

Online Data Security For Accounting Professionals

How to protect your clients' data and stand out from the competition

A GUIDE BY REWIND.IO



Contents

INTRODUCTION	3
STEP ONE: SECURE YOUR PASSWORDS	4
— BEST PRACTICES FOR PASSWORDS	5
— USING A PASSWORD MANAGER	6
STEP TWO: TWO-FACTOR AUTHENTICATION	7
STEP THREE: 3RD PARTY APP INTEGRATIONS	9
— HUBDOC CASE STUDY	10
STEP FOUR: BACKUP YOUR QBO DATA	11
STEP FIVE: USE A VPN CONNECTION	14
STEP SIX: SPREAD THE WORD	16
CONCLUSION	17

Data Security as a Competitive Advantage

Automation is the most commonly cited trend in the cloud accounting industry that will help your “firm of the future” to stand out from the rest.

But one competitive advantage that’s often overlooked is your data security practices.

Most young business owners won’t even engage with an accountant or bookkeeper if they do not offer a cloud-based solution to help manage their finances. And yet, **data security continues to be the #1 concern for cloud users**, as reported by Klein Perkins in their 2017 Internet Trends Report¹.

Your clients are trusting their financial data in your hands and in the cloud accounting software of your choice, but they want additional assurance that it will be kept safe.

So what can you do to increase data security in your firm, and position yourself as the most reliable choice for your target clients?

Establish a data security policy in your firm - even if you work alone - that starts with:

1. Secure passwords
2. Two-factor authentication
3. Vetting 3rd party apps
4. Backing up QuickBooks Online
5. Using a VPN connection

In section 4, we’ll go into why you need to backup company files that are in QuickBooks Online, since most people don’t realize that even data in the cloud is susceptible to data disasters.

Changing the way you and your teammates approach data security might not happen overnight. But once you take these simple steps, you’ll never look back. Your clients’ data will be significantly more protected from data loss and data breaches. As a bonus, you’ll be able to use your data security knowledge as a competitive advantage.

1 Meeker, M. (2017). Internet Trends 2017 - Code Conference. Published by Kleiner Perkins.



— STEP ONE

Secure Your Passwords

A weak password, or reusing the same password for multiple accounts, is the biggest security risk for online accounts. To be clear, we're not just talking about a hacker making a guess at your password using personal information (such as your birth date) or trying the most common passwords.

We're also talking about artificial intelligence (AI) becoming increasingly better at guessing passwords. According to Matthew Hutson¹:

"The strongest password guessing programs, John the Ripper and hashCat, use several techniques. One is simple brute force, in which they randomly try lots of combinations of characters until they get the right one. But other approaches involve extrapolating from previously leaked passwords and probability methods to guess each character in a password based on what came before."

Using AI, someone could target millions of accounts at the same time, including yours or your clients'. That's a scary thought.

The good news is that you can protect your business from human or robotic hackers by simply using stronger passwords with these best practices:

¹ Hutson, M. (2017). Artificial intelligence just made guessing your password a whole lot easier. *Published by ScienceMag.org*

Best Practices For Passwords

Best practices for generating strong passwords:

- At least 13 characters.
- A random mix of uppercase letters, lowercase letters, numbers, and symbols.
- Doesn't contain any names of families, friends, or pets.
- Doesn't contain birth dates, phone numbers, postal codes, or other numbers publicly associated to you.

Best practices for keeping your passwords secure:

- Don't ever share your password with other people. If you need to give an employee access to your QuickBooks Online account or any other application, create a separate user account for them.
- It is also not advisable to let your web browsers store or remember your passwords (i.e. Chrome, Firefox, Internet Explorer), since all passwords saved can easily be revealed.
- Start using a password manager for all your online accounts.

Since it's nearly impossible to remember a unique password for every account that you use, most people tend to rely on one or two passwords for all their accounts. This puts them at risk - if one account is hacked, the rest can easily be hacked as well. You really shouldn't be using the same password for your QuickBooks Online accounts as you are for your online banking or email.

For that reason, we highly recommend using a **password manager**.

Using a Password Manager

A password manager auto-generates complex and unique passwords for all your online accounts and provides a secure, virtual vault in which all of your login credentials are saved for when you need them.

Your password vault is locked by a “**master password**” - and as such, is the only password you need to remember.

At Rewind, our favourite password manager and the one our entire team uses is **1Password**, but there are other options, such as LastPass. 1Password integrates with every major browser and mobile device, and allows you to share passwords safely with your team when it's not possible to use a separate account for each user.

As a business owner that's really serious about data security, a password manager is both a requirement and the easiest thing you can do to secure your online data.

As the 1Password slogan says; “Go ahead. Forget your passwords.”



