PHISHING ATTACKS

No, not a bunch of fishes coming on you!!!

IF NOT FISHES, WHAT EXACTLY IS PHISING ??

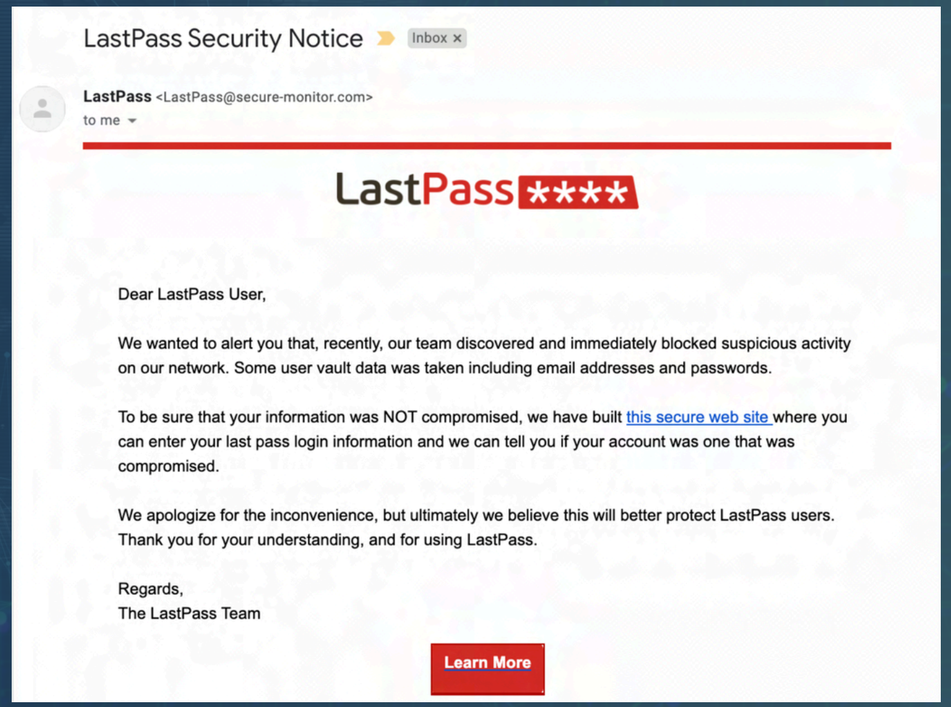
- Phising: The fraudulent practice of sending emails or other messages purporting to be from reputable companies
- Phising Attack: common type of cyber-attack that targets individuals through email, text messages, phone calls, and other forms of communication
- phishing uses psychological manipulation and deception whereby threat actors masquerade as reputable entities to mislead users into performing specific actions

- Most generic phishing attempts contain spelling and grammar errors or feature awkward wording/phrasing.

- Deceptive Content: Links, attachments, or forms that appear legitimate but lead to malicious sites or malware.

- Targeted or Broad: Phishing can target specific individuals (spear phishing) or cast a wide net (bulk phishing).

A phishing website URL often uses subtle misspellings, unusual characters, or redirects to trick users into thinking it's a legitimate site, like http://www.confirme-paypal.com/ instead of https://www.paypal.com.



THE NEED...?...

Malware Distribution

One of the most common known problems or “attacks” for the commoners is Virus and similar to it is malware . So, the commom reason for this phising attack is ingesting any malware to the system. The attackers attach some malicious links or attchments that lead to malware installation in the system.

Financial Gain

One more reason that falls under the obvious reasons is money, who dosent want money? Phising attacks are one of the most easy and common way to gain ransom for the professionals.

Identity Theft

Personal Information like unique government IDs and other important information are collected throug attacks and then used to create fraud accounts

WAYS OF ATTACK (TYPES)

1. Email Phising
2. Spear Phishing
3. Whaling
4. Voice Phishing
5. HTTPS Phishing
6. Clone Phising
7. SMS Phishing
8. Social Media Phishing
9. Website Spoofing

Quick Check: What Did You Learn?

Q1: Which of the following is NOT a type of phishing?
A) Spear Phishing
B) Whale Phishing
C) Sharking
D) Vishing

Q2: Phishing attacks commonly rely on:
A) Strong encryption
B) Social engineering
C) Physical access
D) Firewall breaches

Complete the lesson to know the right answer

1. What it is:

A type in which hackers will copy the exact email format from a legitimate company which are used to trick the recipients into revealing sensitive information and include a malicious link, document, or image file that can trick the user into "confirming" their personal information or automatically download malicious code.

2. Aim:

Gaining personal and sensitive information like login credentials, bank information, important id numbers (Ex. Credit card, Aadhar Card, etc)

3. How:

Achieved by sending emails that appear to be from trusted sources, often containing malicious links or attachments that lead to fake websites or malware.

4. Traits:

These common traits often tell the phishing mail apart from the legitmate ones.

- Non-domain email addresses:

Fraudulent email addresses often use third-party providers or variations of legitimate email domains.Public domains (like @gmail.com) or variants of the authentic domain with extra characters or misspellings may be used in phishing emails.

- Requests for personal information:

Personal Information needed for any important work are never communicated through emails.Phishing emails may ask you to verify your information in order to prevent account termination or other problems.

- Spelling & grammar mistakes:

Phishing emails frequently have poor wording, grammatical faults, and spelling issues.

- File attachments:

Although this is not an obvious sign as emails usually include docs and attachments but opening any file attachments from unknown senders, which are not legitmate can lead to virus or malware download in the system. (especially if they include .exe, .zip, and .scr extensions)

- Urgent problem:

In order to get recipients to act without thinking, phishing emails frequently attempt to instill a sense of urgency or panic. They may threaten to suspend your account or say there is an issue with your payment details or account.

Quick Check: Spot the Red Flag!

