CMSGu2019-02

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Mobile Devices Security (Updated)

CERT-MU

National Computer Board
Mauritius

Version 3.0

August 2019

Issue No. 2

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this document, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

Table of Contents

1.0 Introduction

1.1 Purpose and Scope

The previous guidelines offered a general insight into the risks associated with mobile devices, the security posture of different mobile operating systems available and provided the countermeasures available to minimise them. This guideline has been updated and the most commonly used mobile operating systems in use today are Apple's iOS and Google's Android and the associated best practices have been covered.

1.2 Audience

The intended audience for this document include users of mobile devices, security professionals, IT managers, system and network administrators involved in the support of mobile devices.

1.3 Document Structure

This document is organised into the following sections:

Section 1 provides a brief overview of the document's content.

Section 2 projects a background on mobile devices and their underlying risks.

Section 3 presents the two most commonly used mobile operating systems.

Section 4 gives best practices to protect your mobile device safe from attackers.

Section 5 concludes the document.

Section 6 contains a list of references used in drafting this document.

2.0 Background

Mobile devices, more specifically, smartphones, have become such an integral part of our life that it is hard to imagine how people used to communicate, access and share information, and even pay bills without them. Because of their size, we tend to forget that they are actually extremely powerful computers and that they should be secured as such.

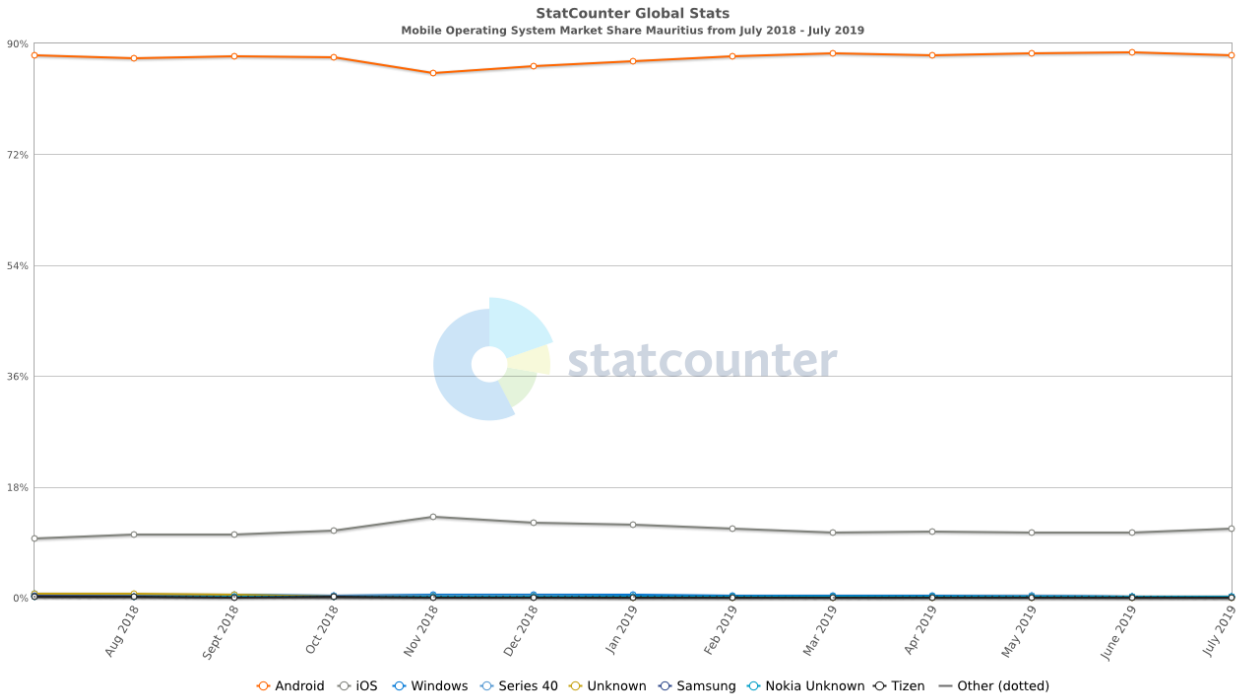
The number of smartphone users around the world has exceeded the five billion mark by 2019. This rapid increase, unfortunately, sees cybercriminals adapting and changing their methods to profit from this growing number of potential victims.

