

## How we help protect you

We realize that you, like many of our clients, rely on the internet for your banking and financial needs. Because Kentucky Bank considers the security of your financial information a top priority, we take extensive security measures to ensure a safe and reliable experience.

1) *Secure transmission and encryption:* We use secure socket layer (SSL) to protect your personal information. SSL converts sensitive information, like passwords, into secure code and then sends them over a secure network. You can tell your data is protected when you see a URL beginning with "https" and a lock in the lower right corner of your computer display.

2) *Firewalls:* All Kentucky Bank systems are protected by firewalls. Firewalls are one of the key safeguards that protect your information. Our Firewalls document every message that enters or leaves our network and blocks any that do not meet our strict criteria.

3) *Virus protection:* To ensure that you can communicate and transact with us in a safe and secure environment, we use the latest virus detection software programs to help us keep our networks virus-free.

How you can help

Although we use a variety of technologies and techniques to secure our services and computer systems, you can also enhance security and help control risks by practicing the following security measures:

4) *Sign off:* Log off and close your browser to end each internet banking session. To further enhance security, your session with Kentucky Bank online banking will automatically end if there is no activity on your computer for 10 minutes. By automatically signing you out, the chance of unauthorized access to your accounts is minimized.

5) *Unique password:* Before you sign on to online banking, you will need to enter a unique password. We recommend that your password use a combination of upper and lower case letters as well as numbers and special characters.

6) *Security questions:* We ask you to select security questions as part of your account profile. Changing these questions often will further enhance your security.

## Other Security Tips

- Keep log in id's and passwords confidential
- Use passwords that are not easily identifiable. For example, do not use your address, phone number or words found in the dictionary
- Change your password frequently
- Do not give your user id or password to anyone