Email Safety Tips

Ever since email was created, cyber criminals have devised all sorts of tricks to get unsuspecting recipients to fall for a variety of scams. Even though most of us are aware of the "prince" in some far away land wanting to give away millions of dollars, scammers are now using more convincing ways to gain our trust and obtain sensitive information. In today's unstable global environment, it's even more important to pay attention and take great care when receiving and replying to emails. I would like to go over what these scams are and several tips to help determine if an email is safe or about to compromise you, your family, or workplace.

Phishing

Phishing is when the sender tries to trick the recipient into revealing a username, password, credit card number, or other sensitive information. They disguise themselves as reputable companies, friends, family, and even college presidents. Sometimes they make it sound like it's an emergency and you have to react right away, and some just sound too good to be true. Whatever scam they use, their objective is to gain your personal information. Once they have this information, they can pose as you and access your accounts and/or services, such as email.

Viruses, Ransomware, & Malware

Viruses attack the recipient's files or computer and make them unusable. They usually come as an attachment, but they can also come from following a link in an email. Ransomware is similar to a virus but typically gives the recipient a way to contact the sender in order to retrieve their corrupted data. They usually supply an 800 number or email and ask for money, Bitcoin or other type of ransom. Malware, like viruses and ransomware, is deployed in a similar fashion, but is more difficult to detect. Once the computer is infected, malware can secretly obtain sensitive data from your computer and/or network, and secretly send it back to the attacker without your knowledge. That data can be financial or healthcare records, email details, and even passwords. All three of these infections can cost users, their families and workplaces thousands of dollars' worth of damage. It's worth noting that all three of these infections can come from an external source such as a thumb drive, external hard drive, or CD/DVD and are not solely sourced from the Internet or other network resource.

What Can You Do

Being able to identify a suspicious email is key, so let's go over some tips to help you identify them. Recently, YCCC has implemented at the top of every external email a statement that looks like this:

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

An external email is any email that is not from a YCCC student, faculty or staff. All the Maine Community Colleges, Brightspace, LibAnswers, and RAVE are also included in this safe list since you may receive multiple emails from them. All others like Amazon, YouTube, Gmail, etc. will have this message in the yellow box appear at the top of the email. When you see this message, it doesn't mean the email is dangerous, but it is your first clue to look more closely.

Take a look at the "From, Sent, To, and Subject" lines. Is the email from someone you know? Were you expecting it? Is it sent to you or a group? Does the subject pertain to you? These are all questions to ask yourself; if something doesn't look right, it probably isn't.

Next, look at the message itself:

- Are they asking for something out of the norm? Are they rushing to have you do it?

Email Safety Tips

- Is the grammar questionable? Many times scams come from outside of the US and the sentence structure is not correct or sounds odd.
- Are they asking for financial information or a payment up front? This is a sure sign of a scam.
- Is there an attachment? Where you expecting an attachment? Attachments as well as links in the email can lead to a virus, ransomware, or malware.
- Are they asking for your username or password? If so they are trying to obtain your information to login as you.

REMEMBER, YCCC will not ask you for your username or password, nor will it have you click a link to reset any of your accounts, such as email.

Passwords
Another good tip is to use strong passwords. We all have many passwords for many accounts, so we tend to use passwords that are easy to remember. Personal information and short passwords are the easiest to crack, and these are usually a minimum of eight characters. An eight character password can be cracked in a couple of hours, so the longer the password, the harder to crack it. Special characters mixed in a long password makes it very difficult to crack. A 14 character password with special characters can take years to crack or even guess. For example, think of a phrase that only you know and mix in some characters.

Pass Phrase Idea: *Swimming is great*
New Pass Phrase: *$wimming1sGreat!*

Updates
Keeping your computer, software, and virus protection up to date is critical! When these items are out of date, you are possibly revealing vulnerabilities for a hacker to exploit. Always check that you have the most recent updates.

Remember the IT Department at YCCC is here to help, so when in doubt contact us. We will gladly answer your questions and look at any suspicious emails or activity.