About connected services and security

Like most people, you may have questions about working with your personal or business finances over the Internet. While Quicken and your financial institution work together to safeguard your financial data, there are factors that we can't control such as whether you're using a well-chosen password, the physical security of your computer, and the effectiveness of safeguards being used when you access the Internet.

Security with online financial services

Quicken uses industry-standard encryption and authentication methods. For more information, see What do I need to know about the way Quicken protects my financial information?

Financial institutions also safeguard the security of customer information on their internal systems by maintaining the physical security of and access to computers, private keys, and customer IDs and passwords.

Security protocols

Encryption methods used by Quicken to provide secure SSL Secure Sockets Layer (SSL) is an industry-standard cryptographic protocol that provides secure message transmission on the Internet. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. connections include 128-bit RC4 and 168-bit triple DES. Financial institutions and processors have the option of using stronger encryption. Additional security precautions include digital signatures and digital certificates.

Take advantage of Quicken's built-in security

Quicken includes the following built-in security features:

- The ability to password protect your Quicken data files.
- The ability to review and delete online payment instructions before you connect and send them over the Internet.
- The ability to store your online passwords in a password-protected Password Vault.

Take standard precautions

Quicken recommends that you take the following precautions to further protect your information, including:

- Memorizing, regularly changing, and not sharing passwords.
- Using and regularly updating antivirus and anti-spyware programs.
- Installing a personal firewall on your home computer.
- Not allowing others to access your financial data files.
- Carefully reading prompts before sending transactions over the Internet.
- Using an Internet service provider with strong security practices.

For additional information see the FTC's Computer Information Security website.

Carefully choose your Internet service provider

The security measures described above are independent of your Internet service provider. Check with your ISP to find out how they are protecting your data when you're on the Internet.