DIGITAL MEDIA LITERACY AWARENESS ON MOBILE DEVICE SECURITY ISSUES

Nik Zulkarnaen Khdzir[1], Shekh Abdullah Al-Musa Ahmed[2]

[1]Global Entrepreneurship Research and Innovation Centre /
Centre of Computing and Informatics
Universiti Malaysia Kelantan
Malaysia.

[2]Faculty of Creative Technology and Heritage,
Universiti Malaysia Kelantan, Malaysia

E-mail: zulkarnaen.k@umk.edu.my, almusa.cl7e002fi@siswa.umk.edu.my

ABSTRACT

Digital literacy is the set of competencies required for full participa- tion in a knowledge society. It includes knowledge, skills, and behaviors involv- ing the effective use of digital devices such as smartphones, tablets, laptops for purposes of communication, expression, collaboration and advocacy. Along with this expansion came a number of security issues to affect mobile devices. A chance to have a tiny and powerful device that is Internet linked and allows communication from anywhere at any time is alluring as well as a problem for companies. Many individuals who have attached their personal smartphones to corporate networks have found out the hard way the cost of doing so. Specifi- cally, there have been a handful of cases where individuals who attached their own personal devices to a company network had their personal phone wiped and all their data and other information lost that was stored on it. Why did this happen? Simply put, a system administrator sent out a remote wipe command to the device and instructed it to wipe itself of all apps and data to keep it from falling in the wrong hands. Or an administrator may have found the device and did not recognize it, so they wiped it in response. If we have an Android device or have read about the operating system, you may have heard the term "rooting the device." In a nutshell, this refers to undertaking a process of gaining root access to a device. Typically, this involves running an application or script that grants root access to the user. Once access is granted, the user can do pretty much whatever they want on the system without restriction. However, one of the downsides of this process is that the device is now exposed to greater danger from external threats as well. Moreover this article focus on how digital devices such as smartphones communication and store information for "media educa- tion" that is used to define the process of teaching and learning about media. It is about developing people's critical and creative abilities when it comes to mass media, popular culture and digital media. Since digital media is using smartphone for store information and article also referring how to maintain se- curity of these smartphone data.

1.0   INTRODUCTION

The rapid adoption of the mobile device in the workplace has already estab
lished two apparent consequences: a rise in productivity and capability
in addition to a corresponding rise in the number of security hazards. The
designers of devices have frequently made a trade off between security and
features by angling toward features, with security being an afterthought [1].

Figure :1.1 : Various aspect of digital literacy awareness

Whilst new security features have helped to somewhat reduce the issues
present, many of the devices have problems to be re- solved . Nevertheless
digital literacy is the set of competencies required for full partic- ipation in
a knowledge society. It includes knowledge, skills, and behaviors involving
the effective use of digital devices such as smartphones , tablets , laptops for
purposes of communication, expression, collaboration and advocacy. While
digital literacy initially focused on digital skills and stand-alone computers, the
focus has shifted from stand-alone to network devices including the Internet
and social media. The term digital literacy was simplified by Paul Gilster in
his 1997 book Digital Literacy. Gilster described digital literacy as the usage
and comprehension of information in the digital age, and also emphasized the
importance of digital technologies as an "essential life skill [2][3] ".

