Just because we the business owners are following government guidelines doesn't mean the Cybercriminals are following them too. While we are working to protect our businesses, employees, friends, and family from COVID-19, Cybercriminals are utilizing the global crisis to target businesses. From posing as resources for COVID news and information to calling/emailing business owners are pretending to be government officials offering assistant, we all need to be ready to protect ourselves.

Are you and your team watching for malicious emails? Is your remote access solution secure? The two easiest ways for cybercriminals to get access to your servers/systems is by stealing your passwords from unsuspecting staff via phishing or by attacking an improperly configured or secured remote access solution.

Ask yourself, have you done these things? Has your technology provider?

Backups

1. Is ALL of your critical data being backed up? Servers, Cloud Storage, Email?
2. Does your backup solution automatically backup off-site? If not, are you taking a copy off-site regularly? Have you checked the off-site copies?

Remote Access

1. Does your remote access solution require Multifactor Authentication (MFA)? E.g. You have to provide a code from an authenticator when you login. Not just a username and password.
2. Are the computers you're using to remotely access the office patched and running antivirus?
3. Is your business using Remote Desktop, aka RDP for remote access? Make sure your technology provider clearly understands how to secure remote desktop and that access if behind a secure gateway or VPN.
4. Are you using strong passwords or multi-word passphrases and MFA on as many applications/systems as you can?
5. Avoid open WIFI hotspots and only utilize WIFI networks with WPA2 or WPA3 security.
6. Don't let your children or other family members use your work computer or the computer you use for connecting to the office.
7. When you walk away from your computer, make sure you logout or lock the screen. Hitting Ctrl-Alt-Delete and Selecting Lock Screen or Hitting the Windows Key + L will lock it quickly.

Phishing Attacks or other social manipulation

As always, Cybercriminals are leveraging current events to manipulate and swindle business owners. If you receive emails about COVID-19, business relief loans, tax returns, or other related items, be very cautious and do your best to verify the authenticity of the emails. These types of phishing attacks are crafted to manipulate you into clicking links or opening attachments that look safe but are in fact malicious.

A COVID-19 or related Phishing email may include:

- Fake links that appear to go to government sites.
- Links to maps showing infection rates or other statistics.
- Links to government or state agencies with a legitimate name, but a fake hyperlink
- A warning to download a document related to COVID-19
- Links to a hospital or other healthcare institutions

How can you identify a phishing email?

- Hover your cursor over the link, and a pop-up should show the URL the link really goes to. Make sure it matches up with where the link says it is going.
- Carefully check the FROM email address to verify that not just the name on the email, but the address is from the correct sender.
- Once you click a link, make sure it takes you to the site you expected by checking the URL bar at the top of your browser.
- If you click the link and it asks you to login, think twice before entering your credentials. Is this an Office365 login on a random site? Does what the site is asking for make sense? Don't just blindly login.

If you have questions or concerns, contact N-Tech Consulting at 855-711-6601 or https://ntech.io/contact.