Phishing Recognition Cheat Sheet

Phishing is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. Recognizing a phishing attempt is the first and most critical line of defense.

Key Red Flags to Look For

1. A Sense of Urgency or Threat

Phishing emails often create a false sense of urgency or threat to pressure you into acting without thinking.

- **Examples:** "Your account will be suspended in 24 hours if you don't act now," or "Your password has expired, click here to update immediately."
- **Your Action:** Pause and verify. Go to the official website directly, do not click the link.

2. Generic Greetings

A legitimate company will almost always address you by name. Phishing emails often use generic greetings to cast a wider net.

- **Examples:** "Dear Valued Customer," "Hello [Email Address]," or "Dear User."
- **Your Action:** Be suspicious of emails that don't use your name.

3. Suspicious Attachments

Be extremely cautious of unexpected attachments, especially from unknown senders. These attachments can contain malware, ransomware, or viruses.

- **Common File Types:** Be wary of `.zip`, `.exe`, `.js`, or `.vbs` files. Even seemingly harmless `.doc` or `.pdf` files can contain malicious scripts.
- **Your Action:** Do not open an attachment unless you are certain of the sender and were expecting the file.

4. Mismatched URLs

This is a classic and easy-to-spot sign. The visible hyperlink text may look legitimate, but the actual URL it links to is different.

- **How to Check:** Hover your mouse over the hyperlink without clicking. The actual destination URL will appear in the bottom corner of your browser.
- **Example:** A link that says "www.google.com" but shows "http://badsite.ru/login" when you hover over it.

5. Typos and Grammatical Errors

Legitimate companies have professional copy editors. Phishing emails, often created quickly by cybercriminals, are riddled with spelling and grammar mistakes.

- **Your Action:** A few typos can be a red flag. Be especially wary if the errors are frequent or significant.

6. Requests for Personal Information

Reputable organizations will never ask you to send sensitive information like passwords, credit card numbers, or social security numbers via email.

- **Your Action:** Never provide personal information in response to an email. If a company needs this information, they will direct you to a secure portal on their official website.

What to Do If You Suspect Phishing

- **Do NOT reply or click any links.**
- **Do NOT open any attachments.**
- **Report the email** to your IT or security department.
- **Delete the email** from your inbox.