General Online & Mobile Banking Safety Tips

Keeping your account information safe is a priority at OUR Credit Union. It is important that you help keep your account safe by protecting yourself while banking on your mobile device and online.

Take these precautions to help guard against threats to your computer and mobile devices.

If you use your smartphone, tablet, laptop, or other device to access your bank accounts be sure to incorporate these safety tips:

Use a Strong Password
Set passwords and enable screen locks to prevent others from using your computer or devices. Use a mix of characters and cases that are unique to each account or site you use.

Maintain Security Software
Make sure your operating systems, software and browsers are up to date and that anti-virus software and firewalls are in place when possible on all computers and devices.

Use Factory Settings
Uninstalling or removing the factory settings (jailbreaking or rooting) from your devices creates additional security risks.

Only Download Apps, Software and Attachments from Trusted Sources
Download apps and software from authorized vendors only. Others may appear credible but could contain viruses that put your device at risk. Only open attachments from sources you trust and understand what the attachments are for. Downloaded attachments are a great way to for outside sources to access your account information.

Keep Bluetooth Off
Keep Bluetooth turned off to help prevent others from accessing your device without your knowledge.

Use Secure Networks
Insecure Wi-Fi networks increase the likelihood your device and account information can be accessed from an outside source, putting your information at risk. Be extra cautious when using public computers or Wi-Fi. Hold off on making financial transactions until you're on a trusted device with a secure connection.

Check Accounts Regularly
Regularly check your account activity so you can report suspicious activity before it becomes an issue.

General Online & Mobile Banking Safety Tips
Store usernames and passwords somewhere other than on your mobile devices

- Clear your device's cache and history so that passwords, payment details and other saved personal information are deleted. Only store what you truly need.
- Check for a padlock symbol and "https" in your browser's address bar when submitting payment information or other personal details online, as these denote a secure site.
- Manually login to all apps
- Always log out of your account to ensure that your session is closed
- Delete text messages containing sensitive information
- Ignore text or emails requesting personal information
- Only click on links from trusted sources
- Mobile users should use their device PIN codes
- Encrypt information
- Limit sharing of your personal information and device
- Avoid lending your mobile phone to strangers to minimize the chance of someone downloading a malicious app onto the device.
- Be aware of privacy policies and terms and conditions on sites you use and anything you download.