Team Pete,

There are increasing public reports of bad actors exploiting present circumstances to act even worse than usual with phishing attempts and other malicious behavior.

While we are unaware of any specific targeting of Team Pete systems or users, please be extra vigilant with email and in all your online activity right now.

The following tips are repeated from earlier traffic and are probably worth reviewing and forwarding as widely as possible:

- Look closely at a sender's email address, realizing that email addresses can be easily spoofed to look like someone you know. Look for subtle differences such as a different country domain (e.g.--b.skoch@us.af.il vs b.skoch@us.af.mil).

- Look at the subject line. Does it create a questionable sense of urgency? Fake emails often do. Does it appear to be a reply to something you did not originate (like "Re: Document")? This is another sign of a fake email.

- Look at the body of the message. If the email originator appears to be a recognized sender, does the email follow typical style, or does it have an uncharacteristic greeting ("Greetings and Salutations") or a generic salutation ("Hello Friend!"). Does it have the company contact information and/or graphics you are accustomed to seeing in his or her email? Is it inexplicably or urgently asking you to open a file or go to a website link?

- Consider any call for action. Does it communicate a sense of suspicious urgency? (Remember, with viruses and other malicious logic, the sole purpose of the email is often to entice you to open an attachment.)

- Look at the file name of any attachment. Does it make sense? How big is it? (If it's really small (1kB to 22kB), it may well be a virus.)

21 Comm is here to serve you. Let us know what we can do better.

"Signed"

21st Communications Squadron