

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

ACCOUNTING

Five Easy Ways to Keep Client Data Safe

Your clients have put your trust in you and your firm. Make sure that you're offering the proper safeguards for keeping their data safe.

Mary Girsch-Bock • Sep. 28, 2022



Your clients trust you to prepare their tax returns and advise them on sensitive financial topics. They also trust you with data that needs to be properly safeguarded

against online criminal behavior. There are actually a lot of things that you can do to ensure that confidential data remains confidential, with many of the suggestions, such as shredding all paper documents, easily accomplished. But there are other ways to safeguard firm data and to keep it out of the hands of criminals.

1. Install the proper safeguards

These safeguards include both anti-virus software and malware scanners. Both are designed to identify and stop threats to your computer system before they happen, and both are necessary to keep your data secure at all times.

2. Provide the necessary training to all team members

Your staff are accountants, not IT people, so they may not recognize a threat when they are presented with one. Keeping everyone up to speed on the latest threats can help keep your company data safe. A good idea is to have all employees go through some initial training as part of an employee onboarding process, with a refresher course taking place at least every six months, since threats change and evolve quickly.

3. Use complicated passwords

This goes for everyone that has access to a computer. Set parameters for passwords, such as making them a certain length. It's also helpful to require symbols, lower case and upper-case letters, and numbers. While many of us tend to create passwords that are easily remembered, the more complicated the password, the less likely it is to be guessed by online criminals. But even a complicated password may not be enough (see #4).

4. Require multi-factor authentication on everything that requires a password

Today, it may not be enough to use a complex password. That's why multi-factor authentication is a great idea. Multi-factor authentication requires you to input a passcode that is delivered through an outside system such as your cellphone or email. This helps identify the person attempting to access the system. On a side note, multi-factor authentication has saved me several times when hackers gained access to my apps using a stolen password. It may save you from a potentially catastrophic data breach as well.

5. Manage application accessibility

Managing application accessibility should start with the onboarding process. Remember, not every employee needs or should have access to all applications. Properly managing application access also means that terminated employees need to have their login and password privileges revoked once they leave.

There are other ways to keep your data safe from hackers, including using an online portal to communicate with your clients. A secure online portal allows you and your clients to share sensitive information, eliminating the need to share confidential documents through less secure means.

Your clients have put your trust in you and your firm. Make sure that you're offering the proper safeguards for keeping their data safe.

Accounting • Advisory • Firm Management • Technology

CPAPA is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.

© 2023 Firmworks, LLC. All rights reserved