



# Online Data Security for Accounting Professionals

Stand out from the competition  
by protecting your client's data.

# Table of Contents

	<b>Introduction</b>	<b>3</b>
1	<b>Secure your passwords</b>	<b>5</b>
2	<b>Two-factor Authentication</b>	<b>9</b>
3	<b>Use a VPN</b>	<b>11</b>
4	<b>Audit 3rd part App Integrations</b>	<b>13</b>
5	<b>Back up your back up</b>	<b>16</b>
6	<b>Communicate your data security practices</b>	<b>19</b>
	<b>About Rewind</b>	<b>22</b>

# Introduction

In 2019, one of the world's largest tax and accounting software providers, Wolters Kluwer, [was hit](#) by a massive cyberattack resulting in clients losing their entire infrastructure for processing payments and weeks worth of work. Automation and cloud based services like Wolters Kluwer's CCH iFirm are becoming the norm for accounting professionals, but how secure are these softwares?

Through experiences like Wolters Kluwer's, accounting experts have come to realize that "cloud" and "data protection" are not synonymous.

Now, you might be thinking: doesn't this kind of attack happen exclusively to big businesses? Sadly, the answer is no. Small to medium sized businesses are also becoming targets for these kinds of cyberattacks. Recent data has shown that over [70 percent](#) of small businesses were attacked by cybercriminals.

Data security for cloud accounting is no longer a "nice to have," but rather a necessity for businesses who are looking to engage with an accountant or bookkeeper. Clients are trusting their financial data in your hands and in the cloud accounting software you choose. They also want additional assurance that it will be kept safe.

A [recent survey](#) by Oracle & KPMG showed that 59% of respondents had their login credentials to their cloud tools phished, and 75% experienced data loss on more than one occasion. In 2020 the Federal Bureau of Investigation saw a 400% increase in cybercrime attacks.

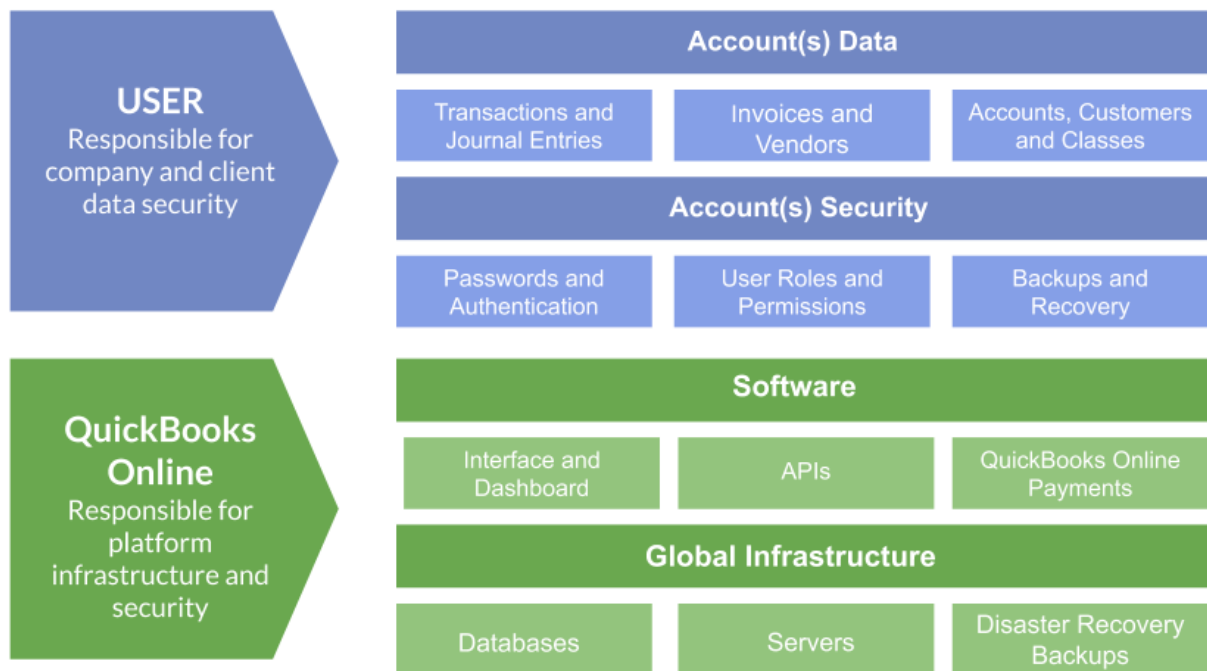
Although risks and threats are increasing along with the use of cloud accounting, the good news is that best practices around data protection are sound and fairly easy to implement.

**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, or at your solo practice, starting with:**

- 1 **Secure Passwords**
- 2 **Two-factor authentication**
- 3 **Auditing 3rd party apps**
- 4 **Using a VPN**
- 5 **Backing up QuickBooks Online**
- 6 **Communicating your security policy**

# The Limitations of the Cloud

You might be wondering: why do I have to protect my cloud data? Doesn't online software already do that for me? Well, when it comes to online software, there's something called the Shared Responsibility Model. In short, this means that keeping your QuickBooks Online account data secure is a shared responsibility between QuickBooks Online and you, the account owner. QuickBooks Online takes care of the software, infrastructure and disaster recovery of the entire platform. You, as the user, are responsible for password security, permissions given to users and third-party apps, and protecting all the data you put into your account.



