

# **Data Security**

## **White Paper**

*Five Technologies to Help Ensure  
Data Security*

*What a Small Business Must Know*

---

## Contents

---

Introduction	4
#1 - Data Backup	4
Security Tip #1 - Data Backup	5
#2 - Virus Protection	5
Security Tip #2 - Virus Protection	5
#3 - Firewall Protection	5
Security Tip #3 - Firewall Protection	6
#4 - ID & Password Protection	6
Security Tip #4 - ID & Password	7
#5 - Audit Trails	7
Security Tip #5 - Audit Trail	7
The On-Demand Solution and Data Security	8
QuickBooks: Online Edition	8
Data Is Automatically Backed-Up	9
Data Is Protected	9
Data Is On-Demand	10
Data Is Always Private	10
Summary	10
Additional Resources	11

---

## Purpose of this Document

---

Intuit recognizes that small businesses often require help in taking appropriate steps to protect the security of their financial data. And they may look for guidance from their accounting software providers.

To assist you in understanding current security-related issues and technologies, Intuit has prepared this white paper. Its primary objectives are to:

- Identify the five most important technological approaches to help you secure data
- For each approach, identify recommended and generic practices
- Discuss the potential advantages of an online model to data security
- Provide detailed information on QuickBooks: Online Edition as a recommended option

We are certain that once you review the five security technologies and the educational information about online accounting you will identify opportunities for improving the way you protect your financial information. And we believe that once you evaluate the product features, ease of use, and other business-building benefits of QuickBooks: Online Edition, you will be able to confidently begin using it.

Please send your comments and questions to <http://oe.quickbooks.com/support.shtml>. We appreciate the opportunity to serve small businesses such as you.

---

## Executive Summary

---

A. There are five key technologies you should know well regarding data security:

- Data Backup
- Virus Protection
- Firewall Protection
- ID and Password Protection
- Audit Trail

B. The online accounting model sometimes referred to as Application Service Provider (ASP) model or On-Demand, is an attractive alternative to the options noted above.

C. QuickBooks: Online Edition is Intuit's On-Demand accounting solution – a Web-based financial software solution for small businesses and accountants. The Online Edition gives you web-based tools to link multiple users, accountants and locations to their business finances--anytime, anywhere.

---

## Introduction

---

*Your data may be at risk.* This is one of the scariest realizations to come to any small business owner.

In the world of accounting, advances like email, broadband internet connections that are always on, online file sharing and web collaboration services continue to influence the evolving processes that small business owners use to manage their finances. The advantages are great, but they can come with a hidden price tag.

Both existing and emerging threats put your sensitive financial information at risk. Some of these threats have been around as long as desktop computing, such as a physical loss from hard drive failure, property theft or natural disaster, and data corruption from system, software and hardware conflicts that can crash computers. Newer threats exist from viruses, worms, Trojan horses, and other malicious code injections. Hackers today include not only the deviant coders looking to build a reputation, but also identity pirates, spammers, and technology zealots that launch massive efforts to steal personal information and create slave computers used to execute large scale denial of service attacks and revenue-generating spam campaigns.

As a small business owner, you need advice on how to mitigate these risks and still reap the benefits associated with the latest technology.

### #1 – Data Backup

#### **If you don't back data up automatically to an offsite location, your data is at risk.**

Ninety-seven percent of small businesses say they back up some or all of their data, but only 30% say they back it up daily.\* And whether you back up regularly or not, it's important to ask yourself additional questions to assess your actual level of protection. To what type of media do you back up to? To an external drive? To another server? Do you bring the data to another physical location? Who is responsible for initiating the backup? Is it automated? How often do they actually perform the backup?

You are only human, so it's likely that there is a great opportunity for improvement in your data backup systems and procedures. Some small business owners won't ever take the proactive steps necessary to perform a periodic data backup. And fewer will take the steps to store the information at an offsite location. If the information is backed up on your computer network, it's still at risk. According to Intuit research, at least 44% of small businesses have experienced failures that impacted their whole system.\*

The most effective yet least common data backup process is an automated offsite backup service. It is effective because the service provider initiates the backup regularly and the data resides at another physical location. The costs for this type of service range dramatically based on the media used and the size of the data files, but can start for as little as \$10-\$20 per month. However, only 3% of small businesses are using this type of service today.\* Many people insure their physical property against loss, but often forget to protect their data and intellectual property, which can be far more valuable and more difficult or even impossible to recreate or replace than a \$79 hard drive.

#### **Data Loss is Common**

75% of small businesses have experienced data loss, e.g., from hard drive crashes, software failure, virus, etc...

