IDENTIFYING PHISHING

Phishing is a type of fraud that uses authentic-looking (but fake) e-mails and websites to gain information from users.

There are **5 common things to look for** when trying to decide if an email is a phishing attempt.

CHECK EMAIL ADDRESSES

Scammers will often try to mimic or spoof a legitimate email address.

Look for:

- **Extra letters or words** in the domain name at the end of the email address.
- **Misspellings or extra characters** in the sender's name.

CHECK URL LINKS

Some scammers will create a spoof site to trick you.

Hover your mouse over a link to preview the URL before clicking.

Look for:

- URLs that look similar to a legitimate site but are slightly off.

BE WARY OF URGENT OR UNUSUAL REQUESTS

Look for **requests for sensitive information** like:

- Passwords
- Bank details
- Personal data

Also look for **unusual or odd requests** such as:

- Money
- Gift cards
- Wire transfers

Scammers use **claims that there are consequences for not acting quickly to get you to panic** and act without thinking.

BE CAUTIOUS WITH ATTACHMENTS

Do not open attachments unless you are sure they are from a trusted source.

Attachments like reports, invoices, and promotional material **can hide the presence of malware**.

CHECK FOR POOR GRAMMAR OR WORDING

Many phishing emails can be identified by **poor grammar, odd word choice, or misspellings**.

Look for:

- Generic greetings.
- Missing **punctuation**.
- Awkward **phrasing**.
- Incorrect **verb tense**.
- **Misspellings** (e.g. "acount" instead of "account")

If you suspect an email is a phishing attempt:

1. Do NOT click any links or respond directly.
2. Forward the email to it@startup.com to report it.
3. Delete the email to prevent accidental clicks