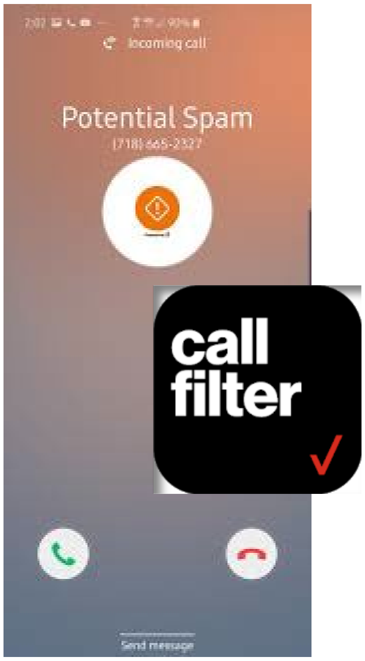
Week 4: Scam calls and securing your phone

It seems 50% of phone calls we receive these days are unsolicited – scammers, robocallers, etc. Even with the government's do not call list, scammers are still able to get through to millions of phones each year. In fact, 33.9 billion robocalls were placed nationwide so far this year. Watch the video from the FCC on how phone scams can play out and how to handle them.

Not only are these calls bothersome, but some people fall victim to the scams and give out personal information. To avoid this pitfall, it is best to let unknown callers go to voice mail. You then have the opportunity to listen to the message and make the best decision on how to respond.

Your other best defense is call filtering or call-labeling technology. The type of technology available to you depends on the phone – whether it is mobile or landline.

Wireless/Mobile



- AT&T: Mobile security and call protection services.
- Sprint: Call blocking options using My Sprint.
- T-Mobile: Call-protection options to identify or block potential scammers.
- U.S. Cellular: Automatic network call identification, labeling, and blocking app options.
- Verizon: Call Filter FAQS for screening and blocking unwanted calls.

Landline

- AT&T: Information on Digital Phone Call Protect service, call blocking, and other features.
- CenturyLink: Customer tips and tools to block unwanted calls.
- Comcast: Call blocking options for XFINITY Voice subscribers.
- Spectrum: Guide for using Nomorobo service to block robocallers.

Our province cell phone carriers, Verizon and AT&T, each offer a free service - Verizon Call Filter and AT&T ActiveArmor

Verizon subscribers automatically have the feature as part of their plan, it just requires you download their Call Filter app.

If you have an iPhone, you can download the app from the Apple store and if you have an Android device (Galaxy, LG, or HTC) you can download from the Play store . Please know, in some cases, these filters may *not* stop callers from getting thru but will help identify those that are potential scam calls.

For those on the AT&T province plan that would like the filtering feature, we ask you reach out to us at helpdesk@ssndcp.org or 1-800-373-7521 so the feature can be enabled on the account. Once enabled, AT&T will send a text message with a link to download their ActiveArmor app. View instructions on installing the app.

If you would like further information on the filters our province providers offer, please visit the following offerings. Check out the Verizon FAQ and How to Use Guide or watch a video with glimpses of how the app works. For AT&T subscribers, FAQs and a video are also available to become more familiar with the feature.

For any questions or if you would like assistance downloading and installing the apps on your smartphone, please reach out to us at helpdesk@ssndcp.org or 1-800-373-7521.

Securing your smartphone (iPhone, Galaxy, etc.)

It's not only about avoiding scam calls, we can take other steps to make our lives more secure when it comes to smartphones. Here are five tips to increase the security of your smartphone and what you store on it.

1. Enable the lock screen feature

Yes, we know it's a hassle. Yet it's the easiest way to prevent anyone from grabbing your phone and gaining instant access to every aspect of your life and job. Most employers won't let you use your personal mobile phone for business use without a passcode or passphrase. Do it! You'll get used to unlocking your phone. Steps on setting up a passcode for an iPhone and on an Android (Galaxy, etc).

2. Keep your operating system and apps up to date

There is a reason behind the regular updates to your phone's operating system and apps. The developers are staying one step ahead of hackers and ensuring your phone is as secure as possible. Don't delay! Install those updates – steps for Apple iPhones and Android phones. You can also set the operating system to automatically install to ensure you get the latest software (Apple | Android). For setting apps to automatically update, there is a separate setting (Apple | Android)

3. Backing up your data

For iPhone users, back up your phone data to iCloud. Android phone users can back up data syncing to Google. Your phone settings, photos, and documents can be easily restored if your phone is lost.

4. Set up Find My Phone and Find My Mobile

Apple iPhones have an app called Find My iPhone and Android has Find My Mobile. Enabling these apps will allow you to find your mobile phone if it is lost. If you can't find your phone, you can remotely wipe the data on it. That way a stranger can't use your mobile phone or access your private data.

5. Use secure WiFi

When you connect to a public WiFi network, such as at an airport, coffee or restaurant, you open your phone to anyone else on that network. Hackers will use an unsecured WiFi network to spy on your mobile phone. General web browsing is fine but ordering that next great book or doing banking should be done on your mobile phone providers network rather than unsecured WiFi.

We are here to help! If you have any questions or need assistance, please contact us at 1-800-373-7521 or via email helpdesk@ssndcp.org. To check out more articles about securing your digital life, visit our security awareness section.

*Statistics courtesy https://robocallindex.com/history/time 33.9 billion **robocalls were placed** nationwide so far in 2020**, equaling roughly** 103.4 **calls per person affected.***