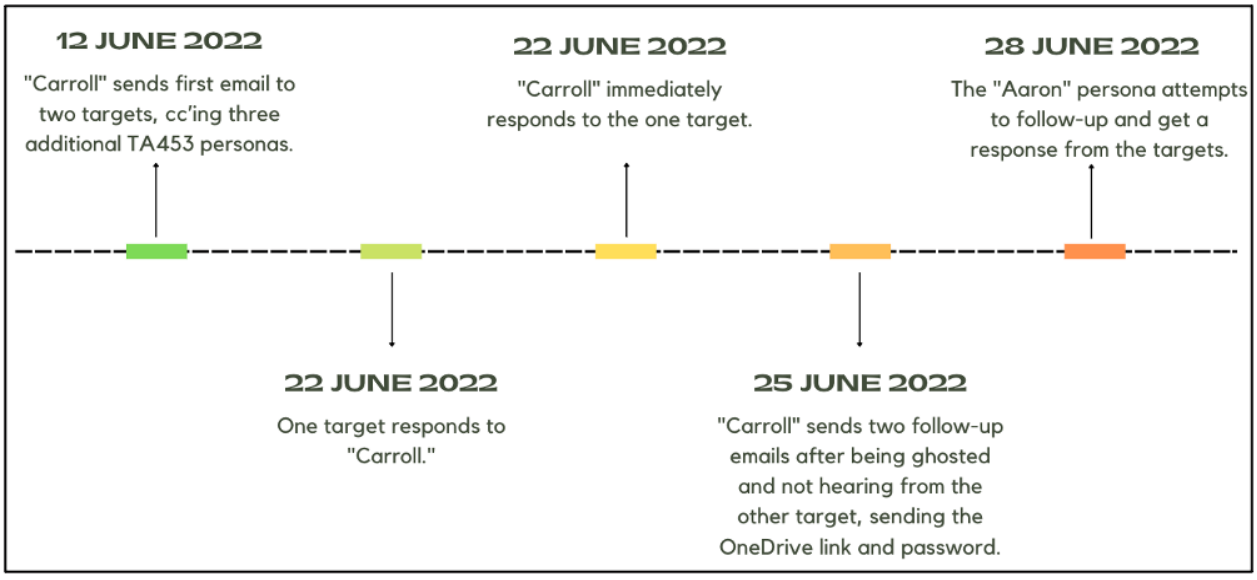
An example shared in Proof point's report dates to June 2022, with the sender masquerading as the Director of Research at FRPI and the email sent to the target and CC ing a Director of Global Attitudes Research at the PEW Research Center.



Phishing message sent to the target and a second fake persona *(Proofpoint)*

The next day, the impersonated PEW director answered the questions sent by the FRPI director, creating a false sense of an honest conversation that would be enticing for the target to join.

In a third MPI phishing attack launched by TA453 against two academics specializing in nuclear arms control, the threat actors CCed three personas, going for an even more intricate attack.



Timeline of the third MPI attack example *(Proofpoint)*

In all cases, the threat actors used personal email addresses (Gmail, Outlook, AOL, Hotmail) for both the senders and the CCed persons instead of addresses from the impersonated institutions, which is a clear sign of suspicious activity.

4. Facebook and Google

Between 2013 and 2015, Facebook and Google were tricked out of $100 million due to an extended phishing campaign. The phisher took advantage of the fact that both companies used Quanta, a Taiwan-based company, as a vendor. The attacker sent a series of

fake invoices to the company that impersonated Quanta, which both Facebook and Google paid.

5. Akasa Air- the country's newest airline has faced a data leak of its passenger database, the airline announced on Sunday. The airline said that it has self-reported the incident to CERT-In- nodal agency tasked to deal with incidents of cyber security threats like hacking and phishing.

CONCLUSION AND SUGGESTIONS

Indian Computer Emergency Response Team (CERT-In) which has been mandated all the organisation concerned to track and monitor cyber security incidents in India has observed that the total number of known phishing incidents has gone up from 280 in 2020 to 523 in 2021 and so on presently.

After looking at the whole scenario of past, present types of attacks, the conclusion could be very tricky & difficult to conclude. After all remediating these attacks are almost impossible. As these kind of Digital exploits are like CAT & RAT race, no real Permanent Solution or tools to mitigate the risks. Probably being vigilant or be updated with latest trends of criminal activities is preventive measure. An IT security norm says "TRUST but VERIFY" could be better solution as of Now.

