Beware of Scammers/Phishers

Whenever large-scale events occur, such as the emergence of COVID-19, there will always be people looking to take advantage of the situation. One of those groups is scammers/phishers.

By utilizing phone, email or social media, scammers will attempt to prey upon your heightened emotions. Although cybersecurity experts will always be monitoring the climate as it unfolds, the speed at which threats can change makes users an invaluable resource in stopping potential threats from turning into a security compromise.

With that in mind, here are some things we would like you to be aware of:

- Work email and personal email sometimes have different protections put in place to protect the business versus the individual. If your employer utilizes “external email” tags, URL tracking and additional scrutiny on attachments, those measures alone won’t always stop threats from breaching your system. On any email client, paying attention to a few key pieces of an email can provide a solid perspective on the legitimacy of the email.
    - Is this the first time this person has emailed you? New contacts aren’t necessarily inherently bad, but merit extra attention.
    - Are there spelling/grammatical errors? Not every email contact has the same native language as you, but this can be an indicator of a potentially malicious email.
    - Is the email personalized to you, or just a generic email? A mass email isn’t a bad thing, but sending out phishing emails en masse increases the probability of someone clicking on a link or opening an attachment.
    - Is the email asking for you to do something that is time sensitive that doesn’t seem right? Deadlines can exist, but if it’s around something that doesn’t seem important, or is an unusual request, that is something to be aware of.

All of these things shouldn’t be looked at in a bubble and should be considered as indicators to lead to an overall assessment of whether an email is legitimate or not. If you are unsure, it is always best to err on the side of caution and reach out to the sender via a phone number that you already have for them, or one found online at a reputable website. Do not use a phone number from the email that you are unsure of.

- Even with a shift in communication to be more electronic, phone calls will continue to be a source of compromise. People tend to ask leading questions over the phone and provide just enough information to prompt you to inadvertently provide the rest of the information. If scammers are able to glean a little bit more information from you than they had previously, they can now use the new information, coupled with your name, to engage someone else and gain even more information. If you receive a phone call and something seems off, ask for their extension and tell them you will call them back via their main line. Then go online and find the contact number for that organization and use the extension provided. If they become upset with you for attempting to confirm their validity, that should be an indicator that they may not be who they say they are.

- While social media may be a group avenue to share information, it can be also be used to gather information about you and also to share misinformation. Be aware of what you post online and what your privacy policies for that particular platform are. Keep in mind that just because you are secure, if a contact you have doesn't utilize the same level of privacy settings, someone can use them to learn more about you than you intended. Along the lines of misinformation, stay critical of social posts, and attempt to vet the legitimacy of them via another, independent source. Things like the World Health Organization supposedly conducting an informal survey into the cleanliness habits of US citizens may not be legitimate, and by clicking on the article you may expose yourself.

If you can take an extra couple of seconds to reflect and analyze before clicking attachments, responding to contacts or acting online, you may end up saving yourself from a potential compromise.