CSU COMPUTER SERVICES UNLIMITED

February 2023

# Coffee Break To-go

## 10 Common Traits of Phishing Emails

**1. Requests Personal Information**

Most reputable organizations will never email you asking for your address, phone number, national ID number, or other personal data.

**2. Threatening tone!**

Phishing emails often feature threatening language, such as "Payment overdue!" or "Your account has been compromised!", in order to generate a response from their targets.

**3. Inconsistencies In Links**

Always hover over links with your mouse pointer to display the full URL. If it leads somewhere that doesn't logically belong within the context of the email, or generally looks nonsensical, don't click!

**4. Generic Greetings**

Unlike legitimate entities that will address you by your full name or username, phishing emails usually opt for generic greetings, such as Dear Customer or Dear Sir/Madam.

**5. A Sense of Urgency**

Similar to unrealistic threats, emails that urge you to click on a link or download an attachment or update your account immediately are likely scams.

**6. You're Asked to Send Money**

Whether it be overdue taxes or an upfront payment to cover expenses, any email that asks for money should immediately raise your suspicions.

**7. Suspicious Attachments**

Attachments aren't always malicious, but use caution when you receive them unexpectedly.

**8. Too Good To Be True**

The old saying remains: "if it's too good to be true, it's likely untrue". Remember this if you get an email about winning the lottery or being due a family inheritance

**9. Poor Spelling & Grammar**

Most generic phishing attempts contain spelling and grammar errors or feature awkward wording/phrasing.

**10. It's from a Government Agency**

9 times out of 10, government agencies don't use email to communicate anything of consequence. The IRS, for example, will never email you about your taxes or payments.