THE QBC
Growing Your Business Thru QuickBooks®

FROM THE OFFICE OF
ACCOUNTING ADVANTAGE
6276 Jackson Road, Suite B
Ann Arbor, Michigan 48103
888 503-6265 • www.AcctgAdvant.com

June 2017

How to Keep Your QuickBooks Data Safe

You work hard to make sure your QuickBooks data is accurate. Make sure it's safe, too.

Your QuickBooks company file contains some of the most sensitive information on your computer. You may have customers' credit card numbers and employees' Social Security numbers. An intruder who captured all that data could create tremendous problems for you and a lot of other people.

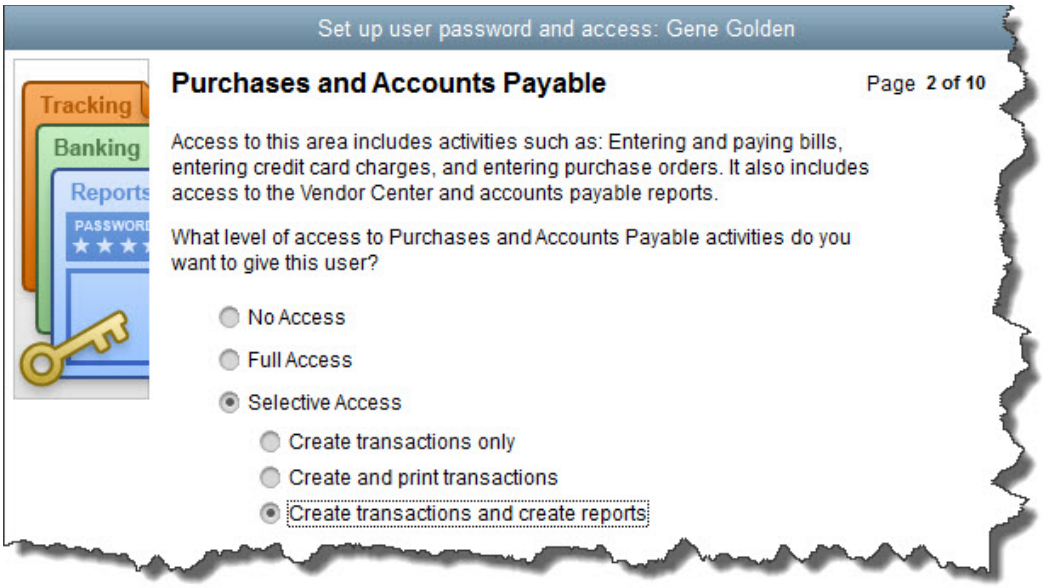
That's probably the worst-case scenario. But other situations could also spell disaster for your business, which involve losing your company data through fraud, hacking, or simple technical failures.

We can't overstate the vital importance of protecting your QuickBooks company file, especially your customer and payroll information. Whether someone steals it or it's inaccessible for another reason, it's gone. Keeping your business going after such a loss would be very difficult – maybe even impossible.

Here's what we suggest to prevent that.

Internal Safeguards

No business owner wants to believe that his or her employees could use their QuickBooks access to commit fraud. But it happens. Your company file contains credit card and checking account data that could be used for nefarious purposes. As we discussed last spring, you can restrict user access to specific areas and actions of QuickBooks.



You can limit your employees who have QuickBooks access to certain areas and activities.

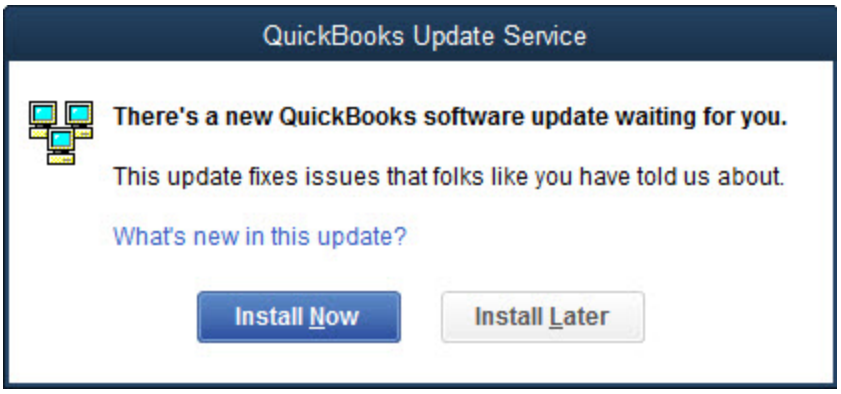
To get started, open the **Company** menu and select **Set Up Users and Passwords | Set Up Users**. The **User List** window opens. It should have at least one entry there, for you (**Admin**). Click **Add User** and enter the employee's name and password in the next window that opens, then click **Next**.

*Tip: Your QuickBooks license limits you to a specified number of users. If you're not sure how many you're allowed, click **F2** to open the **Product Information** page. The number of user licenses you've paid for appears in the upper left.*

On the next page of this wizard, click the button in front of **Selected Areas of QuickBooks**. The following screens will let you define that employee's access permissions in areas like **Sales and Accounts Receivable**, **Inventory**, and **Payroll and Employees**. When you've clicked through every screen and reviewed the summary displayed, click **Finish**. Your user will now be able to sign in and access the areas you specified.

You can—and should—take numerous other steps to keep your QuickBooks data safe. If your company is big enough to have a dedicated IT expert, he or she will handle most of this. But there's a lot you can do on your own to prevent data loss and theft.

Keep Your Operating System and Applications Updated



Don't ignore this dialog box.

Software companies' occasional updates offer more than just adding new features and fixing bugs. They sometimes refresh your software to ensure greater security based on new threats. Don't forget about those all-important antivirus and anti-malware applications, as well as QuickBooks itself.

Keep Your Networks Safe

Just as a cold virus spreads around your office, so, too, can unwanted intrusions like computer viruses. Don't allow an electronic epidemic to get started; take steps ahead of time to prevent it:

- **Discourage employees from excessive web browsing.** This can be a hard rule to enforce, as some employees probably need internet access for research, timecard entry, and other work-related tasks. Create a firm policy legislating what workers can and can't do on company-issued equipment (including tablets and smartphones) or any personal devices that use your wireless network.
- **Ask employees to refrain from using public networks on work equipment.** Enforce the rules vigorously, and make compliance an element of performance evaluations.
- **Minimize app installations on business smartphones.** Employees should ask for approval. Viruses and malware get in that way, as well as through some websites and email attachments.
- **Use monitoring software**. If you can't afford to pay for "managed IT" (a la carte, third-party IT services), install an application that alerts you to problems.

Use Common Sense

You can fight data loss and theft by being cautious. Be diligent about backups, and if you create them on a local, portable device, don't leave them in the office. Cloud-based solutions are better. Shred papers that have sensitive information on them. Log out of

QuickBooks when you’re not using it or when you leave your office. Be aware of who may be around you, looking over your shoulder.

We take data security very seriously in our own office, and we strongly encourage you to do the same. Contact us if you’re at all concerned with your own data safety, and we’ll come up with a plan together.

Stock image courtesy of FreeDigitalPhotos.net

Social media posts

Concerned about the safety of your QuickBooks data? We can help you take security measures.

Lose your QuickBooks data, and you’ll face serious consequences. Make sure you keep backups in a safe place.

Do you issue smartphones to employees? Make sure they’re not used on public networks.

Even if you don’t have an IT specialist, you can protect your QuickBooks data from viruses and malware. Ask us how.