DON'T GET HOOKED!

WHAT IS PHISHING?
Phishing is a psychological attack used by cyber criminals to trick you into giving up information or taking an action. Phishing originally described email attacks that would steal your online username and password. However, the term has evolved and now refers to almost any message-based attack. These attacks begin with a cyber criminal sending a message pretending to be from someone or something you know, such as a friend, your bank, or a well-known store.

These messages then entice you into taking an action, such as clicking on a malicious link, opening an infected attachment, or responding to a scam. Cyber criminals craft these convincing-looking emails and send them to millions of people around the world. The criminals do not know who will fall victim, they simply know that the more emails they send out, the more people will respond to the opportunity to hack. In addition, cyber criminals are not limited to just email but will use other methods, such as instant messaging or social media posts.

WHAT IS SPEAR-PHISHING?
The concept is the same as phishing, except that instead of sending random emails to millions of potential victims, cyber attackers send targeted messages to a very few select individuals. With spear phishing, the cyber attackers research their intended targets, such as by reading the intended victims' LinkedIn or Facebook accounts or any messages they post on public blogs or forums. Based on this research, the attackers then create a highly customized email that appears relevant to the intended targets. This way, the individuals are far more likely to fall victim.

WHY SHOULD I CARE?
You may not realize it, but you are a phishing target at work and at home. You and your devices are worth a tremendous amount of money to cyber criminals, and they will do anything they can to hack them. If you are the most obvious target, the cyber criminal may try to trick you into clicking on a malicious link or opening an infected attachment. Even if you are not the most obvious target, the cyber criminal may try to trick you into giving up your password or other sensitive information. If you are asked for your password or other sensitive information, do not give it to anyone unless you are sure it is necessary.

PHISHING INDICATORS
A. Check the email addresses. If the email appears to come from a legitimate organization, but the “FROM” address is someone’s personal account, such as @gmail.com or @hotmail.com, this is most likely a phishing attack. Also, check the “TO” and “CC” fields. Is the email being sent to people you do not know or do not work with?
B. Be suspicious of emails addressed to “Dear Customer” or that use some other generic salutation. If a trusted organization has a need to contact you, they should know your name and information. Also, ask yourself, am I expecting an email from this company?
C. Be suspicious of grammar or spelling mistakes. Most businesses proofread their messages carefully before sending them.
D. Be suspicious of any email that requires an immediate action or creates a sense of urgency. This is a common technique to rush people into making a mistake. Also, legitimate organizations will not ask you for your personal information.
E. Be careful with links, and only click on those that you are expecting. Also, hover your mouse over the link. This shows you the true destination of where you would go if you clicked on it. If the true destination is different then what is shown in the email, this is an indication of an attack.
F. Be suspicious of attachments. Only click on those you are expecting.
G. Be suspicious of any message that sounds too good to be true. No, you did not just win the lottery.
H. Just because you get an email from your friend does not mean they sent it. Your friend’s computer may have been infected and their account may be compromised. If you get a suspicious email from a trusted friend or colleague, call them on the phone.