WFG National Title

SAFE Tipsheet

Think Before You Click

June 2020

When it comes to cybercrime, email is the most effective way for criminals to deliver malware to an unsuspecting victim. The use of text-based threats is rising as more people work from home and do more on mobile devices. *If you are even a little bit suspicious of a text message or email, don't click*. Immediately report it or delete it!

Before You Click...

- **Verify to Clarify.** If you receive an email or text message requesting you to confirm or submit financial information, your login information, or any other sensitive personal information by clicking a link, ***don't.*** Contact the organization to verify the request, but not using the contact information contained in the email. Use the company's legitimate website and log into your account to verify.
- **When in Doubt, Throw it Out.** Links in email, tweets, texts, posts, social media messages and online advertising are an easy way for cyber criminals to get to you. Be wary of clicking on links or downloading anything that comes from a stranger or that you were not expecting.
- **Stranger Danger.** Remember what you learned about not accepting candy from strangers? Apply that to the online world as well. Do not click links in emails, text messages, chat boxes, etc. from people you do not know – or from someone you do know if it seems out of place.
- **Pay Attention.** Is the sender asking you to do something they wouldn't normally ask you to do, such as bypass your company policy? Does it seem weird the credit card company is asking you to verify your credit card number or SSN? (Yes!--they have that information already). Are there misspelled words, unusual phrases, or a sense of urgency to act immediately? These are often context clues that something is not right.
- **"Unsubscribe" Might be a Hack.** Sometimes a suggested action in an email can trick you - such as "unsubscribe" or "reply to stop receiving these messages." It is better to just delete the email or mark it as spam if it is spam.

continued on next page

WFG National Title

SAFE Tipsheet

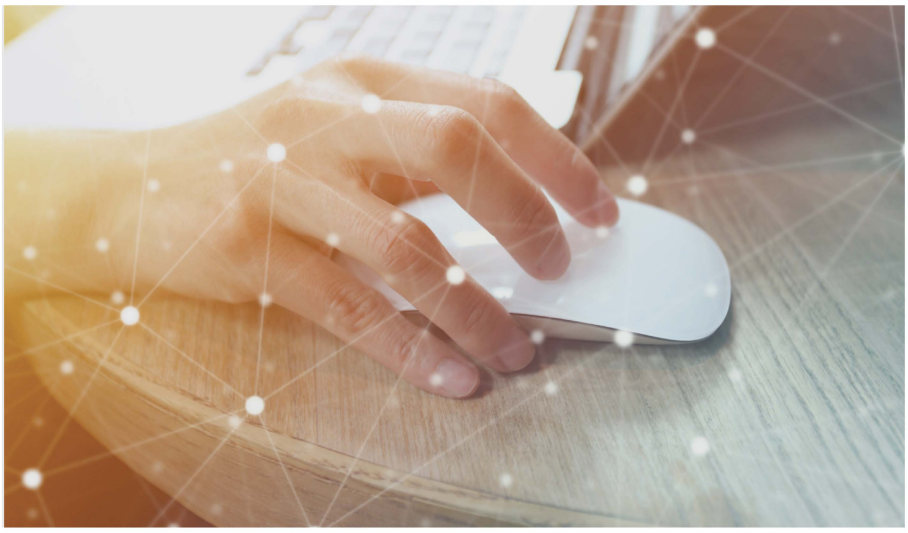
Think Before You Click

June 2020

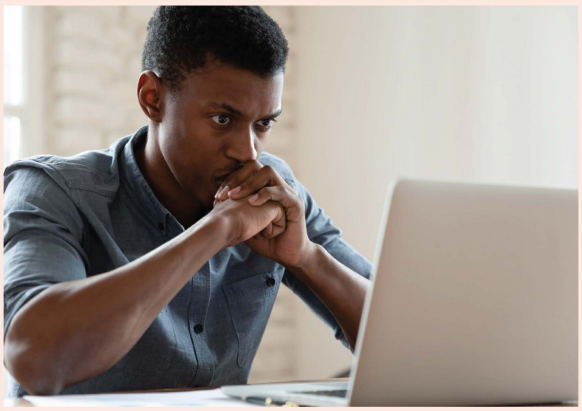
continued from previous page

Want a Few Tricks?

- **Configure Your Email.** In your email account, configure the settings so they display the sender's email address and not just their display name. This will help you verify that the sender's email address is legitimate.
- **Plug-in Assistance.** There are some plug-ins you can use in your internet browser that will display a URL's true path. You might consider enabling that security feature in your internet browser's security settings.
- **Hover to Discover.** You can put your cursor on top of a link (be careful not to click!) which brings up the actual path it is going to. Does the destination of the link align with what you would think? If it doesn't look legitimate, *do not click*. Immediately delete the email.



- **What are They Hiding?** Often, hackers will use shortened URLs to make a malicious link appear safe to click. If you receive a short URL that you can't trust, you can just delete the email or text message and go to the company's main site to access whatever deal or event you're trying to access.
- **Install Anti-malware & Anti-virus software on all devices.** You can even install it on your phone. This will add an extra layer of protection, though it won't replace you needing to be cautious and vigilant.



What is Malware?

Malware, short for "malicious software," includes any software (such as viruses, worms, spyware, adware and ransomware) that is installed on your computer or mobile device. It is most commonly used to give attackers access to your infected computer and can damage it, destroy it, or lock you out.