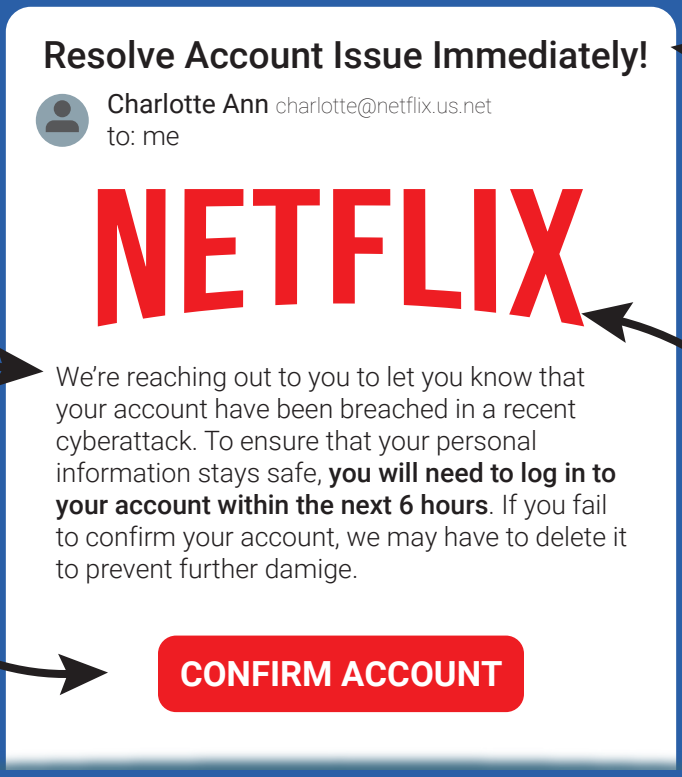
PHISHING EMAILS

Phishing refers to fraudulent emails that trick the receiver into sharing their personal, financial, or security-related information. Phishing emails typically:

...appear **nearly identical** to the types of emails the real organization would send

...ask you to **download** an attached file or click on a link



...use language that transmits **a sense of urgency**

...**replicate the logos**, layout, and tone of real emails

Cybercriminals rely on impatience or fear to get their targets to respond blindly. Watch out when using a mobile device, as it's harder to spot phishing on a phone or tablet.

WHAT CAN YOU DO?

- *Keep your software updated, including your browser, antivirus, & operating system*
- *Be especially vigilant if an email requests sensitive information from you*
- *Look at the email address closely: compare the address with previous messages*
- *Check for bad spelling and grammar*
- *Don't reply to a suspicious email*
- *Don't click on links or download attachments; instead type the address by hand*
- *When in doubt, double check with the organization's website or give them a call*

Church Educational System
Security Operations Center