Phishing Red Flags

Kurt Lutterman, IT Manager, Saint Andrew's Lutheran Church
November 5, 2022

Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a human victim. The human receiver of phishing is significantly more likely to thwart phishing attempts than technology can.

One of these Red Flags should make you very suspicious. Two or more of these **strongly** suggest a phishing message:

- ☐ **If you have ever replied to another phishing attempt using this email address or mobile number**
  - Even innocent replies like "I don't understand your request", or Unsubscribe requests
  - "Dark web" sites keep track of who has responded.
- ☐ **Urgent or threatening language**
  - Pressure to respond quickly
  - Threats of closing your account, legal action, reporting to authorities, publishing webcam video
  - Technical Support: you have a virus, expired subscription, declined credit card
  - Related to current event: natural disaster, war refugees, "Act Now to help"
- ☐ **Requests regarding sensitive personal or financial information**
  - Name, SSN, birth date, bank or computer account name or password, credit card number
  - Updates to account information or password
  - Any type of financial transaction: gift cards, direct deposit, crypto-currency, PayPal, Venmo, Cash App, Zelle
- ☐ **Anything too good to be true**
  - Winning a lottery, prizes you must pay to receive, inheritance, holding or distributing someone else's money
- ☐ **Unexpected email**
  - Receipt for something you didn't purchase, "Call this number to cancel"
- ☐ **Information mismatch (hover mouse over address or link, but DO NOT click)**
  - Incorrect sender email address: second to last part of address should be *<companyname>*
  - Substitution characters in address or subject line: ÇOMCÁ$T versus COMCAST (what are the 4 here?)
  - Links to non-official websites
- ☐ **Suspicious attachments**
  - Attachments you didn't ask for
  - Weird file names
  - Uncommon file types: HTML, DOC, XLS files can hurt you, among others
- ☐ **Unprofessional design**
  - Incorrect or blurry logos
  - Image-only emails (no selectable text)
  - Little, poor or no formatting
  - Spelling or grammar error
- ☐ **Something seems "off"**
  - Unusual request
  - Sender "tone"

Safety precautions you should take (based on *The Washington Post*)

- Don't pick up calls from unknown numbers. If it's important, they will leave a message.
- Assume people and companies are not who they say.
- Reach out to the person or company through an official channel published on their website.
- Ask a friend or family member about suspicious messages.
- Call the sender on a number you know is good.
- Slow down and trust your gut.
- Be VERY SKEPTICAL of links or phone numbers in texts, emails, or other messages.