

Phishing Awareness Training

Sanil Gajbhiye

Importance of this Training

Cybercrime has become a powerful tool for stealing information. The anonymity and convenience of the internet has enabled criminals to launch highly targeted attacks with very little effort. The most successful and dangerous of all the cyber-attacks is phishing. Security vendor research found over 94% of detected malware is delivered via email, which makes phishing the #1 cyber threat to organizations. With black market demand for information at an all-time high, many organizations are experiencing more phishing attacks. The attacks are becoming more sophisticated, targeted, and increasingly difficult to identify. The information in this training will increase your ability to identify a phish.

Content

1. What is Phishing?
2. Types of Phishing Attacks
3. Results of Successful Phishing Attacks
4. Tips for Identifying a Phish
5. Phishing Email Examples
6. Best Practices

1. What is Phishing?

Phishing is an online scam where criminals send fraudulent email messages, appearing legitimate. The emails contain links or attachments that trick recipients into entering confidential information (e.g. account numbers, passwords) into fake websites, or they infect computers with malware.

2. Types of Phishing Attacks

- **Spear Phishing:** Spear Phishing is a targeted attempt to steal sensitive information, typically focusing on a specific individual or organization. These types of attack use personalized facts in order to appear legitimate. Generally, cybercriminals turn to social media and company sites to research their victims
- **Vishing:** Vishing is a phone scam, and has the most human interaction of all the phishing attacks. The fraudsters deceive victims by creating a sense of urgency to divulge sensitive information. Calls are often made through a spoofed ID, so it looks like a trustworthy source.
- **Whaling:** A Whaling attack is an attempt to steal sensitive information from senior-level management. Whaling emails contain highly personalized information about the target or organization, so they are more difficult to detect.
- **Smishing:** Smishing is a type of phishing that uses text (SMS) messages, as opposed to emails, to target victims. Fraudsters send a text message to an individual, usually calling for the individual to act.
- **Clone Phishing:** In Clone Phishing, a legitimate and previously delivered email message is used to create an identical email with malicious content. The cloned email will appear to come from the original sender and will contain malicious links or attachments.

3. Successful Attacks Result in...

- Identity Theft
- Loss of Sensitive Information (personal or professional)
- Loss of Intellectual Property
- Data Sold to Criminals and Third Parties
- Financial Losses •Unauthorized Transactions
- Exposed Usernames and Passwords
- Malware and Ransomware Installation
- Backdoors (access to systems) to Launch Future Attacks
- Reputational Damage

4. Tips for Identifying a Phishing Attempt

Look for Messages with:

- Mismatched URLs
- Poor Grammar or Spelling
- Unexpected Correspondence/Unsolicited Requests
- Urgent or Threatening Language

4.1 Mismatched URLs

Before clicking on any link, check the validity of the URL.

- Hover your cursor over the URL link—without clicking on it. The full hyperlinked address appears. If the URL does not match the address displayed, the message is most likely fraudulent.