27% of those who experienced data loss were unable to recover their data

*Source: Intuit 2003 Back-up Study; statistical validity to within +/- 4 percentage points*

---

## Security Tip #1 – Data Backup

An automated, regular offsite backup service is strongly recommended to reliably protect your data and hard to replace intellectual property. Using annual or quarterly accountant copies and periodic onsite data file backups are at best fair backup solutions for small business.

---

## #2 – Virus Protection

### You face a daily threat of 60,000 known viruses.

Over one million PC's were infected in North America during the month of May 2004 by over 60,000 known viruses, according to McAfee Associates regional virus tracking system. Viruses and worms with scary names like sobig.f W32/Netsky.p@MM and CODE RED, which historically were brought into a computer environment through email, are now finding ways in through dozens or even a hundred open ports on a PC. Once released, these viruses can wreak havoc on individual machines and even entire networks, often corrupting information on multiple hard drives at once.

Today, hackers are more interested in making a profit than a name for themselves. Many of the recent attacks focus on disabling security, broadcasting personal information, and creating slave or zombie networks that do their bidding by distributing spam or mounting large scale attacks on people or companies they take issue with. These types of infestations are not focused so much on destroying information, but instead attempt to use as much processing power and bandwidth as possible. The result is that you can be crippled in your ability to use your machines. It's even possible to be infected by viruses today while surfing the internet by clicking on 'spoofed' internet links, clicking on embedded links or other disguised executable files.

Fortunately, the services from leading providers like McAfee and Symantec can help protect a computer from these nasty threats. Some services will automatically push updates to the subscriber PC to protect against newly emerging threats.

Worries remain for small businesses with older operating systems that will likely need to manually update their virus protection files to stay current. You will also need to remember to apply critical patches to your operating systems and other software; as such updates and upgrades are made available by the software vendors.

---

## Security Tip #2 – Virus Protection

Use services with automatic updates to reduce the risk of missed detection from outdated definition files. Upgrade to the latest operating systems to enable real-time definition file updates and consistently apply critical patches to the operating system as they become available.

---

## #3 – Firewall Protection

### The Virus Problem is Growing

88% of company managers said it got worse in 04. Impacts:

- 67% of these companies say PC was unavailable
- 58% had corrupted files
- 50% lost data access

*Source: ICSA Labs 2003 9th Annual Computer Virus Prevalence Study*

## **Identity thieves and hackers want to steal sensitive personal and financial information from you.**

With the advent of always-on broadband and wireless networks, many small businesses unwittingly expose their computers and data to anyone with an Internet connection of their own and a desire to break in. To keep out unwanted visitors and identity pirates, and to protect valuable business information, you must have robust firewall protection, especially if you maintain a wireless network, an always-on broadband connection, or both.

A firewall is a combination of software and/or hardware that provides a protective barrier between a computer or network and the public Internet. It essentially acts as a traffic cop, policing your online gateway and blocking unauthorized access to your computer or network. Although firewalls aren't too expensive, many small business owners don't take the time to buy and properly install one because they don't understand the technology. Once the firewall is in place, it's important to monitor it for attacks by checking the logs regularly. To further reduce risks, close any ports and disable any system services you aren't using or don't need.

---

### **Security Tip #3 - Firewall Protection**

Properly install, configure and regularly monitor your firewall to keep out identity thieves and other malicious hackers.

---

## **#4 – ID & Password Protection**

### **Weak password protocols are a common security flaw that can increase your risk of internal fraud.**

Passwords are a common form of authentication and are often the only barrier between a user and personal information. Attackers can use specially designed software programs to help guess, or crack passwords. However, by choosing good passwords and keeping them confidential, you can make it more difficult for an unauthorized person to access your information.

Many small business users will have relatively simple User ID & passwords. A larger problem can be that many of these businesses will share their User ID & passwords with others to make it easier to work together, share access to products, and reduce software license and subscription fees. This lack of protection can leave an employer exposed to embezzlement by a disgruntled employee or unscrupulous business partner.

Finally, you should learn to recognize ploys from authentic sounding strangers to obtain password and other information. This approach – sometimes called “social engineering,” can take the form of a hacker calling and impersonating an authorized technical support agent. To fix the fictional problem, the phony agent asks for a password or other sensitive information.

