May 4, 2020

As an update to our message last month, Cyber-attacks remain a concern during the current pandemic and remote work environments.

We thank you for your continued cyber diligence, including:

- limiting the amount of personal data that you share on social media
- never using your business email address when registering for personal apps or accounts
- updating your devices and programs as patches and updates are available
- **following guidelines for printing from home and data destruction**
- staying alert for Phishing and fraud schemes

What to look for:

In just one week, Google saw more than 18 million COVID-19-related malware and phishing emails **per day** and IBM X-Force reports a more than 6,000 percent increase in COVID-19-related spam.

Be on guard if a message demands an immediate call to action or uses emotional bait such as a financial incentive, fear, or a sense of urgency. The scams include impersonating government organizations like the World Health Organization to solicit donations or to trick users into downloading malware; pretending to have information about government stimulus payments; grocery delivery, and other phishing aimed at remote workers. About 2,000 coronavirus-themed websites are being set up each day.

In the News:

Hacking group attacks IT services firm, Cognizant with Ransomware; Pharmaceutical firms compromised
Cognizant's internal security teams are working with leading cyber defense firms to contain the compromise. Cognizant is one of the largest IT-managed services companies in the world, provides IT services to manufacturing companies, financial services, oil and gas, technology, and healthcare fields.

In the UK, the same hacking group accessed and published the sensitive data from the London-based vaccine test center, Hammersmith Medicines Research. Meanwhile, a California biotech research firm studying COVID-19 is investigating a recent data breach but was able to isolate the source of the attack and restore their business operations.

Gallagher has controls in-place (and has been adding additional capabilities) to account for the risks above however, we appreciate your diligence and reach out if you have any concerns to **Cyber_security@ajg.com**

Zoom on personal devices

In addition to the earlier warnings on Zoom and "zoombombing", the Zoom app is under scrutiny for its lenient settings for security. Case in point, criminals are now selling Zoom exploits that not only allow

someone to hijack or spy on your web conference, but to remotely access anything on your machine. Google and NASA have banned all employees from using Zoom due to the security and privacy risks.

Gallagher recommends meeting hosts to only use approved web conferencing services, such as WebEx, and review the audience to make sure all participants were invited. I've been impressed by Zoom's response to rapidly improve their security posture however, please exercise caution.

As a reminder, if you do need to use Zoom at home follow these tips to help secure your videoconference:

- Control who enters a meeting with the Waiting Room feature.
- Allow only signed-in users to join.
- Lock your meeting after it starts.
- Disable file transfer

Again, thank you for your continued attention to cyber safety as we strive to keep our systems and employees secure from cyber threats and attacks.

We love to hear from you. If you have questions or comments, feel free to reach out to your security team at **Cyber_Security@ajg.com**. Feel free to share this guidance with your clients if you believe it may be helpful.

Thank you,

Robert S. Allen
Global Chief Information Security Officer (CISO)

D 630-228-6647
M 312-952-1405
Robert_Allen@ajg.com