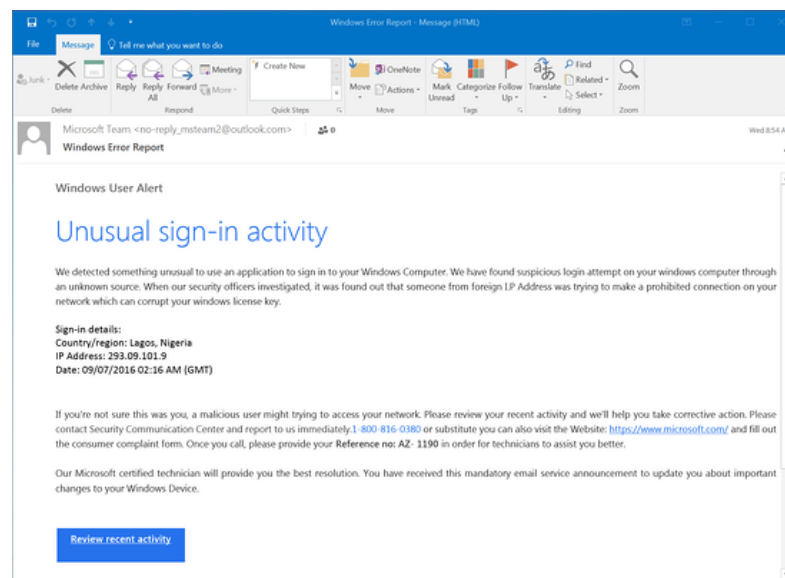


If you question the validity of the link,

- Call a known phone number (not one from the email) and ask about the message.
- Visit a trusted website (by manually typing the address in your browser).

4.2 **Poor Grammar and Spelling**

- Many phishing emails contain misspelled words and poor sentence structure. If you easily detected grammar-related errors in a message, it may be a phish. In the email example to the left
- No individual word is misspelled, but the message is full of grammatical errors that a native speaker wouldn't make, e.g., "We detected something unusual to use an application," and a string of missed words, such as "a malicious user might trying to access."
- Look for obvious errors! This is not to say an email with a mistake is a scam. Everyone makes typos from time to time.
- Another strong indication of phishing scams is a misspelled or incorrect domain name.



- Anyone can buy a domain name, and although every domain name must be unique, there are plenty of ways to create addresses that are similar to the domain being spoofed.
- For example, a hacker bought the domain 'gimletrnedia.com' (that's r-n-e-d-i-a, rather than m-e-d-i-a). The scam was so successful, it even tricked Gimlet Media's CEO.

4.3 Unexpected Correspondence/ Unsolicited Requests

Reputable companies do not randomly send emails asking for personal information—such as account numbers, passwords, or pins—nor will reputable companies try to invoke some type of urgency to receive an immediate reply.

If you receive an email,

- Informing you that you have won a competition that you did not enter, or
- Requesting that you click on a link to receive website content you did not request, it is highly likely a phishing email.



In the example, the phisher claims to be sending an attached invoice. The attachment in this message may look fine; however, it contains malware.

When the recipients open the attachment, they will soon realize the invoice is not an invoice for them. Clicking the attachment releases malware, which could perform any number of nefarious activities on the victims' computers.

Never open an attachment unless you are confident that the message is from a legitimate party.