Get a 6-month free membership with 1Password when you use this link to signup:

<https://start.1password.com/sign-up/plan?c=REWIND-K28HTN2S>

Rewind doesn't get any referral bonus or other financial benefit if you use the link above. It just makes us feel better about the security of your data!



— STEP TWO

Two-Factor Authentication

Most online applications, including QuickBooks Online, now offer two-factor authentication as **an extra layer of security on top of your password**. It's also referred to as two-step verification or 2FA. Even if someone steals your password, they will still need your unique verification code in order to get into your account. This makes it incredibly difficult to hack into your data.

Two-factor authentication works by generating a unique 6-digit code on your mobile device (using text message or an authenticator app), which you enter as a second verification step after signing in. 1Password, which we mentioned above, can generate that unique 6-digit code, but you can also use the free Google Authenticator app.

How to enable 2-factor authentication in QuickBooks Online

1. From your QuickBooks Online account, select the **Security** tab.
2. Select **Turn On** to expand the **Two-step verification** section.
3. Choose to receive the one-time verification code either by text message or voice message and select **Turn On**.
4. Enter the code you received and select **Continue**.

"Software updates often fix security problems, so download updates as soon as they become available."

— CALIFORNIA SBDC



— STEP THREE

3rd Party App Integrations

The QuickBooks App Store gives you access to hundreds of great apps that can help you automate your work, grow your business, and offer a better service to clients. However, you need to carefully vet these 3rd party apps before installing them into your QuickBooks Online accounts.

Remember: many installed apps can read and write data into your company file. This means you're not only giving the app permission to read your data, but the ability to also change or delete it.

All apps in the QuickBooks App Store have been reviewed by Intuit to make sure they meet certain security requirements. But this isn't a guarantee that the app won't cause problems in your account. (See Hubdoc case study on page 10)

Best practices for vetting 3rd party apps:

- Check the app's reviews and ratings.
- Review what permissions the app is requesting - do these make sense for the functionality of the app?
- Is the app developed by a single developer, or a team of developers?
- Does the company have a 1-800 number where you can reach them?
- Have a test account where you can install an app and see how it integrates with your QuickBooks Online file before installing it to your client files.

Hubdoc Case Study

In December of 2017, we saw a great example of how data loss due to a 3rd party app can affect QuickBooks Online customers who don't have their own backups.

Hubdoc is one of the most used and trusted apps for QuickBooks Online. But an incident on their part resulted in the deletion of source documents attached to transactions in some QuickBooks company files.

Since this issue affected a large subset of customers, Intuit stepped in to work with Hubdoc to help recover this data.

It wasn't until February of 2018 - two months after the incident - that Intuit was able to restore some of the documents. But as they reported¹:

"Unfortunately, some of the source documents that were deleted from your QuickBooks Online account during this incident cannot be automatically restored. Recovering them will require you to take some additional steps to find the documents and manually re-attach them."

This incident serves as a great reminder that anytime there's an integration from one system to another through an API, there is the possibility of an error that can result in a major data disaster. In situations like these, a secondary backup is often the fastest and most reliable way to recover lost data.



— STEP FOUR

Back up Your QuickBooks Online Data

The Hubdoc case study brings us to step 4: start backing up QuickBooks Online. That's right - even data that's in the cloud needs to be backed up. This comes as a huge surprise to many QuickBooks Online users, who are under the impression that Intuit will be able to restore any lost data if needed. But that's not exactly the case.

In the Intuit Community help documents, you can read that the answer to "*Does QuickBooks Online backup my data?*"¹ is *yes*. However, this is followed by an important caveat that should not be overlooked: "*we cannot restore your file to a previous point in time.*"

Does Quickbooks Online Back Up My Data?

This article refers to QuickBooks Online

Yes. In addition to always maintaining two copies of your data, we automatically back up your updated data every day. It's stored on firewall protected, redundant servers so your data is safe from hardware and software failures, hackers and viruses. Because we update your records with every change, **we cannot restore your file to a previous point in time.**

What Intuit provides for QuickBooks Online users is a disaster recovery backup. If something were to happen to the QuickBooks platform or their servers, Intuit will try to recover *everyone's* data to the last backup. We like to call this a platform-level backup.

As a user, you don't have access to this backup in order to restore your data. This means that you risk having to manually undo changes or permanently lose data if:

- An app integration causes problems
- You need to unroll a series of changes
- The client made changes without consulting you
- A disgruntled employee deleted items
- An item was deleted due to an honest mistake

QuickBooks isn't unique in this situation. If you look at most cloud vendors (Xero, Shopify, Wordpress, Mailchimp, etc.), users are faced with the same issue.

This is why you need access to your own account-level backups of QuickBooks Online, in addition to Intuit's platform-level backups. It's also the reason why we started Rewind, since we identified this issue with so many cloud vendors.

