Wanigas Mobile Banking Security Tip FAQs

Q. How can I protect my mobile device from fraud?
A. Keep your mobile device with you or secure the device when not in use with a password. Password protecting your mobile device with a pass-code lock can help keep your mobile device information safe and secure.

Q. Is it important to only download from trusted sources?
A. Yes, you should only download signed applications from trusted sources. If your mobile device is using the Android operating system, do not enable Android's "install from unknown sources" feature.

Q. I lost my phone, what should I do?
A. Change your online banking password immediately. Contact Wanigas to deactivate text banking from your mobile device. Report the loss to your phone carrier, and ask them to disable the old phone. As always, whenever there is a possibility of unauthorized access to your account, you should watch your account closely to ensure no unauthorized transactions appear.

Q. What daily steps can I do to keep my mobile device secure?
A. Frequently delete text messages received from the credit union and monitor your accounts frequently. Notify the credit union of any unauthorized transactions.

Q. I received a text message requesting my personal information. Should I send my personal information?
A. No. Do not respond to text messages requesting personal information, such as Social Security numbers, credit/debit/ATM card numbers, and account numbers.

Q. Should I consider antivirus software?
A. Yes, antivirus software can help keep your phone secure. Keep in mind not to modify your mobile device as it may disable important security features.

Q. Are there any safe practices I should use with my mobile device?
A. Yes, adopt safe practices as you would using your personal computers, including not opening attachments or clicking on links contained in emails received from unfamiliar sources.