Most cloud based programs like QuickBooks Online have a backup system that protects them from incidents on their end, but should a disaster strike with your specific account, their systems cannot be used to restore that account back to a previous point in time or to recover just a selection of your data.

We'll help you avoid this kind of disaster in section five.

Changing the way you and your teammates approach data security likely won't happen overnight. But these four simple steps will help you avoid falling victim to online security disasters, including ones that are often overlooked. Your clients' data will be much more protected from data loss and data breaches. As a bonus, you'll be able to use your data security knowledge and policy as a competitive advantage.

## Let's get started.

# STEP 1:

**Secure your  
passwords**



# Secure Your Passwords

A weak password, or reusing the same password for multiple accounts, is one of the biggest security risks 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 world's 25 most common passwords](#).

**We're also talking about artificial intelligence (AI) becoming increasingly better at [guessing passwords](#):**

"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:

### **Best practices for generating strong passwords:**

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

### **Best practices for keeping your passwords secure:**

- ✓ Don't share your password with other people. If you need to give access to an employee to your QuickBooks Online account or any other application, create a separate user account for them.
- ✓ Don't allow your web browsers to store or remember your passwords (i.e. Chrome, Firefox, Internet Explorer) since all passwords saved can easily be revealed.
- ✓ Use 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 since if one account is hacked, the rest can easily be hacked as well. You shouldn't be using the same password for your QuickBooks Online accounts as you are for your online banking or email. This could put your accounts in jeopardy.

For that reason, we highly recommend 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.

One of the leading tools is **1Password**, but there are other options, like **LastPass**. 1Password integrates with every major browser and mobile devices 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 serious about data security, a password manager is the easiest thing you can do to better secure your online data.



# STEP 2:

## **Two-factor authentication**

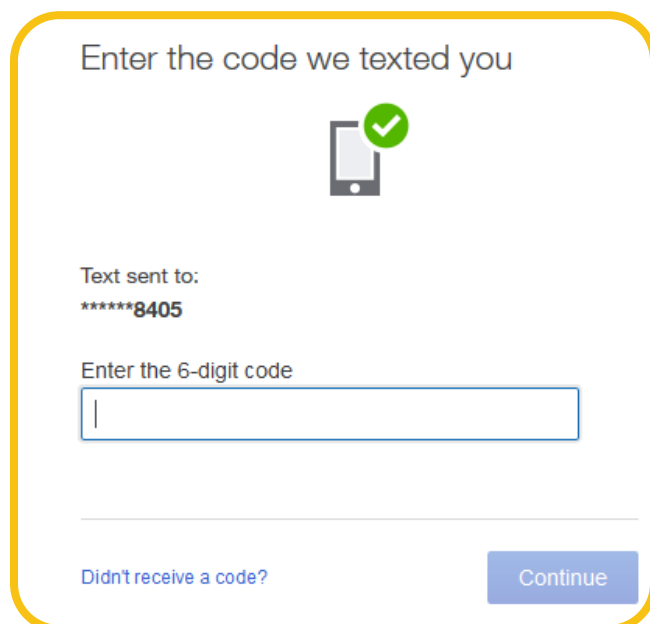


# Two-factor authentication

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. This means that even if someone steals your password, they will still need your second piece of verification in order to get into your account. This makes it incredibly difficult to hack your accounts.

Two-factor authentication often uses a unique code, a secondary email address, or even a fingerprint as the second method of verification. For example, many online apps will send you a unique code using text message over SMS or an authenticator app as a second step after signing in. While it is possible to use SMS messaging as a second factor for authentication, we don't recommend it. This is because SMS is not secure and therefore susceptible to attackers. Instead, we recommend using a secure authenticator app, such as 1Password. 1Password can generate that unique 6-digit code but you can also use the free Google Authenticator app.

## The process would look something like this:



Enter the code we texted you

Text sent to:  
\*\*\*\*\*8405

Enter the 6-digit code

Didn't receive a code?

Continue

## Wondering how to enable 2-factor authentication in QuickBooks Online? Follow these steps:

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**.

# STEP 3:

## Use a VPN



# Use a VPN

In the modern world of remote and virtual work, using a Virtual Privacy Network (VPN) has become the new normal when it comes to security. Working outside of an office comes with its own host of privacy issues, and a VPN can help you avoid some of them.

Using a VPN can help keep your data protected whether you're working in a coffee shop with an open network or at your home office. They accomplish this by encrypting data and hiding your identity. This is especially important when your work includes dealing with client's sensitive financial information.

