

✓ **Recognize What You Have is Valuable**

Even the smallest insurance agency has information that is valuable to cybercriminals. You work with details about people's homes, health, and financial status. You constantly gather information about clients and prospects to help them make the best decisions about their coverage. All of this information is information that a criminal may want to collect – recognize that you have valuable information and need to keep your security tight.

✓ **Keep Your Virus and Spyware Protection Updated**

It may seem simple, but just one small virus can bring down a whole website or send information to a hacker. Ensure all company devices are equipped with antivirus software, have automatic updates enabled, and are scanned regularly to ensure there are no viruses in your system. When building a website for your insurance agency, ensure all pages are protected by a security application – not just pages with financial information.

✓ **Train Your Employees Well**

Having thorough and continuous employee training can help your team identify issues and work with information in the safest way possible. For example, employees should not store any documents with sensitive information on an unsecured computer or drive. Also, ensure employees know they're acting safely when interacting on social media sites.



Keep Passwords and Payments Secure

One stolen password is an easy entry point into your insurance agency's computer systems. Ensure you have a company policy that ensures your employees use complex passwords. When employees make online payments, make sure they don't use the same computer to download from the internet. Password safety is just as important when downloading free things as well.

Do Your Due Diligence After An Attack

If your agency is unlucky enough to fall victim to an attack, make sure to contact the proper authorities and resolve any problems that caused the data breach. This can prevent future attacks.

Here are some steps you need to take post-attack:

- *Talk with the relevant law enforcement agencies*
- *Talk with your lawyer and communicate with your customers about the breach and the next steps*
- *Report fraud to the Federal Trade Commission*
- *Report any stolen personal or financial info to the Internet Crime Complaint Center*
- *Talk with US-RECT about any computer vulnerabilities*
- *Work with your web host and web designer to fix and problems that could have leadled to the breach*
- *Rebuild your reputation and let customers know you are going to work to ensure this will never happen again*