



Protect your personal
information, because
confidentiality matters.

User ID and Password Guidelines

- Create a strong password with at least 12 characters that includes a combination of mixed case letters, numbers, and special characters.
- If you use a password vault, use lengthy random-generated passwords and store them there.
- Change your password periodically (on the Security Preferences screen).
- If you suspect your User ID has been compromised, change it (on the Security Preferences screen) or contact customer service at the Bank.
- Never give your username and password information to others.
- Never store your username and password in the browser's cache.

General Guidelines

- Avoid using public computers for logging into Online Banking.
- Verify the last login date/time each time you log in. If you see a date and time that was not your activity, change your password and contact the Bank.
- Review account balances and detail transactions regularly (daily if possible) to confirm payments and other transaction information and immediately report any suspicious transactions to the Bank.
- Whenever possible, use Bill Payment instead of handwritten checks to limit exposure of your account number and for better electronic record keeping.
- Take advantage of and regularly view system alerts; examples include:
 - Low Balance alerts
 - High \$ debit transaction alerts
- Never leave a computer or phone unattended while logged in.

Tips to Avoid Phishing, Spyware and Malware

- Do not open e-mail from unknown sources. Be suspicious of e-mails claiming to be from a financial institution, government department, or other agency requesting account information, account verification, or banking access credentials such as usernames, passwords, PINs, or similar information. Opening a file attachment or clicking on a web link in a suspicious e-mail could expose your system to hackers.
- Install antivirus and antimalware software on all computers. Free software may not provide protection against the latest threats compared with an industry standard product.
- Ensure your computer's operating system, internet browsers, other major programs and antivirus software are kept updated and a firewall is active.
- Check your browser settings and select at least a medium level of security.
- Run anti-virus scans of your computer at least weekly.

Tips for Wireless Network Management

Wireless networks can provide an unintended open door to your network. It is recommended that wireless networks be secured as follows:

- Change the wireless network hardware (router/access point) admin 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).
- Be sure your router is set to use strong encryption. WPA2 is best.
- 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.

Contacting the Bank

If at any time you receive suspicious e-mails or phone calls claiming to be from Alliance Bank, or you identify or suspect unauthorized activity on your bank account, please contact the Bank immediately.

- Call or visit a Personal Banker at an Alliance branch.
- Call 704-867-5828 and ask for Operations.
- Email support@alliancebankandtrust.com.

If at any time you suspect unauthorized access to your account(s) through Online Banking and the Bank is not open, please log in and change your password as soon as possible, and then contact the Bank as soon as possible on the next business day.