TREND MICRO™

How to Protect Data in Mobile Devices

A **TrendLabs** Digital Life E-guide

Carrying a mobile device nowadays is like having a second wallet. Instead of containing money though, your device contains data. This makes it an obvious attack target for hackers and cybercriminals. One careless move and your data can easily fall into the wrong hands. That's why it pays to learn how to protect the data in your mobile devices.

What's in Your Device?

You may not realize how much data is in your mobile device. Sending email, accessing social media, and banking online have become ordinary mobile device tasks.

What do bad guys want from your mobile devices? Pretty much anything that has to do with your identity. Examples would be your call logs, text messages, emails, photos and videos, app passwords, and GPS location.

They also want access to your online accounts like those for social networks, banks, app stores, and games. Those accounts might contain information like credit card numbers, addresses, and contact details, all of which are valuable to cybercriminals.

What should you look out for to protect your data from these bad guys?

Oversharing Online

Some view social networks as extensions of themselves but there is such a thing as oversharing. Personal details like vacation plans shared via social media can inadvertently wind up in the wrong hands. Your physical possessions are put at risk when you let people know you're away from home.

Oversharing also happens when you freely give out all your contact details. Did you know that this is how scammers and spammers can get to you? This is how 419 or Nigerian scam spam, emails that seek donations to fake causes, end up in your inboxes.

You might not even be aware that you're already oversharing. Most apps can sync with your social media accounts. This means that any activity on that app could be broadcasted to all your contacts. You may even be sharing everything with the public if your privacy settings aren't set properly.

Suspicious and Malicious Apps

The number of malicious and high-risk apps has risen over the past year. Malicious apps can account for data leakage incidents. These steal data by spying on your location history, reading your saved text messages, and sniffing out your personal details like user names and passwords.

But did you know that legitimate apps can also expose your data? Some legitimate apps seek too many permissions and have access to too many of your social networking accounts and information stored in your mobile devices.

Your privacy can also be at risk because of the ads in your apps. Apps with aggressive ad libraries can perform suspicious activities on your devices without user consent. These include collecting sensitive data such as call logs, phone numbers, and contact lists.

Open Connections

When you access open wireless networks through your mobile device, anyone on the same network can possibly see your online activities. Sniffer apps monitor and record unprotected data sent across a network. These can even allow others to access your Facebook, Twitter, and YouTube accounts if you're on the same Wi-Fi network. This means they can hack into your accounts and steal, change, or delete your personal data.

Weak Passwords

We all know the importance of creating a strong password but we don't always do so. People can easily hack into your accounts if you use weak or easy-to-guess passwords. Using the same password for different accounts like banking and email is even worse. That single password is like a master key for a wealth of information.

Password use shouldn't be limited to online accounts. Almost all mobile devices have a security lock function but only few choose to use it. Most opt not to use a password or PIN for convenience's sake. This is risky for users who lose their devices because anyone can immediately gain control of the sensitive information in it.

Unreliable Cloud Services

More and more cloud storage service providers are cropping but not all are created with security and data protection in mind.

In fact, some cloud services can put your data at risk. System downtime and legal problems encountered by the company can render your data inaccessible. Cloud storage providers can also shut down, forcing you to search for another provider to store your files.

Are You Protecting Your Data?

Protecting data your device should be a priority given the amount of information you store in it. Here's how:

- Use built-in security features. That way, only you can access the data stored in it. This adds another layer of protection should you lose your smartphone.
- Create strong passwords. Choose complex passwords. Investing in a password manager is also a good idea.
- Access only trusted Wi-Fi networks. Do not automatically connect to open Wi-Fi networks. If you need to use a public network, use a virtual private network (VPN) service to ensure your connection is secure and private.
- Scrutinize apps. Read reviews and check the developers' pages before downloading and installing apps. Verify permissions an app seeks before granting them.
- Invest in a security app. It would even be better if the security app can remotely lock a stolen device or wipe out the data in it.
- Periodically back up data. You can do so on your computer or via a trusted cloud service. Backing up data in the cloud allows you to access your data anywhere, anytime. Some apps even let you access all your data across multiple devices, saving you time.

Trend Micro Incorporated, a global leader in security software and solutions, strives to make the world safe for exchanging digital information. For more information, visit www.trendmicro.com.

Enjoy your digital life safely

Created by:
TrendLabs, The Global Technical Support & R&D Center of TREND MICRO