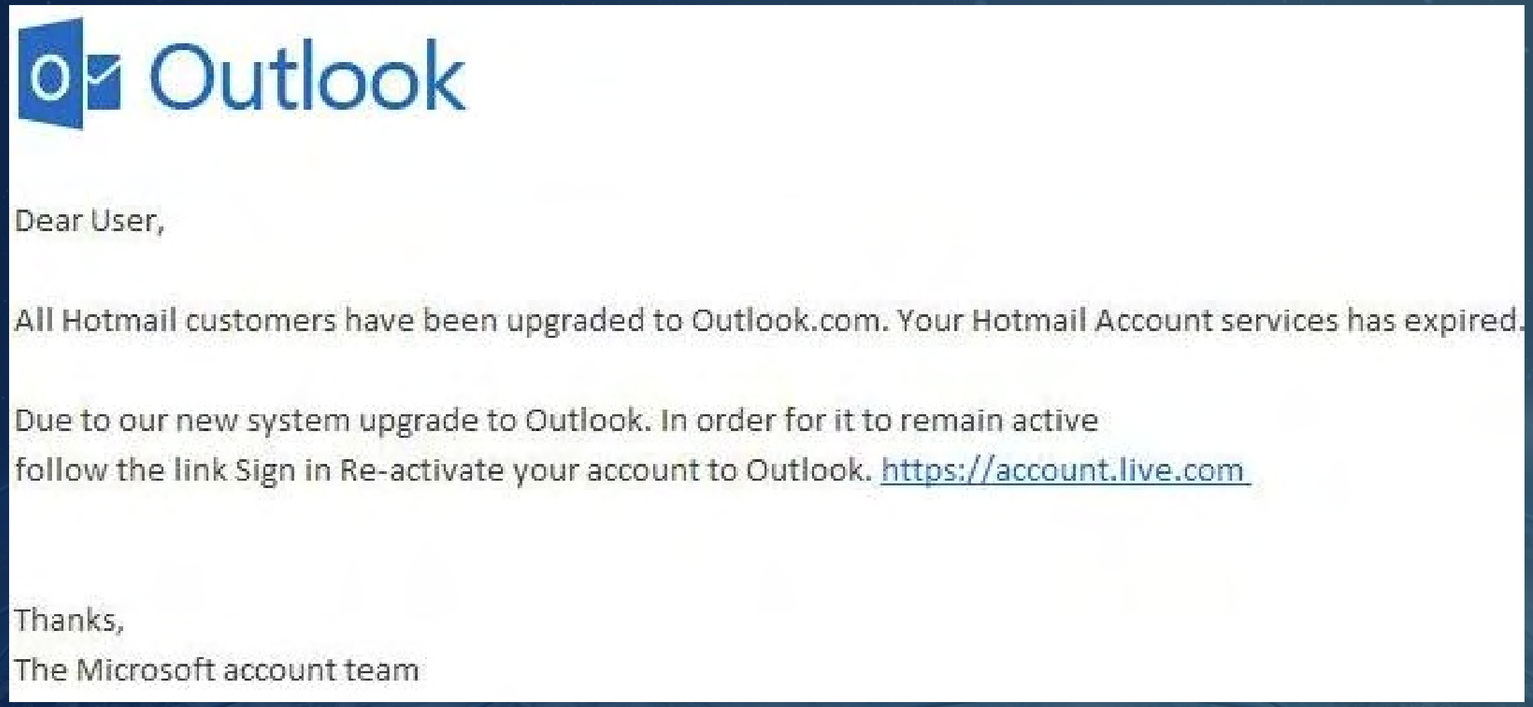
Q3: You receive an email from “support@micr0soft.com” asking you to reset your password. What’s suspicious here?

- A) The sender’s domain spelling
- B) Asking for password reset
- C) No issue, it seems legit
- D) The email has an attachment

Q4 (True/False): Public domain emails like @gmail.com can be used in legitimate corporate communications.

Complete the lesson to know the right answer

EXAMPLE SCENERIO:



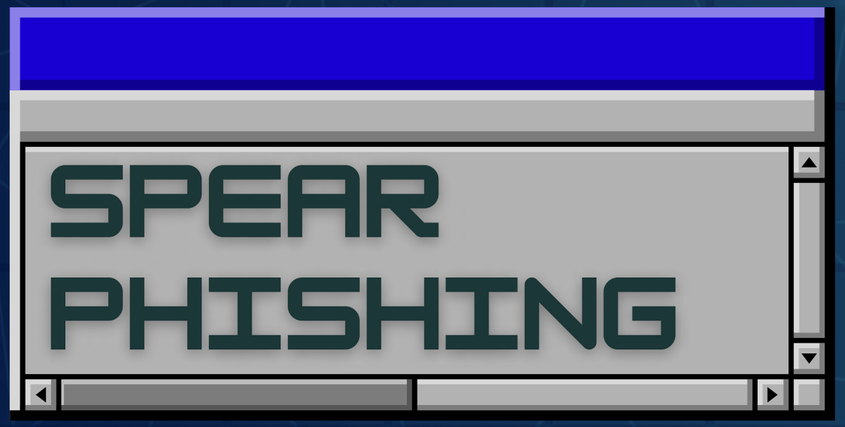
Outlook

Dear User,

All Hotmail customers have been upgraded to Outlook.com. Your Hotmail Account services has expired.

Due to our new system upgrade to Outlook. In order for it to remain active
follow the link Sign in Re-activate your account to Outlook. https://account.live.com

Thanks,
The Microsoft account team



1. What it is:

A type that is similar to the previous type but spear phishing targets specific organizations or individuals unlike a broad aproach like email phishing.

2. Aim:

Gaining sensitive information of the targeted organization or individual. And this is mostly for financial gain or obtaining very valuable data.

3. How:

There are essentially five steps to successful spear phishing scams. These are:

1. Defining the goals of the attack
2. Choosing the target(s) through preliminary research
3. Identifying a shortlist of targets and researching them thoroughly
- 4. Creating the spear phishing email using the information gathered and social engineering techniques.

4. Traits:

These common traits often tell the phishing mail apart from the legitmate ones.

- Specific mentions of personal details:

Fraudsters might attempt to validate their credibility by sharing irrelevant details about you. Clear efforts to earn your trust should be regarded with caution.

- Unusual requests:

Personal Information needed for any important work are never communicated through emails.Phishing emails may ask you to verify your information in order to prevent account termination or other problems.

- Pretexting:

Fabricating a realistic story or situation that the target recognizes and can relate to. For example, a spear phisher might pose as an IT worker and tell the target it is time for a regularly scheduled password update.

- Urgent problem:

In order to get recipients to act without thinking, phishing emails frequently attempt to instill a sense of urgency or panic. They may threaten to suspend your account or say there is an issue with your payment details or account.

