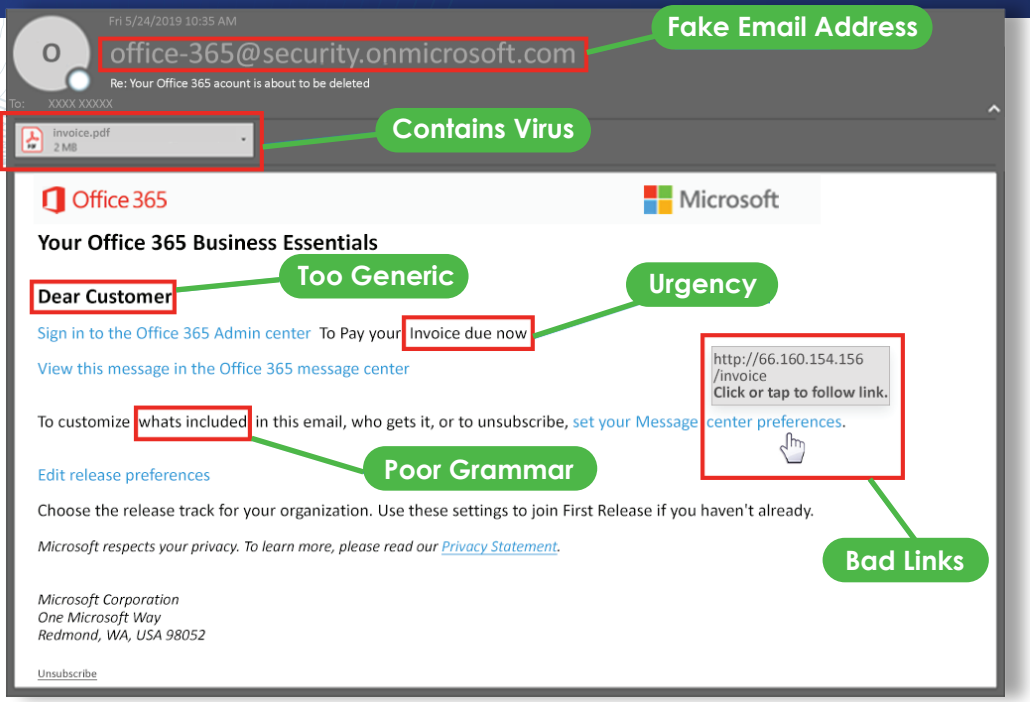
7 TIPS For Detecting A PHISHING EMAIL & What To Do If You Take the Bait

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 look legitimate, but the last part might be off by a letter or may include a number in the usual domain.

3 LOOK FOR URGENCY, DEMANDING ACTIONS OR A TONE OF DESPERATION

"You've won! Click here to redeem prize," or "We have your browser history pay now or we will report you."

4 CAREFULLY CHECK ALL LINKS

Hover over the link and see if its destination displays differently.

5 NOTICE MISSPELLINGS, INCORRECT GRAMMAR & ODD PHRASING

This might be deliberate attempts 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

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

What to Do If You Receive a Phishing Email

If you receive an email that looks suspicious, follow these phishing email best practices:

- Don't open the email
- Immediately delete the email
- Do not click on or download any attachments
- Whatever you do, don't click any internal embedded links
- Don't reply to the sender
- Inform your IT department and others (consider taking a screenshot to help others identify potential scams), but do not forward a suspicious email, even to your IT department.

Better yet — avoid these attacks in the first place. At Elevity, we use our own **4S** approach to protect your technology and assets: **Strategy**, **Security**, **Solutions** and **Support**.

To see how prepared you are for a cyberattack, we encourage you to take our **free Cybersecurity Risk Assessment.**

What to Do If You Suspect You've Taken the Bait

Think you might have fallen for an email phishing scam? Here are some immediate steps you should take:

- Immediately **turn off Wi-Fi** and disconnect from the internet in hopes you can limit a hacker's access to your network
- **Contact your IT department** or technology management provider
- If you clicked on a link to a fraudulent website, **write down any information you entered** (username, password, address, etc.)
- Change your **passwords**
- Scan your device for **viruses or malware**
- **Report** incidents of successful breaches to the Federal Trade Commission (FTC)
- **Improve your security posture** by working with an experienced technology management provider

elevITy®

888.733.4060 | elevityIT.com