2.0   THE CHALLENGE OF DIGITAL MEDIA LITERACY ON MOBILE SECURITY

Several steps have recently been taken, but overall there is an attempt to strategy the challenge of digital media literacy on mobile security through five key areas. [4] Each addressing a specific problem or need.
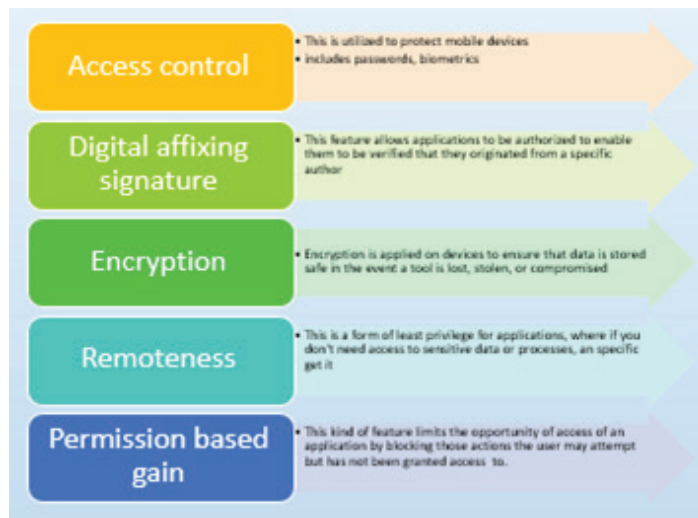

Figure 2.2 : Showing the challenge of Digital media literacy

2.1   ACCESS CONTROL

This is utilized to protect mobile devices, which includes passwords, biometrics, and least-privilege technologies, to name a few.

2.2   DIGITAL AFFIXING SIGNATURE

The digital affixing signature to is now part of the application model of most if not all mobile OSs. This feature allows applications to be authorized to enable them to be verified that they originated from a specific author, and in addition they simply cannot be tampered with without such activities being recognized . While digital signing is not necessary, Android will not allow the setting up of applications from unidentified sources by default. In iOS, applications from unidentified sources may not be installed at all unless the particular owner specifically modifies or "jailbreaks" the phone to allow this.

2.3   ENCRYPTION

Encryption is another essential component for digital media literacy of the security model of a mobile OS. Encryption is applied on devices to ensure that data is stored safe in the event a tool is lost, stolen, or compromised. Although not constantly   im- plemented on many mobile devices during the past, this has changed, with Android 6. 0 (codename Marshmallow) even requiring storage space encryption by default[5][6].

2.4   REMOTENESS

Remoteness , which seeks to limit the access an software has, is an important issue addressed in mobile devices. Essentially, this is a form of least privilege for applica- tions, where if you don't need access to sensitive data or processes, an specific get it.

2.5   PERMISSIONS-BASED GAIN

Permissions-based gain access to control works much as it will on server and desktop operating systems. This kind of feature limits the opportunity of access of an applica- tion by blocking those actions the user may attempt but has not been granted access to.

3.0   DIGITAL MEDIA LITERACY

Whether a new to smartphone or have some experience, digital media literacy will help to develop a fundamental understanding of smartphone or tablet or laptop. It help learn the essential skills to begin digital media with confidence, be more produc- tive at home and at work, stay safe online, use technology to complement our life- style. Digital media literacy is the marrying of the two terms digital media and litera- cy. However, there is a large significance as a result of the combination of these two terms. Digital media information is a symbolic representation of data, and literacy refers to the ability to read for knowledge, write coherently, and think critically about the written word. A digitally media literate individual will possess a range of digital media skills, knowledge of the basic principles of mobile devices, and skills in using internet. The individual has the ability to engage in online communities and social networks while adhering to behavioral protocols. The individual is able to find, cap- ture, and evaluate information [7]. Digital media literacy

requires the individual to understand the societal issues raised by digital technologies and possess critical think- ing skills. These skills can be possessed through digital experiences that pushes indi- viduals to think in a variety of ways through a multitude of media platforms. The evolution of digital media has quickly integrated into literacy. Digital education for media literacy often uses an inquiry-based pedagogic model that encourages people to ask questions about what they watch, hear, and read [8]. Media literacy education provides tools to help people critically analyze messages, offers opportunities for learners to broaden their experience of media, and helps them develop creative skills in making their own media messages .