EXAMPLE SCENERIO:

The following is an example of a phishing email:

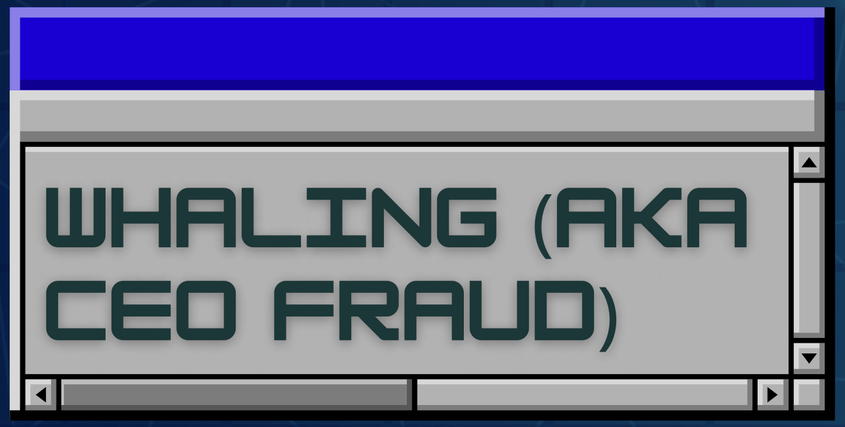
Subject Line: Change of Bank Details

Body:

Dear [name of your employee],
Please find attached a copy of the most recent invoice, dated [last day of the month]. Please note that we recently switched banking providers from [name of their real bank] to [name of new bank] and have included the new account details on this invoice.
We appreciate your swift payment and have recently implemented an early payment discount for all of our partners. If paid within 24 hours of receiving the invoice, we will automatically deduct 10% from the bill.

Many thanks,
[name of real contact at Supplier].

- This is a common instance of an assailant employing social engineering methods. This scammer has conducted their investigation. They are aware of your employee's name, the actual bank associated with the merchant, and the name of your usual contact at the supplying firm.
- The criminal employs incentives to tempt the payee to make the payment right away, saving them the trouble of checking the bank information. This is a typical strategy for putting victims under a lot of pressure and stealing



1. What it is:

Whaling, like spear phishing, also focuses on individuals and organizations but on an upper level. Meaning , they target high level comapnies and execitives for example CEO's , CFO's, etc

2. Aim:

Gaining sensitive information of the targeted organization or individual. And this is mostly for financial gain or obtaining very valuable data.

3. How:

- Relying on OSINT, plenty of research into the company's business practices, and even a deep dive into social media accounts.
- Spoofing and Impersonation: faking the emails and drafting a trust worthy seeming draft to gain information.

4. Traits:

These common traits often tell the phishing mail apart from the legitmate ones.

- Use of personal email :

Higher level executives never use personal emails for communication of any work related stuff, so any kind of personal mail id's used for such communication should v

- Use of publicly available information:

Attackers often leverage information from social media and other online sources to personalize their attacks and make them more believable.

- New contact requests :

An email from an organization or partner who has never been in touch with you for business needs could be a phishing attempt. Check your communication with the person in charge of the account through the appropriate channels.

EXAMPLE SCENERIO:

Snapchat:

In February 2016, Snapchat experienced a whaling phishing attack. An individual posing as CEO Evan Spiegel sent an email to an HR employee, requesting payroll data for both current and former employees, including stock options and W-2s.

Ubiquiti Networks:

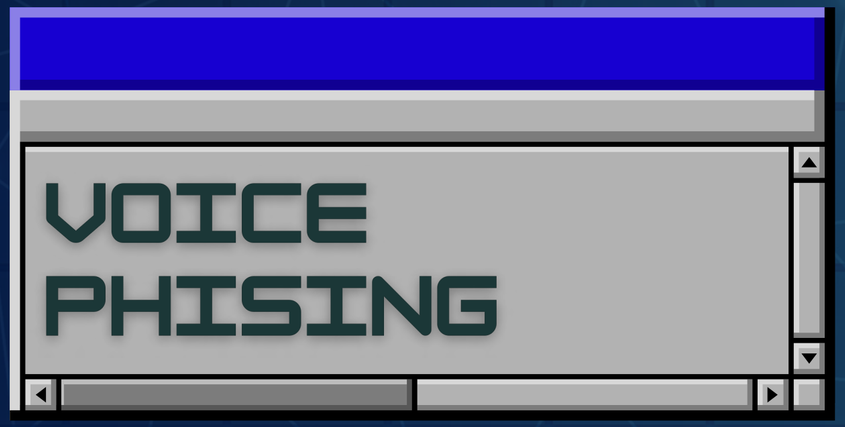
In 2015, Ubiquiti Networks fell victim to a sophisticated CEO scam. Fraudsters successfully convinced the finance department of one of its Hong Kong-based subsidiaries to transfer $46.7 million to unrelated overseas accounts. Although the company managed to recover $14.9 million, the damage to its reputation was irreversible.

Quick Check: Who's the Target?

Q5: Whaling attacks typically target:

- A) College students
- B) IT Helpdesk staff
- C) C-Level executives
- D) Freelancers

Complete the lesson to know the right answer



1. What it is:

Vishing, short for voice phishing, refers to fraudulent phone calls or voice messages designed to trick victims into providing sensitive information, like login credentials, credit card numbers, or bank details. These details can then be exploited for criminal activities such as fraud, identity theft, or financial theft.

2. Aim:

Vishing is mostly used to obtain sensitive, private information from people or companies without authorization. The victim's financial loss is the main objective of a vishing attack.

3. How:

Attackers manipulate telecommunication systems to falsify the caller ID information, making it appear as though the call is coming from a trusted source, such as a bank, government agency, or even a colleague.

Quick Check: Would You Fall for This?

Q6: You get a call saying your tax documents have mismatches. The caller asks for your Aadhaar number and OTP. What should you do?

- A) Provide it to avoid penalty
- B) Hang up and verify with the official agency
- C) Call them back later
- D) Share partial info only