Cybercriminals continue to look for ways to exploit vulnerabilities in apps, operating systems, and software, trying to capitalize on security flaws before manufacturers find and patch them. User data is a major target of cybercriminals. From credit card credentials to email passwords and contact lists. Victims have also been baited into downloading adware or subscribing to paid services. The mobile threat landscape is not just filled with rooting malware and information thieves. The increasing usage of mobile devices, particularly by businesses, continues to draw attention to new types of threats.

Since cybercriminals usually cast wide nets to reach more potential victims, mobile users should protect their devices early on to defend against threats.

3.0 The two most commonly used Mobile Operating Systems

According to StatCounter, Android and iOS remain the most widely-used mobile operating systems in Mauritius and worldwide. The below graph shows that Android is more popular than iOS.



2.1.1 Android OS (Google Inc.)

The Android mobile operating system is Google's open and free software stack that includes an operating system, middleware and also key applications for use on mobile devices, including smartphones. Updates for the open source Android mobile operating system have been developed under "dessert-inspired" version names (Cupcake, Donut, Eclair, Gingerbread, Honeycomb, Ice Cream Sandwich) with each new version arriving in alphabetical order with new enhancements and improvements.

2.1.2 iPhone OS / iOS (Apple)

Apple's iPhone OS was originally developed for use on its iPhone devices. Now, the mobile operating system is referred to as iOS and is supported on a number of Apple devices including the iPhone, iPad, iPad 2 and iPod Touch. The iOS mobile operating system is available only on Apple's own manufactured devices as the company does not license the OS for third-party hardware. Apple iOS is derived from Apple's Mac OS X operating system.

4.0 Keeping your mobile device safe from attackers

The below security tips will help you secure your phone and prevent malicious programs or people from accessing it. The more of these you implement, the safer your device will be.

4.1 Protecting your Android Device

This section gives you a couple of security best practices for your Android device.

1. Only buy smartphones from vendors who release Android patches quickly

Google ensures that its smartphones, such as the Pixel, the Pixel 2, Nexus 5X, and 6P get the latest updates. This means they get the newest security patches as soon as they are released. As for other major vendors, Android Authority, the leading Android publication, found, the best vendors for keeping their phones up to date were, in order, from best to worse: LG, Motorola, HTC, Sony, Xiaomi, OnePlus, and Samsung.

2. Lock your phone

The traditional Personal Identification Number (PIN) remains the safest way. Fingerprints, patterns, voice-recognition, iris scanning, etc. are also other ways to set a screen lock.

3. Use two-factor authentication

While you are securing your phone, it is recommended that you lock down your Google services as well. The best way of doing this is with Google's own two-factor authentication:

- Login-in to your Google account and go to the two-step verification settings page.
- Once there, choose "Using 2-step verification" from the menu.
- From there, follow the prompts.
- You will be asked for your phone number. You can get verification codes by voice or SMS on your phone.
- In seconds, you will get a call with your verification number.
- You then enter this code into your web browser's data entry box
- Your device will then ask you if you want it to remember the computer you are using.
- If you answer, "yes" that program will be authorized for use for 30-days.
- Finally, you turn on 2-step verification and you are done

You can also make this even simpler by using Google Prompt. With this you can authorize Google apps by simply entering "yes" when prompted on your phone.

4. Only use apps from the Google Play Store

The vast majority of Android malware comes from unreliable third party application sources. Rogue apps are very often implanted into the Google Play Store.

Google has made the Play Store safer than ever. For example, Google Play Protect can automatically scan your Android device for malware when you install programs. Make sure it is on by going to Settings > Security > Play Protect. For maximum security, click Full scanning and "Scan device for security threats" on.

5. Use device encryption

To encrypt your device, go to Settings > Security > Encrypt Device and follow the prompts.

6. Use a Virtual Private Network (VPN)

If you access free Wi-Fi on your mobile device, make use of a mobile VPN. Examples are F-Secure Freedome VPN, KeepSolid VPN Unlimited, NordVPN, Private Internet Access, and TorGuard.