Here's some advice to help you choose more secure passwords and help you avoid other breaches in security:

- Don't use passwords that are based on personal information that can be easily accessed or guessed
- Don't use words that can be found in any dictionary of any language

- Develop a mnemonic for remembering complex passwords
- Use both lowercase and capital letters
- Use a combination of letters, numbers, and special characters
- Use different passwords on different systems
- Don't write down a password

Learn to recognize "social engineering" techniques where thieves try to con you into revealing passwords or other sensitive information.\*

*Adapted from National Cyber Alert System "Cyber Security Tip ST04-002," Copyright © 2004, Carnegie Mellon University. [<http://www.us-cert.gov/cas/tips/ST04-002.html>]*

Don't write down passwords on a sticky note and then paste it to your monitor, under your keyboard or in a nearby drawer. Those are the places that someone looking for access will search first.

---

## **Security Tip #4 – ID & Password**

Choose a password with a combination of letters, numbers and special characters that you can remember with a mnemonic and make sure you don't write it down.

---

## **#5 – Audit Trails**

### **Small businesses are 100 times more at risk for Internal Fraud than a bigger business.**

According to the Association of Certified Fraud Examiners' (ACFE) '2002 Report to the Nation on Occupational Fraud and Abuse,' the per-employee losses from fraud in the smallest businesses are 100 times the amount of their largest counterparts.

As much as you look for the best in the people you hire, unfortunately, not all employees turn out to be trustworthy. So, it becomes necessary to set up internal controls and other precautions to minimize the risk of theft and fraud. One very important measure to consider in an accounting system is the audit trail.

---

## **Security Tip #5 – Audit Trail**

Keep your Audit Trail trails turned on to better track your transactions and to help keep employees honest.

---

## **Summary on Five Technologies**

---

Technology in the market today is evolving quickly and so are the resulting problems. A small business should take advantage of productivity advances to compete and succeed in the marketplace, but need to know the risks it is exposed to. A small business may be a hog farmer, a restaurant owner or a small retailer, but the one thing they are not usually, is a security expert.

Most small business owners are neither likely to understand, nor have time to learn, how to secure their

PC or network.

So far, all of these discussions have been about responding to security threats in scenarios where the small business maintains the data on a local PC – and subject to the threats noted above. There is an optional model you may want to consider.

---

## **The On-Demand Solution and Data Security**

---

As an alternative to purchasing and installing an application on a local PC, the On-Demand model runs or “hosts” software for you within a Data Center specifically designed to secure and manage all aspects of operating the application. Similar to online banking and online trading services, a small business will benefit from the data security protection levels available to the largest businesses.

The On-Demand solution has built-in data security. While some small businesses unfamiliar with On-Demand data security may initially resist the idea due to a perceived lack of control, even more small businesses are becoming open to using an online accounting system. This is because educated small businesses learn that the built-in security available with an online accounting service is far better than most small businesses can afford on their own.

Typically On-Demand solutions have the following built-in security features, at no additional cost:

- Automatic, offsite backup
- Automatic, redundant firewall protection
- Automatic, 24/7 virus protection
- Multiple levels of password protection
- Audit trail always on; all transactions remain on record

The Nightmare Scenario. Many small business owners see the value of an On-Demand solution at once if they consider a nightmare scenario where all their hard drives crash or are lost in a fire or act of God. The small business is back in business as soon as they find a new computer with an Internet connection.

### **The On-Demand Solution – The Real Story**

- Your data is at much greater risk on a PC hard drive than they realize.
- An On-Demand solution provides data security most small businesses could never otherwise afford.
- The market is learning these facts and On-Demand adoption rates are growing quickly.

---

## **QuickBooks: Online Edition**

---

QuickBooks: Online Edition is Intuit’s On-Demand accounting solution – a Web-based financial software solution for small businesses and their accountants. The Online Edition gives you a web-based tool to link multiple users, accountants and locations to their business finances--anytime, anywhere.

It works like desktop versions of QuickBooks, but instead of installing it on a computer; you, your staff you designate, and your accountant access it through a Web browser. The application and your data are

hosted at Intuit's professionally managed Data Center—the same data center which stores millions of consumer's TurboTax® tax returns. A high-speed Internet connection provides the flexibility to stay on top of business finances, no matter where and when you work.

*In March, 2004, we had a lightning storm and my motherboard and hard drive were both damaged beyond help. I had failed to back up my data since 2001! Our accounts receivables were over \$5,000 and I had no idea who they were. I have tried to re-create our customer base and determine who had paid, who hadn't, etc. It's been a nightmare!*

*Then I saw QuickBooks Online advertised and knew that this was the safest way for us to maintain our accounts. I have been very pleased with the fast response to my questions and I can sleep at night knowing that my data is being safely stored and backed up!*

Debbie Valentine, Valentine Pest Control

QuickBooks: Online Edition keeps your financial information protected, private, and available on-demand. Specifically,

### **Data Is Automatically Backed-Up**

The Online Edition has automatic, continuous, and redundant backups 24 hours a day, 7 days a week.