Complete the lesson to know the right answer

4. Traits:

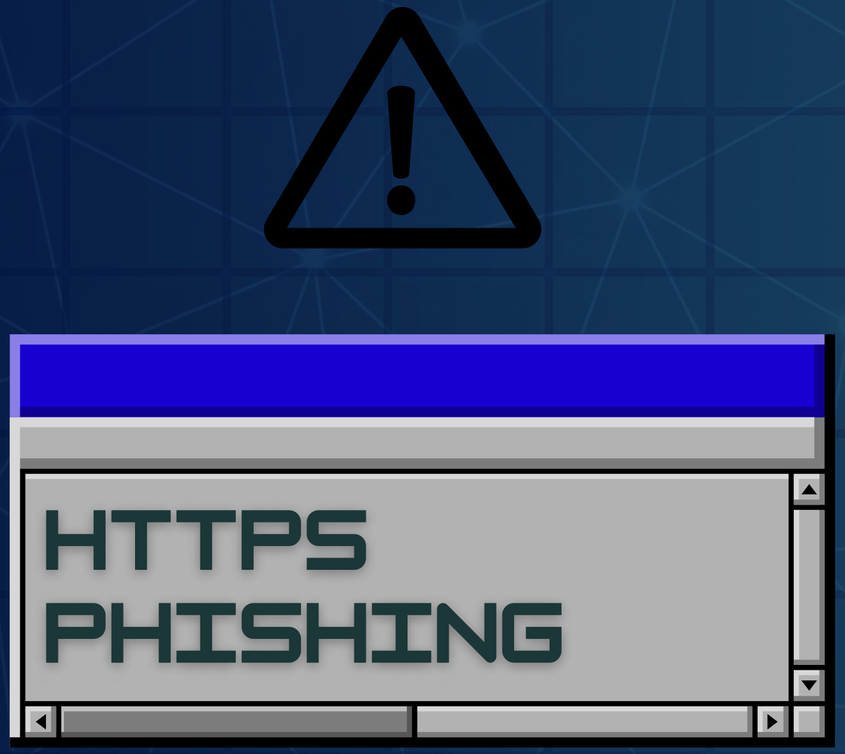
These common traits/tactics to identify vishing calls:

- Vehicle qualifies for extended warranty
- Guaranteed returns on investment opportunities
- Pretending to be from a bank and claiming the victim's account has been compromised, requiring immediate action to "fix" it.
- Scammers may pose as tech support personnel from large companies like Amazon, Microsoft, or AT&T.

Example Scenerio:

Victim: Hello?
Scammer: Good afternoon, ma'am. I'm calling from the Income Tax Department. There seems to be a mismatch in your PAN details and we need to verify it immediately to avoid penalties.
Victim: Oh... okay. What do you need?
Scammer: Just confirm your PAN number and your Aadhaar-linked mobile number. You'll get an OTP — read that out so I can link it in the system.
Victim: Alright... My PAN is ABCDE1234F and the OTP is 675849.
Scammer: Thank you, ma'am. We'll resolve this.

Scammer uses info to access financial services or steal identity



1. What it is:

HTTPS phishing is a URL based attack where attackers impersonate a trusted website that uses the HTTPS protocol to deceive victims into providing sensitive information.

2. Aim:

The aim is similar to others, to obtain important or sensitive information. By using the fake HTTPS encryption tag, the work of attackers become easier to acheive the aim.

3. How:

- Domain Spoofing/Typosquatting:
- Attackers register domains that closely resemble legitimate websites (e.g., "amaz0n.com" instead of "amazon.com") or use slightly misspelled versions.
- Obtaining SSL Certificates:
- They acquire SSL certificates (often Domain Validated (DV) certificates which are easy to obtain) for these fake domains to display the HTTPS padlock and reassure users.

4. Traits:

These common traits often tell the phishing websites apart from the legitmate ones.

- Assess the content within a site:

Simple spelling mistakes, broken English, grammatical errors, or low-resolution images should act as a red flag that you are on a phishing site and should leave immediately.

- . Check who owns the website:

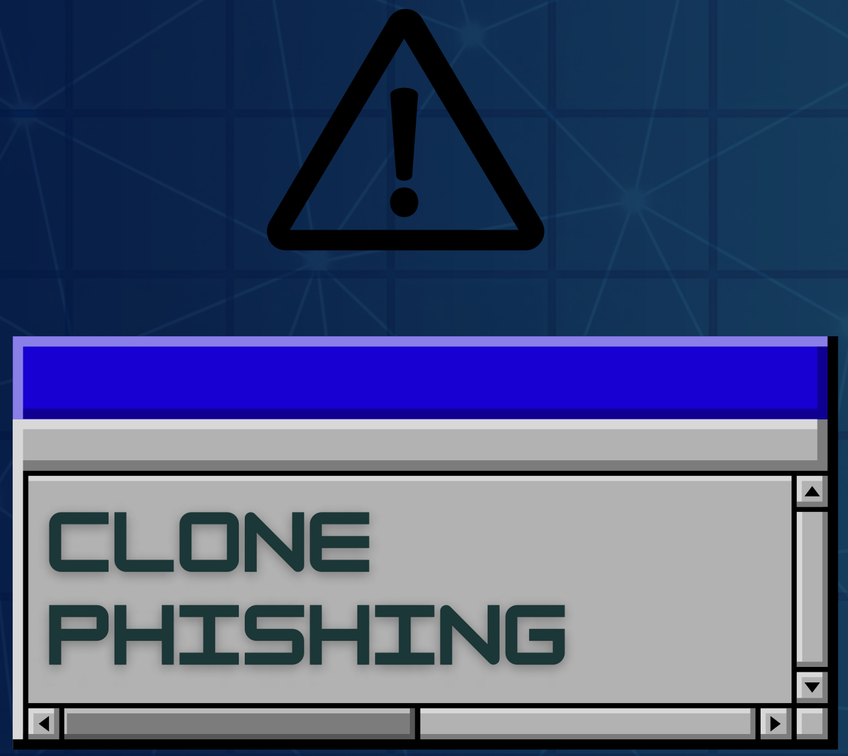
If the website has been up and running for less than a year, or if you believe you are on the website of a well-known company, but the domain name is registered to a person in another nation, you should be suspicious. It is more likely to be a phishing attack if this is the case.

- 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.

- URL misspellings:

Any misspellings in the email domain are an immediate telltale sign that the email is fake.



1. What it is:

The attack is carried out by copying an email message commonly sent by a known business entity and sending a targeted recipient a copy of the legitimate email

2. Aim:

The aim is similar to others, to obtain important or sensitive information. By doing this , they attach malicious links or ransomwares to the email.

3. How:

1. Email Interception
2. Cloning the Email:
The hacker makes an almost flawless duplicate of the original email. Replicating the sender's address, subject line, body, and any attachments is part of this.
3. Malicious Modification:Substituting malicious URLs or attachments for the original, authentic ones is a key step
4. Resending the Email

4. Traits:

These common traits often tell the phishing mail apart from the legitmate ones.

