THE FIVE WARNING SIGNS OF AN INSECURE NETWORK

...THAT MOST CEOS FAIL TO LOOK AT.

Save this list somewhere you'll see it and review it AT LEAST once a month.
Consider attaching this list to the side of your monitor to keep it top of mind. Make absolutely certain YOUR organization can identify these security shortcomings by answering the following questions:

1. **Have you ever experienced a breach, ransomware, or data loss?**
   Lightning never strikes twice, right? Wrong. In cybersecurity, **hackers always come back to their victims.** Why? Hackers identify their past victims as future targets. In their eyes, your organization is an easy mark. They already have a playbook from the first time they attacked you; why not come back and see if there are new opportunities? (Sometimes, they even leave backdoors to make the return visit even easier.)
   ○ YES ○ NO

2. **Can you log in to your business email or network without being prompted for an access token on your phone?**
   Are you prompted for multifactor authentication when you access critical business assets? Hackers are constantly trying to bypass your security, and **one of the best ways to do that is to get one of your team member's passwords**. If you aren't being prompted for an access token when you log in with your password, not only is your data is vulnerable, but your entire business is at risk.
   ○ YES ○ NO

3. **Is spam and unwanted email constantly appearing in your mailbox?**
   You probably already know that 91% of cyberattacks start with a phishing email. Did you know that **1 in 5 users click on phishing links**? We both know that *you'd* never fall for a phishing attack, but what about one of your crazy-busy employees? Would someone else on your team click a malicious link?
   ○ YES ○ NO

4. **Are you getting lots of warning messages or popups?**
   Many businesses are just depending on antivirus to protect them, and guess what? Today, **antivirus isn't enough.** If you are seeing a bunch of pop-up messages or warning messages, you already have a problem. Chances are high that you've already been breached.
   ○ YES ○ NO

5. **Are you allowed to go to any website you choose with your work computer?**
   Have you ever been blocked when attempting to follow a link? Tricking users into clicking malicious links is the easiest way for an attacker to get into your network. Research has shown that one in five employees will click malicious links in email messages. Blocking those links is a critical component of an effective security program.
   ○ YES ○ NO

If you answered YES to any of the questions, or are not 100% sure your security is completely protecting you, **schedule a third-party assessment immediately.**

Contact us at:

(205) 408-0600

computer assistance program CAP I.T.®