REFERENCE

[1] Roseline Oluwaseun Ogundokun, Micheal Olaolu Arowolo, Robertas Damaševičius, and Sanjay Misra

[2] Phishing Detection in Blockchain Transaction Networks Using Ensemble Learning., *Telecom* 2023, *4*(2), 279-297; https://doi.org/ 10.3390/ telecom4020017

[3] Saad M. Darwish, Dheyauldeen A. Farhan,and Adel A. Elzoghabi

[4] Building an Effective Classifier for Phishing Web Pages Detection: A Quantum-Inspired Biomimetic Paradigm Suitable for Big Data Analytics of Cyber Attacks by https://www.mdpi.com/2313-7673/8/2/197

[5] Singh, C. Phishing website detection based on machine learning: A survey. In Proceedings of the IEEE International Conference on Advanced Computing and Communication Systems, Coimbatore, India, 6–7 March 2020; pp. 398–404. [Google Scholar]

[6] Whittaker, C.; Ryner, B.; Nazif, M. Large-scale automatic classification of phishing pages. In Proceedings of the Annual International Conference on Machine Learning, Montreal, QC, Canada, 21–24 June 2010; pp. 1–14. [Google Scholar]

[7] Benavides, E.; Fuertes, W.; Sanchez, S.; Sanchez, M. Classification of phishing attack solutions by employing deep learning techniques: A systematic literature review. In Developments and Advances in Defense and Security, Smart Innovation, Systems and Technologies; Springer: Singapore, 2020; Volume 152, pp. 51–64. [Google Scholar]

[8] Basit, A.; Zafar, M.; Liu, X.; Javed, A.R.; Jalil, Z.; Kifayat, K. A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommun. Syst. 2021, 76, 139–154. [Google Scholar] [CrossRef]

[9] Jain, A.K.; Gupta, B.B. A survey of phishing attack techniques, defense mechanisms, and open research challenges. Enterp. Inf. Syst. 2021, 16, 527–565. [Google Scholar] [CrossRef]

[10] Khonji, M.; Iraqi, Y.; Jones, A. Phishing detection: A literature survey. IEEE Commun. Surv. Tutor. 2013, 15, 2091–2121. [Google Scholar] [CrossRef]

[11] Azeez, N.A.; Salaudeen, B.B.; Misra, S.; Damaševičius, R.; Maskeliūnas, R. Identifying phishing attacks in communication networks using URL consistency features. Int. J. Electron. Secur. Digit. Forensics 2020, 12, 200–213. [Google Scholar] [CrossRef]

[12] Jain, A.; Parashar, S.; Katare, P.; Sharma, I. Phishskape: A content based approach to escape phishing attacks. Procedia Comput. Sci. 2020, 171, 1102–1109. [Google Scholar] [CrossRef]

[13] Alkawaz, M.; Steven, S.; Hajamydeen, A. Detecting phishing website using machine learning. In Proceedings of the IEEE International Colloquium on Signal Processing & Its Applications, Langkawi, Malaysia, 28–29 February 2020; pp. 111–114. [Google Scholar]

[14] Tupsamudre, H.; Singh, A.; Lodha, S. Everything is in the name—A URL based approach for phishing detection. In Proceedings of the International Symposium on Cyber Security

Cryptography and Machine Learning, Be'er Sheva, Israel, 27–28 June 2019; Springer: Cham, Switerland; pp. 231–248. [Google Scholar]

[15] Day. (2021). Phishing attacks in india: issues and challenges. Sambodhi (ugc care journal), 44(1), 27–31.

[16] Joshi, M. C. A. (2019, May 23). Phishing in India is becoming innovative. India forensic. https:// indiaforensic.com/understanding phishing-india/

[17] Shubhangi Taneja; Ruchi Pal; Shiwangi Vishwakarma; Rakesh Kumar. "A Case Study on Cyber bullying". *International Research*

[18] *Journal on Advanced Science Hub*, 2, 7, 2020, 29-31. doi: 10.47392/irjash.2020.60

[19] Zuhair, H.; Selamat, A.; Salleh, M. Feature selection for phishing detection: A review of research. Int. J. Intell. Syst. Technol. Appl. 2016, 15, 147–162. [Google Scholar] [CrossRef]