Destroy any old or unused debit or credit cards.

Make sure no one sees your PIN when you enter it.

Memorize your PIN and do not write it down.

Only use your card at merchants you trust.

Securely store or dispose of your transaction receipts.

When using an ATM always be aware of your surroundings when withdrawing funds and watch for suspicious persons around the ATM. Make sure no one sees your PIN as you enter it. If you notice anything suspicious, or are in the middle of a transaction, cancel it. Return later or visit an ATM elsewhere. Report all crimes immediately to local law enforcement.

Put away any cash as soon as your transaction is complete.

Scam Prevention Tips

Promptly retrieve US Postal mail and consider paperless options to reduce chances of theft.

Shred or destroy all personal information and mail solicitations that you are not interested in.

Always use common sense. If it sounds too good to be true, it probably is.

Never give personal information to a stranger who contacts you, whether by telephone, email, or even in person.

Remember you are responsible and liable for items which you cash or deposit into your account, whether they are a check, money order, transfer, etc.

Do not accept payments for more than the amount of any service, if expected to provide back the difference.

Do not accept checks from individuals you have met online.

Do not accept payment for conducting money transfers through your account.

Be Cautious of any offers related to mortgage modification, foreclosure rescue, or short sale scams involving money-back guarantees, title transfers, up-front fees, or high pressure sales tactics.

No matter how urgent someone claims a deal or job offer is, you should research and confirm its legitimacy.

Review your Credit Report at least annually

Helpful Websites

Online fraud is on the rise, and the techniques for creating deceptive e-mail messages and websites are getting more sophisticated.

The FTC (Federal Trade Commission) works for the consumer to prevent fraudulent, deceptive and unfair business practices and provides information to help consumer's spot, stop, and avoid them.

Contact the following agencies:

If you notice spam that is phishing for information www.spam@uce.gov

If you feel someone is scamming you www.ftc.gov

For Identity Theft www.consumer.gov/idtheft

To avoid email scams and deceptive emails www.ftc.gov/spam

Hearthside Bank

Middlesboro, KY	Harlan, KY	Harrogate, TN
606-248-1095	606-573-1440	423-869-1095
	606-573-7050	
New Tazewell, TN	Jacksboro, TN	
423-626-2030	423-566-4663	

Member FDIC

H0714

Best Ways to Stay Safe Online

Security Best Practices

Hearthside Bank

800-354-0182 | hearthsidebank.com

As use of the Internet continues to expand, more financial institutions are using the Web to offer products and services or to otherwise enhance communications with customers.

The Internet offers the potential for safe, convenient new ways to shop and conduct financial business. However, staying safe online involves making good choices -- decisions that will help you avoid costly surprises or even scams.

In this brochure you will find information and tips to help protect you when using the web. It is not intended to be a legally binding document.

Before you go online, read the following safety tips.

Online Security Tips

Use hard to guess usernames and passwords, with combinations of letters, numbers, and special characters. Do not use the same username and passwords as credentials for all websites.

Protect your online passwords. Do not write them down or share them with anyone.

Select questions and provide answers that you can easily remember but hard to guess by someone else. Do not use security questions with easily found answers such as the name of your high school. Do not use the same security questions for all your website access. Please note that Hearthside Bank will never ask you to provide answers to your security questions, usernames or passwords via email.

Ensure you are using secure websites for transactions or purchases. Check for secure symbols like a lock symbol in the lower right-hand corner of your web browser window, or "https://…" in the address of the website. The "s" indicates "secured" and means the web page uses encryption.

Always log off from online banking or any website after using your debit card, or other sensitive information, versus using the back button. If you cannot log off, close your browser to prevent any potential unauthorized access to your account information.

Keep your browser closed, when not using the internet.

Avoid using unsecured wireless (Wi-Fi) for any online activity requiring a login. If you use wireless take these precautions: Change the default wireless network name or SSID; change the default password and enable encryption.

Use a current version of your web browser, as many times updates include new security features.

Only download from trusted sources and turn on pop-up blockers.

Keep your computer operating system and other software programs up to date to ensure the highest level of protection. Even set your operating system to receive automatic updates. The "Help" menu or the software vendor's website may be checked periodically for updates.

Install or turn on your computer's firewall

Install, turn on, and keep anti-virus software up to date, along with frequently scheduled scans.

Turn your computer off completely when not in use versus leaving it in sleep mode.

Avoid online banking activities on public computers (computers at internet cafes, copy centers, hotels, etc.) Online banking activities, purchases, and viewing or downloading documents (statements, etc.) should only be performed on a computer you know is safe and secure.

Minimize the amount of personal information published on social networking websites and use the security features offered.

A business may want to utilize a separate computer for banking purposes versus other internet accessibility.

Download Rapport from Trusteer for malware prevention and ensure additional online banking security with Hearthside Bank.

Email Security Tips

Never open attachments, click on links, or respond to emails from unknown senders.

Do not include sensitive information in emails.

Be suspicious of requests for personal information in an email. Hearthside Bank will never ask for this type of information in an email.

If concerned or suspicious of an email requesting personal information, contact the sender using a telephone number or website you know is legitimate to verify the information or request, not by selecting a link in the email itself.

Mobile Device Security Tips

Always use the keypad or phone lock on your mobile device when not in use. This password-protects your device to make it harder for someone to view your information. Be sure to store your device in a secure location.

If using Text Banking delete text messages from Hearthside Bank or any other institution frequently. Also delete these before loaning out, discarding or selling your mobile device.

Never disclose personal or financial information, including account numbers, passwords, Social Security number or birth date, through a text message, phone call, or email on your mobile device.

Download mobile apps from reputable sources, to ensure the safety of personal information.

For additional security, sign off when you finish using a Mobile App rather than just closing it.

Bank Account Security Tips

Immediately report any lost or stolen debit card, credit card, or checks to the issuer.

Review all account statements carefully and report any fraudulent activity as soon as it is discovered.

Use online Banking to monitor your accounts.

Do not print your Driver's License number, Social Security number, or any other personal information on checks.

Make sure to store checks and statements in a secure location.

Always keep your credit or debit card in a safe and secure place, as if it were cash or checks.

Do not put your card number in an email.

Do not provide your card number over the phone, if you did not initiate the call.