



## Security Q & A

Watertown Savings Bank recognizes the importance of protecting your personal information. The following are answers to some very important security questions related to our Internet Banking product, **WSB Online**.

### **How does Watertown Savings Bank protect my information on the Internet**

Watertown Savings Bank utilizes several layers of technology to ensure the confidentiality of its transactions across the Internet. Security begins with your browser. SSL protocol (Secure Sockets Layer) is used to provide privacy for the data flowing between the browser and the bank server.

SSL is an open protocol for securing data communication across computer networks, and it provides a secure channel for data transmission through its encryption capabilities. It allows for the transfer of digitally signed certificates for authentication procedures, and provides message integrity, ensuring that the data can't be altered en route.

Public/private key pairs are used specifically for authentication. The public key can be distributed, using a certificate that verifies the identity of the owner. The private key is kept secret. A message encrypted with a public key can only be read after decryption with the private key.

To start a transaction, the customer uses his or her browser to send a secure message via SSL to the bank's service provider. The bank's service provider responds by sending a certificate, which contains the bank's public key. The browser authenticates the certificate, and then generates a session key that is used to encrypt data traveling between the customer's browser and the bank server.

The session key is encrypted using the bank's public key, and sent back to the bank's service provider. The bank decrypts this message using its private key, and then uses the session key for the remainder of the communication.

By exchanging messages using the public/private key pair, the customer can be assured they are actually communicating with the bank's service provider, and not a third party trying to intercept the transaction. When a session is encrypted, the key icon or gold lock at the lower left corner of the browser's screen becomes solid or locked. If the key icon appears broken (Netscape browser) or the lock is unlocked (Internet Explorer browser), encryption is not in use and the current session is not secure.

### **What kind of protection has the Bank put in place to protect my data from potential hackers**

Watertown Savings Bank has gone to great lengths to ensure that your money and personal data are protected against any type of intruder or attack.

The bank's customer information is protected by a system of filtering routers and firewalls, which form a barrier between the outside Internet and the Bank's service bureau network. The filtering router verifies

the source and destination of each network packet, and determines whether or not to let the packet through. Access is denied if the packet is not directed at a specific, available service.

The firewall is used to shield the bank's customer service network from the Internet. All incoming IP traffic is actually addressed to the firewall, which is designed to allow only e-mail into the customer service environment. Traffic through the firewall is subjected to a special proxy process that operates in much the same way as a filtering router, verifying the source and destination of each information packet.

The proxy then changes the IP address of the packet to deliver it to the appropriate site within the customer service network. In this way, all inside addresses are protected from outside access, and the structure of the bank's internal networks is invisible to outside observers.

### **What else can be done to protect me from other users accessing my accounts**

Strict internal procedures are in place within Watertown Savings Bank and its Internet Banking service provider, controlling every aspect of bank administration from training employees to confirming customer transactions to preventing service interruptions.

New advances in security technology are happening daily, and Watertown Savings Bank and its Internet Banking service provider are constantly evaluating their security architecture to ensure that they provide the highest level of privacy and safety for bank customers.

Customers have their own set of responsibilities in providing security for their WSB Online bank account. Passwords must be kept secret. Users should make sure that no one is physically watching as passwords are entered. It is important to remember to exit the browser when leaving the computer.

If the PC is left unattended with the browser running and a valid user name and password cached, anyone can gain access to the account. Users should also take precautions to keep computers clean and free from viruses that could be used to capture password keystrokes.

For more information on security and other technical issues, you may e-mail our technology department at [technology@watertownsavings.com](mailto:technology@watertownsavings.com).

**IMPORTANT:** E-mail is generally not a secure form of communication. Please do not include account number or social security information in this correspondence.