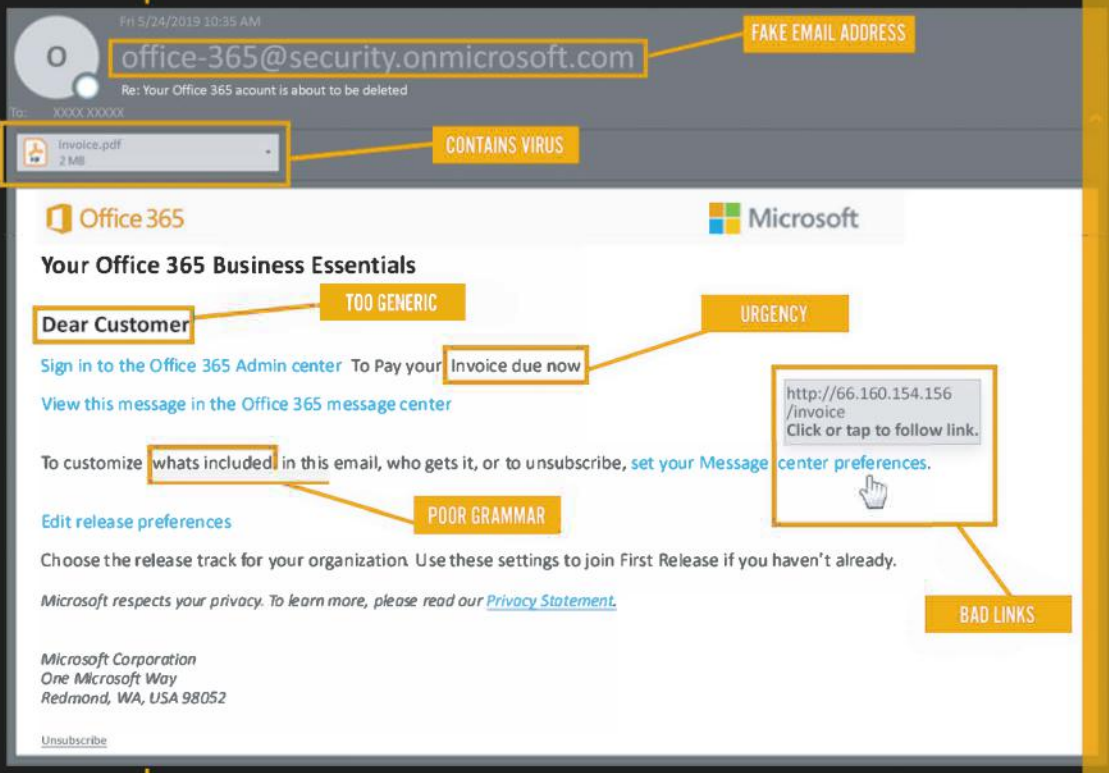
AGB
CYBER DIVISION

WWW.AGBCYBER.COM

# TIPS FOR DETECTING A PHISHING EMAIL

Cyber criminals might send an email that looks legitimate, known as a phishing email, but you can take steps to avoid the traps




## .01 WATCH FOR OVERLY GENERIC CONTENT AND GREETINGS

*Cyber criminals will send a large batch of emails. Look for examples like "Dear valued customer."*

## .02 EXAMINE THE ENTIRE EMAIL ADDRESS

*The first part of the email address may be legitimate but the last part might be off by letter or may include a number in the usual domain.*

## .03 LOOK FOR URGENCY OR DEMANDING ACTIONS

*"You've won! Click here to redeem prize," or "We have your browser history, pay now or we are telling your boss."*

## .04 CAREFULLY CHECK ALL LINKS

*Move your mouse over the link and see if the link's destination matches where the email implies you will be taken.*

## .05 NOTICE MISSPELLINGS, INCORRECT GRAMMAR, & ODD PHRASING

*This might be deliberate attempt to try to bypass spam filters.*

## .06 DON'T CLICK ON ATTACHMENTS RIGHT AWAY

*Virus containing attachments might have an intriguing message encouraging you to open them such as "Here is the Schedule I promised."*

## .07 CHECK FOR SECURE WEBSITES

*Any webpage where you enter personal information should have a url with https://. The "s" stands for secure.*