The second reason why you want to backup QuickBooks Online yourself is to take control of your data. Especially when it comes to highly important data such as finances, having a secondary backup in a different location from the cloud vendor's servers gives you greater control and freedom.

If something were to happen to their QuickBooks Online files, even if it's not your fault, the client will depend on you to help them recover their data. In that situation, you want to have the ability to help your client, instead of waiting on Intuit to fix the situation.

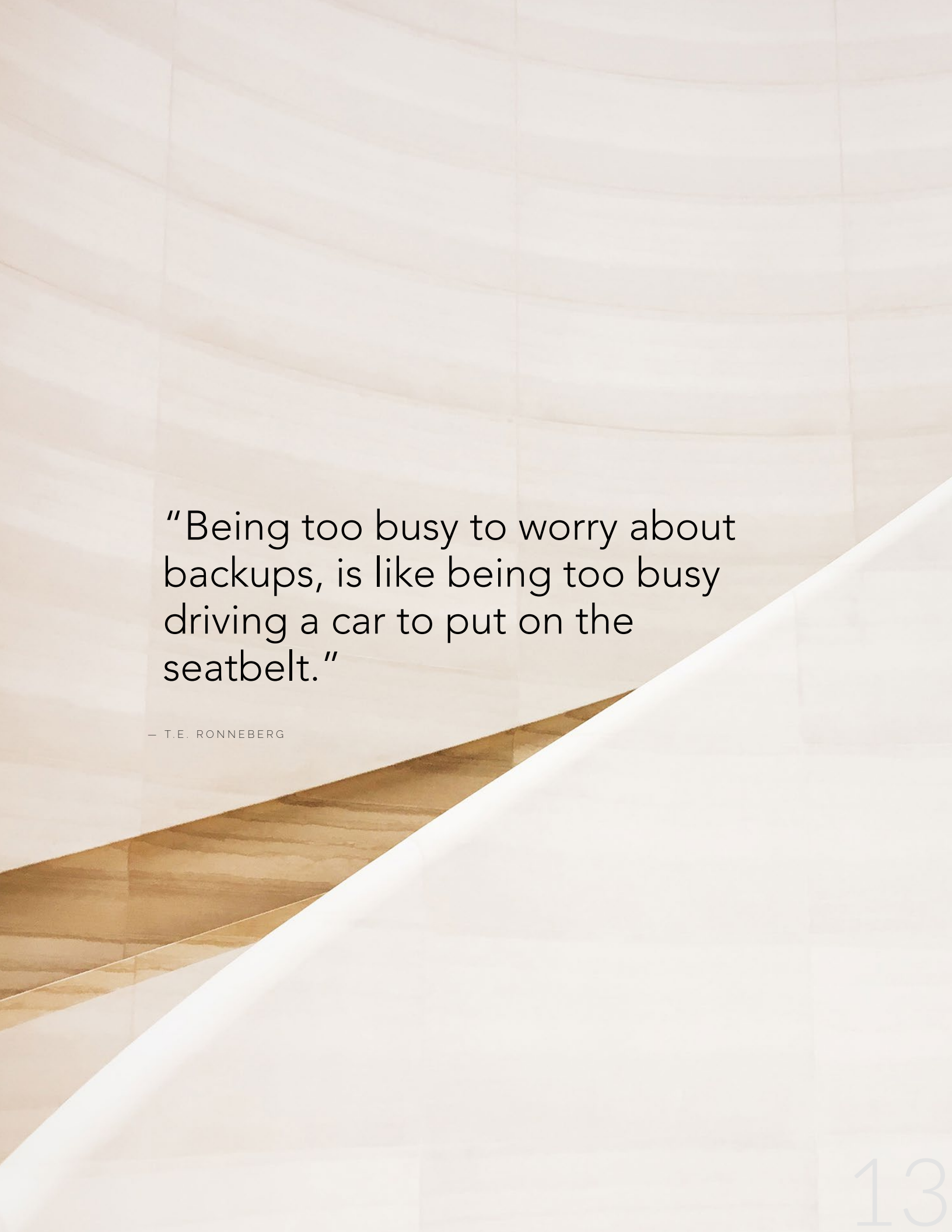
How to Backup QuickBooks Online

The easiest way to backup QuickBooks Online is using **Rewind** since we leverage Intuit's APIs to be able to backup and restore data. With Rewind, you can **automate a daily backup of your company files** and it stores the backup in a separate server from Intuit's, following the best practice of having copies of your data in different locations.

You can set it and forget it until the moment that you need to restore a single transaction or an entire company file or verify what changes have been made in the account.

