Don't Get Catfished: Spot the Online Imposters

Vaibhav Kant Nawani

INTRODUCTION

- Phishing is a type of cybersecurity attack during which malicious actors send messages pretending to be a trusted person or entity.
- Phishing messages manipulate a user, causing them to perform actions like installing a malicious file, clicking a malicious link, or divulging sensitive information such as access credentials.

TYPES OF FISHING

Email Phishing

Most phishing attacks are sent via email. Attackers typically register fake domain names that mimic real organizations and send thousands of common requests to victims.

Whaling

Whaling attacks target senior management and other highly privileged roles. The ultimate goal of whaling is the same as other types of phishing attacks, but the technique is often very subtle.

Smishing and Vishing

This is a phishing attack that uses a phone instead of written communication. Smishing involves sending fraudulent SMS messages, while vishing involves phone conversations.

What are the Signs of Phishing?

- Threats or a Sense of Urgency: Emails that threaten negative consequences should always be treated with skepticism. Another strategy is to use urgency to encourage or demand immediate action.
- Message Style :An immediate indication of phishing is that a message is written with inappropriate language or tone.
- Unusual Requests: If an email requires you to perform non-standard actions, it could indicate that the email is malicious.
- Linguistic Errors: Misspellings and grammatical misuse are another sign of phishing emails. Most companies have set up spell-checking in their email clients for outgoing emails.
- Inconsistencies in Web Addresses: Another easy way to identify potential phishing attacks is to look for mismatched email addresses, links, and domain names.
- Request for Credentials, Payment Information, or Other Personal Details: In many phishing emails, attackers create fake login pages linked from emails that appear to be official.

RECOGNISING THE PHISHING WEBSITES

- **URL Shenanigans**: Misspelled Domain Names, Strange Characters, No Padlock
- **Suspicious Content and Design**: Poor Design, Urgency and Threats, Generic Greetings
- **Missing Information**: Lack of Contact Details, Unrealistic Promises
- **Don't Click on Links in Emails**
- **Hover, Don't Click**
- **Bookmark Trusted Sites**

RECOGNISING THE SOCIAL ENGINEERING TACTICS

- Creating a Sense of Urgency or Fear
- Appealing to Your Curiosity or Greed
- Faking Authority
- Preying on Your Helpfulness
- Unexpected Contact
- Poor Communication

Shields Up for Emails

- **Scrutinize the Sender:** Don't just skim the name. Check the email address for typos or close-but-no-cigar variations of legitimate addresses. "BankofAmericaa" instead of "BankofAmerica" is a red flag.
- **Beware of Urgency:** Phishing emails thrive on panic. If the email screams "act now or lose your account!" take a beat to breathe. Legitimate companies won't pressure you like that.
- **Inspect the Links and Attachments:** Hover your mouse over a link to see the actual URL (it might be different from what's displayed). Never click links or open attachments from suspicious emails.
- **Check for Grammar Gremlins:** Typos, grammatical errors, and awkward phrasing are hallmarks of phishing attempts. A professional company wouldn't send emails riddled with mistakes.

Website Watchdogs

- **Beware of Lookalikes:** Phishing websites mimic real ones. Check the URL for misspellings, extra characters, or anything out of the ordinary. Look for the padlock symbol in the address bar, indicating a secure connection (https://).
- **Unrealistic Claims:** Don't get hooked by unbelievable deals or guaranteed results. If it sounds too good to be true, it probably is.
- **Missing Contact Info:** Legitimate websites typically have a "contact us" page with a physical address, phone number, and email. A lack of contact details is a warning sign.
- **Don't Click from Emails:** If you're unsure about a link in an email, even from a seemingly familiar sender, go directly to the website by typing the address into your browser.

Social Engineering Savvy

- **Don't Be Rushed:** Scammers will try to pressure you into acting quickly. If someone creates a sense of urgency, take a step back and assess the situation calmly.
- **Question Everything:** Don't be afraid to ask questions and verify information through trusted sources before taking any action. If an offer sounds too good to be true, it probably is.
- **No Personal Information Sharing:** Legitimate companies won't ask for sensitive information through unsolicited emails, calls, or texts.
- **Unmask the Imposters:** If someone claims to be from a trusted organization, verify their identity through official channels, not the information they provide.

THANK YOU