June 2011

Are Your QuickBooks Company Files Tamper-Proof?

I love to show clients how to better use QuickBooks. By implementing the best methods for managing your accounting data, you can actually save time, grow your business, and improve your financial bottom line.

But all of your careful work is for naught if a malicious hacker gets into your computers, or if you experience identity theft by an employee. Social security and credit card numbers, home phone numbers and addresses, an excruciatingly detailed profile of your company – all can be lost in the time it takes to realize that it's gone.

Are you guarding all of that precious data? QuickBooks provides ways to help you. Some are automatic, but you have to initiate others.

Control cyberspace

QuickBooks displays some screens using Internet Explorer; the browser opens when you access certain features. It's important that you set the security level correctly so that you're not exposed to shady outside influences.

To check your configuration, launch IE and go to **Tools | Internet Options.** This window opens:

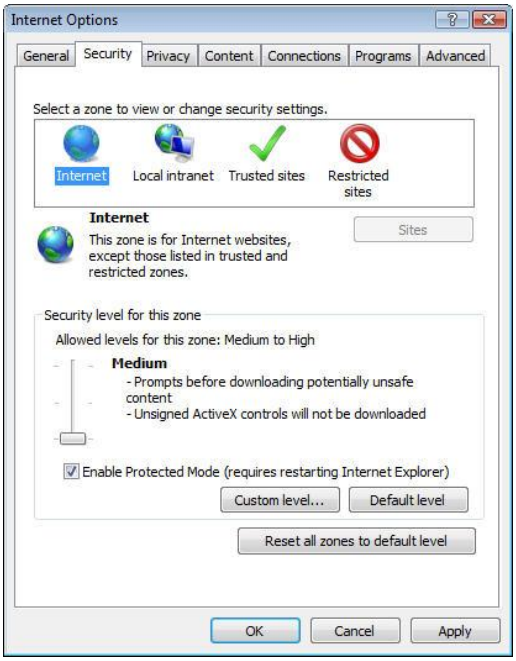

Figure 1: Be sure that your Internet zone in Internet Explorer is set to Medium.

Click on **Security**, then on **Internet**, and move the slider bar to **Medium** (Intuit recommends this). Click **OK** and close IE.

Your best defense is a good antivirus program. If you've hesitated to buy one because of the price or the software's intrusiveness, consider *Microsoft Security Essentials*. It's free, it's good, it can be used in businesses that have up to ten PCs, and it guards against viruses, spyware, and other malicious software (malware).

Limit access

If you have QuickBooks on a network, or multiple people sign in and out on the same PC, you will want to limit the access of employees to only their work areas. Go to **Company | Set Up Users and Passwords | Set Up Users**, and you'll see the **User List** window. Click **Add User**, and enter a user name and password in the next window (if you've already set up passwords but not permissions, highlight a name and click **Edit User)**. Click **Next**.

Unless the person should have full access, choose **Selected Areas of QuickBooks** and click **Next**. You'll see this:

