Cybersecurity Considerations

Criminals, cyber threat actors and scammers are leveraging the COVID-19 pandemic to steal your money, your personal information, or both. With so many of us working at home because of the virus, the criminals are hoping to steal our confidential data. Don't let them. Protect yourself and do your analysis before clicking on links purporting to provide information on the virus; donating to a charity online or through social media; contributing to a crowdfunding campaign; purchasing products online; or giving up your personal information in order to receive money or other benefits. Be on the lookout for the following:

- **Fake CDC E-Mails** - Email claiming to be from the Centers for Disease Control and Prevention (CDC) or other organizations claiming to offer information on the virus. Do not click on links or open attachments you do not recognize. Be wary of websites and apps claiming to track COVID-19 cases worldwide. Criminals are using malicious websites to infect and lock devices until ransoms are paid.
- **Phishing E-Mails** – Beware of phishing messages asking you to verify your personal information in order to receive an economic stimulus check from the federal government. Government agencies will not communicate with you via unsolicited emails. Other phishing topics include:
    - Airline carrier refunds
    - Charitable Donations
    - Face cures and vaccines
    - Fake testing kits
    - Clinical Trials requiring personal information
    - Financial Relief & Grant Programs
    - Pandemic Updates
    - Various Stimulus Campaigns
- **Counterfeit Treatments or Equipment** – Be cautious of anyone selling products that claim to prevent, treat, or cure COVID-10. Be wary of counterfeit products such as sanitizing gels, personal protective equipment IPPE), respirator masks, goggles, gowns, etc.
- **Common Brands mentioned** include the World Health Organization (WHO), Centers for Disease Control & Prevention (CDC), Johns Hopkins University, Small Business Administration, Internal Revenue Service (IRS), State \ City Departments of Health and political leaders.

BIT is reminding you to always use good cyber hygiene and security measures. By remembering the following tips, you can protect yourself and help stop criminal activity:

- Double-click on the From: address to confirm the identity of the sender.
- Do not open attachments or click links within emails from senders you don't recognize.
- Do not provide your username, password, date of birth, social security number, financial data, or other personal information in response to an email or robocall.
- Always verify the web address of legitimate websites and manually type them into your browser. Hover over any links in a message to confirm the web address.
- Check for spelling, grammar, misspellings or wrong domains within a link (for example, an address that should end in a ".gov" ends in ".com" instead).
- https://cybersecurity.sd.gov/ and https://phishing.sd.gov/ are good reference resources.

Cybersecurity Considerations

There has been considerable conversations and messages around the use of video conferencing and Zoom. This is not an endorsement of the product, yet if you are going to use it – please be aware of the security considerations to use it safely. Like any piece of software – please take a few minutes to understand the best usage of the tool. If the best practice security settings are not utilized – the meeting / conference can be "ZoomBombed" – somebody else can hijack the meeting and the results can be disastrous. The following information is compiled from the FBI and various state resources.

- In late March 2020, a Massachusetts-based high school reported that while a teacher was conducting an online class using the teleconferencing software Zoom, an unidentified individual(s) dialed into the classroom. This individual yelled a profanity and then shouted the teacher's home address in the middle of instruction.
- A second Massachusetts-based school reported a Zoom meeting being accessed by an unidentified individual. In this incident, the individual was visible on the video camera and displayed swastika tattoos.

Zoom Best Practices:

- **Do not make meetings or classrooms public**. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests.
- **Invite with care. Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post**. Provide the link directly to specific people.
- **Add a passcode** to your meeting, then share that passcode with your guests. Once set, the passcode is required in order to enter the meeting.
- **Manage – Limit screensharing options**. In Zoom, change screensharing to "Host Only."
- Ensure users are using the **updated version** of remote access/meeting applications.
- **Do not use Facebook to sign in**: It might save time, but it is a poor security practice and dramatically increases the amount of personal data Zoom has access to.
- **Do not use your Personal Id** for meetings. Select the option to generate a unique meeting id automatically.
- **Use two devices during Zoom calls**: If you are attending a Zoom call on your computer, use your phone to check your email or chat with other call attendees.
- **Lock the door.** You can close your meeting to newcomers once everyone has arrived. Hosts can click the Participants tab at the bottom of the Zoom window to get a pop-up menu, then choose the Lock Meeting option.
- **Preparation**. Make sure participants have the latest version of Zoom's software, which was updated in January 2020. That update added meeting passwords by default and disabled a feature allowing users to randomly scan for meetings to join.
- **Use your silencer features.** You can disable video for participants and mute an individual or all attendees.

Cybersecurity Considerations

- **Cut out the chatter.** The host can disable the ability to text chat during the session to prevent the delivery of unwanted messages.
- **Consider turning on the "waiting room**" for your meeting so that you can scan who wants to join before letting everyone in.
- If you don't want participants to join/interact before the host enters, **uncheck "Join Before Host**". Set an alternate host if you need a backup host.
- **Disable "Allow Removed Participants to Rejoin**" so that participants who you have removed from your session cannot re-enter.
- **Disable "File Transfer**" unless you know this feature will be required.
- **Disable annotation** if you don't need it.

Make sure you are using the legitimate Zoom.us domain to register your meeting. Here is a graph depicting suspicious Zoom domains registered since January.