## Security

U.S. Century Bank understands that the security of your personal and business account information is important to you. We also understand that our continued success as a leading financial institution relies both on our ability to offer banking services to you in a secure manner.

U.S. Century Bank representatives will never call or email you and ask for your account numbers, password, PIN, credit card number, ATM/debit card number or social security number. Always keep this information private, even at home.

1) **How we protect you**

2) **How you can protect yourself and your identity**

3) **How to report fraud**

4) **Additional Resources**

## How we protect you

U.S. Century Bank's web site is protected by "SSL" or "Secure Socket Layer" encryption technology. SSL encryption of user activity is one way that U.S. Century Bank protects you from potential threats. In addition, you will notice the appearance of an "s" after the "http" on the Web address. The "s" in "https" indicates your session is secured. This provides you a stronger layer of protection while using online banking.

While, the encrypted transfer of information between your computer and the U.S. Century Bank website is secure and safe, it is important that you keep your operating system and browser up-to-date with the vendor provided updates to ensure you have applied the latest security levels on your system. Scammers often target known holes in popular browsers because many people use older versions of the software. You can avoid from having your computer compromised with malware by not downloading programs from the Internet, opening unknown email attachments or by sharing USB devices from unsafe sources.

U.S. Century Bank recommends that you use a hardware firewall, anti-malware software and that you stay current with all security patches for your computer. These additional layers of protection will assist to detect and deter potentially malicious activity on your computer.

**Protecting our Customer Information**
The Gramm-Leach-Bliley Act (GLBA) of 1999 requires all financial institutions to provide their customers with notice of their privacy policies. This act also prohibits financial institutions from sharing non-public identifiable customer information with non-affiliated third parties without giving customers an opportunity to opt out and prohibits the release of information to non-affiliated third parties for marketing purposes.

AT U.S. Century Bank, we are committed to protect the security and confidentiality of our customer's information. This is why our employees are educated on a yearly basis on the GLBA program, that way our customers' non-public information is kept confidential. Additionally, we have electronic, physical and procedural controls in place to protect this information.

U.S. Century Bank does not release any private identifiable information about former customers to third parties unless is permitted or required by law.

**Children's Online Privacy and Protection Act**
U.S. Century Bank complies with all the requirements of the Children's Online Privacy and Protection Act (COPPA). We will not collect any information from or about a child under 13 years of age unless we receive a parent's or guardian's signed statement of content. Such information will be protected and will not be disclosed to any third party without a parent or guardian authorization, except when is permitted or required by law. *"Please note that the responsibility for a child's online privacy rests in their parent or guardian's hands".*

## How you can protect yourself and your identity

**Below are tips on fraud prevention for online banking users:**

**User ID and Password Guidelines**

Create a “strong” password with at least 8 characters that includes a combination of mixed case letters, numbers, and special characters.
Change your password frequently.
Never share username and password information with third-party providers.
Avoid using an automatic login feature that saves usernames and passwords.

**General Guidelines**

Do not use public or other unsecured computers for logging into Online Banking.
Check your last login date/time every time you log in.
Review account balances and detail transactions regularly (preferably daily) to confirm payment and other transaction data and immediately report any suspicious transactions to your financial institution.
View transfer history available through viewing account activity information.
Whenever possible, use Bill Pay instead of checks to limit account number dissemination exposure and to obtain better electronic record keeping.
Take advantage of and regularly view system alerts; examples include:

Balance alerts
Transfer alerts
Password change alerts
ACH Alerts (for cash management users)
Wire Alerts (for cash management users)

Do not use account numbers, your social security number, or other account or personal information when creating account nicknames or other titles.
Whenever possible, register your computer to avoid having to re-enter challenge questions and other authentication information with each login.
Review historical reporting features of your online banking application on a regular basis to confirm payment and other transaction data.
Never leave a computer unattended while using Online Banking.
Never conduct banking transactions while multiple browsers are open on your computer.
Best practice is to suggest that company users dedicate a PC solely for financial transactions (e.g., no web browsing, emails, or social media).

**Tips to Protect Online Payments & Account Data**

Take advantage of transaction limits. Establish limits for monetary transactions at multiple levels: per transaction, daily, weekly, or monthly limits.
When you have completed a transaction, ensure you log off to close the connection with the financial organization's computer.
Use separate accounts for electronic and paper transactions to simplify monitoring and tracking any discrepancies.
Reconcile by carefully monitoring account activity and reviewing all transactions initiated by your company on a daily basis.

**Account Transfer**

Use limits provided for monetary transactions at multiple levels: per transaction, daily, weekly, or monthly limits.
Review historical and audit reports regularly to confirm transaction activity.
Utilize available alerts for funds transfer activity.

**Below are specific guidelines for Online Banking cash management Functionalities**

**ACH (Automated Clearing House Batches)**

Use pre-notification transactions to verify that account numbers within your ACH payments are correct.
Use limits for monetary transactions at multiple levels: per transaction, daily, weekly, or monthly limits.
Review transaction reporting regularly to confirm transaction activity.
Utilize available alerts for ACH activity.