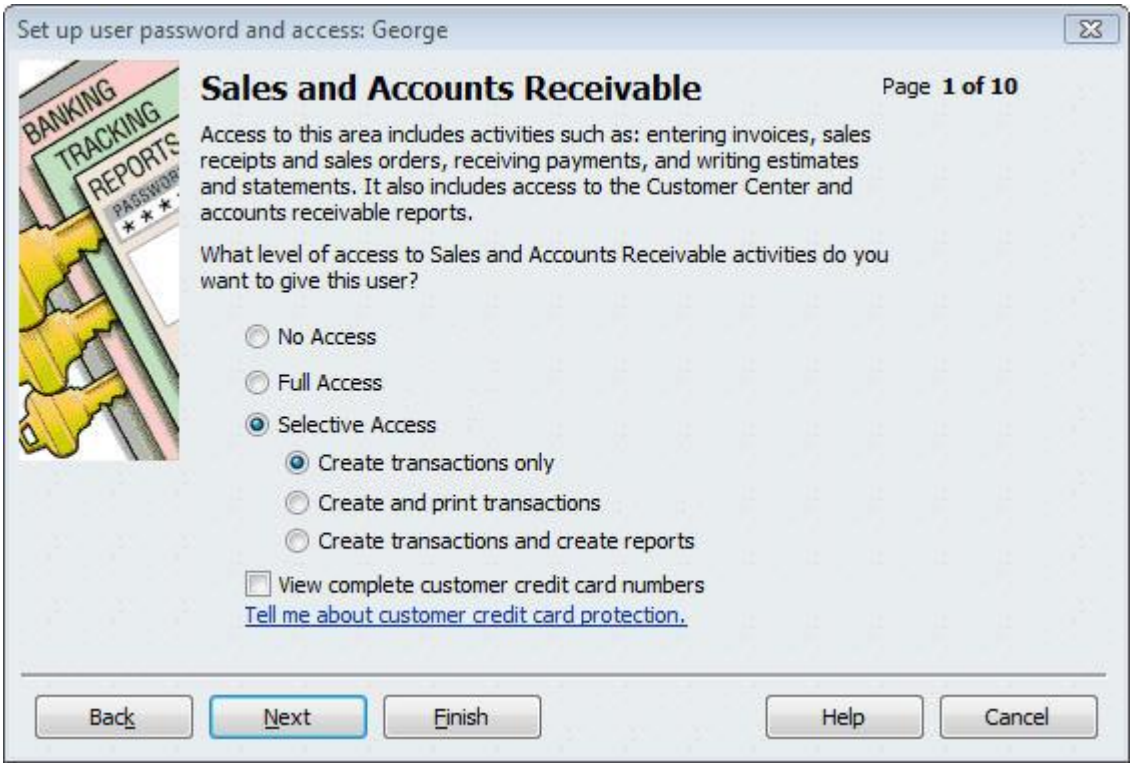

Figure 2: As you go through each module, you'll select an access level for the current employee.

You'll work through a series of windows, including **Inventory**; **Checking and Credit Cards**; and **Payroll and Employees**, indicating how much access should be granted. When employees sign in, they will only see the allowed screens.

Payroll a special case

Be very careful when you assign **Payroll** permissions. Employee social security numbers are stored there, and anyone granted full access can see them. If you've assigned **Selective Access** to an employee for creating and printing payroll transactions and reports, he or she will still be able to view them on printouts and in reports.

To prevent this, go to **Edit | Preferences** and click the **Payroll & Employees** tab, then **Company Preferences**. At the bottom of the window, you'll see a line that reads, **Display employee social security numbers in headers on reports**. Make sure this is checked only if you want the numbers to appear.

And of course, you may not want social security numbers printed on paycheck stubs and vouchers (though you may not have a choice; the state of California, for one, requires it). In this same window, click on **Pay Stub & Voucher Printing** to make your wishes known. You'll see this:

*Figure 3: Do not check the box next to **Employee social security number** unless you want it printed on paycheck vouchers.*

Intuit and you

Intuit, publisher of QuickBooks, works hard to keep your data safe. The company:

- uses a data encryption technology similar to that used by major financial institutions for QuickBooks' online banking and online vendor payment tasks
- does not know your passwords
- offers a subscription-based, automatic online backup service, so that your files are safe in case of loss or damage (QuickBooks 2011 only; QuickBooks Online Backup works with all versions)

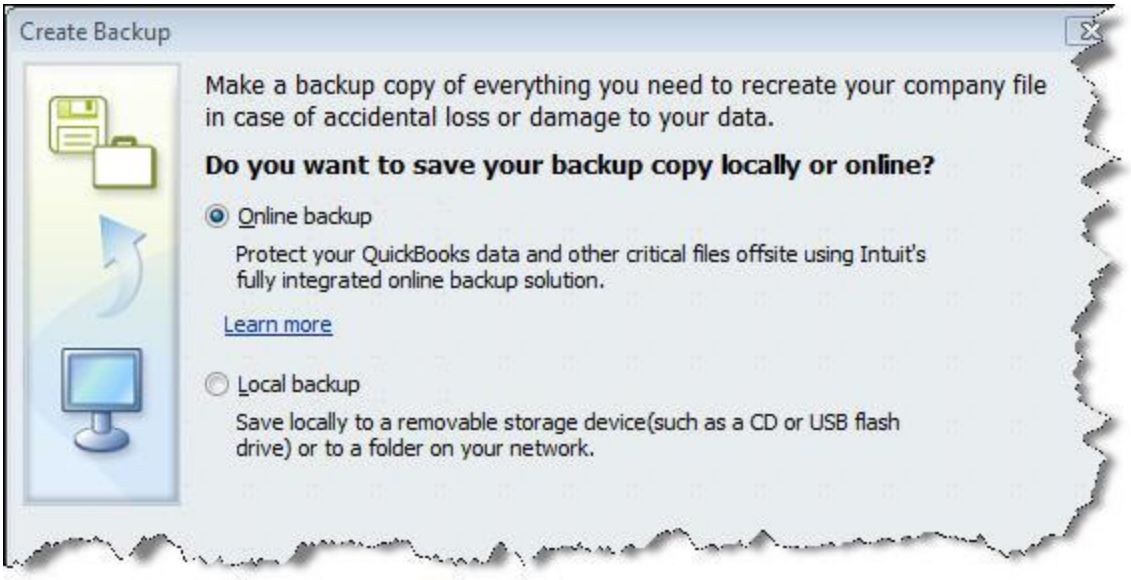

Figure 4: Regular backup is more than a good idea. It could save your business someday.

But it's important that you do your part. Use passwords wherever offered, make them complex, and change them frequently. Maintain regular backup files on your own if you don't subscribe to Intuit's service. Cross-train employees so that if you experience a disaster, more than one employee knows the ropes. Know a lot about who is managing your network.

To be doubly safe, ask your us to evaluate your whole system's security profile. We can help you if your business suffers a breach, but better to try to avoid it ahead of time.