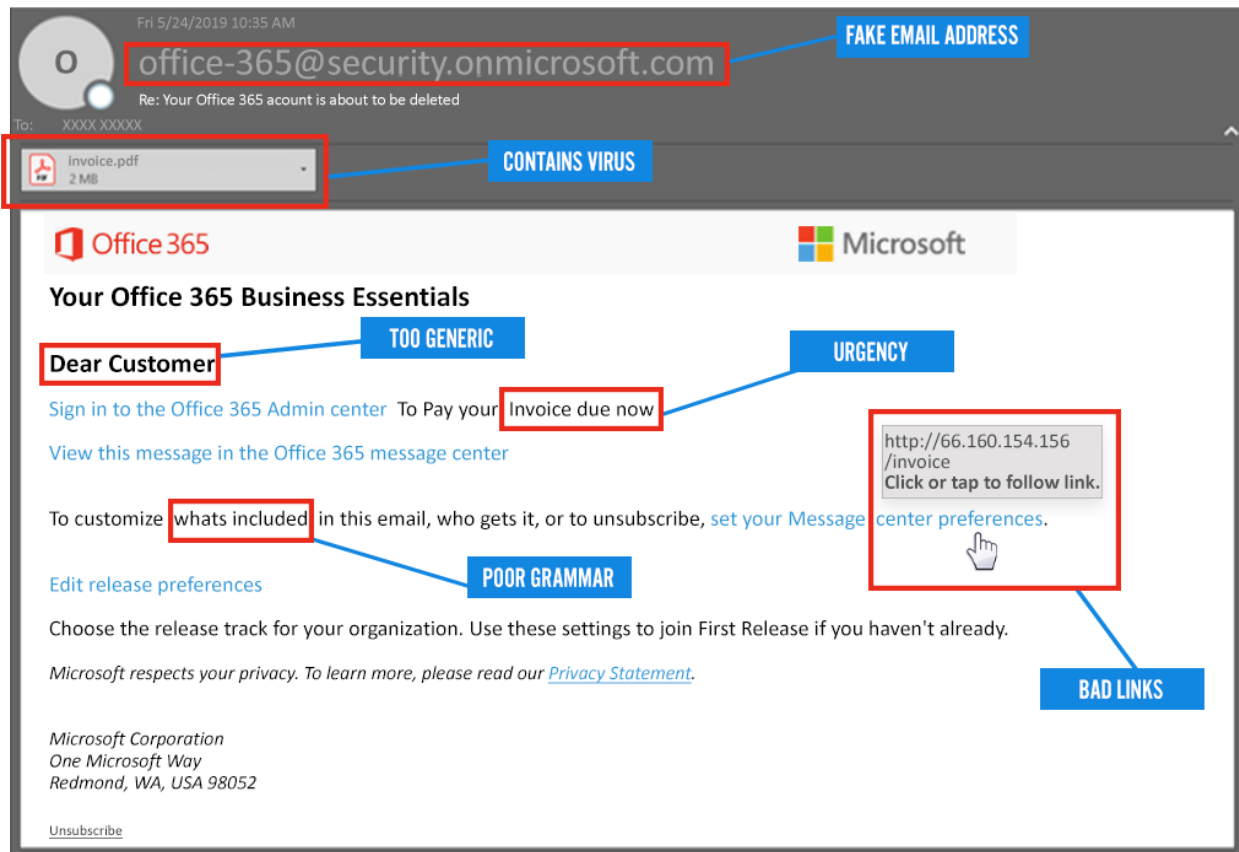


TIPS FOR DETECTING A PHISHING EMAIL

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



1 WATCH FOR OVERLY GENERIC CONTENT AND GREETINGS

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

2 EXAMINE THE ENTIRE FROM 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.

3 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."

4 CAREFULLY CHECK ALL LINKS

Mouse over the link and see if the link's destination matches where the email implies you will be taken.

5 NOTICE MISSPELLINGS, INCORRECT GRAMMAR, & ODD PHRASING

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

6 CHECK FOR SECURE WEBSITES

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

7 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."



The business IT experts

newcmi.com 0800 023 2696