you can do to ensure that your system remains secure and out of the hands of criminals.

Mary Girsch-Bock • Feb. 09, 2022

As hackers become savvier, and ransomware attacks cripple more businesses, it's more important than ever before to keep your electronic devices safe.

Data security is essential for any business, but as a CPA firm, not only must you keep your own data safe, but your also responsible for keeping your client's personal information protected from hackers as well.

There are a variety of tools on the market such as antivirus software and malware that can help protect your system from intrusion. But there are many other things

not interested in obtaining your client's data illegally, they just want to cause trouble.

3. **Ransomware:** Ransomware attacks have increased in recent years as more hackers seek to profit from their criminal activity. In a ransomware attack, malicious software is used to infect the computers of a business or organization, taking control of the computer and restricting user access until a ransom has been paid.

But it's not only hackers who can pose a threat to your data. Disgruntled former employees can also wreak havoc on an unprotected system. And careless acts such as leaving a laptop or computer unattended, particularly in public places, can threaten your data as well. Here are 5 ways you can keep your computers and your valuable data safe.

1. **Provide sufficient security training to staff**
   Training should include basics such as how to create a strong password, as well as how to recognize suspicious emails. If you have staff working remotely, they should also be schooled in how to keep data safe on their own devices. Remember to create a password for any electronic device that is provided to your employees, and make sure that passwords are changed regularly.

2. **Install anti-virus and malware on all systems**
   All computers in your office and at your employee's homes if they work remotely, need to have anti-virus and malware installed on their computers. It's also imperative that the software be kept up-to-date. Viruses can change by the minute, and if you don't have the latest protection, your system can be easily infected.

3. **Create and use multiple access levels**
   One of the most important things you can do to keep data safe and keep confidential records off-limits is to create multiple access levels for your employees. It's also important that any employees that leave the business are immediately removed from the system and access levels deleted.

4. Consider email attachments suspicious

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

detail such as answering a security question or entering a code that is texted or emailed to the person trying to log in. While many consider two-factor authentication tedious, it's a good way to protect your network from outsiders.

With the amount of sensitive data that can be found in a CPA firm, your firm is a good target for online criminals. And with cloud computing becoming standard operating procedure in most offices, it's essential that the proper safety measures be put in place to keep data safe from hackers and other unauthorized individuals. Taking the proper security measures will protect both the integrity of your business and your client's data. Be sure your security measures are up to date.

Firm Management