

# SECURITY ONLINE

---

## Security Online

At Arrow Financial Corporation, the security of your financial information is a top priority. We employ extensive security measures in order to insure a safe and reliable online experience for our customers. Described below are some of the security measures employed.

## Password Protection

If you are utilizing Internet Banking through one of our affiliate banks, no one can access your bank's account(s) online without your User ID(s) and Password(s). You must select a Password(s) when you initially log on to Internet Banking for the first time. You may change your Password(s) as often as you like after successfully logging on to our Internet Banking service. If you enter your Password(s) incorrectly three times, our service will lock your access. You can use the Forgot Password link on the Login screen to reset your password.

## SSL Encryption

Data exchanged over the Internet is divided into small units and sent in envelope-type packets. For Internet transactions and communications, we employ a method of securing these packets as they travel across the Internet. Secure Socket Layer (SSL) is the leading method for encrypting and decrypting these packets of data as they are exchanged using a code known only to the data's sender and intended receiver. SSL locks the data as it travels along the Internet and once it is received by the intended end user, they have the proper key or combination to unlock the data. We require the use of a browser which supports 128-bit SSL encryption.

Each of the most popular modern Web browsers notifies end users that SSL is active through the use of special icons, colors, or other visual notifiers added to the browser chrome that make it clear something good is happening. In fact the display is quite different depending on the \*type\* of SSL certificate purchased and used on the site. The prominent Extended Validation (EVSSL) certificate gets the best branding. Use of an EVSSL certificate will often be presented with colorful green indicators in the Web browser. Unfortunately each browser presents this information in a different way.

The following is a summary of standard SSL certificate displays:

| <u>Browser</u>      | <u>Standard SSL</u>  | <u>EVSSL</u>   |
|---------------------|--|--|
| Internet Explorer 9 | Gray padlock in address bar  | Gray padlock plus full green address bar with company name or CA     |
| Internet Explorer 8 | Yellow padlock in address bar                                      | Yellow padlock plus full green address bar with company name or CA   |
| Firefox 4           | Blue security emblem in address bar                                | Green security emblem in address bar with company name               |
| Firefox 3           | Padlock at bottom plus blue security emblem in address bar         | Padlock at bottom plus green emblem in address bar with company name |
| Chrome 11           | Green padlock in address bar                                       | Green padlock plus green emblem in address bar with company name     |
| Opera 11            | Dark padlock plus yellow emblem in address bar written as "Secure" | Dark padlock plus green emblem in address bar written as "Trusted"   |
| Konqueror 4         | Green shield with white check mark in address bar                  | Green shield with white check mark in address bar                    |
| Safari 5            | Gray padlock in address bar  | Gray padlock plus green company name in address bar                  |

## Automatic Time Out

You should always select "Sign Off" after using Internet Banking. However, for enhanced security, Internet Banking has an automatic sign-off warning window that will appear after 10 minutes of inactivity. You can either select to continue your online session or to sign off. If you select "continue" to continue your session and another 10 minutes of inactivity follows, you will see the same window again. If you do not select "continue" within 60 seconds automatic sign-off occurs.

## Enhanced Login Security

Enhanced Login Security allows us to provide you with more security and peace of mind when using our Internet Banking and some of our other Web-based services. With Enhanced Login Security, we are able to authenticate you through a combination of your User ID and the computer you choose to make a trusted machine. If you try to access your Internet Banking service on a computer other than your trusted machine or if you clear your cache you will be asked to enter a security code to continue the log in process. The security code will be sent to you through email, text or a phone call. The email address, text telephone number or call telephone number is set up by you at the time you register for Internet Banking.

## **Firewalls**

Arrow Financial Corporation's computer does not connect directly to the Internet. Data transmitted over the Internet to an affiliate bank must pass through a validation and control center known as a Firewall. A Firewall serves to authenticate every request for information, and provides only the information that person is authorized to have while documenting every event.

## **Security Tips**

Even though we employ the latest technologies and security precautions to ensure you a safe and secure online experience, you play an important role in helping us make your accounts as secure as possible. We strongly encourage you to do the following:

- 1) Keep your User ID(s) and Password(s) confidential;
- 2) Use Password(s) that are not easily discernible; use a combination of alpha, numeric and special characters in your passwords (refrain from using birthdays, child's names, etc.);
- 3) Change your Password(s) routinely and often; and
- 4) Use different Password(s) for each online service.

## **Arrow Financial Corporation**

March 2012