Best Practices for Personal Online Banking

FIRST BANK
The **one** who's here.

First Bank strives to offer online banking products that are secure and easy to use. Since First Bank does not implement, oversee or monitor the computer security for your Internet enabled devices such PCs and tablets, we are providing a partial list of things you can do to protect your accounts and information from fraudulent activity.

1. Your user id should not contain sensitive information such as an account or Social Security number. Create a strong password with at least 8 characters that Includes a combination of mixed case letters, numbers and special characters. **Do not share usernames and passwords.** Change your password a couple times each year.

Note: If you do not change your First Bank Online Banking password within a one year period, Online Banking will require our users to change their password.

2. Customers should familiarize themselves with **First Bank's account agreement** and with the customer's liability for fraud under the agreement.

3. **Never access bank or other financial services information at public hotspots** such as Internet cafes, airports, hotels, public libraries, or any other networks where you do not control. Unauthorized software may have been installed to trap account number and sign on information leaving the customer vulnerable to possible fraud.

4. **Verify use of a secure session (https, not http)** in the browser for all online banking or when submitting sensitive information online.

5. **Avoid using an automatic login feature** that saves user names and passwords for online banking.

6. After using online banking, **be sure to log out of the session and close out the Internet browser.** Never leave a computer unattended while accessing online accounts.

7. **Watch out for sudden pop-up windows** asking for personal Information or warning of a virus, or a warning of virus protection that has expired. This is called "scareware' because it frightens people into providing information, downloading malicious software or paying for removal.

8. **Pay attention to the toolbars at the top of your screen.** Current versions of the most popular Internet browsers often will indicate if you are visiting a suspicious website.

9. **Conduct all online banking activities from a dedicated and completely locked down computer.** Do not allow access to any email or websites other than the online banking site.

10. **Install anti-virus and anti-malware software on all computer systems**. Ensure virus protection and security software are updated regularly. Anti-virus is only secure if it has the most recent signatures and updates.

11. **Ensure computers are patched regularly** with security patches, especially operating system and key applications.

12. Enable your system's **firewall**.

13. **Utilize a sign-on password** on your computer.

14. **Never share User IDs and passwords with anyone**, and do not leave any such information or items in an area that is not secured. Use a unique login identification and password for online banking than any other website or software. Passwords should not contain predictable terms or numbers.

15. **Monitor & reconcile your accounts frequently.** Immediately review any electronic account transactions. Immediately report any suspicious activity on your accounts to Bank personnel.

16. **Do NOT click on a link in any email purported to be sent from the Bank.** Be suspicious of any emails purporting to be from any financial institution, federal, state or local government departments or agencies or taxing authorities that request account information. If you provide financial information and passwords for financial services in response to unfamiliar or suspicious websites, emails, text messages, telephone calls, mobile phone applications or social media messages, you should change your password immediately.

Note: First Bank will never send an Email requesting your Online Banking Sign On and password, personal information or information regarding your accounts with First Bank.

Thank you for choosing First Bank for all your banking needs. We are protecting your identity and funds with all the diligence as being your neighbor requires. If you have any questions concerning these precautions, we welcome your phone call at the Electronic Banking Center at 1-888-220-4446.