- 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

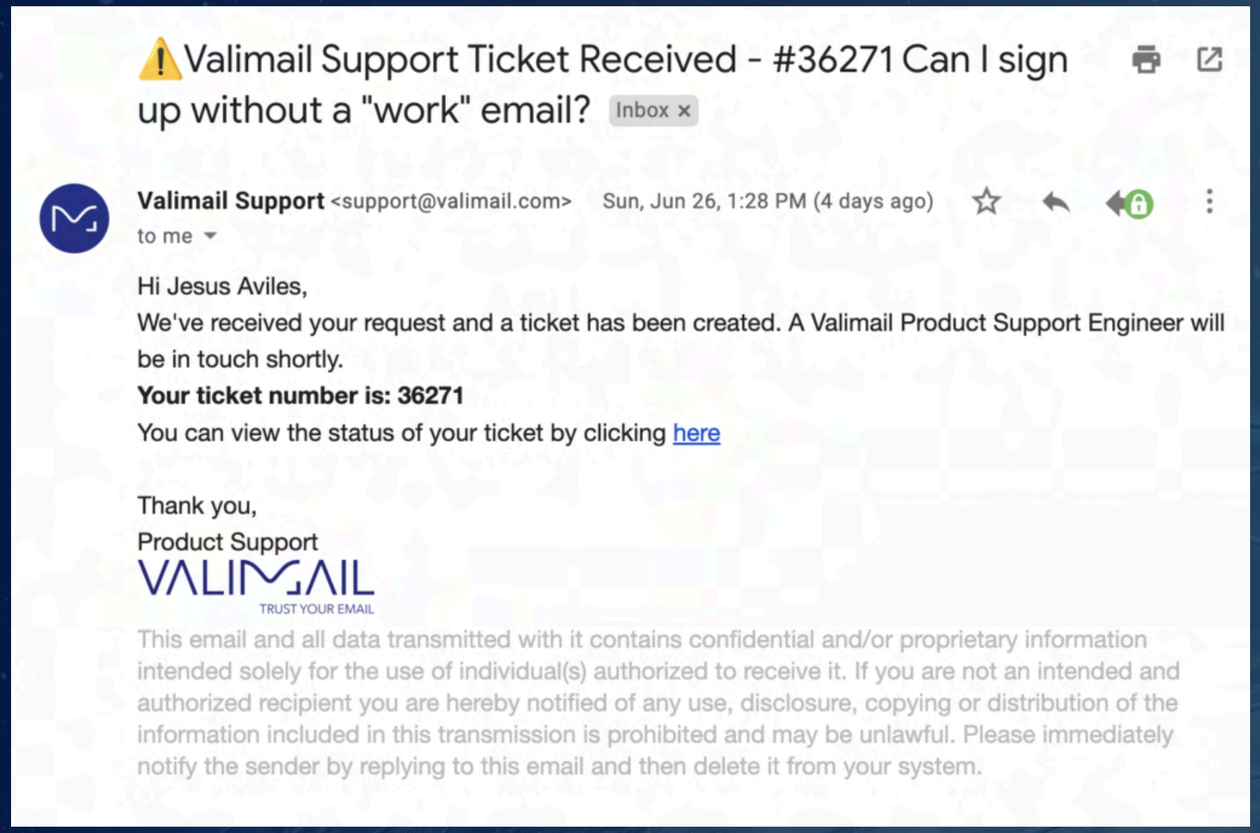
- Mismatched hyperlinks:

Mismatch between hyperlink text and the domain the link points to.

- Spoofed hyperlinks :

Even if you think the email is authentic, you should always hover over any link to see the entire URL before clicking on it since hackers can hide the actual hyperlink address with formatting or radio buttons.

EXAMPLE SCENERIO:



⚠️Valimail Support Ticket Received - #36271 Can I sign up without a "work" email? Inbox ×

Valimail Support <support@valimail.com> Sun, Jun 26, 1:28 PM (4 days ago)

to me

Hi Jesus Aviles,

We've received your request and a ticket has been created. A Valimail Product Support Engineer will be in touch shortly.

Your ticket number is: 36271

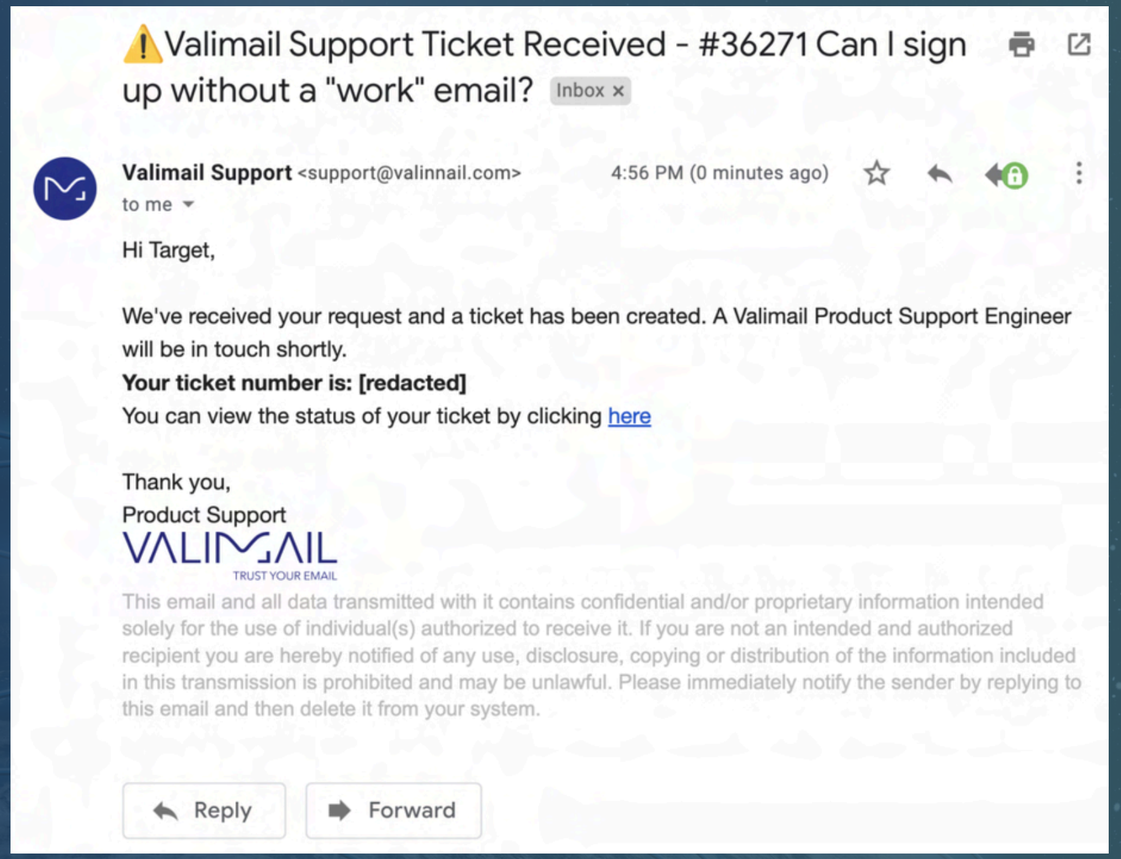
You can view the status of your ticket by clicking here

Thank you,

Product Support

VALIMAIL TRUST YOUR EMAIL

Original Email



⚠️Valimail Support Ticket Received - #36271 Can I sign up without a "work" email? Inbox ×

Valimail Support <support@valinnail.com> 4:56 PM (0 minutes ago)

to me

Hi Target,

We've received your request and a ticket has been created. A Valimail Product Support Engineer will be in touch shortly.