## When choosing a VPN provider, there are a few things to consider.

Start by reviewing its safety and security policies and make sure that you are comfortable with the outlined terms and conditions. Next, check that it's compatible with your laptop and mobile device. If you work abroad, don't forget to do your research on geographical limitations. For those who are not tech savvy, VPNs with good customer support will help you stay protected. Finally, be sure to consider speed. Some VPNs are faster than others.

This is an excellent step for those who work in offices and need to safely share documents, or even individuals operating their businesses directly out of their home. It's one more step in ensuring system security.

# STEP 4:

## **Audit 3rd party app integration**

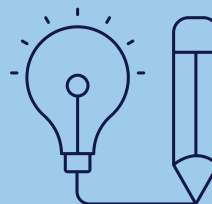


# Audit 3rd party app integrations

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

## Remember:

**Any installed app can read and write data into your company file. This means you're not only giving the app permission to read your data, but they could 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. However, this isn't a guarantee that the app won't cause problems in your account.

## Here are a few best practices for auditing 3rd party apps:

- ✓ Check the app's reviews and ratings.
- ✓ Is the app developed by a single developer (high-risk) or a team of developers (low-risk)?
- ✓ Does the company have a 1-800 number where you can reach them?
- ✓ Install the app on a test account and see how it integrates with your QuickBooks Online file before installing it to your client files.

## When 3rd party apps go wrong

Picture this: In order to help your accounting processes run smoother, you've decided to integrate a seemingly helpful new app with QuickBooks Online. Then, disaster strikes. The new app records billions of dollars of inventory, which is nowhere near the actual inventory numbers. This error has a domino effect on the rest of the accounts, with errors accumulating for weeks on end.

This is exactly what happened to a client of Lynn Marsh, the founder of [HealthyBOOKS](#) Bookkeeping Services. This led to Lynn having to spend about 15 hours cleaning up the books, leaving her [wishing she had a way to easily roll back the data](#).

For Lynn, this was the incident that made her realize a secondary backup for her clients data was needed. When another client called to inform her that they were about to integrate an app with QuickBooks Online, she decided to set them up with [backup software](#) first.

“

Because I had that one experience with the inventory app integration and saw what an unbelievable disaster integrations can cause, I thought 'ok, now's the time.' Now I just set it up for every client that I deal with.

- Lynn Marsh

”



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 could 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 5:

**Back up your  
back up.**

**De-risk your data  
liabilities in the cloud.**





# Store Backups in More Than One Place

Lynn Marsh's experience brings us to step five: 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?" 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.**

But 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 losing 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**

What Intuit provides for QuickBooks Online users is a disaster recovery backup. If something were to happen to the QuickBooks platform or their servers, they try to recover everyone's data to the last backup.

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

## Here's an Example:

[Geni Whitehouse](#), CPA and international keynote speaker, learned this lesson the hard way. Tax deadlines were quickly approaching when Geni learned that the cloud-based software she had been relying on was no longer accessible. After numerous rejected login attempts, she received a notice from the service provider, informing her that the system had been subjected to a ransomware attack. This started a panic: what about her clients' sensitive & critical data? It soon became clear that their online backup systems had been compromised as well. While her team was able to continue to provide monthly accounting services, crucial client working papers were no longer accessible. After a few days of work, Geni was able to solve the problem, but in the process realized that by moving her work to the cloud, she had taken on an even greater responsibility.



“ We assume the cloud has us covered, that's why we're putting it there. ”

**- Geni Whitehouse**

This is why you need access to your own backups of QuickBooks Online in addition to Intuit's disaster recovery backup. Backup softwares like Rewind can help you do this easily, allowing accounting professionals to quickly recover data in the wake of a cloud-based disaster. Whether it's exporting your files manually to a separate server, building your own solution, or buying backup software, it's important to have a strategy in place to help avoid massive data losses.

Without a backup strategy to protect client files, Bookkeepers and Accountants are at risk of permanently losing the data which powers a client's business. And the risks come in a variety of ways; Human error, third-party software integrations and malicious attacks like Ransomware.

# STEP 6:

**Communicate  
your data security  
practices**



# Communicate your data security practices

Once you've put in the work to complete steps 1-5, don't let it go unnoticed. Now is the time to communicate this plan to your internal team, your customers, and your potential customers. 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 promoting your practice as one with a strong focus on privacy and security include:**

- ✓ Writing a blog post about the reason why data security is important to you and the changes you've made to increase security.
- ✓ Creating 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.
- ✓ Discussing data security as part of your sales and onboarding process with new clients.

## Taking the steps towards data security

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 that 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 in turn expect their accountant or bookkeeper for advice on keeping their financial data safe. Make sure you have the answers they're looking for, and the ability to prove that you've already established yourself as a data security expert.





## About Rewind

Since 2015, Rewind has been on a mission to help businesses protect their SaaS and cloud data. Today, over 70,000 customers in more than 100 countries use Rewind's top-reviewed apps and support to ensure their software-as-a-service applications run uninterrupted. The Rewind platform enables companies to back up, restore and copy the critical data that drives their business.



© REWIND 2021  
[REWIND.COM](https://REWIND.COM)