TAG SOLUTIONS
empowering people to transform and succeed

Cybersecurity Tips and Resources for COVID-19

What are some common types of cybersecurity attacks?

- Phishing – many hackers will use COVID-19 or the coronavirus as a way to entice you to open an email. This can include making the sender appear to be someone you know or have the email look like it is coming from a reliable source (i.e. government or healthcare organizations).
- Malware – these are often attached to suspicious emails that reference COVID-19 or the coronavirus, and when you click on this attachment, it unleashed a virus or malware into your network.
- Ransomware – this is the most damaging threat to your business because it involves accessing your network (through malware or an unsecured VPN, among other methods), taking private and sensitive data, and forcing you to pay them a ransom in order to retrieve that data. This is extremely dangerous because you might not receive your data back even after paying a ransom, and you don't know where else that data might be on the internet.

What are the best practices to maintain a secure network?

- Don't click on links in unsolicited emails or open any suspicious attachments at all.
- Use only trusted sites, such as CISA's Coronavirus page, to get reliable and updated information regarding cybersecurity.
- Do not provide any personal, financial or other sensitive information in an email, even if the sender looks familiar.
- Enable multi-factor authentication whenever possible – this will provide an additional layer of security should your passwords become compromised.
- Ensure that your VPN and all essential remote networking tools are patched and fully updated to protect against cyber-attacks.
- Make sure your employees are all aware of the cybersecurity threats they might face and encourage them to report ANY suspicious emails or web traffic to your IT department or cybersecurity team immediately.

What do I do in case of a cybersecurity breach?

- Immediately disconnect your computer from the network.
- Contact your IT department or cybersecurity team right away and let them know how the breach occurred and what information could be compromised.
- Change the passwords on any accounts that share the same password as the one that was compromised.
- In case of any financial information being compromised, notify your bank at once.
- You can also submit information about the breach to the FTC using their Compliance page.