The Who, What, Why, and How of Mobile Privacy

A **TrendLabs** Digital Life E-guide

Now more than just tools for work and communication, tablets and mobile phones have tremendously become a huge part of our normal day-to-day activities.

You go about your normal day sending business or personal e-mails, downloading apps, or just updating your social media status, when up comes a little pop-up that has nothing to do with what you're actually doing. Then it simply dawns on you. You may have seen this product page before.

A simple search you've done in the past has come searching back for you.

Accessing user information both for legitimate and malicious purposes is no longer uncommon in the age of mobilization, where you do just about everything using a mobile device. But can breaching one's privacy be stopped? What should you do to protect your privacy from mobile threats like this?

Who?

You and Your Right to Mobile Privacy

Inherently, we are all given our right to privacy. But this easily gets violated whenever someone tries to access our personal information on any platform, without our consent or any given lawful reason. Breaching could be as simple as a friend spying on your Facebook account to marketing agencies deliberately studying the types of websites you visit.

With everything going mobile these days, it's not surprising that some, if not most of us, often disregard the value of privacy. Sometimes, we ourselves, enable data leaks by leaving traces of personal information that cybercriminals are more than happy to take advantage of.

In social media alone, a Trend Micro survey noted that only 38% of internet users know how to limit what they post online. Oversharing becomes a springboard for more severe types of cybercrime like identity theft with the creation of a number of malicious apps engineered to steal sensitive user data.

What?

Key Areas to Look Over

Your Device Settings

Your default device settings serve as suggestions you can use to increase protection. By familiarizing and modifying these settings to suit your mobile needs, you can be assured that no one has easy access to your mobile device. Getting familiar with these settings could gain you more security.

Your Connectivity Features

As much as Bluetooth and wireless connections were designed to make communication easier, these have also been exploited for malicious reasons. Bad guys who hack into your network use sophisticated tools to sniff out credentials and information transmitted to and from your devices.

This has happened in MAC desktops using the INQTANA worm, which sent malicious files to available Bluetooth devices that accept them. This then opened doors to more malicious routines like malware dropping and information theft.

Your Mobile Behavior

Owning mobile devices gives you the freedom to access the online world more frequently. But does it change your behavior when it comes to security? This freedom often makes mobile users more vulnerable to threats through mobile activities like social networking, shopping and banking.

Cybercriminals are stepping up the production of threats that affect not only desktop computers but mobile devices as well—be it in social networking sites, online stores, and even banks—and they won't just stop at creating apps that could easily be mistaken for legitimate ones.

The 2013 TrendLabs Security Report noted a significant growth of crimeware that went after the victim's money. 2013 statistics saw the growth of almost a million new banking malware variants—an alarming figure that doubled from where it was in 2012.

In this regard, vigilance on bad URLs accessed through mobile devices is needed to ensure you do not enable the execution of more malicious routines in your device.

Why?

Money as the Driving Force

Mobile devices have impressively democratized one's online activities. But at the same time, it has opened doors to vulnerabilities exploited by cybercriminals driven by one agenda: money.

By the end of 2013, malicious and high-risk apps reached the 1.4 million mark and those with information-stealing abilities grew from 17% at the start of 2013 to almost a quarter by year's end. We also projected a more alarming figure of over 3 million malicious and high-risk apps to be released by the end of 2014.

Not only did the number grow, the sophistication and capabilities associated with these threats grew as well. Cybercriminals are always on the lookout to steal information stored in smartphones and tablets that can be used for profit.

How?

Scenarios that Put Privacy in Peril

Are Your Apps Really Free?

It is so easy to get lost in the number of free apps you can download these days. One click and you can enjoy the game everyone's talking about or a music app that gets you going at the gym.

But remember that there's always a trade-off. If they don't charge you for using their app, they could be earning by reselling your personal information. And it is surprising to know that a majority of consumers are willing to trade their data for free access to a mobile service or app? After all, who doesn't love free stuff?

But remember that even the smallest bit of information you give out could cause you more trouble than good. Your address or your birthday can be used by cybercriminals to milk you for profit.

Device Loss or Theft

No matter how careful you are with what you store in your mobile device, once it gets lost or stolen, you have little-to-no control over what happens with the sensitive files or data you have in them.

End-User License Agreements (EULAs)

Online service developers will always look out for themselves. You see it on the terms they ask you to agree with that they can change at any time, with or without notice. Before saying yes to these EULAs, you should read up and familiarize yourself with what's stipulated. You may end up allowing them to sell your photos, track your online activities or hand over information to authorities without your knowledge.

Bring Your Own Device (BYOD)

The BYOD trend continues with companies that allow their employees to use their personal devices for work-related activities. But one should be wary of using their laptops, smartphones and tablets for work, since even a company's IT department could use a set of protocols that can give them the liberty to access your personal files and information.

What now?

Reinforcing Mobile Privacy

Anyone could fall victim to cybercriminals trying to breach your privacy. But there are still stops you can pull to prevent this.

General Checklist:

- Configure your device' privacy and browser settings to control the amount of information it shares.
- Activate screen locks and passwords to minimize chances of hacking and change passwords every three months for security.
- Refrain from storing compromising files (photos and videos) you're not comfortable with on your device
- Clear your mobile browser cache regularly to avoid data leakage and information-stealing malware.Constantly monitor your app and account settings to make sure sharing and connectivity are secure.

- Enable your device's data encryption and configure your passwords.

The Lowdown on App Use

- Download only from trusted sources like the developer's website or from Google Play. Remove apps not in use.
- Always check the app's permissions to ensure that it doesn't perform functions outside of its intended use.
- Use your mobile browsers' private browsing settings, especially for sensitive transactions like online banking.

Device Loss or Theft Readiness

- Take note of your account credentials or make use of a convenient password manager when the need to reset them arises.
- Backup files with irreplaceable information in the cloud.
- Prepare to contact the authorities, your service provider, and concerned organization to avoid the

malicious use of your identity and to block bill charges.

- Sign up for a reliable remote service that allows you to find, lock or wipe your device when you need to.

Check your BYOD Agreements

- Are you required to produce personal devices for forensic analysis?
- Does this apply to devices shared with other family members?
- Who can access personal information stored in your device?
- Can your company track your location? Is this a requirement? Do they have notifications if the need for this arises? Under what circumstances?
- Are your personal online activities monitored? Are these systems active outside regular work hours?
- Is this information retained when you leave the company?

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

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