Newsletter

It's the Most Wonderful Time of the Year

The holiday season is upon us! 2019 was filled with blessings. All of us at Total are grateful for the continuing support and faith that our wonderful clients, staff and vendors have shown. Warmest wishes to you and yours for good health and prosperity in the new year!

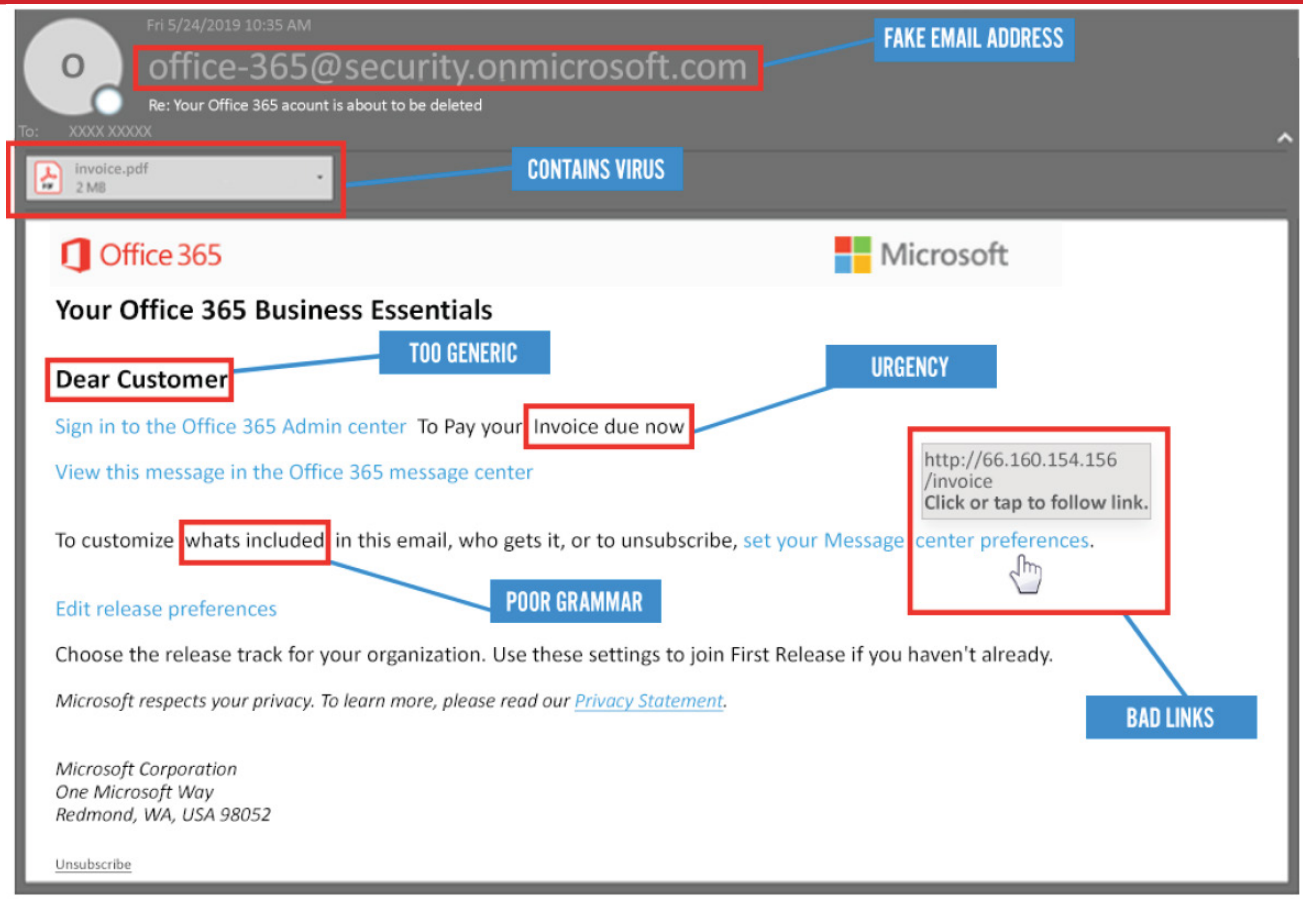
A FRIENDLY REMINDER

With the New Year just around the corner - don't get left out in the cold.
Extended Support for Windows 7 ends January 14, 2020. Upgrade to Windows 10 NOW!

TOTAL TECHNOLOGY SOLUTIONS

HEADQUARTERS: 1895 Walt Whitman Road • Melville, NY 11747 USA
631-777-7477 • 888-777-8093
www.total.us.com

TIPS FOR DETECTING A PHISHING EMAIL



1. **WATCH FOR OVERLY GENERIC CONTENT AND GREETINGS.**
Cyber criminals send mass emails. Look for examples like "Dear valued customer."

2. **EXAMINE THE ENTIRE FROM EMAIL ADDRESS.**
Check the last part of the email address to see if it is off by a 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're telling your boss."

4. **CAREFULLY CHECK ALL LINKS.**
Mouse over the link and see if the link destination matches where the email implies you will be taken.

5. **NOTICE MISSPELLINGS, INCORRECT GRAMMAR, & ODD PHRASING.**
These might be deliberate attempts to bypass spam filters.

6. **CHECK FOR SECURE WEBSITES.**
Any web page where you enter personal information should have a URL with https://. The "*s*" stands for *secure*.

7. **DON'T IMMEDIATELY CLICK ON ATTACHMENTS.**
Virus-containing attachments might have an intriguing message encouraging you to open them such as "Here is the Schedule I promised." Think first, then open if it is right for you!