7. Password management

The same password should not be used for everything, which makes it difficult to memorise all passwords. Hence, a password management program could be utilised. Google comes with one built-in. However, if you do not want to store your passwords in a single repository on the cloud, there are others such as LastPass, 1Password, and Dashlane.

8. Use anti-virus software

Google Play Protect does a good job of protecting your phone, however, it does not protect against malware. Some of the best freeware antivirus programs that can be used for malware protection are Avast Mobile Security & Antivirus and Norton Mobile Security

9. Turn off connections when you do not need them

If you are not using Wi-Fi or Bluetooth, turn them off. Besides saving some battery life, network connections can be used to attack you.

10. If you do not use an app, uninstall it

Every application comes with its own security problems. Most Android software vendors do a good job of updating their programs. If you are not using an application, you should uninstall it. The fewer program doors you have into your smartphone; the fewer chances an attacker has to invade it.

4.2 Protecting your iOS Device

In addition to the some of the above tips which are applicable, this section gives you specific security best practices for your Apple (iOS) device.

1. Use Passcode protection

By default, the user's passcode can be defined as a numeric PIN. On devices with Touch ID or Face ID, the minimum passcode length is four digits. Users can specify a longer alphanumeric passcode by selecting Custom Alphanumeric Code in the Passcode Options in Settings > Passcode.

Longer and more complex passcodes are harder to guess or attack, and are recommended. The following passcode policies are available:

- Allow simple value
- Require alphanumeric value
- Minimum passcode length
- Minimum number of complex characters
- Maximum passcode age
- Passcode history
- Auto-lock timeout
- Grace period for device lock
- Maximum number of failed attempts
- Allow Touch ID or Face ID

2. Use strong Apple ID passwords

An Apple ID is the account that is used to sign in to Apple services such as iCloud, iMessage, FaceTime, the iTunes Store, Apple Books, the App Store, and more. It is important for users to keep their Apple IDs secure to prevent unauthorized access to their accounts.

Creating strong Apple ID passwords Apple IDs are used to connect to a number of services including iCloud, FaceTime, and iMessage. To help users create strong passwords, all new accounts must contain the following password attributes:

- At least eight characters
- At least one letter
- At least one uppercase letter
- At least one number
- No more than three consecutive identical characters
- Not the same as the account name

3. Use two-factor authentication

To help users further secure their accounts, Apple offers two-factor authentication, an extra layer of security for Apple IDs. It is designed to ensure that only the account's owner can access the account, even if someone else knows the password. With two-factor authentication, a user's account can be accessed only on trusted devices, such as the user's iPhone, iPad, or Mac.

To sign in for the first time on any new device, two pieces of information are required, the Apple ID password and a six-digit verification code that is automatically displayed on the user's trusted devices or sent to a trusted phone number. By entering the code, the user verifies that they trust the new device and that it's safe to sign in. Because a password alone is no longer enough to access a user's account, two-factor authentication improves the security of the user's Apple ID and all the personal information they store with Apple.

4. Use two-step verification

Since 2013, Apple has also offered a similar security method called two-step verification. With two-step verification enabled, the user's identity must be verified via a temporary code sent to one of the user's trusted devices before changes are permitted to their AppleID account information; before signing into iCloud, iMessage, FaceTime, or Game Center; and before making an iTunesStore, Apple Books, or App Store purchase from a new device.

Users are also provided with a 14-character Recovery Key to be stored in a safe place in case they ever forget their password or lose access to their trusted devices. While most new users

will be encouraged to use two-factor authentication, there are still some situations where two-step verification is recommended instead.

5. Turn on Find My iPhone

When Find My iPhone is turned on, the device cannot be reactivated without entering the owner's Apple ID credentials or the previous passcode of the device.

5.0 Conclusion

Many people have ample knowledge about different mobile phones and their companies, but a very few of them know about operating systems. It is important to learn about the major mobile operating systems in use today so that you can know what is behind your smartphone's smooth and colourful touchscreen and how to protect yourself and your devices against potential threats.

6.0 References

- www.it.ucla.edu
- www.trendmicro.com
- www.zdnet.com
- www.webopedia.com
- https://gs.statcounter.com
- https://mybroadband.co.za
- www.apple.com
- www.shoutmeloud.com