BRANDPROTECT EXECUTIVE THREAT BRIEF

brandprotect™

February 2015 | Briefing 3

## WHAT'S ON YOUR PHONE?

Do you know where your mobile phone or tablet is? Of course you do. When your phone is misplaced, or offline it is a big deal. For most professionals, the phone is the first, last, and primary piece of technology that is used during the day.

You carry your device everywhere, and you trust it with your most intimate information – personal and corporate, address books, business email and attachments, schedules, and health data. And you use your phone to connect to everything that matters to you – work, colleagues, classmates, family and friends. You use it to document and communicate everything, from taking snapshots of people you are with, places you are and even the food you eat, and you post your latest news on LinkedIn Facebook, Instagram, Twitter and YouTube.

## IS IT SECURE? *Do you trust the apps that are on your phone.*

All of the apps you download, from news sites, to social media, to banking apps to games have access to some or all the personal information in your mobile device. And the apps that you download, even seemingly trusted apps from reputable vendors, may have been altered or hacked to pirate that information and transmit it to criminals.

## BEWARE: MOBILE APP MALWARE CAN...

- Access and transmit sensitive passwords or financial information
- Make international calls from your phone number
- Access your contacts via address books and social media lists
- Send SMS messages or emails to your contacts and friends "from" the owner of the device
- Obtain GPS location information in real time
- Seize your photo albums and cameras
- Capture other applications, such as shopping apps, or worse yet online banking or investment apps

## PROTECTING YOUR PERSONAL INFO

**Is this happening to you? You might have a rogue app on your**

**Illegitimate mobile apps may drain your phone battery fast.** If your battery is running low quicker than usual, it might be a sign of infection with malware.

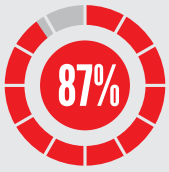
**Check your phone bill usage periodically**, at least a few times a month – and keep tabs on any suspicious activity. If you spot something unusual in your phone bill, contact your mobile network provider

**Always have a mobile security app** from a trusted vendor installed on your device, this will enable you to spot any malware trying to access your phone

# BRANDPROTECT STATPACK

*Source Arxan, State of Mobile App Security, November 2014*


**97%** of top paid android apps have been hacked




**87%** of top paid iOS apps have been hacked


**80%** of the most popular free Android apps have been hacked


**75%** of the most popular free iOS apps have been hacked

Malicious apps don't necessarily break anything - making them difficult to detect -instead they run silently, tracking movements and periodically **TRANSMITTING NEW CONTACTS, PASSWORDS** and other data to the bad guys.

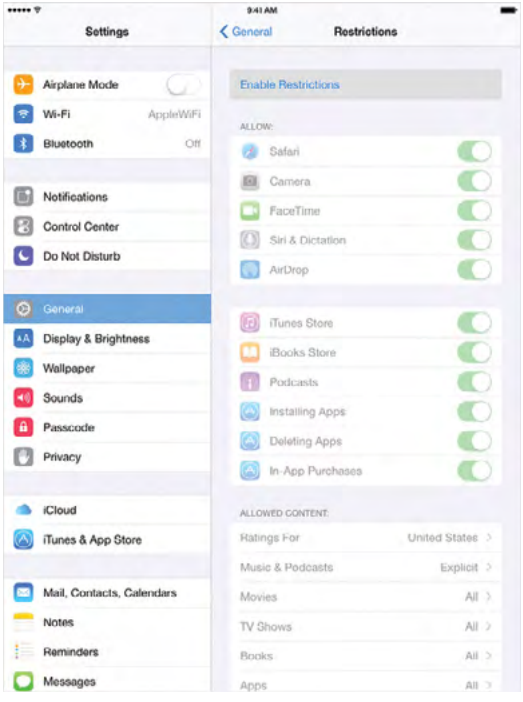
## YOU ARE JUST FOUR STEPS FROM REDUCING YOUR MOBILE THREAT PROFILE

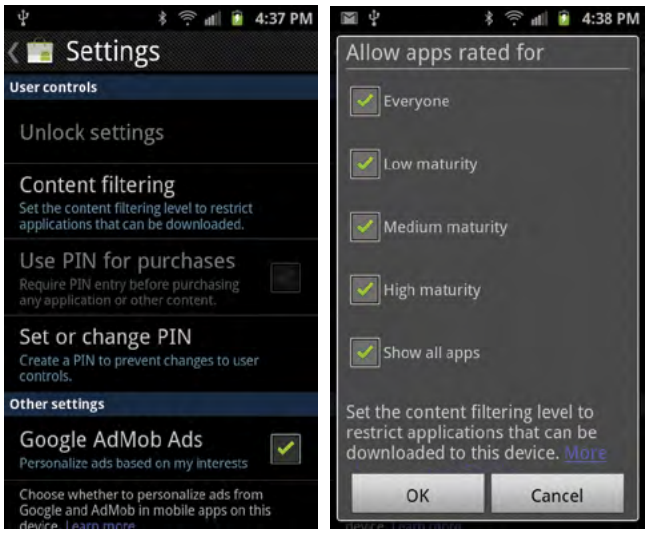
1) **Conduct a self-audit of your device.** Do you know what all those pages of applications are? *Do you really need them?* Android users can use a special tool "RescueTime" (available at GooglePlay) to log the actual time you spend in each application on your device.

2) **Remove the applications you don't need**, and make sure you have downloaded the latest version of the applications you do need from a reputable online store.

3) **Use your "street smarts" when downloading apps.** Download only from trusted sites. Check that you recognize the publisher. When in doubt, look online for news or alerts about the app.

4) **Limit downloads of new apps, especially by others.** It is easy to use the parental controls and settings (available in both iOS and Android) to password protect, limit, or disable application downloads. In just a few seconds, you will dramatically reduce your vulnerability to unexpected malware.



## FLAPPY BIRDS CLONES – FRIEND OR FOE?? FOE!

Last summer new media widely reported that approximately 80% of the copycat version versions of one of the most popular mobile games – Flappy Birds – had been hacked. AntiMalware company McAfee reported that "cyber crooks were able to remotely hijack users' phones to make calls without permission, steal contact list data, and track their exact GPS location. Even worse, many of the clones also enabled attackers to establish root access for "uninhibited control over anything on the device, including the recording, sending, and receiving of SMS messages." **Ouch!**

Knock-off or copycat apps are especially dangerous. Sometimes they appear to be "free" versions or clones of the most popular applications, especially games. These knock-off applications often times contain adware or malware. While adware is invasive and annoying, malware can wreak havoc on your personal information and the information of your contacts.

brandprotect™

www.brandprotect.com
sales@brandprotect.com | 1.866.721.3725



For enterprises concerned about their business exposure to increasing online risk, BrandProtect™ provides a complete suite of world class Internet threat detection services to monitor the entire social Internet spectrum and mitigate business risk arising from fraudulent or unauthorized online activity. BrandProtect, helps security, risk management, and marketing organizations at leading financial services institutions, large-scale retailers, insurance providers, telecoms, pharmaceuticals and more, protect their brand value and business bottom line.