Keeping your Information Private

Posted At : December 17, 2019 10:31 AM | Posted By : Admin
Related Categories: Security

There's a robust discussion relative to whether any personal data is really private anymore. There are those who are totally paranoid about data privacy and those who don't care at all - assuming that everything about them is public (somewhere). Like most of us, if you're in the middle, here's some good suggestions relative to keeping your personal information nominally private.

The Internet has blurred the lines between real world and the virtual one. Technology is barreling into our hands through smartphones at an unbelievable pace. This is good for productivity and progress, but it makes it easy for thieves to do their job.

The anonymity and location independence that comes with the Internet muddles the moral character of even the most ethical person. There's no assuming your phone and the information it stores is safe from the malicious intentions of the human mind.

Remember, the first line of defense in protecting your data is you. Learn about new threats, stay current and take the necessary precautions to keep your data safe. Here are tips that will give you some insight into keeping your devices safe:

1. Create strong passwords and change them often. Never save passwords on your device. Yes, it's convenient. Yes, it saves time. If you need to safely store passwords, look into a secure password manager. Criminals are getting smarter and need just one chink in the armor to get into the system to rob you blind.

2. Be conscious of privacy settings. Most apps offer privacy settings for users. This gives you the freedom to know how much and what kind of information is shared. Always choose the least amount of data sharing.

3. Obtain reliable security for your phone. Phones need as much protection as any other device, if not more. There are many security providers that offer free services. These can be risky as they mine data from your phone. Always go for a well-known service provider. Norton Mobile Security has a gamut of features that can protect your phone from most threats.

4. Back up your data via reliable hardware or software. Backing up data is often overlooked, but remains a very important aspect of data protection. Ransomware is a type of attack where hackers hold your data hostage for a ransom. There are cloud-based services that offer backup, or you can opt for Norton Security Premium, which includes backup capabilities.

5. Anti-theft your device. If your gadget is lost or stolen, tracking apps will help you find it. But how do you protect your confidential data before it gets into the wrong hands? Norton Mobile Security allows you to perform a "factory reset" to completely erase your lost/stolen Android device. This includes your confidential contact lists, text messages, call history, browser history, bookmarks and any other personal data.

6. Be careful what you do with your phone, and use a password. Entering a password every time you want to use your phone may be tedious, but it's also the first line of defense if your phone gets lost or stolen. Additionally, when you consider the vast amount of malware, Trojans and worms finding sneaky ways to get into your device, it is better to stay protected with a security system that does the work for you. App Advisor is a special feature provided by Norton Mobile Security. It prompts privacy risks, intrusive behavior of apps, excessive battery drainage and data plan usage. It also has call/sms blocking, anti-theft, contacts backup and protects your mobile phone from malware.

7. Watch out for Bluetooth vulnerabilities. Bluetooth technology offers incredible convenience. It also opens doors for security weaknesses. Make sure you turn off your Bluetooth when you are not using it. While there are options to place your Bluetooth activity in an invisible or undetectable mode, there are some malicious apps that can change that mode and expose your device to threats. That's one more reason to have a security system in place.

8. Keep your operating system up to date. "A hindrance" is what many people call operating system updates. They are annoying and sometimes time-consuming but are very important. Besides improving the functionality of the device, updates and patches contain critical security updates. Make it a point to update as soon as possible.

9. Beware of public Wi-Fi. Most home Wi-Fi connections are encrypted. Some public Wi-Fi connections are not. This means you're at risk of people monitoring your online activity. Sometimes, malware from someone else's device can infect your device. Ensure you've turned on your firewall, and have up-to-date malware protection, or you could run into problems.Delete data that you no longer use.

10. Close down any online service that you no longer use. There are many social networks that come and go. If you have signed up for any of these, they may have a wealth of your personal information that you willingly gave. But eventually when these services disappear, they take with them your information that can be sold as an asset.

No protection method is 100% foolproof, but there's clearly plenty you can do to keep your information safe. Educate yourself on the latest security tactics and tricks, use good 'ol common sense, and use Norton's advanced protection products to protect what's yours.