Your ticket number is: [redacted]

You can view the status of your ticket by clicking here

Thank you,

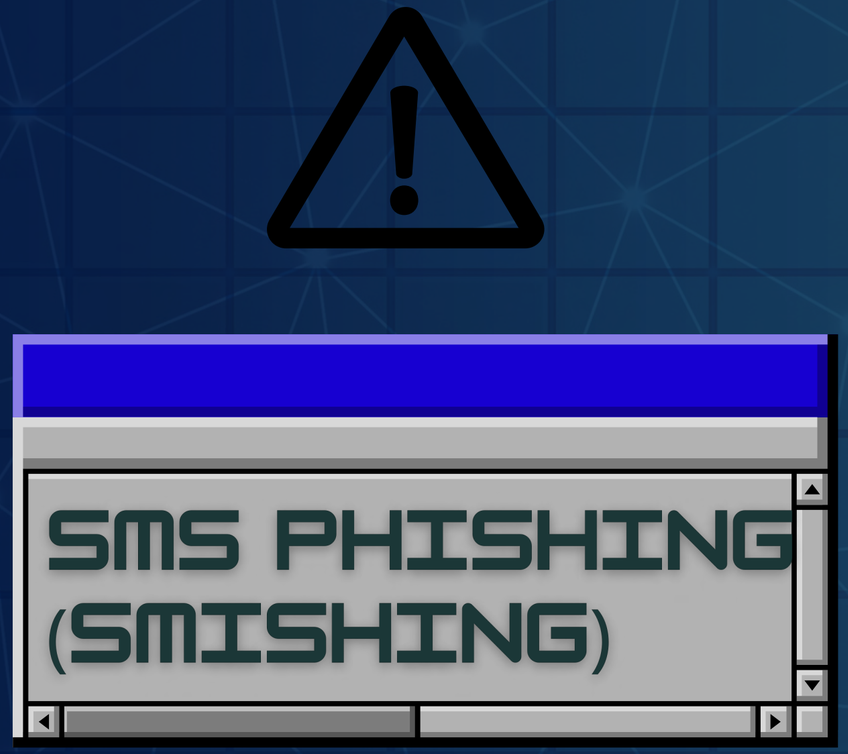
Product Support

VALIMAIL TRUST YOUR EMAIL

Reply Forward

Cloned Email

Would you notice that the domain has a double ‘n’ instead of an ‘m’? This email doesn’t end up in spam, so you only have two clues in this case: the domain in the visible From: address is wrong, and the hyperlink points to a phishing domain.



1. What it is:

SMS phishing, or "smishing," is similar to vishing, but instead of calling, scammers will send SMS text messages with links or attachments.

2. Aim:

uses fake mobile text messages to trick people into downloading malware, sharing sensitive information or sending money to cybercriminals

3. How:

1. Crafting the Message: Scammers create messages that look like official correspondence, frequently alerting victims to account difficulties, missed deliveries, or legal issues. Often, these communications contain a phone number to contact or a link to a fake website.
2. Spreading the Message
3. Clicking the Link or Calling the Number
4. Revealing Information:On the fake website or through the phone call, the recipient is asked to enter personal information like login credentials, credit card details, or other sensitive data.

4. Traits:

These common traits to tell the phishing SMS apart from legit ones:

- Unfamiliar greetings:

At times, a signoff or greeting's tone can be an indication that something is off. Observe a person who always begins communications with "Hello!" but then substitutes "Dear friend" instead.

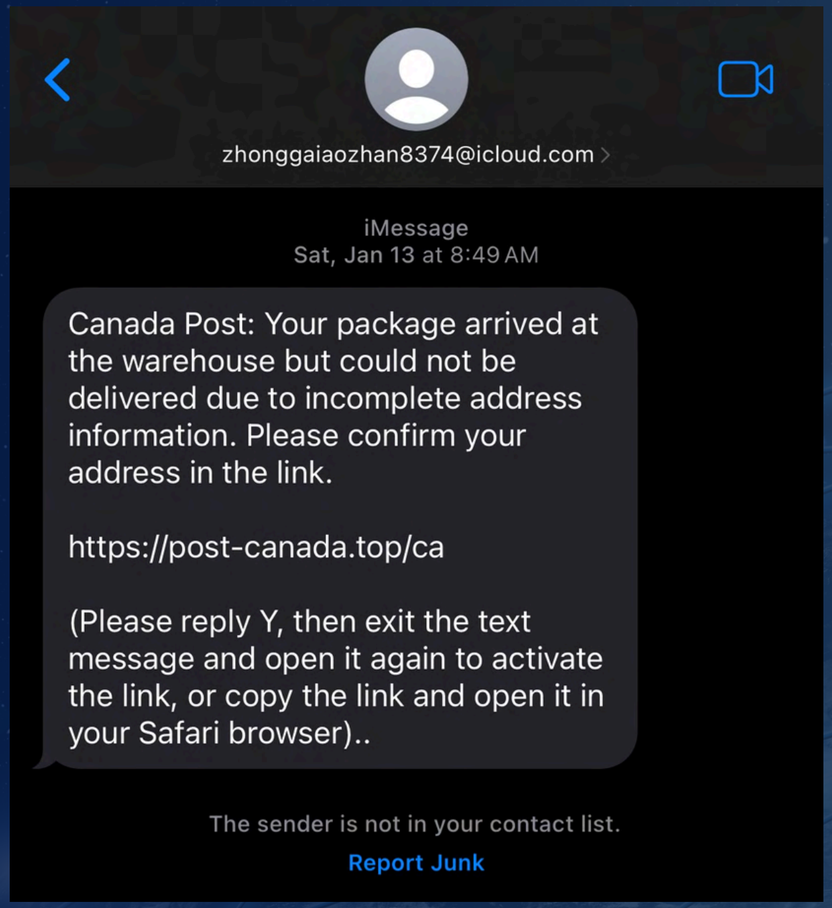
- Unknown numbers:

