

Important Notice!

Please be aware that Century Bank Direct, a division of Century Bank of Kentucky, Inc., will NEVER solicit its customers by e-mail or telephone requesting personal information, passwords, or account information such as your credit card number, debit card PIN or social security number.

SECURITY STATEMENT

The banking professionals of Century Bank Direct, a division of Century Bank of Kentucky, Inc., place a high value on you and your business. The foundation of each relationship is built on trust, integrity, and character. Your trust in us depends on how well we keep your personal, business, and account information secure. We have in place an **Information Security Program** that is designed to ensure that your information is secure whether you choose to bank with us via the Internet, ATMs, telephone or our branch offices.

No matter which avenue of banking you choose, we verify you are who you say you are before granting access to your account information.

Security is everyone's responsibility. We, at Century Bank, take the safeguarding of your information seriously and instruct every employee to take responsibility to ensure your information is safe and secure. We also encourage you, the customer, to take steps to protect your personal information. For more information on how to prevent identity theft and what to do if you are a victim, view the [Federal Trade Commission](#) web site or call (877) ID-THEFT (877) 438-4338.

HERE IS HOW YOU CAN HELP

It is extremely important that you share in the responsibility of security. The following are some ways you can protect yourself and your accounts.

- Never provide personal financial information, including social security number, account numbers or passwords, over the phone or Internet if you did not initiate the contact. Contact the bank if you are in doubt. *Remember, Century Bank will NEVER ask you for this information. We already have it!*
- Shred all financial information when it is no longer needed. This includes all credit applications received by mail, insurance and investment information, and utility bills. Your mailbox and garbage are prime targets for fraudsters.
- Don't carry credit cards, social security card, passport or other documents if they are not needed.
- Don't place your social security number or driver's license number on your personalized checks.
- Review your account statements to ensure that all transactions are legitimate; if anything is suspicious, contact the bank and all card issuers.
- Obtain a free copy of your credit report once a year by contacting the three major credit-reporting agencies.
- Regularly log into your online accounts. Don't leave it for as long as a month before you check each account
 - Ensure that your browser is up to date and security patches applied; always visit your browser's home page to download the latest security patches even if they don't alert you to do so.
 - Always ensure that you are using a secure website when submitting credit card or other sensitive information via your web browser. A secure web server designation can be found by checking the beginning of the web address in your browser's address bar – it should read <https://> rather than <http://>.
 - When you are done with your transactions on the Internet Banking site, always click the Logoff button. When using a public PC (such as in a library or school), also close the browser when you are finished.

WHAT SHOULD I DO IF MY IDENTITY IS STOLEN?

- Contact Century Bank Direct **immediately** at (877) 444-2259. Report any fraudulent activity on your deposit account such as lost or stolen checks or VISA® Debit Card, or unauthorized transactions found in your account statement.

- Contact one of the three credit-reporting agencies. Request a copy of your credit report and look for any unknown inquiries or approved credit. Request that no further credit be approved unless you are contacted directly before approval is granted.

	Equifax	Experian	TransUnion
Report Fraud	(800) 525-6285	(888) 397-3742	(800) 680-7289
Address	P.O. Box 740214 Atlanta, GA 30374-0241	P.O. Box 9530 Allen, TX 75013	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92634
Dispute Credit Report Online	www.equifax.com	www.experian.com	www.transunion.com
Other Credit Report	(800) 685-1111	(888) 397-3742	(800) 916-8800
Address	P.O. Box 740241 Atlanta, GA 30374-0241	P.O. Box 2002 Allen, TX 75013	P.O. Box 1000 Chester, PA 19022

- Close any accounts that were opened fraudulently.
- Contact your local police and file a criminal report and keep a copy for your records.
- Contact the *Social Security Administration's Fraud Hotline* (800) 269-0271 to report the unauthorized use of your personal identification number.
- Notify the *United States Postal Inspectors Office*. Contact your local post office to report any crime involving stolen mail, or use of mail in a fraudulent scheme.
- Contact the *Federal Trade Commission* web site or call (877) ID-THEFT (877) 438-4338.
- Contact your credit card issuer(s) and have them close all accounts and issue new cards and PINs.

HOW DO PHISHING SCAMS WORK?

Phishing scams may take many forms, but they usually start with an e-mail, instant message or pop-up window asking you to update your personal information. One of the following often accompanies the request:

- A threat or warning that failure to update your information will result in the closure of an account or cancellation of a subscription
- An offer of a prize or some other form of financial compensation
- A note that you have received pictures or an instant greeting
- A confirmation of an online purchase

Phishing attempts may masquerade as official notifications from reputable companies, such as your bank, your credit card company, or a credit reporting firm. The message will usually encourage you to click on a link that takes you to a "copycat" web site designed to look identical to a legitimate site. Such copycat sites are also known as "spoofed" sites.

Once at the spoofed site, you may be asked to enter your screen name or username and password, your credit card number and expiration date, your Social Security number, or other personal information. Entering this information can give the phisher access to your account to send spam, steal your identity, make fraudulent purchases or otherwise use your identity.

HOW TO AVOID PHISHING SCAMS

- **Be suspicious of any e-mail or other message containing an urgent request for your personal information.** Phishing scams typically include upsetting or exciting (but false) statements to encourage victims to act immediately. They typically ask for information like screen names or other usernames and passwords, credit card numbers, Social Security numbers and more.
Remember, bank employees will NEVER ask for your password in an e-mail or instant message.
- **Even if you think a request for information may be legitimate, don't click the links in the e-mail to visit a web site.**

Sometimes links can be disguised to look like they are taking you to a real site, when they're actually taking you to a scam site. Instead of clicking a link, type the web site's address by hand to ensure that you go to the company or organization's real site.

If the request for information is coming from a company or organization with which you have a relationship, call them directly to confirm whether they actually need the information and, if so, whether you can provide it over the telephone.

- **Be extremely careful if you share personal or financial information online.**
Never provide sensitive information via e-mail or instant message. Providing this information via a web site is acceptable only if you are certain that the site is legitimate, and the site is secured (see below for additional information about secure web sites).
- **If you submit information to a web site, make sure the site is secure.**
Look for the "lock" icon on the status bar at the bottom of your browser window. The lock icon typically appears in the lower right-hand corner of the browser window. In addition, check the beginning of the URL or web address – if it starts with <https://> rather than simply <http://>, you are on a secure server.
- **Review credit card and other account statements regularly.**
If you see anything suspicious, contact your bank(s) and credit card issuer(s) immediately. If your statement is late by more than two or three days, call your credit card company or bank to confirm your billing address and account balances.
- **Keep your operating system and web browser up to date.**
To update your Windows® operating system and your Internet Explorer® browser, go to windowsupdate.microsoft.com. Follow the instructions there to check for updates, then download and install any critical updates.
- **Install and run anti-virus software and update it frequently.**
No matter which anti-virus program you use, make sure you keep it up-to-date, or it will provide less and less protection over time. Instructions for updating your software should be included in your program's manual or help area. You can also check the program manufacturer's web site for instructions.
- **Run firewall software on your computer.**
A firewall is your computer's first line of defense against harmful attacks from the Internet. If you have a broadband connection, use firewall software to hide your computer from hackers and help protect it from destructive computer Trojans and worms.
- **Report any phishing scams you receive to the following organizations.**
Forward the scam e-mail to the company featured in the e-mail if it is a legitimate company. Also, forward the entire e-mail to the [Federal Trade Commission](http://www.ftc.gov).