

united states

- [global sites](#)
- [licensing](#)
- [archives](#)
- [shop](#)
- [newsletter](#)
- [trialware](#)
- [products](#)
- [enterprise security](#)
- [about symantec](#)
- [search](#)
- [feedback](#)

## Trustworthy Transactions



As e-commerce grows in popularity and almost every bank provides some form of online services, more and more small business owners are turning to the Internet for their money management solutions. You can do just about anything online, from investing and trading to paying your bills and applying for a business loan. While the ease and convenience of doing your banking online may appeal to you, sending financial data over the Internet poses certain security risks. You need to be aware of these risks, and do your part to help make every online transaction a secure one.

## Possible Security Risks

When you send information or funds from your computer over the Internet, there are several security breaches that could take place. Hackers that snatch the information in transit can steal and use it, manipulate it, sell it, or combine it with other facts about you to make it more useful. Even if you have secured and protected your computer at work, business financial transactions made from your home computer may not be so safe. These are some of the possible abuses of your information:

- **Password theft.** If a hacker obtains the password to your company's electronic banking account, he or she may suddenly have access to all of your business' financial records and sensitive information under that login, including name, address, transactions, balances, and even the ability to schedule bill payments to the account of their choice.
- **Credit card theft.** Although most people place their concern in the area of credit card theft, online credit card use is one of the safer financial transactions. When you use a credit card online for company business, you are covered by several different kinds of consumer protections. Most credit companies only hold you responsible for the first \$50 in the event that your card number is stolen and used online.
- **Account number theft.** If an online thief intercepts your account number in transit, they may be able to get access to your funds. In order for your account number to be useful to the hacker, additional information is usually required. For instance, they might need to steal your password as well.
- **Identity theft.** This is one of the more frightening uses of private information by an outside source and is often the most detrimental. A thief builds or obtains a complete profile of you and your small business including your name, address, tax ID, and telephone number. Then they apply for loans using your name to open lines of credit, wireless phone accounts, and other frauds. The victim may not find out until they are denied a loan years down the line, discovering their credit history is ruined.

## Institutional Protection

There are many ways both you and your financial institution can protect your accounts and your identity against fraudulent abuse. If you are working with a reputable bank, they should have a battery of defenses to keep your information private and your money safe.

- **Encryption.** This is one the strongest lines of defense when exchanging information online, disguising the data so it cannot be read in transmission. This method of incoherently scrambling information varies in strengths, but the industry standard for banks is 128-bit encryption. No one has been able to crack this strength of encoding yet. This encryption requires use of both a public and a private key to encode and decode the text. In general, to send encrypted data to someone, you encrypt the data with that person's public key, and that person decrypts the data with the corresponding private key. This method offers added protection since even if someone cracks the public key, they still don't know the private key, and vice versa.
- **Firewalls.** A filter for traffic flowing into the bank, the bank's firewall has a list of criteria that one must meet in order to be allowed through the firewall. It can block out certain users, certain areas, or unregistered users. A password may also be used to guard the site from unwanted intruders.
- **Monitoring for suspicious activities.** Banks monitor accounts for activity they deem suspicious, such as a specific amount of money

Not sure what you need?  
Small Business  
**ProductSelector** go

### smallbiz products

- [antivirus](#)
- [problem solving](#)
- [remote/productivity](#)
- [internet security](#)
- [Macintosh products](#)

multi-user packs  
Save Time  
and Money  
go

### smallbiz resources

sign up to receive our  
**monthly newsletter** go

### smallbiz security

**virus alert** go

W32.Goner.A@mm

is your system safe?  
find out... **Symantec Security Check**  
a free service to help you understand and protect against security threats  
go

deposited repeatedly in select accounts from one source or large withdrawals from accounts that are not usually withdrawn from.

- **Secure Socket Layer (SSL).** The SSL protocol was designed by Netscape Communications Corporation as a safer way for a Web server and a computer to connect. The SSL allows both computers to verify that they are who they say they are, and to establish an encrypted connection between them. Using an SSL allows you to make sure you are sending sensitive information, such as a credit card number, to the proper site, and not to a hacker pretending to be that site.
- **Security guarantees.** Find out if the bank offers a guarantee of security. Ask if they replace money lost to hacker theft, and how much of the balance you are responsible for if your credit card number is stolen and used.
- **Password policies.** Ask the financial institution about their password policies. Do they lock you out after so many unsuccessful attempts, or do they allow unlimited guesses? With unlimited guesses, it is easier for a hacker to try to break into your account. What is their procedure for issuing a new password if you forget yours? Do they only require the easily obtained "mother's maiden name," or can you choose a more difficult question? Better yet, do they mail a sealed, unmarked computer-generated replacement to the home address you have on file? Since passwords are one of the easiest ways in for a hacker, it is important to be sure your bank guards that password.
- **Membership.** Does the site you are doing business with offer you the protection of VeriSign®? Sites that are members of the VeriSign® Secure Site Program allow you to learn more about them before you submit any confidential information. Using VeriSign®, you can verify that the site is secure, while also confirming the owner of the site and its physical location. Is the institution a member of the Better Business Bureau? The BBB allows you to check the history of a business for previous consumer complaints or alerts against them.

## Taking Control

While your bank may be doing a fantastic job of protecting your online transactions, you can bolster security on your end as well. These steps are relatively easy and can definitely make your investments, transfers, and other online banking more secure:

- **Use an encrypted browser.** Make sure your browser supports 128-bit encryption. This will allow your bank's security efforts to work the best for you. The newest versions of both Netscape and Internet Explorer feature 128-bit or "strong" encryption, so if you're not using a recent version it's time to upgrade. You can go to the Netscape or Microsoft® Web site to download the latest versions.
- **Use a firewall.** Firewalls make your Internet connection safer by screening out unwelcome guests. Firewalls, such as Norton® Personal Firewall, are an excellent addition to your small business security for all of your online transactions – not just for banking. Firewalls provide a barrier for information flowing into and out of your network. The firewall examines the information and compares it to a list of criteria determined by you. If the information satisfies the criteria, it is allowed through. If it does not, it is blocked. You can use firewall hardware or a firewall software package. If you're not sure what kind of firewall you need, read the article "What Firewall Is Best for You?" You can also use intrusion detection software to find out if someone is attempting to hack in and steal your information.
- **Check for certification.** A digital certificate is a confirmation of site ownership. Checking the certificate reassures you that you are sending your sensitive data to the right site, and not someone disguised as your bank. You can check for certification using your browser's "view certificate" menu option.
- **Choose a good password.** One of the easiest steps you can take to boost your security is to create a difficult password, memorize it (don't write it down), and change it often. Then if someone obtains information about you, such as your spouse's or children's names, your password will not be compromised. Hackers may also make use of easily available software that systematically runs through combinations of dictionary words and numbers, searching for a match. Many people use their birth date or name of their child or pet as their passwords, but the most difficult to crack is an alphanumeric combination that is at least six characters and includes punctuation, if possible. Changing it often makes it even more secure.

There are online banks springing up all over the Internet, and many of them may be an excellent choice for you to do your small business banking. The Web can save you time, money, and travel, so use it well, but make sure you use it wisely. If you choose a financial institution with your safety in mind, and add your own efforts to theirs, you can perform trustworthy transactions.

[> home](#) [> find a solution](#) [> need more than 10?](#) [> tech resources](#)