Growing Your Business Thru QuickBooks®

May 2015

Preventing Data Theft in QuickBooks

Be proactive about the security of your QuickBooks company file, and you'll be less likely to encounter data theft.

Thanks to the internet, privacy has been on the wane over the last few years. We assume that our addresses and phone numbers are public information, thanks to sites like Switchboard and 411.com. We *hope* that our dates of birth are private (though the number of birthday wishes on Facebook makes that doubtful), and we assume that our Social Security numbers are hard to get.

Your customers trust you enough to provide you with additional private information, like credit card numbers. And you've seen what an uproar occurs when major corporate entities like Target and Home Depot get hacked.

Your small business may not have hundreds of thousands of customer information files, but you can still be targeted by external hackers and even your own employees. Are you taking measures to ensure the security of that data stored on your hard drive and/or in the cloud?

Your Inner Circle

The last thing you want to imagine is that one of your own employees has been tampering with your QuickBooks company data. It happens, though, and you need to protect yourself from potential internal attacks.

One of your internal controls, then, should include the establishment of boundaries for every employee who has access to QuickBooks. You can restrict each staff member to specific areas of the program instead of sharing a master password and giving everyone free rein. Go to **Company | Set Up Users and Passwords | Set Up Users** to do this.
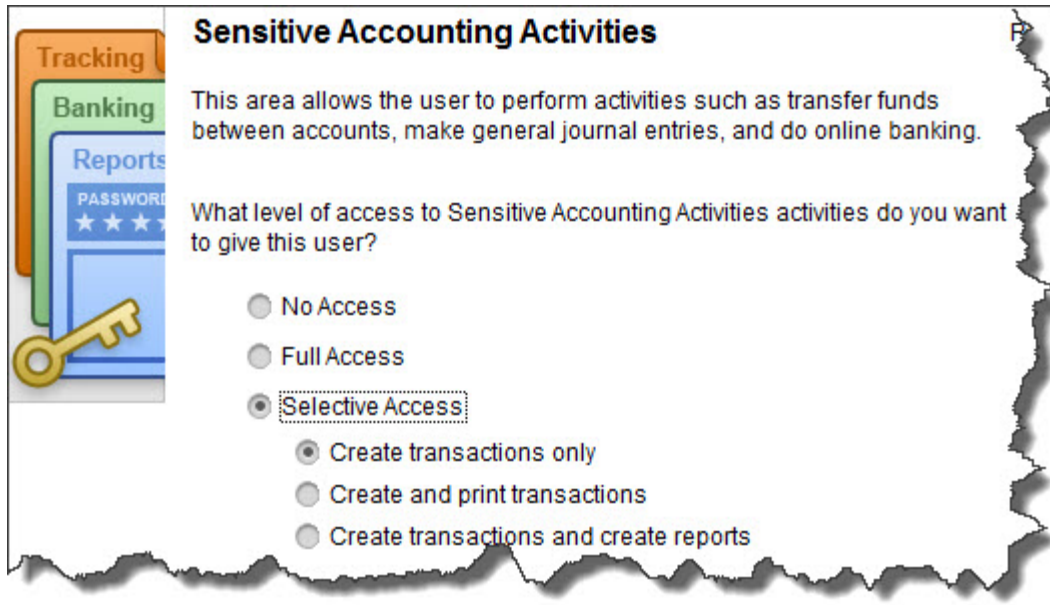
*Figure 1: If you click on **Selective Access** in this window, you can restrict your employees' activities to specific areas and actions.*

The **User List** window opens, which will display all users who have been set up already, including you as the **Admin**. Click **Add User** and enter a name and password. Click the box in front of **Add this user to my QuickBooks license**, then click **Next**. Click on the button in front of **Selected areas of QuickBooks**. Click **Next**.

The next 10 screens break QuickBooks down into separate activities and activity areas, like **Sales and Accounts Receivable**, **Checking and Credit Cards**, and **Sensitive Accounting Activities.** On each screen, click on the button in front of the correct option:

- **No Access**

- **Full Access**

- **Selective Access** (lets you specify what areas and actions will be allowed for that employee)

Other Internal Controls

QuickBooks' **Audit Trail** is your friend. It records everything that is entered or changed in the software, by whom, and precisely when. To view it, open the **Reports** menu, then click on **Accountant & Taxes**, then **Audit Trail**. Like all QuickBooks reports, it can be customized to display the entries you need to see.

Num	Entered/Last Modified	Last modified by	State	Date	Name	Memo	Account	Split	Amount
12/15/19					**Audit Trail** **All Transactions**				
Transactions entered or modified by Admin									
Inventory Adjust									
	12/15/2019 14:35:13	Admin	Latest	12/15/2019		T-10155 Op...	30000 · Opening B...	12100 · Inven...	-249.75
						T-10155 Op...	12100 · Inventory ...	30000 · Open...	249.75
Invoice 1100									
1100	12/15/2019 15:41:53	Admin	Latest	12/15/2019	Melton, Johnny:De...		11000 · Accounts...	-SPLIT-	646.50
					Melton, Johnny:De...	Monthly soc...	40100 · Construct...	11000 · Acco...	-600.00
					State Board of Equ...	CA sales tax...	25500 · Sales Tax...	11000 · Acco...	-46.50

*Figure 2: QuickBooks' **Audit Trail** provides a detailed history of all activity in the software.*

There are other reports that you should review frequently, and some that we should create and analyze for you at least every quarter, if not monthly. We can suggest reports that would help you look for fraud, and tell you what to look for.

Common Sense Practices

- It goes without saying that protecting your entire hardware/software/cloud configuration will help keep your QuickBooks company file safe from external marauders. You must employ state-of-the-art antivirus and anti-malware applications and keep them updated. Talk to us if you need recommendations and/or help implementing them.

- If you're a sole proprietor or you work from your home, restrict the computer where QuickBooks resides to business software and websites only. Never let anyone install applications, play interactive games, etc. on it.

- Change your own QuickBooks password at least every 90 days, and do backups to secure drives or websites.

- When you run into problems with QuickBooks' functioning, please let us help. Even a computer troubleshooting specialist will not understand the program well enough to solve problems, and he or she may compromise your data file further.

As security software and systems get smarter, so do the hackers. Don't let your company and its customers be victims of data theft.