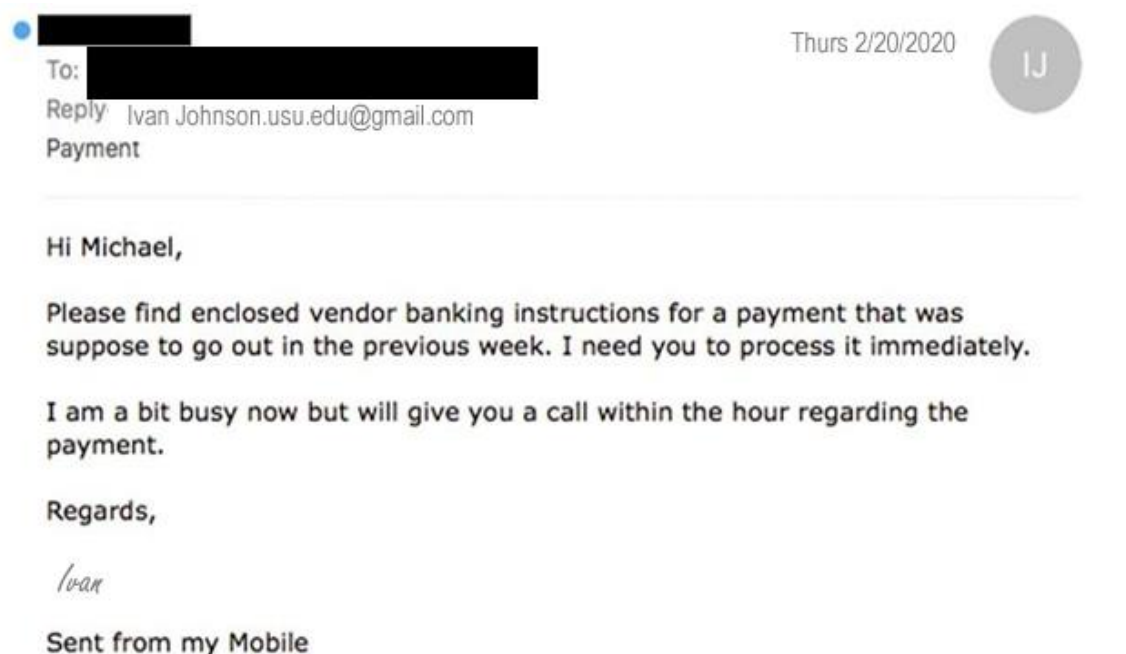
4.4 Urgent or Threatening Language

A common phishing tactic is to promote a sense of fear or urgency, pressuring the recipient to quickly click on a link.

Cybercriminals will often use threats that your security or privacy is compromised and that urgent action is required to remedy the situation.

Therefore, be cautious of subject lines that claim “Unauthorized login attempt” or “Your account has been suspended.”

If you are unsure if the request is legitimate, contact the company directly via its official website or official telephone number.



Scammers will use common services, such as PayPal and Netflix, in a phish because individuals do not like problems with accounts could cause immediate inconveniences.

A sense of urgency is equally effective in workplace scams. Criminals know that most of us will drop everything if a boss emails us with a request, especially when other business processes are supposedly waiting on you.

Example Subject: [EXT] RE: Introduction

A caution message appended at the end of the incoming e-mail.

CAUTION: This email originated from outside of USU. If this appears to be a USU employee, beware of impersonators. Do not click links, reply, download images, or open attachments unless you verify the sender's identity and know the content is safe.

Use the tags as effective mental triggers to recognize phishing and impersonation attempts.

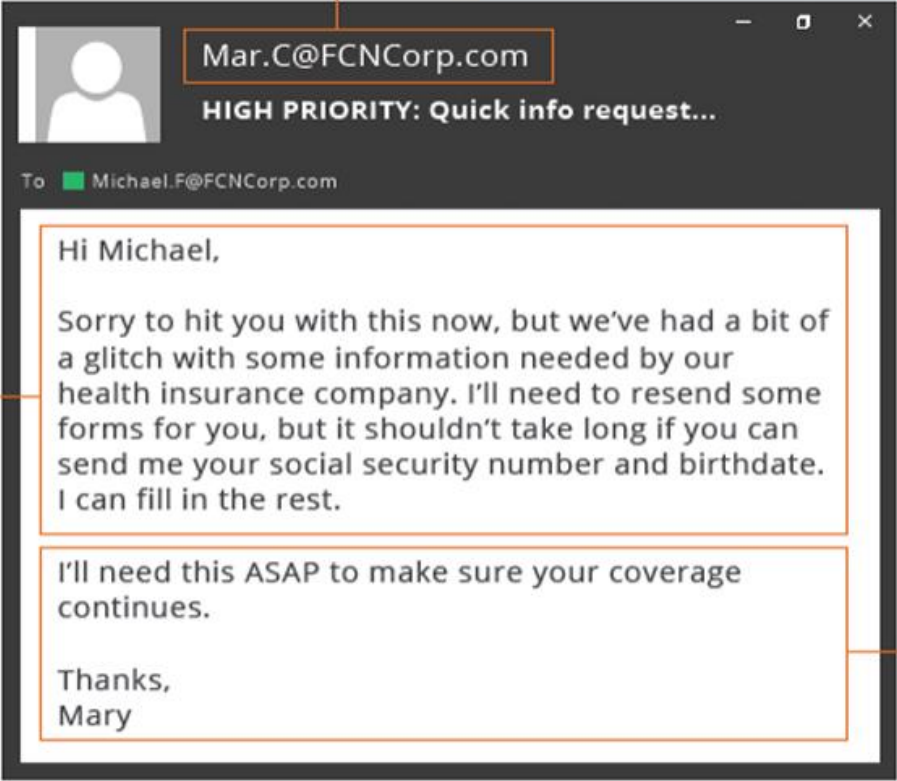
5. Examples

The diagram illustrates a phishing email interface with several annotations pointing to suspicious elements:

