Wake Forest Federal

We pay more than interest. We pay attention!

Protect Yourself Online and Your Mobile Device

Although online and mobile banking has many advantages, it can also make users vulnerable to fraud, identity theft and other scams. We recommend that you consider the tips below to keep your information and your money safe.

- **Keep your computers and mobile devices up to date.** Having the latest security software, web browser or operating system is the best defense against viruses, malware and other online threats. Turn on automatic updates so you receive the latest fixes and security patches as they become available.
- **Establish strong passwords.** A strong password is at least eight characters in length and includes a mix of upper and lower cases letters as well as numbers and special characters.
- **Logout** completely when you have finished your mobile banking session.
- **Use caution when downloading apps.** Apps can contain malicious software and viruses. Beware of apps that ask for unnecessary "permissions." Read reviews and download only apps that show they have been downloaded countless times.
- **Avoid storing sensitive information** like social security numbers, passwords and account numbers on your devices.
- **Tell us immediately** if you change your phone number or lose your mobile device.
- **Use the PIN, passcode or other biometric lock** to secure your mobile device. This will make it difficult for a thief to access your phone should it become lost or stolen.
- **Be aware of shoulder surfers** who attempt to observe sensitive information you are entering. Be aware of your surroundings.
- **Wipe your mobile device before donating or trading it.** Use the manufacturer's recommended technique for removing all personal information.
- **If you lose your mobile device,** check to see if there is a procedure for remotely deleting all personal information on the phone.
- **Beware of phishing.** Phishing scams attempt to trick users into disclosing private account or login information. Avoid opening website links and attachments in emails or texts. Be leery of ads claiming that your device is infected.
- **Keep personal information personal.** Hackers use social media sites to figure out passwords and security questions for password resets. Lock down your privacy settings on social media sites. Be wary of requests to connect with people you do not know.
- **Secure your internet connection.** Always secure your home wireless network with a password. When connecting to a public Wi-Fi network, be cautious of the information you are accessing. If you are connecting to our mobile banking app or our online banking site, always use your data plan versus a public W-Fi platform.
- **Shop safely.** Before shopping online, make sure the website uses secure technology. Make sure the website address begins with" https". Also see if locked padlock symbol appears on the page.
- **Rooting or Jail breaking** involves customizing your phone for the express purpose of removing the tether to a particular service provider or operating system. Jail breaking a mobile device typically weakens the built in security features and can cause operating updates to fail. Both of those consequences may make it easier for fraud to occur.