Phishing: Don't Get Hooked!

By: Ashwitha Sajeev_

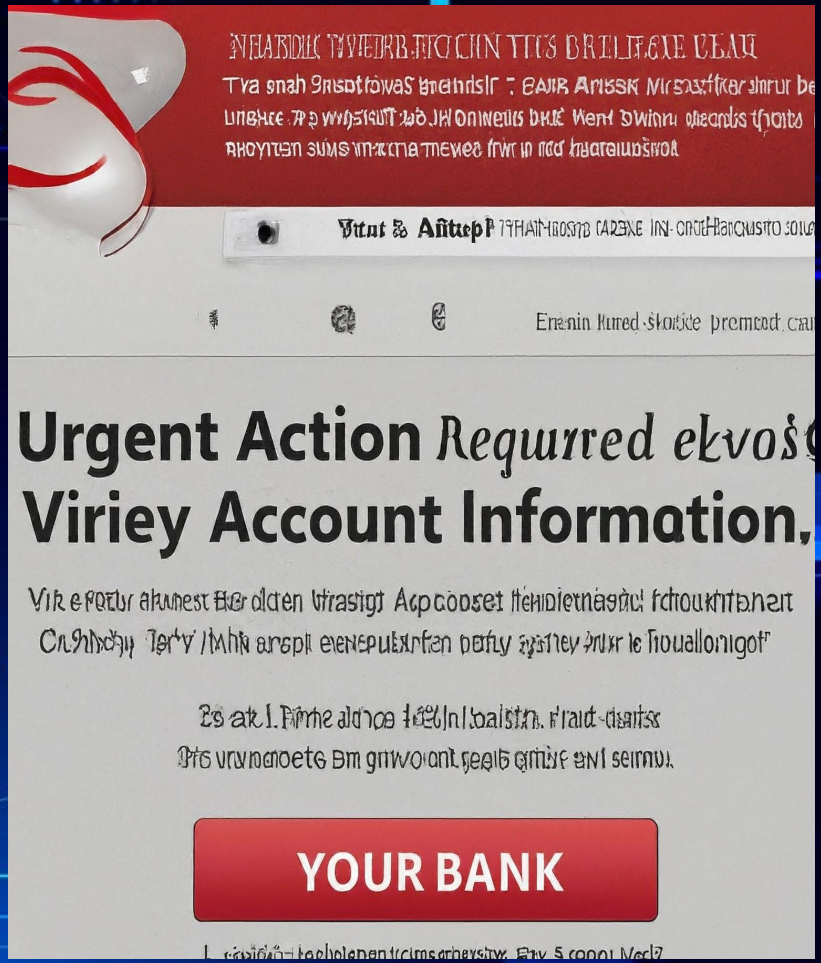
What is Phishing?

- A fraudulent attempt to steal sensitive information like passwords, credit card details, or Social Security numbers.
- Uses emails, text messages, phone calls, or fake websites to appear legitimate.
- Aims to trick you into clicking a malicious link or downloading malware.

How to Recognize Phishing

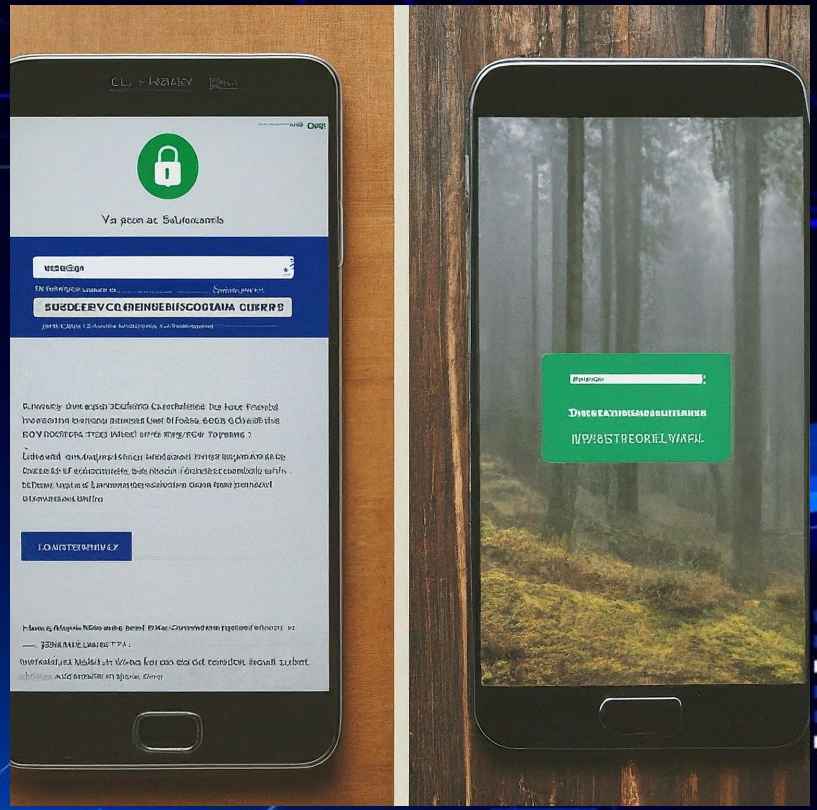
Look for red flags:

- Misspelled sender addresses (e.g., [email address removed] instead of bankofamerica.com)
- Generic greetings ("Dear Customer")
- Urgent requests for personal information
- Grammatical errors or poor formatting
- Suspicious links or attachments



Spotting Phishing Websites

- Check the website address (URL) for typos or unfamiliar characters.
- Look for a padlock symbol in the address bar for secure websites (HTTPS).
- Be cautious of websites with poor design, grammar, or spelling errors.



Social Engineering Tactics

- Phishers may use phone calls or text messages to impersonate trusted sources.
- They may create a sense of urgency or fear to pressure you into compromising your information.
- Never give out personal information over the phone or text message unless you initiated the contact.

Protecting Yourself from Phishing

- Be cautious of unsolicited emails, texts, or calls.
- Don't click on suspicious links or open attachments.
- Verify the sender's identity before responding.
- Go directly to the official website (by typing the URL yourself) to verify any claims.
- Use strong, unique passwords for all your accounts.
- Enable two-factor authentication (2FA) for added security.


THANK YOU
STAY SAFE