You can also link as many clients as you want under one Rewind account - keeping their backups separate while making it easier for you to manage.

[Start your first backup at app.rewind.io](https://app.rewind.io)

The background of the page is an abstract composition. It features a grid of light beige squares that are slightly curved, creating a sense of depth. A diagonal band of warm, golden-brown wood grain texture runs from the bottom left towards the center. A large, smooth, white curved shape sweeps across the bottom right corner, partially overlapping the wood grain.

“Being too busy to worry about
backups, is like being too busy
driving a car to put on the
seatbelt.”

— T.E. RONNEBERG



— STEP FIVE

Use a VPN Connection

Many people love to step outside the office and get work done at their favourite coffee shop. Just the aroma of coffee is enough to get you in work mode. As wonderful as it sounds, it might actually be putting your data at risk. Your clients' info on QuickBooks Online, login credentials, banking information, all becomes vulnerable on public WiFis and someone with the right technical knowledge and motivation can easily access that data.

So how can you keep your coffee habit while protecting your data? Use a Virtual Private Network (VPN) anytime you are working remotely. **Having a VPN blocks anyone using the same internet network (even the person managing it) from seeing what you are doing and the data you are working with.**

Benefits of having a VPN:

- **Security:** Your data is encrypted - meaning that if someone gets a hold of your data and online activity, they will see encrypted data, not raw data.
- **Privacy:** VPNs make it extremely difficult to identify your computer as the source of traffic which protects you from tracking. For example, advertisers will not be able to track your activity.
- **Accessibility:** Some content on the internet is restricted based on the location of the viewer. Using a VPN allows you to set your own location (or at least where you appear to be) so you can keep browsing as you do at home while you're travelling abroad.

How does a VPN work?

When you use a VPN software, it encrypts your data before the Internet Service Provider (ISP) sees it. The ISP will, in turn, see your data as coming from the VPN server and its location, rather than your computer.



How do I choose a VPN?

Now that you've got the basics down, it's time to decide which VPN will work best for you. There are five factors you should consider when evaluating a VPN service:

1. **Safety and Security:** The most important factor when looking for a VPN. Investigate the VPN security encryption and privacy policy terms and conditions.
2. **Speed:** Look for a VPN that will improve your internet connection so you aren't waiting for apps or webpages to load.
3. **Compatibility:** You want your data to be secured not only on your laptop but also on your phone! Ensure that the VPN can be used across all your devices.
4. **Accessibility:** A VPN that only works in a limited geographical area will not work for frequent travellers. Make sure the VPN is available from anywhere.
5. **Customer Support:** Setting up a VPN is not always easy, especially if you aren't familiar with its technology. Talking to a support team that is responsive and informative is always helpful!

Here are some VPNs we recommend:

- **TunnelBear:** extremely user-friendly, compatible with all devices, and great price.
- **Hotspot Shield:** offers fast internet speeds, WiFi security, malware protection, and is compatible on all devices.
- **NordVPN:** encrypts your data twice to ensure military-grade data security.

The security of your business-critical data is not something you want to be gambling with. Having a VPN on your work devices ensures that your data will not be compromised by outsiders.



— STEP SIX

Spread the Word About Your Data Security Practices

Once you've put in the work to complete steps 1-4, don't let it go unnoticed. Now is the time to communicate to your internal team, your customer, and your potential customers what you're doing to keep their data safe. These efforts will help establish you as an accounting professional who understands the risks of cloud applications, and is proactive about keeping client data safe.

Some suggestions on how you can start:

- Write a blog post about why data security is important to you, and the changes you've made to increase security.
- Create a page on your website to talk about your commitment to data security. Outline what measures you've implemented to increase data security, and how all employees are trained to follow these practices.
- Discuss data security as part of your sales and onboarding process with new clients.

— CONCLUSION

Taking The Steps Towards Data Security

It might not sound exciting, but the way you approach data security in your firm can either be a deal-breaker or what *seals* the deal for new clients that want the reassurance in knowing you're doing everything in your power to keep their data safe.

The steps outlined in this guide are fundamental in ensuring that your business is protected from data loss and breaches. Luckily, they're also simple to implement with the help of tools like 1Password and Rewind.

As cloud accounting and banking software continues to rise in popularity, more and more clients will turn to their accountant or bookkeeper for advice on keeping their financial data safe. When that happens, make sure you've already established yourself as a data security expert.



Safe, Automatic Backups

Rewind is the leading online backup service for SaaS applications, including Shopify, BigCommerce, and QuickBooks Online. Since 2015, Rewind has been on a mission to help business owners quickly recover their cloud data after a disaster. Thousands of business owners and brands trust Rewind to safely backup millions of items. To learn more, download the Rewind app from the QuickBooks App store or visit <https://rewind.io/>