Secure and Protect | Mobile and Online Protection

As your enduring financial partner AB&T is always looking out for you, especially when it comes to protecting your personal and financial information.

As consumers increasingly rely on digital platforms to manage their lives, including online and mobile banking, fraudulent activities conducted through these platforms is on the rise. Cybercriminals engaged in these activities exploit vulnerabilities to steal sensitive financial information, commit identity theft, or conduct unauthorized transactions, and it's a massive issue.

It's estimated that 76% of U.S. adults used mobile banking in 2023 and the global cost of cybercrime is expected to reach $10.5 trillion annually by 2025, with financial services being the top target. This puts customers' data and money at significant risk.

But once again, we're here to help

Here are some important tips that will help you keep yourself protected

- **Enable Two-Factor Authentication (2FA):** Add an extra layer of security to your accounts by enabling 2FA. This ensures that even if your password is compromised, your account remains secure.
- **Use Strong, Unique Passwords:** Avoid using easily guessed passwords like "123456" or "password," and avoid using the names of relatives or places you are associated with. Use a combination of letters, numbers, and special characters, to create unique passwords, or phrases, for each of your accounts. And avoid using the same password in multiple places.
- **Keep Your Software and Apps Updated:** Regularly update your mobile apps, operating system, and antivirus software on your computers, tablets and mobile devices to protect against the latest security vulnerabilities.
- **Be Wary of Phishing Scams:** Be on the lookout for suspicious emails, texts, or calls asking for personal or financial information. AB&T, and other legitimate companies will never ask for sensitive details through these channels.
- **Avoid emailing or texting sensitive information:** While you may have a need to send sensitive information digitally, never send this information through email or text without utilizing some form of secure portal system or encryption service.

- **Avoid Public Wi-Fi for Banking or other sensitive activities:** Public Wi-Fi networks are not secure. Avoid accessing your bank account or making transactions while connected to public Wi-Fi.
- **Install Banking Apps Directly from Trusted Sources:** Only download apps from official sources, like the App Store or Google Play, to avoid malicious versions.
- **Monitor Your Accounts Regularly:** Regularly check your AB&T and other financial accounts for unauthorized transactions and take the time to set up account alerts to stay informed of any unusual activity.
- **Use a Virtual Private Network (VPN):** When accessing sensitive information on public or unsecured networks, use a VPN to keep your data encrypted and private.
- **Log Out After Each Session:** Always log out of your banking apps or websites when finished, especially if you're using a shared or public device.
- **Report Suspicious Activity Immediately:** If you suspect fraudulent activity on your account, report it to us immediately. The faster you act, the better protected you are.

By following these steps, you can protect yourself and your financial information from cyber threats. Remember, your safety is our priority. If you have any questions, please don't hesitate to reach out.

Together, we can make our digital world safer for everyone.