Should the unexpected ever occur, your QuickBooks Online data is automatically and continuously backed up in the same offsite, Intuit-owned Data Center that handles millions of TurboTax for the Web® tax returns each year.

This means you have the convenience of automatic, offsite storage of your most critical business information without the extra effort and cost of creating and managing physical copies of your data.

### **Data Is Protected**

Intuit uses advanced, industry-recognized safeguards and procedures, such as password-protected login, the toughest commercially available encryption technology (128 bit SSL), and firewall protected servers.

- **Password Protected Access**
  - Each person you invite to use your QuickBooks Online account creates his or her own unique password.
  - You control who accesses your QuickBooks Online Edition data and what they can see and do. Once you set up a company, only trusted Data Center operational staff plus the people you explicitly invite can access your data. We offer multiple permission levels that let you limit the access privileges of each user.
- **Encrypted Transmission of Data**
  - As your data travels between your computer and ours, it is encrypted by a technology called Secure Sockets Layer (SSL) using 128-bit encryption. This is the same technology used by banks and offers the highest level of encryption currently supported by commercial Web browsers. The lock icon in the bottom of your browser window indicates that your data is shielded from unauthorized access while in transit.
- **Protection Against Intruders and Viruses**

- Your financial data resides on a server in Intuit's Data Center that is heavily guarded both physically and logically against viruses and other forms of intrusion. Our data servers sit behind layers of network security and are not directly connected to the Internet, so your private information is available only to authorized users from authorized computers. We employ a 24x7 on-site operations staff who monitor the integrity of incoming network traffic
- Audit Trails
  - In QuickBooks financial software, you can set up an audit trail that is always-on to record the transactions that are being entered, edited or deleted from the system. Without a reliable audit trail, it becomes possible for employees to produce fraudulent transactions and then cover their tracks by deleting or editing the transactions to appear normal.

## Data Is On-Demand

Access your data from any Internet Explorer browser with reliable uptime.

The Online Edition utilizes redundant servers and a self-correcting error detection program, so even if one server becomes impacted or unavailable, your use of the service will likely not be affected. Intuit's professional staff and automated tools monitor service performance twenty four hours a day seven days a week for problems. If a problem occurs, our staff immediately starts diagnosing issues and implementing solutions to bring performance back to acceptable service levels.

## Data Is Always Private

Intuit follows strict guidelines and practices to protect your private data.

We do not sell, rent, or share your information with third parties for their promotional use. Intuit is a licensee of the TRUSTe Privacy Program. TRUSTe is an independent, non-profit organization whose mission is to enable individuals and organizations to establish trusting relationships based on respect for personal identity and information by promoting the use of fair information practices.

## Summary

The following table summarizes the advantages of this Web-based solution.

	QuickBooks: Online Edition	QuickBooks Basic, Pro, Premier
	<a href="http://oe.quickbooks.com">oe.quickbooks.com</a>	<a href="http://quickbooks.com">quickbooks.com</a>
<b>Offsite Backup</b>	Continuous, automatic, 24x7 physical security with offsite backup	Prompts for backup automatically, can backup to remote location. Optional automated remote backup solution available at additional charge

	QuickBooks: Online Edition	QuickBooks Basic, Pro, Premier
<b>Firewall</b>	Automatic, redundant hardware and software protection	\$50–100 to purchase a retail software product; support extra
<b>Anti-Virus</b>	Automatic, 24x7 network monitored protection	\$50–100 to purchase a retail software product; support extra
<b>Password</b>	Multiple levels	Multiple levels
<b>Audit Trail</b>	Always-on visibility to track any access or updates	Audit trail available and can be turned on and off by users

## Additional Resources

CNET for software and service reviews

<http://cnet.com>

Iron Mountain

<http://ironmountain.com>

McAfee Associates

<http://www.mcafee.com>

QuickBooks: Online Edition

<http://oe.quickbooks.com/security/>

Security Docs

<http://www.securitydocs.com/>

Small Business Computing

<http://www.smallbusinesscomputing.com/>

Symantec Corporation

<http://www.symantec.com/index.htm>

TRUSTe

<https://www.truste.org/validate/8257>

U.S. Computer Emergency Readiness Team

<http://www.us-cert.gov/>

U.S. Data Trust

<http://usdatatrust.com>