NEW YORK STATE OF OPPORTUNITY. | Division of Consumer Protection

Know Your Settings

Electronic devices are an integral part of everyday life – computers, phones, tablets, gaming consoles, baby and pet monitors, security cameras, etc. There are even devices to help you manage your devices. Each device comes with settings, and every additional app or software on that device has its own settings. Add in software updates and new services with each app or device, and it can be overwhelming.

New software, apps and devices are generally defaulted to share the maximum amount of your data as possible. Without making any changes to settings, you can be "leaking" tons of personal data to all sorts of places.

The Division of Consumer Protection recommends looking at one device at a time and applying the following:

Location, Location, Location: Your device will broadcast your location - unless you tell it not to. Location settings can be tricky – sometimes you may want to use apps that tell you what is around, like restaurants and addresses. However, by regularly broadcasting your location, you not only inadvertently give away your personal information, you also drain your phone battery. Check your location settings for apps and software – either turn them off or **make the location only available when the app is active**.

Cameras and Microphones: Cameras and microphones are a part of every phone but live independently. **When you lock a phone, it does NOT lock the camera or microphone.** Any apps can access either the camera, microphone or both whether or not the phone is locked. Go into your settings for each of your apps to limit or stop access to cameras and/or microphones and prevent unwanted surveillance.

Passcode Protect: Most people are permanently connected with their phones, tablets and other devices. But at some point, we put them down. All it takes is a few seconds for someone to grab it and take a peek. Biometrics (finger prints or facial recognition) can help with additional security. However, the key to passcodes is to make the passcode unique (rather than "1234") and update them frequently.

Don't Become the Product: Everything you do on your computer or device creates a digital imprint. That information is often compiled, tracked and sold to interested parties to better market products directly to you. This new platform can create psychological marketing plans and often get consumers to buy more than normal. You can shut this feature off for your devices. Go to your device's main settings and look for the settings marked "Privacy." In your "Settings," look at the settings for each app. There are also sometimes settings within an app - particularly for social media - where there are more options for privacy within the application. For those types of apps, you should open the app and adjust those settings since those apps and software can still gather other information, even if information collection is turned off on the phone.

Social Media Logins: Many apps and software programs allow you to create an account by using your social media accounts. However, when you delete those apps, the social media app is not notified of the removal. That account and data are still accessible to someone who obtains or uses your social media app credentials. If you decide not to use an app that you accessed using your social media account, be sure to go into your social media account's settings and disallow that app's account. Annually check the list of apps you allow access through your social media account and delete any you do not recognize or no longer use.

Autofill: Saving usernames, passwords, and credit card information on your device saves time. Unfortunately, it also makes it easier for thieves to get access to that information if they access your account or device. Re-entering important information each time – as opposed to autofill – is an extra step to safeguard personal information.

Privacy Settings: Many apps, services and software have additional privacy settings, particularly those related to social media networks. To review, go into the "Settings" menu for each app, service and software program and see what "In Device" settings you can review. Review these app settings annually to catch any new setting changes. For instance, your internet and cell phone providers track your usage but sometimes you can limit what they have access to by adjusting the settings.

The Division of Consumer Protection's Consumer Helpline is 800-697-1220, available Monday to Friday, from 8:30 a.m. to 4:30 p.m. Consumer complaints can be filed at any time via the Division's website. The Division can also be reached via Twitter at @NYSConsumer or Facebook at www.facebook.com/nysconsumer.