- Annotation 1:** "Any messages addressed generically, especially ones asking for login credentials for a specific web-based service, are suspicious." Points to the "To" field showing "marketing@FCNCorp.com".
- Annotation 2:** "Watch out for mass email sends or unexpected emails to email aliases." Points to the "From" field showing "support@salesfierce.com".
- Annotation 3:** "Keep an eye out for 'from' addresses that look odd, such as misspelled or mis-configured domain names. Phishers will often gain access to domain names that are just one letter off from legitimate ones." Points to the "From" field showing "support@salesfierce.com".
- Annotation 4:** "Hello Valued User:" Points to the salutation.
- Annotation 5:** "It has come to our attention that your account information may have been compromised. Please use the link below to confirm your username and account ID number." Points to the body text.
- Annotation 6:** "[https://login.customersupport.salesfierce.com](\"https://login.customersupport.salesfierce.com\")" Points to the URL link.
- Annotation 7:** "Many phishing emails involve an attempt to trigger an emotional, rather than logical, response. Here the idea of a compromised account is meant to cause a quick, unthinking action." Points to the body text.
- Annotation 8:** "Extreme caution should be exercised with any link appearing in an unexpected or unsolicited email. In the case of suspicious looking login information requests, visit the site of the service referenced in the email directly to ensure you're logging in to the correct place." Points to the URL link.

Display names can be spoofed by cybercriminals. Blindly hitting "reply" without taking a second look at the recipient could put sensitive PII in the hands of hackers.

Notice the conspicuous lack of links in this particular spear phishing attempt. Some phishing emails, such as those targeting an individual, will simply request information, relying on a blind "reply" to acquire the desired data.



If something about the text of email feels off, even if it seems to come from a trusted source, you should follow your gut. You know your company's procedures, so ask yourself: is this the way we do business? Additionally, follow up outside of email (such as a phone call) may be warranted for requests of this nature. If PII is at stake, extra precautions are warranted.

6. Best Practice

Top Tip: Look at the email address, not just the sender

- Ensure the message is not sent from a public email domain; no legitimate organization will contact you from an address that ends '@gmail.com', not even Google. Legitimate emails from Google will read '@google.com'.
- If the domain name (after the @ symbol) matches the apparent sender of the email, the message is more likely to be legitimate.
- Never click on suspicious links or attachments, especially from unsolicited messages

- Go to the source if you have questions about the validity of the URL or message.
- Check the website security
- Ensure there is a padlock symbol in the URL address bar OR
- Ensure the URL begins with https:// or shttp://. The added “s” indicates that the data will be encrypted in transit.
- Create strong passwords on all accounts
- Educate your coworkers and family members
- Others’ actions can result in a compromise of your data as well
- Be careful with online posts; do not give away too much personal information
- The more information criminals can gather on social media, the more targeted their attacks will become
- Enforce privacy options and restrict access to your social media accounts

7. Resources

- IT Governance, IT Governance Blog, 6 Jun 2019, <https://www.itgovernance.co.uk/blog/5-ways-to-detect-a-phishingemail> [extracted 28 Feb 2020]
- MediaPro, 3 PII Phishing Tactics, 14 Nov 2017, <https://www.mediapro.com/blog/infographic-3-pii-phishing-tacticslook-out-for/> [extracted 17 Jan 2019]
- PhishLabs, Phishing: Number One Cause of Data Breaches: Lessons from Verizon DBIR, 27 Jun 2019, <https://info.phishlabs.com/blog/phishing-number-1-data-breaches-lessons-verizon> [extracted 28 Feb 2020]