Northwest Community Bank
YOUR COMMUNITY - YOUR COMMUNITY BANK FOR OVER 150 YEARS

Member FDIC

Mobile Banking Security Tips

Quick Tips to Protect Your Phone or Mobile Device

Lock it up. Ensure that your phone automatically locks after not being used for a specified period of time and if possible require a strong alphanumeric password to unlock the device. This will help to protect the data stored on your phone if it's lost or stolen.

Enable password protection. It's usually a four-digit numeric combination that is required to unlock and access the data on a mobile device. Use complex passwords whenever possible. Make sure you're not storing your User ID or passwords anywhere they could be easily discovered or stolen.

Be Wary of Unknown Text Messages. If you don't recognize the sender or the message seems strange or out of character, even if from a known friend, do not open the message or click on any Internet links within the message.

Disable Bluetooth. In public areas, others can detect your phone and access it through Bluetooth. If that happens, you will be sent a message alerting you. However, it's often safer to turn Bluetooth off or put it in non-discoverable mode to render them invisible to unauthenticated devices.

Know your apps. Be careful about downloading applications or other files to your mobile device, they may contain malicious content. Before you download files, make sure applications come from trusted sources.

Upgrade the firmware. Visit your phone manufacturer's Web site to download the latest firmware. Refer to your phone's user manual or contact your mobile carrier for more information.

Be Alert at Wi-Fi Hot Spots. In public spaces where your phone is using a Wi-Fi network, be careful about conducting sensitive business on your phone, like banking.

If your phone has the capability to Ask to Join Networks function you should enable it. This will ensure that you don't unknowingly connect to Wi-Fi networks while on the go.

Northwest Community Bank
YOUR COMMUNITY - YOUR COMMUNITY BANK FOR OVER 150 YEARS

Member FDIC

It's also a good idea to disable Wi-Fi whenever it's not in use. This reduces the chance of accidentally connecting to an unsecured or suspect network and saves the life of your battery.

Avoid joining unknown Wi-Fi networks.

Use anti-virus software. Review and utilize the security options available on your device and consider additional measures such as security software and antivirus solutions. Refer to your phone's user manual or contact your mobile carrier for more information on these features.

Back it up. Especially for smart phones that contain large amounts of data, it's important to periodically back up your device in case it's lost or stolen.

What to do if Your Device is Lost or Stolen. If your device is lost or stolen, notify your service provider immediately so they can disable your device to reduce the risk of information being accessed or charges being accrued. Also contact the bank so we disable your Online Banking account if necessary.

Know your phone. Keep a record of your phone's make, model, phone number, and serial number. Police will need this information during their investigation if your device is stolen.

Verify Your Personalized Image and Text During Online Banking Login. Reverse Authentication is designed to combat “phishing”* by providing two-way or “reverse” authentication. Specifically, this means that the Online Banking application is authenticating itself to you after entering your User ID and prior to inputting your password. This is accomplished by displaying the personalized image and text that you have chosen when you setup your Online Banking application. If your personalized image and text does not appear stop the login process and contact the bank immediately.

*Phishing is the practice of trying to trick someone into giving their secret bank information by sending them an e-mail that looks as if it comes from their bank and that asks them to give their account number or password