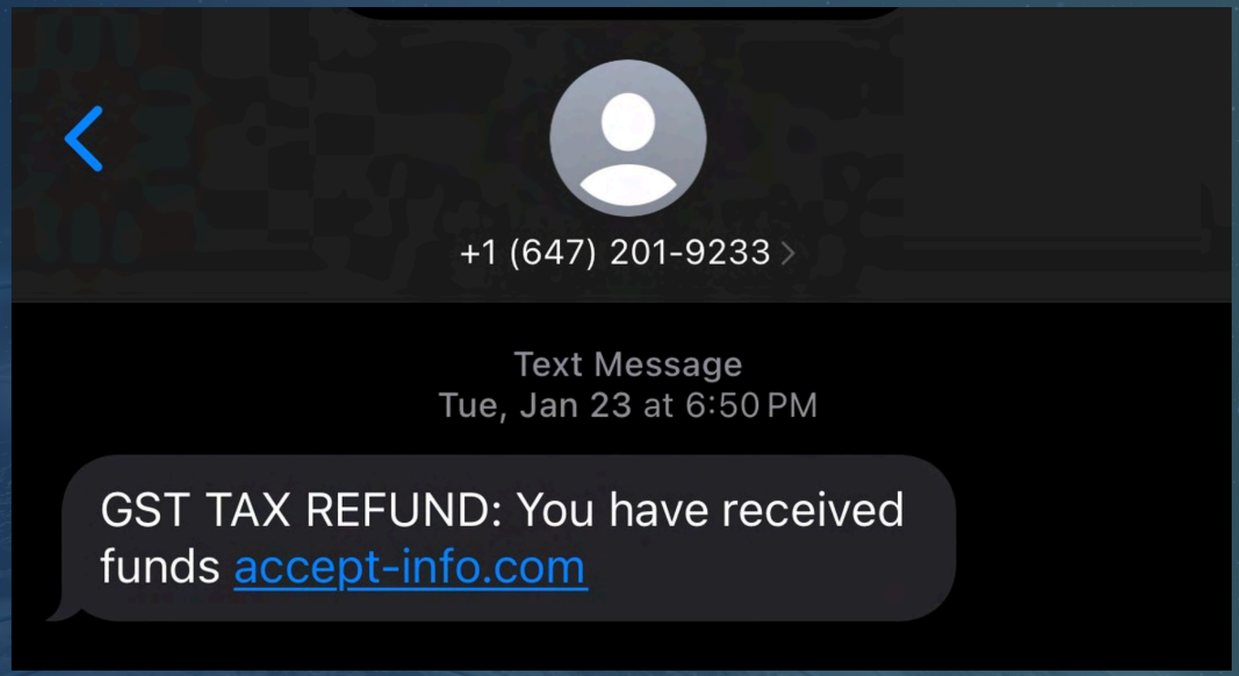
Getting a request for information over text messaging should be a red flag.

- 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..

EXAMPLE SCENERIO:





1. What it is:

It is just like sms phishing but instead of normal sms, attackers use social media as a platform to send messages.

2. Aim:

To capture personal information and sometimes also gain social media platform credentials through fake links.

3. How:

1,Reconnaissance and Profile Creation: Scammers create fake profiles or pages that mimic legitimate accounts or brands, using logos, language, and even similar profile pictures.

2. Crafting the Deceptive Message: Attackers research potential victims on social media, gathering information like their name, job title, interests, and connections and then craft a fake message accordingly.

4. Traits:

These common traits to tell the phishing message apart from legit ones:

- Offers or online discounts
- Friend requests
- 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.

Quick Check: Real or Phish?

Q7 (True/False): A friend request from someone with no profile pic and 1 post is likely a phishing attempt.

Q8: Which is a sign of smishing?

- A) Email from HR
- B) Message with shortened link about a delivery
- C) New browser extension
- D) Payment request through invoice

Complete the lesson to know the right answer

1. What it is:

The practice of cybercriminals creating a website that closely mimics a reputable brand and a domain that is almost identical to that company's web domain is known as website spoofing.

2. Aim:

The goal of website spoofing is to lure a brand's customers, suppliers, partners and employees to a fraudulent website and convince them to share sensitive information like login credentials, Social Security numbers, credit card information or bank account numbers.

3. How:

In order to make these websites look authentic, attackers frequently use social engineering strategies, such as posing as reliable organizations (such as banks or online services) in emails, texts, or even pop-up advertisements.

4. Traits:

These common traits to tell the phishingwebsite apart from legit ones:

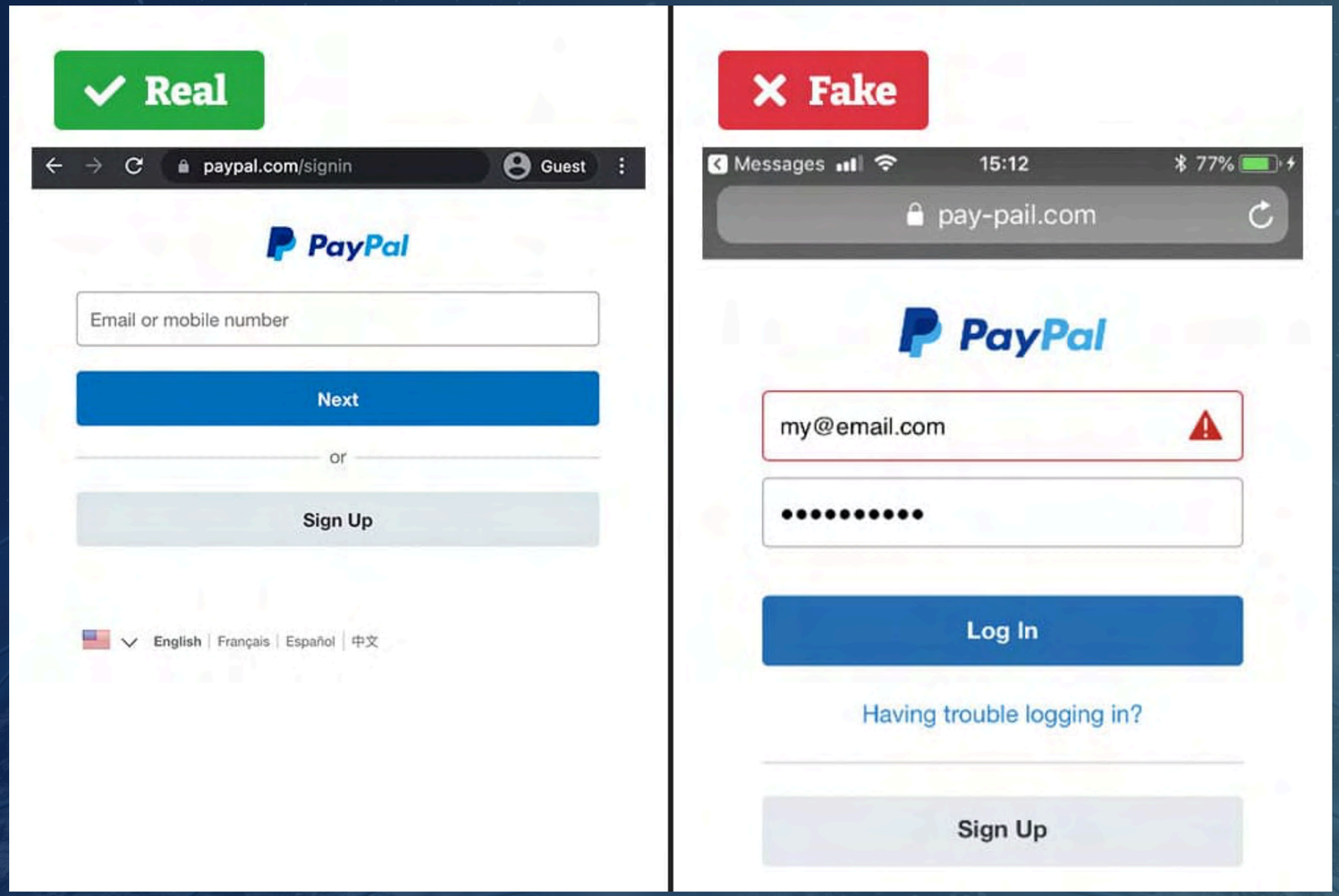
- URL misspellings:

