PHISHING – SPAM 101

One of the best solutions for avoiding these scams is vigilance. Some of the most common examples of scams include hackers attempting to procure usernames, passwords, credit card details, or bank information.

Here are 2 of the most common tricks to avoid with phishing scams:

Manipulative Web Links
A typical phishing trick is to send users a link that seems as if it might be heading to one website, but instead, it directs you to a malicious alternative; this can be accomplished by showing you the text of a trustworthy site, while the link itself sends you to a more malevolent option. For example, the link you click on may say 'google.com,' but thanks to tricky web coding, the results may direct you to a different site designed to harvest your information.

This trick can easily be identified by right clicking on the link (see image below) and selecting Edit Link.

Remember to eye the web link carefully before you click on it. Using slight typos in a web link is an efficient way to make you think you are secure when you are really at risk – heading to y0urbank.com' instead of 'yourbank.com.' Other keywords may even be added to the web address to create a plausible-sounding, but unofficial, link such as 'yourbanklogin.com.'

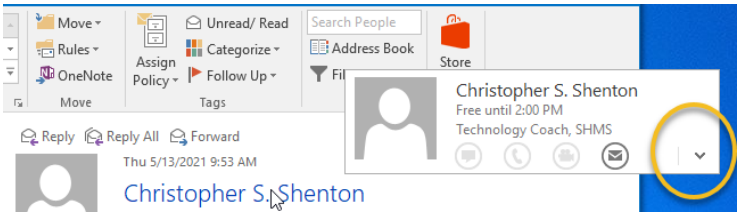
The Moral of Lesson 101
Do not trust anyone who asks you for a password or other personal information. Just delete the email, ignore the text-message or hang-up the phone call without giving any personal details. Then contact the institution or company that person claimed to represent by visiting their official website to verify the phishing attempt.

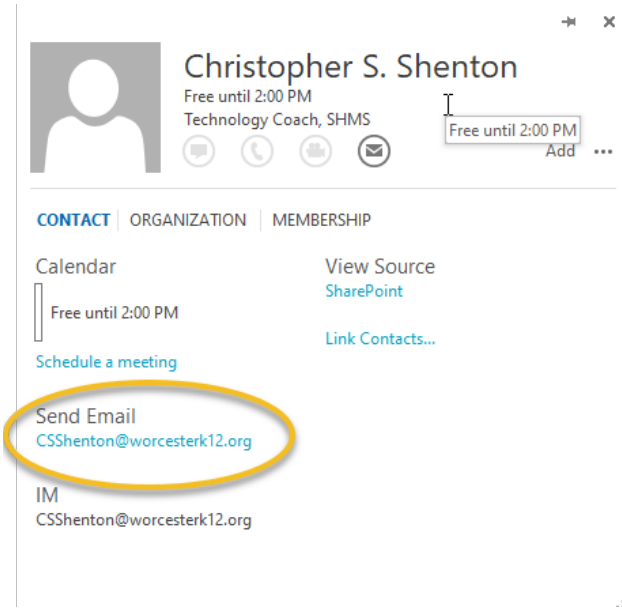
Phishing scams can be dangerous to our personal security and be confusing to identify, but rather than feel powerless at this sentiment there are options to keep your personal information safe. Use antivirus software on all your devices and follow best security practices to help you avoid becoming caught in a phishing scam net.

2 Way to be sure

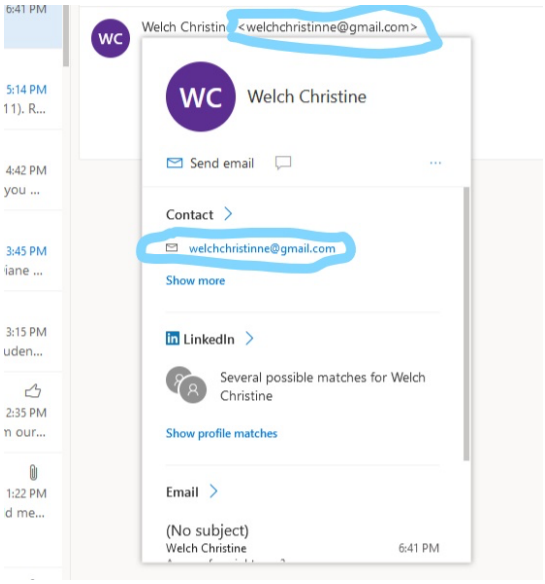
1. Double check who is sending the email to you by hover over the address.

    a. In Outlook the email address will look like this.

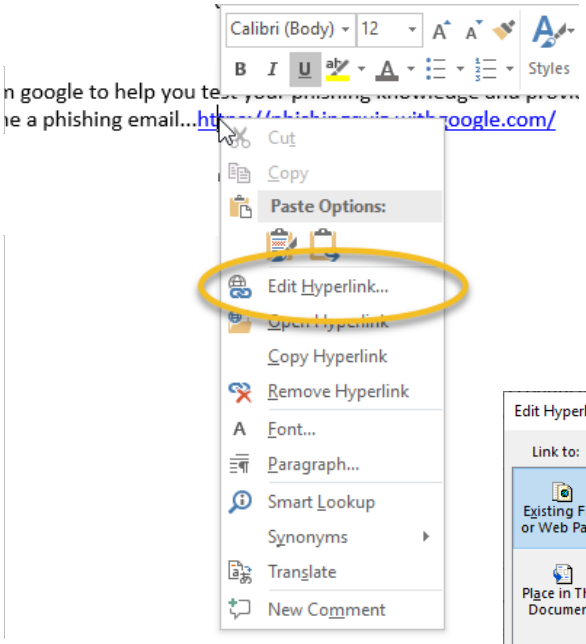


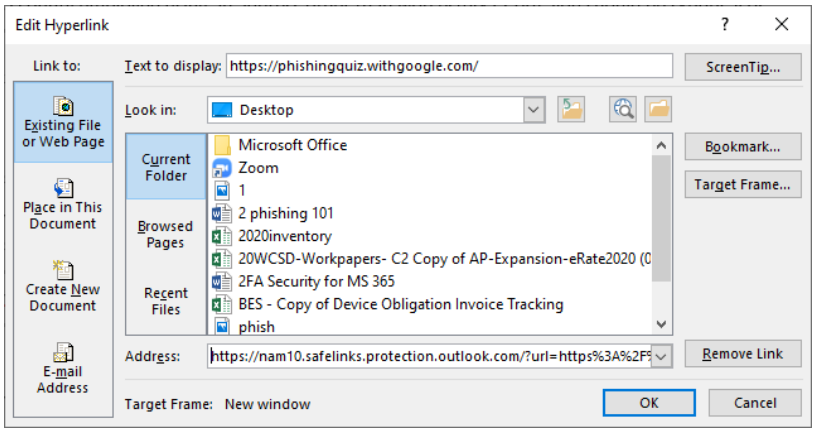


b. In Office 365 in the browse the email address will look like this.



2. Right click the link that in the email. Select Edit Hyperlink… This will bring up a window of the actual URL. If the URL is not familiar, then do not click.





If you have any double about what you are seeing please attached the email in question to a new email and send to “support@worcesterk12help.zendesk.com”

Here is a great new resource from google to help you test your phishing knowledge and provide you with tips on how to determine a phishing email...https://phishingquiz.withgoogle.com/