Cybersecurity in Uncertain Times

There are so many examples of people and communities coming together to help each other right now, just when it's needed most. Unfortunately, there are also those who will take advantage of the situation and are targeting individuals and organizations alike with cybercrimes and virtual shenanigans.

Watch Out for Phishing Schemes

Phishing is a type of cyberattack that uses disguised email as a weapon, with the intent of getting the recipient to give away sensitive information or download malware. While phishing has been a common cybersecurity threat for several years, the Coronavirus pandemic has seen a related outbreak of COVID-19-related scams in 2020.

To prevent falling prey to these schemes, start by always confirming the sender's identity before replying to email requests, opening attachments or clicking on links. Watch for these red flags in messages you receive:

- Includes a fake invoice or shipment notification
- Looks like it comes from someone you know, but the "from" email address doesn't match their actual email address
- Contains a request to confirm some of your personal information
- Makes a claim that there is a problem with your account or payment information
- Asks you to click on a link to make a payment
- Mentions suspicious activity or log-in attempts
- Includes an attachment that you did not expect
- Contains misspellings in the email address or the body of the email (these may be subtle)

If a message looks suspicious, **do not click on any links in it or download any attachments**. If you have an IT professional you work with, let them know you received a potential phishing email. If not, delete the message without clicking on it or replying to it.

Secure Your Virtual Meetings

With more of us conducting and participating in virtual meetings, the use of virtual conferencing and collaboration tools is on the rise. This opens the door for malicious people to exploit the increased use of these tools. One of the most popular virtual conferencing tools right now is Zoom, and there are a few things to watch for when meeting this way.

- **"Zoombombing"** – Hackers disrupt your meeting and share unwanted content.
  To avoid this:
  - o Allow only the host to share content during your meetings
  - o Require a password for meetings
  - o Don't make your meeting public
  - o Don't allow users that you have eliminated from your meeting to re-join
- **False Zoom links** – Cybercriminals register lookalike domains to get your login credentials.
  To avoid this:
  - o Only join meetings from known contacts
  - o Look closely at the Zoom link in your invitation – it should send you to **zoom.us** and not "zoom-meeting.org" or any other "strange" site.
- **Malware** - Attendees send you a malicious file using Zoom, or any other collaboration tool.
  To avoid this:
  - o Never open up an unexpected file, even from a known contact
  - o Verify via phone if you believe a file shared with you is suspicious
  - o Disable file sharing in your meetings if it's not required

Zoom has responded to these vulnerabilities with new features and settings to help prevent misuse of their software. Requiring passwords and waiting rooms for all meetings and restricting participants to specific domains can help prevent unwelcome participation.

General Security Pointers

While many workplaces have an IT team to help keep us protected from the biggest cybersecurity threats, working from home presents new vulnerabilities to be aware of. Here are a few final pointers to consider.

- **Secure your Wi-Fi access point.** Set a strong password on your home networking equipment to reduce unauthorized access.
- **Don't mix personal and work devices.** Employees should use their work devices to do work and their personal devices for personal matters.
- **Lock your screen when not in use.** Limit the opportunity for someone to access your machine while you're away by locking your screen before you go.
- **Use a Virtual Private Network (VPN).** Working from home means your internet traffic is now flowing over public networks. A VPN creates a private secure tunnel inside of a public connection.

Cybercriminals have more time on their hands now than ever, with many seeking to exploit our thirst for information as we navigate through this public health crisis. We hope these tips and best practices help keep you more secure during the weeks and months to come.