Phishing Attack Example - How to Spot a Scam Email
https://www.youtube.com/watch?v=PTE2oqMcfSw

Be on guard for suspicious emails that ask you to contact the sender immediately, send money, make a purchase, give up personal information, and more. Most often, these emails appear to come from a trustworthy source. You may recognize the sender's name and think it's attached to a personal account. Stop! Beware. Do not respond. It may be a scam!

If you reply, the scammer may use your information to verify your email address or your cell phone number or to set up fraudulent accounts at other websites using your social security number.

Alert the GPS IT department. Once we are aware of a possible problem, we respond by blocking the sender's email address.

Activity: Test your phishing smarts with Google's eight-question online phishing quiz (https://phishingquiz.withgoogle.com/). After you complete the activity reflect on your answers. What did you learn?

Stay Safe!
Watch out for emails that contain:

1) Errors of spelling, punctuation, word spacing, and grammar.
2) Embedded links. Clicking a link embedded in that email may download and install software with a malicious payload. Or it may take you to bogus website made up to look like a website you normally visit. Once at the site, you'll be asked for your credit card information to make a purchase on behalf of someone you know, or enter personal information that you should never share.
3) Requests for personal information. Never send passwords, banking information, or your social security number in reply to an email request.

Activity: Watch the PayPal anti-spoofing activity to learn how you can protect against spooking attempts, https://www.paypalobjects.com/webstatic/en_US/unified-help-center/SpoofWebsifeEmail.mp4

Discussion/Reflection.

1. Legitimate emails from reputable corporations like PayPal always use a personal greeting with your first and last name and never ask for your username and password. The same is true for other trustworthy vendors including Citigroup, Google, and Apple
2. Closely examine the sender's email address. Look for odd spelling or a questionable domain in the address
3. Before visiting a website or link embedded in an email, hover your mouse over the link to see where it will take you.
4. Does the URL of the link you are being sent to begin with an http:// or https://? Which one is more secure? Why? (See *What is https, and why should I care?* https://www.howtogeek.com/181767/htg-explains-what-is-https-and-why-should-i-care/)
5. For more information about social engineering attack methods, visit ***KnowBe4*** https://www.knowbe4.com/what-is-sociaal-engineering/. Explore KnowBe4's online mini-course on cybersecurity at https://www.knowbe4.com/homecourse. Enter ***homecourse*** as the password. Work through each of the topics, but if time is limited, choose one or two for detailed investigation.
6. Visit *Have I Been Pwned*? (https://haveibeenpwned.com/) run by security researcher Troy Hunt) to enter your email address. After entering your email address, click ***pwned***? Scroll the page of results to see the breach incidents where your email address and that site's login password were compromised and unintentionally exposed to the public in a data beach. If you haven't already changed the password for your username at these pwned sites, do so as soon as possible.

Carol S. Holzberg, PhD, CETL
Director of Technology, Greenfield Public Schools
09/27/19