In order to make these websites look authentic, attackers frequently use social engineering strategies, such as posing as reliable organizations (such as banks or online services) in emails, texts, or even pop-up advertisements.

- Visual Similarity:

Spoofed websites meticulously replicate the appearance of the target website, including its logo, color scheme, and overall design.

EXAMPLE SCENERIO:



HOW TO AVOID THE ATTACKS?

Now that the attcks are well known , it would be unfair not to know the methods of prevention for the same.

Since most of the traits include very similar social engeneering tactics , lets learn how to prevent them with these:

1. Email Phishing

2. Whaling

3. SMS Phishing

4, Website Spoofing

1 Email Phishing :

1. Never provide personal financial information
2. Never click on the link provided in an email you believe is fraudulent
3. Protect your computer by using security software
4. Protect your accounts by using multi-factor authentication.
5. Use an endpoint protection solution: Anti-malware tools scan devices to prevent, detect, and remove malware that enters the system through phishing attacks.

2. Whaling:

1. Incident Response Plan: Create a well-defined and tried-and-true incident response strategy in event of a security breach
2. Frequent Audits: To find and fix vulnerabilities, do risk assessments and security audits.
3. DMARC: Implement Domain-based Message Authentication, Reporting, and Conformance (DMARC) to authenticate emails and prevent domain spoofing.
4. Encryption: To prevent sensitive information from being intercepted or exploited in the event that an employee is tricked into sharing it, encrypt it while it's in transit and at rest.
5. Simulated Attacks: Run simulated phishing and whaling attacks to test employee awareness and

3. SMS Phishing :

1. Never provide a password or account recovery code via text
2. Download an anti-malware app
3. Never text back or call the associated number
4. verify the sender when you receive a suspicious text message

4. Website Spoofing:

1. Check for HTTPS: Ensure the site is secure by checking for "https://" in the URL
2. Try a password manager – software used to autofill login credentials does not work on spoofed websites
3. Use Anti-Phishing Browser Extensions
4. DMARC: Implement Domain-based Message Authentication, Reporting, and Conformance (DMARC) to authenticate emails and prevent domain spoofing.
5. Monitor the Web for Clones

Do people really fall for all this easily?!!!

Not just people, big establishes companies have faced phishing attacks....

Lets take a look

GOOGLE AND FACEBOOK PHISHING SCAM (2013-2015)

Impact

- Scammer stole over $100 million from Google and Facebook using fake invoices.

Execution:

- A Lithuanian man, Evaldas Rimasauskas, created a fake company mimicking a real supplier (Quanta Computer).
- He sent phishing emails with fake invoices, contracts, and letters.
- The companies wired large payments to fraudulent bank accounts.

Prevention:

- Implement strict vendor verification protocols.
- Use email authentication (DMARC, SPF, DKIM) to prevent spoofing.
- Enforce multi-level approvals for large financial transactions.

STARBUCKS PHISHING EMAIL CAMPAIGN (OCTOBER 2024)

Impact

- Over 900 reports received by Action Fraud UK in just two weeks.
- Users tricked into sharing personal and financial details.
- Some victims had systems infected with the ZeuS banking Trojan, leading to credential theft and financial compromise.

Execution:

- Victims received phishing emails pretending to be from Starbucks.
- Subject: Free “Starbucks Coffee Lovers Box” or a “Gift from a Friend”.
- Emails contained links or attachments:
- Some led to fake sites requesting sensitive info (card numbers, passwords).
- Others embedded the ZeuS Trojan, which:
    - Installed silently
    - Captured banking credentials
    - Deployed rootkits to hide its presence

Prevention:

- Check the email domain carefully; Starbucks will never use random URLs
- Monitor brand impersonation with domain spoofing detection tools..
- Use email authentication protocols (SPF, DKIM, DMARC) to reduce spoofing.
- Enable two-factor authentication on banking and email accounts.

Quick Check: Phishing Awareness Final Challenge

Q9: Which of the following is the best prevention method?

- A) Clicking only colorful links
- B) Replying quickly to suspicious emails
- C) Using Multi-Factor Authentication (MFA)
- D) Avoiding the internet altogether

Q10 (True/False): Legitimate companies will never ask for your password via email or SMS.

Lesson Completed!!

Phishing Awareness Quiz – Answer Key

1. C — Sharking
2. B — Social engineering
3. A — The sender’s domain spelling
4. False
5. C — C-Level executives
6. B — Hang up and verify with the official agency
7. True
8. B — Message with shortened link about a delivery
9. C — Using Multi-Factor Authentication (MFA)
10. True

Thank You

"Think before you click — one wrong move can cost everything."