**Wire Transfer**

Use limits provided for monetary transactions at multiple levels: per transaction, daily, weekly, or monthly limits.
Review historical and audit reports regularly to confirm transaction activity.
Utilize available alerts for wire transfer activity.

**Administrative Users**
Limit administrative rights on users' workstations to help prevent the inadvertent downloading of malware or other viruses.
Dedicate and limit the number of computers used to complete online banking transactions; do not allow Internet browsing or e-mail exchange and ensure these computers are equipped with latest versions and patches of both anti-virus and anti-spyware software.
Delete online user IDs as part of the exit procedure when employees leave your company.
Assign dual system administrators for online cash management services.
Use multiple approvals for monetary transactions and require separate entry and approval users.
Establish transaction dollar limits for employees who initiate and approve online payments such as ACH batches, wire transfers, and account transfers.

**Tips to Avoid Phishing, Spyware and Malware**
Do not open e-mail from unknown sources. Be suspicious of e-mails purporting to be from a financial institution, government department, or other agency requesting account information, account verification, or banking access credentials such as usernames, passwords, PIN codes, and similar information. Opening file attachments or clicking on web links in suspicious e-mails could expose your system to malicious code that could hijack your computer.
Never respond to a suspicious e-mail or click on any hyperlink embedded in a suspicious email. Call the purported source if you are unsure who sent an e-mail.

If an e-mail claiming to be from your financial organization seems suspicious, checking with your financial organization may be appropriate.

Install anti-virus and spyware detection software on all computer systems. Free software may not provide protection against the latest threats compared with an industry standard product.
Update all of your computers regularly with the latest versions and patches of both anti-virus and anti-spyware software.

Ensure computers are patched regularly, particularly operating system and key application with security patches.
Install a dedicated, actively managed firewall. A firewall limits the potential for unauthorized access to your network and computers.

Check your settings and select, at least, a medium level of security for your browsers.
Clear the browser cache before starting an online banking session in order to eliminate copies of Web pages that have been stored on the hard drive. How the cache is cleared depends on the browser and version you are using. This function is generally found in the browser's preferences menu.

**Tips to avoid becoming a victim of scams:**
Use online statements to reduce the volume of paper mailed. Today, paper is the cause of more actual instances of identity fraud than are electronic thefts.

Do not complete forms in email messages that ask for personal financial information. U.S. Century Bank would never ask you to complete such a form within an email message. Only communicate information, such as credit cards numbers or account information, via a secure website. When submitting financial information to a website, look for the padlock or key icon at the browser’s address bar, and make sure the internet address begins with “https:”. A secure web server designation can be found by checking the beginning of the web address in your browser’s bar and the address should begin with https:// rather than http://.

**Tips for Wireless Network Management**
Wireless networks can provide an unintended open door to your business network. Unless a valid business reason exists for wireless network use, it is recommended that all wireless networks be disabled. If a wireless network is to be used for legitimate business purposes, it is recommended that wireless networks be secured as follows:
Change the wireless network hardware (router /access point) administrative password from the factory default to a complex password. Save the password in a secure location as it will be needed to make future changes to the device.

Disable remote administration of the wireless network hardware (router / access point).
If possible, disable broadcasting the network SSID.
If your device offers WPA encryption, secure your wireless network by enabling WPA encryption of the wireless network. If your device does not support WPA encryption, enable WEP encryption.
If only known computers will access the wireless network, consider enabling MAC filtering on the network hardware. Every computer network card is assigned a unique MAC address. MAC filtering will only allow computers with permitted MAC addresses access to the wireless network.

## How to report fraud

If you are a U.S. Century Bank Customer and need to report fraud or identity theft, immediately contact the Bank at 1-888-809-9145.

To report fraud at the three major credit bureaus, contact their fraud departments directly and request that a fraud alert be placed on your credit file. The fraud alert requests creditors to contact you before opening any new accounts or making any changes to your existing accounts.

Equifax (www.equifax.com): 1-888-766-0008
Experian (www.experian.com): 1-888-397-3742
TransUnion (www.transunion.com): 1-888-909-8872

Next, close the accounts that you know or believe have been tampered with, and file a police report – be sure to retain a copy for your records. Also, contact all your banks, credit card issuers and other creditors on your own to report identity theft and protect your rights.

If you suspect your Social Security number has been compromised, call the Social Security Administration hotline at 1-800-772-1213 or locate and contact your local Social Security office.

Finally, file a complaint with the Federal Trade Commission (FTC, www.ftc.gov), which maintains a database of identity theft cases used by law enforcement for investigations, and can advise you on your next steps. You may also report identity theft to the FTC by calling 1-877-438-4338.

## Additional Resources

**Visit the following resources to get more information on fraud, identity theft and protecting yourself online.**

OnlineOnGuard.gov (https://www.onguardonline.gov/)
FTC Consumer Information (https://www.consumer.ftc.gov/)
Cyber Safety (https://www.dhs.gov/stopthinkconnect)
Common Internet Fraud (https://www.fbi.gov/scams-safety/fraud/internet_fraud)
Don't be an On-line Victim (https://www.fdic.gov/consumers/consumer/guard/)