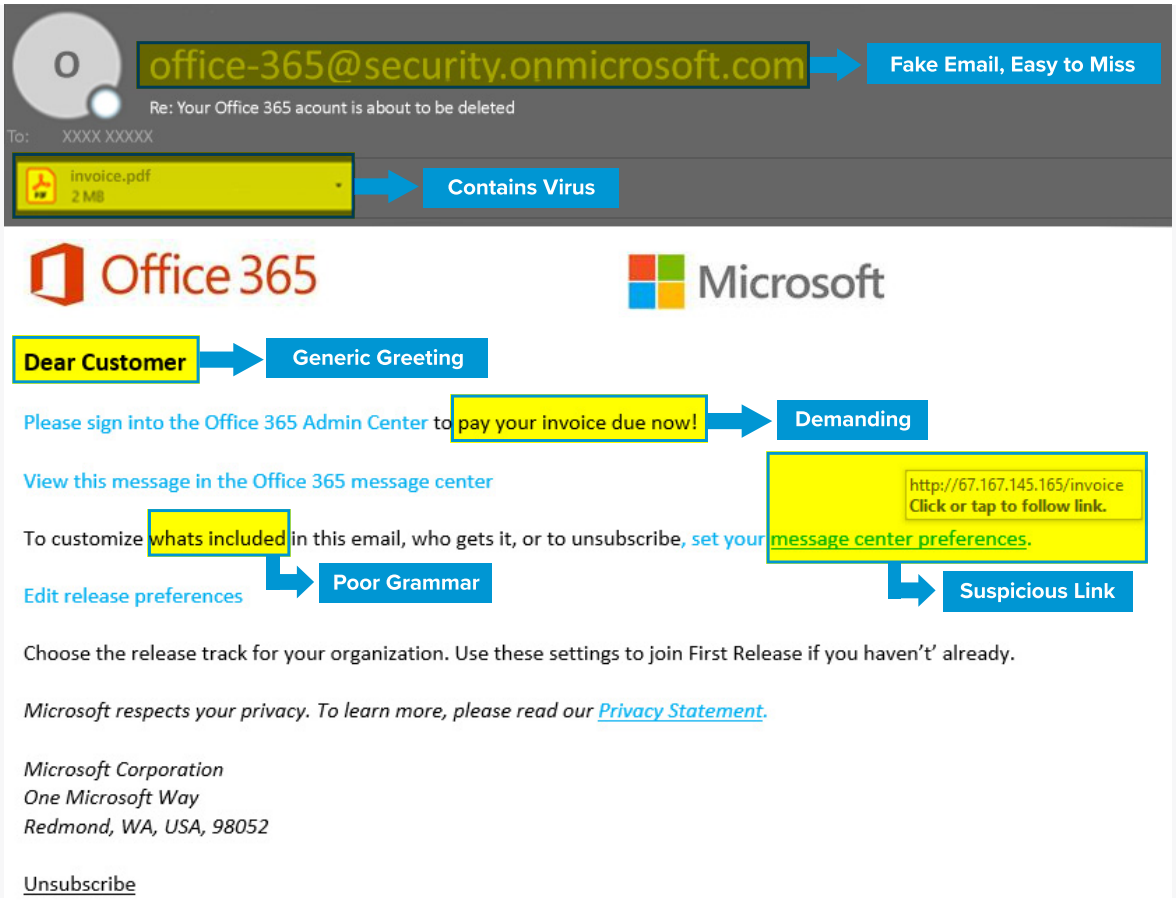
8 TIPS FOR DETECTING A PHISHING EMAIL

Net@Work



1 THE "FROM" EMAIL ADDRESS DOESN'T LOOK RIGHT

You might recognize the first part of the email address but pay attention to the tail end after the "@" symbol, as it might be off by a letter or may include a number in the usual domain.

2 REQUESTS FOR PERSONAL INFORMATION

Most legitimate businesses have a policy that they do not ask you for your personal information through email. Be very suspicious of a message that asks for personal information even if it might look legitimate.

3 ASKING TO SEND MONEY TO COVER EXPENSES

Sooner or later, phishing artists will likely ask for money to cover expenses, taxes, fees, or something similar. If that happens, you can bet that it's a scam.

4 CHECK ALL URL AND LINKS CAREFULLY

Place your mouse over the links and see if the destination matches where the email implies you will be taken. Any webpage where you enter personal information should have a URL with https://. The "s" stands for secure.

5 OVERLY GENERIC CONTENT & GREETINGS

Watch out for general greetings like "Dear Customer." Cyber criminals will send emails in bulk, so non-personal greetings can be a red flag.

6 POOR SPELLING AND GRAMMAR

Notice misspellings, incorrect grammar, & odd phrasing. This might be a deliberate attempt to try to bypass spam filters.

7 PAY ATTENTION TO SUSPICIOUS ATTACHMENTS

Alarm bells should be ringing if you receive an email from a company out of the blue that contains an attachment, especially if it relates to something unexpected.

8 LOOK FOR URGENT WORDING OR DEMANDING ACTIONS

To increase the number of responses, people try to create a sense of urgency so that you immediately respond without thinking. Examples include "You've won! Click here to redeem prize," or "We have your browser history pay now or we are telling your boss."