4.1 METHODOLOGY OF MOBILE SECURITY FOR DIGITAL MEDIA LITERACY

Mobile operating systems come in four flavors: Blackberry, Windows Mobile, Google Android, and Apple OS. Of these, the Apple OS and Google Android operating sys- tems are by far the ones most commonly found on modern devices. Both of these operating systems have been designed to address some of the most basic threats and risks right out of the box, such as the following:

- Trojan Horse Attacks
- Network-based attacks
- Various types of Viruses
- Social engineering attacks
- Resource and service availability abuse
- Malicious and unintentional data loss
- Attacks on the integrity of data

Before analyzing the security models of these two operating systems, a brief recap of each of these attacks as they relate to mobile devices might be helpful.
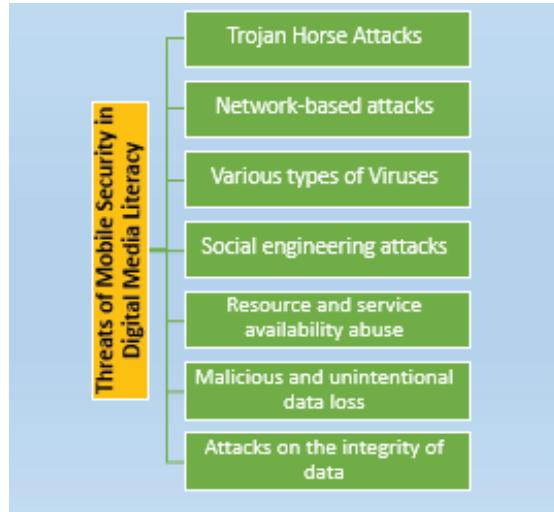
Figure 4.4 : Showing the threats of mobile security in digital media literacy

4.1   TROJAN HORSE ATTACKS

These are typically launched by malicious websites or compromised legitimate web- sites. The attacking website sends malformed network content to the victim's brows- er, causing the browser to run malicious logic of the attacker's choosing.
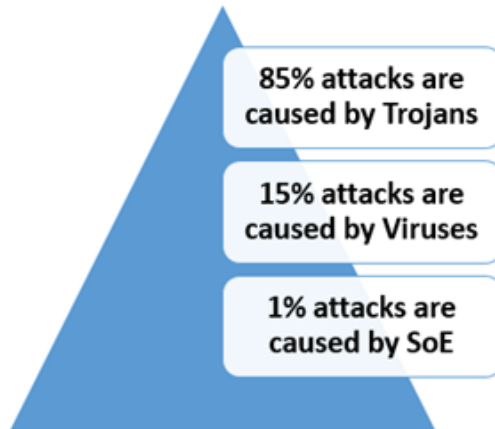

Figure 4.1.2 : survey of some secondary data which shows the different types of malware

4.2   DIFFERENT TYPES OF VIRUS

Viruses can be broken into three high-level categories: traditional computer viruses, computer worms, and Trojan horse programs. Much like traditional systems, mal- ware does plague mobile systems, and in fact there are pieces of malware designed exclusively for mobile devices.

4.3   SOCIAL ENGINEERING ATTACKS

Social engineering attacks such as phishing attempt to trick the user into disclosing sensitive information. Social engineering attacks can also be used to entice a user to install malware on a mobile device. In many cases social engineering attacks are easi- er to accomplish on mobile devices largely because of their personal nature and the fact that they are already used to share information on social media and other similar services.

4.4   DATA LOSS

Data loss occurs when a device used to store sensitive data is either carried away by a malicious person or is lost. While many of these situations can be mitigated through encryption and remote wipes, the problem is still very serious.

4.5   DATA THEFT

This is one of the bigger problems that have emerged with mobile devices because criminals target them for the information they contain. Malware has been observed on mobile devices that steals sensitive information.

