10 Cyber Hygiene Tips for Small and Medium-Size Businesses

Cybercrime can pose a significant risk to any business – regardless of size. That's why it's better to be proactive than reactive when it comes to your protection. Below is a list of 10 tips that will help keep your business safe from cybercrime.

1. **Require Complex Passwords:** Regardless of whether they are for business emails, server access, POS system, or reporting, passwords should always require upper- and lower-case letters, numbers, and special characters. Don't allow passwords to be fewer than eight characters, but longer is better.

2. **Install Anti-Virus Protection** (or Endpoint Detection and Response for medium-larger businesses): This should be installed on every computer, including servers. Make sure to password protect it and set it to update automatically to ensure it remains current. Only an administrator should have access to change it or turn it off. Current reviews can be found online from reputable technology sources.

3. **Educate Your Employees on Email Safety:** Train employees to not click on attachments or links of unknown origin – or even those coming from known contacts if they reference topics that were not previously discussed (e.g., "regarding this invoice"). If in question, train employees to call the contact after looking up the phone number or using an internal contact phone list (as opposed to calling a phone number listed on the suspicious email) and confirm email legitimacy. Ongoing education and reminders are important to keep email safety top of mind.

4. **Update Your Computer Operating Systems:** Keep your operating system updated and ensure that third-party apps like Adobe Acrobat and Java are updated/patched. There are some lower cost tools that can help keep software updated by automating the process.

5. **Create an Incident Response Plan:** Have at least an informal plan immediately available to provide guidance on what to do if your systems are attacked. Include an internal response team – key people that need to know – as well as entities you will need to contact such as Wind River Financial, local IT help, law enforcement, legal, etc.

6. **Consider a Cyber Risk Insurance Plan:** Explore the costs of purchasing a cyber risk insurance policy. You may find a policy that fits your business goals. Your commercial insurance provider should be able to assist with this.

7. **Add Multi-Factor Authentication (MFA):** MFA requires users to provide two or more verification factors to gain access to an application. An example may be username and password plus one or more additional factors, such as a code that has been sent via text message. Adding MFA to accounts you access is usually very quick and simple. However, setting up MFA for remote access your network may require IT support but is critical in today's environment.

8. **Backup your data**: Having backups for your critical data is highly important. In the event of ransomware getting into your network, having a sufficient backup provides your business with options for restoring data as opposed to being forced to pay a hefty "ransom" to cybercriminals in the hope they will unlock your data. Because attackers are also using methods to try to get their ransomware into backups as well, a backup strategy to help avert this is important. Techniques such as offline backups, immutable backups, and encrypted backups can help. Your IT provider should be able to make recommendations based on your business needs.

9. **Install Firewalls:** The size and complexity of a business will dictate the type of firewalls you need, but firewalls should always be in use. For smaller businesses with just one computer connected to the internet, you may be able to get by with the firewall on your router in conjunction with enabling the firewall on your computer's operating system or one that is included with an anti-virus product.

   Larger, more complex businesses will likely need a firewall hardware appliance that sits between the internet and other networking hardware such as switches, servers, etc. Someone who understands firewall settings should review the settings at least once per year to help ensure they are set to the desired attributes of the business.

10. **Email Security Tools:** Consider using email security tools that scan attachments and overwrite links in emails to a sandbox/virtual environment where they can be opened safely without causing damage or exposing the user's computer to actual malware. Phishing is the number one way in which attackers initially gain access to computer networks as employees open attachments or click on links they shouldn't. Additional security around email can be well worth the additional cost.