PHISHING & SPOOFING eMAIL CHECKLIST

01

Compare the sender's EMAIL ADDRESS to the WEBSITE of the company they claim to represent. They should match exactly.

EXAMPLE:
www.acmebank.com vs. johnsmith@acmebank1.com

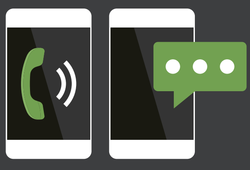
02

Outlook may report an email is UNSAFE or is a potential phishing ATTACK with a warning message.

DO NOT DISREGARD THIS WARNING!

03

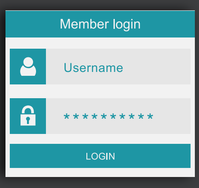
DO YOU KNOW THE SENDER?
If so, does the subject line or body of the email seem out of character or unusual? If you do not know the sender, be extra cautious of links.



VERIFY THEIR IDENTITY WITH A PHONE CALL.

04

Most large organizations, such as banks and insurance companies, DO NOT send emails with hyperlinks asking you to VERIFY YOUR INFORMATION or UPDATE YOUR PASSWORD.



THESE ARE ALL SCAMS!

05

05

When in doubt, enter the SENDER'S WEB ADDRESS directly into your Web browser bar and use the website's navigation to find the information referred to in the email message.
Is the main purpose of the email to get you to click a link?

IF YOU'RE BEING URGED TO DO SOMETHING THAT SOUNDS DIRE OR THREATENING, **IT IS MOST LIKELY SPAM.**

06

Does the subject line or body of the email contain POOR GRAMMAR or SPELLING ERRORS?

THESE ARE BOTH RED FLAGS.

07

FAKE ANTI-VIRUS, or SCAREWARE, is one of the leading ways malicious hackers make money from unsuspecting internet users. The email typically warns the recipient that they have various security threats present on their computer. The warnings are fake but often backed up by believable descriptions of the supposed malware.

DELETE ALL ANTI-VIRUS SOLICITATIONS.

CGS®