From Our Technology Risk Management Team

You may be using videoconferences to maintain both work and social activities during the Coronavirus pandemic. Popular videoconferencing app Zoom has seen a sharp increase in use — including fake Zoom sites and files used to steal personal information and plant malware. These attacks typically occur via emails containing malicious links or files.

In addition, most Zoom meetings have a public link that, if discovered, could allow uninvited users to sign into other people's calls, usually to share inappropriate information. The tactic is known as "Zoom-bombing" but can happen on other videoconferencing tools as well.

Phishing, Zoom-bombing and other malicious incidents are a rapidly growing threat to unsecured videoconferencing. Some tips to help stay above that fray are:

Meeting hosts should use approved web conferencing services, such as WebEx or GOTO Meeting, and review the audience to make sure all participants were invited. If you do need to use Zoom, at home or for your family, follow these tips to properly secure your videoconference, or really any web conferencing system:

- Generate a random Meeting ID when event scheduling and require a password to join.
- Control who enters a meeting with the Waiting Room feature
- Lock your meeting after it starts.
- To prevent participants from screen sharing, choose "Only Host" under "Who can share?"
- Disable file transfer.

Practicing good Cyber hygiene while working from home

- Be skeptical of unexpected attachments and links in emails and posts. Phishing emails, like those that could contain fake Zoom meeting invitations, often convey a sense of urgency, deceiving claims of familiarity or a request to ignore policy. Please be alert to these red flags.
- Never use your business email address to register personal apps or accounts such as Hulu or WhatsApp.
- Update and maintain your home network's security (remove default passwords from home routers and use a strong password).
- Make sure each of your computers, mobile devices and apps is running the latest version of all the software you use. Enable automatic updates whenever possible.
- Manage your work data and devices separate from your personal ones. Make sure family and friends understand they cannot use your work devices.