



Personal Online Banking Fraud Prevention Best Practices



Protect your personal information, because confidentiality matters.

User ID and Password Guidelines

- Create a “strong” password with at least 8 characters that includes a combination of mixed case letters and numbers.
- Change your password frequently.
- Never share username and password information.
- Avoid using an automatic login feature that saves usernames and passwords.
- Never use parts of your Social Security Number in your password or part of User ID
- Never use names or phrases that relate directly to you.

General Guidelines

- Do not use public or other unsecured computers for logging into Online Banking/Bill Pay.

- Check your last login date/time every time you log in. You'll find this on the left side of your screen after you enter your password.

Bank of Tennessee

Account Summary Transfers & Payments

Account Summary

Show Account Detail ▾

- Item Correction
- Export File
- Request Report
- Upcoming Transactions
- Account Alerts
- Mobile Banking

Last Login Date
1/18/2012 3:08:33 PM ET

Message Center

You have no unread messages.

- View Messages
- Send a Message
- View Sent Messages

Quick Links

Show Account Detail ▾

Change Quick Links

- Review account balances and detail transactions regularly (preferably daily) to confirm payment and other transaction data and immediately report any suspicious transactions to Bank of Tennessee.
- View transfer history available through viewing account activity information.
- Whenever possible, use Bill Pay instead of checks to limit account number distribution and to obtain better electronic record keeping.

- You can set up your online banking to send you emails or text messages when certain situations or conditions occur on your account. Examples include:
 - Balance alerts
 - Transfer alerts
 - Transaction alerts
- 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.

Tips to Protect Online Payments, Account Data, Account Transfer

- When you have completed a transaction, ensure you log off to close the connection with the Bank of Tennessee's computer.
- Utilize available alerts for funds transfer activity.
- Read alerts scheduled to be sent to your email. Do not assume the emails you receive are expected and correct. Double check all transactions and amounts.

Tips to Avoid Phishing, Spyware and Malware

- Do not open e-mail from unknown sources. Be suspicious of e-mails posing to be from Bank of Tennessee, 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 e-mail.

- Call the purported source if you are unsure who sent an e-mail.
- If an e-mail claiming to be from Bank of Tennessee seems suspicious, you may contact us by calling 866.378.9500.
- 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, especially if using a broadband or dedicated connection to the Internet, such as DSL or cable.
 - 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.
- Back-up your device's data. This will allow you to restore your computer back to default factory settings and still allow you to maintain and reinstall data.