

## Customs Credit Union's Top 10 Safety Tips for Smartphones

- **Never store passwords on your smartphone**

Many people still try to hide passwords or PIN numbers within the body of text or phone numbers. However, despite how cleverly you may think you've concealed them, criminals know what to look for and where. It's always best to commit these security details to memory and not record them anywhere this includes ticking applications that remember them automatically.

- **Turn off tethering, Wi-Fi™ and Bluetooth when not in use**

The most likely way your smartphone can be compromised is by downloading malicious software (malware) concealed in a file or application. Your Wi-Fi™ and Bluetooth™ are the entry point to your smartphone. When activated they are constantly scanning for other signals trying to connect – criminals can exploit this to send malware to your smartphone without your knowledge. Tethering also gives access to your computer, so if you don't need to connect, switch them off and close the door.

- **Only use Wi-Fi™ hot spots that are reputable and password protected**

If you connect to a shared **Wi-Fi™** hotspot, you are completely dependant on the security of the host network. If the network is unsecured, fraudsters can hijack it, give their own network a similar name and fool you/your smartphone into connecting to theirs instead. Here they can spoof all kinds of websites and trick you into divulging your personal details.

- **Installation of smartphone security software**

Once you connect your device to the internet vulnerabilities from fake phishing sites as well as viruses increase. Today security software tailored specifically for smartphones is available in the marketplace. Its important though as with your home PC to keep protections and software up to date and current. Ensure you "Activate smartphone security settings and password protection" and familiarise yourself with the features of your smartphone.

- **Programs that can remotely wipe data if you lose your smartphone are now available**

These are useful to stop any personal data being accessed by persons who may misuse it. Find out how they work and how you can activate them.

- **All smartphones have built-in security features** such as auto locking and password protection. While it may seem like a bit of an inconvenience at times, these physical security measures are your first line of defence in keeping your smartphone and your personal details safe.

- **Don't be tempted to 'jailbreak' your smartphone as this makes it vulnerable to malware**

If you crack the manufacturer's security on your smartphone, you not only make your warranty invalid but you make it much more vulnerable to attacks by cyber-criminals.

- **Limit the amount of personal information on your phone**

Criminals are interested in more than just your Internet Banking details. Any kind of personal information can be used to steal your identity and commit other kinds of fraud. They can apply for credit cards, personal loans – even mortgages, using your credentials. By being careful about the information you have stored on your smartphone to protect your identity in case of theft or loss.

- **Make sure you delete all personal details if you sell or discard your smartphone**

If you sell or discard your smartphone, it's crucial you delete all personal information first. This can include SMS messages, emails, photographs, contact details and Internet links. Criminals can use such information to commit fraud against you, or by pretending to be you.

- **Never open attachments or download applications from untrusted sources**

Criminals use infected documents and applications to spread their malware and compromise victims smartphones. Never open an attachment or download an application from a person or website that you don't know or have doubts about.