10 digital safety tips to keep customers safe.

So much of our world has moved online. Where businesses once kept physical files, held papers with customer information, and sent payments through the mail, much of these operations are now managed digitally. While our current systems are more efficient and, in many ways, more secure, the digital world comes with its own safety threats.

That means business owners have added responsibilities. Cybercrimes are threatening consumer data at new levels, and businesses should implement digital safety tips today to build better protection for tomorrow.

Not sure where to begin? Follow our 10 digital safety tips.

1. **Create a cyber security plan.** The first step in better protection for your business and customers is a cyber plan. This plan should help detect and protect against cyber security threats like ransomware, machine or account hacks, data breaches, and more.

2. **Know your vulnerabilities.** Take a step back and think: What areas of my business are most essential to keep operations running smoothly? When was the last time you added protection or updated security in those areas? Identifying your key vulnerabilities can help you build proper protection and guard weaknesses. In addition, always assuming you are vulnerable can help you think ahead and stay on guard.

3. **Implement complex passwords.** These passwords should be strong and unique, and all team members should be trained in complex password utilization. Find ways to make your passwords more secure with these eight password safety tips.

4. **Protect physical devices.** If clients or customers frequent your business, safeguard your devices with passwords only your team members know. Adjust the lock time on computers so they don’t stay open when team members walk away, or instruct team members to password-protect screens when they step out. Screen protectors can also be effective at keeping

information secure from all angles.

5. **Use multi-factor authentication.** The more steps there are in the authentication process, the more secure customer information will be.
6. **Move items to the cloud.** If customers fill out physical information or paper files are kept on hand, consider moving this information to the cloud and forgoing physical files. Doing so will protect against theft, building fires or floods, or wear and tear. And, when you build the right protection around information on the cloud, it’s far more secure than physical documentation.
7. **Guard your Wi-Fi.** Keep your guest Wi-Fi network separate from your employee network. Use strong passwords for networks and hide your team’s network from unauthorized users if possible.
8. **Be careful what you click.** To keep viruses and cyberattacks at bay, team members should be wary of websites that aren’t secure or email links that look suspicious or are from unknown senders.
9. **Test your team.** When team members fall for phishing scams, it can put customer and business data at risk. Give employees information on what to look for and avoid. Some companies even implement phishing tests where they send test scam emails to their team and encourage them to report the communication.
10. **Keep improving.** Digital safety isn’t a one-time fix. In fact, it’s important to continue adapting your safety practices as scammers adapt their tactics. The best cyber hygiene comes from following these digital safety tips, running internal audits for safety, and continuing to improve your safety strategies.

After you’ve implemented these digital safety tips, talk to a local, independent agent about your business protection and supplemental coverage options.