5.0   RESULTS, DISCUSSIONS AND FINDINGS OF GOOGLE ANDROID OS

Initially, the market leader, Android, in our exploration of mobile operating systems. Android required condition way back in 2003 at the hands of Android Inc, which was acquired by Yahoo in 2005. Right from the start, the operating system was designed to be considered a mobile platform that has not been only feature rich, powerful, and mobile but also open source. As designed, Android can be installed on an array of hardware, and it supports and has a build-in with a lot of advanced software technol- ogies. It absolutely was also designed to integrate with exterior data sources, cloud services, and other technologies

as well as to run applications locally. In order to pro- vide these features is to do so safely and securely. This lead in to safeguard users, data, applications, these devices, and the network around it. Android was envisioned and created with a multi-layered security model that allows for the versatility essential within an open system, while providing protection for users and applications. An ad- ditional goal of the operating system is to compliment developers and make the plat- form easy to work with and easy to interact security controls. In practice, program- mers should be able to easily call on the safety controls of the system, of course, if they are experienced programmers , they can weak the controls as needed. Less- experienced developers or those not familiar with proper security configurations are protected because the system puts default configurations in destination to ensure that safety and security are maintained. Just as Android originated to make it easy on de- velopers to develop and deploy applications, the system was created with the user in brain. For this end the system was developed with the expectation that attacks would happen, including the common adware and spyware issue, data theft, while others. It also was designed with the concept the users themselves might try things that may negatively impact the system. Google android was designed to enable the user to work with the system is to do everyday duties but not provide them with a high level of gain access to specifically, Android does not let the user have root access to the de- vice without the user intentionally overriding this protection. Google android, under the hood, is a series of components working together to make the system work. Every single component in the system is self-contained and concentrates on performing whatever activity it was designed to do. Each component concentrates on security measures for itself and assumes that every other component is also doing the same. In addition, in a normal installation, only a very small area of the Android OS ever oper- ates with root access, this being the kernel, and everything else runs with less access and in a software sandbox to further isolate and protect each application.

6.0   FINDING RESULTS OF APPLE IOS

The second most popular mobile operating system in the market is Apple's iOS, which is present on multiple devices including the iPod, iPad, and iPhone. Much as Android is based on the Linux kernel, iOS is a slimmed-down version of OS X for the Mac. However, while it is based on OS X, which is based on FreeBSD, it is not fully Unix compatible. Unlike Android, which covers all

five core components of system design, iOS covers only four. Specifically, it addresses these areas:

6.1   TRADITIONAL ACCESS CONTROL

Traditional Access Control iOS provides traditional access control security options, including password configuration options as well as account lockout options.

6.2   APPLICATION PROVENANCE

Application Provenance just as Android items that are in the Google Play store have been verified and therefore trusted, in iOS it's the same type of deal with apps being created by Apple-approved developers, who have the ability to sign their app before placing it in the store.

6.3   ENCRYPTION

Encryption iOS uses hardware-accelerated AES-256 encryption to encrypt all data stored on the device as well as additional encryption for email and other services.

6.4   ISOLATION

Isolation The iOS operating system isolates each app from every other app on the system, and apps aren't allowed to view or modify each other's data, logic, and the like.

7.0   PENETRATION TESTING FOR MOBILE SECURITY ISSUES

In many ways the process is similar to what we are already using in a traditional set- ting but with some minor differences along the way .Here is a showing of how to evaluate the Penetration Testing for Mobile Security Issues .

7.1   FOOTPRINTING

Footprinting Many of the scanning tools we examined in our footprinting phase can be used to locate and identify a mobile device plugged into a network. A tool like Nmap, for example, can be used to fingerprint an OS under many conditions and re- turn information as to its version and type. Once you find mobile devices in the envi- ronment, make sure to note their

information such as MAC address, IP address, ver- sion, type, and anything else of value[9].

7.2   SCANNING

Scanning For mobile de vices attached to the network you are evaluating, use a piece of software such as Kismet to find out which wireless networks the devices are look- ing for.

7.3   EXPLOITATION

Exploitation Use man-in-the-middle attacks, spoofing, ARP poisoning, and other such mechanisms to attack a device. Use traffic insertion attacks to deliver client-side ex- ploits to vulnerable systems and devices or manipulate captured traffic to exploit back-end servers.

7.4   POST EXPLOITATION

Post Exploitation Inspect sensitive data areas on mobile devices for information such as the Short Message Service (SMS), and browser history databases. Note that foren- sic tools are available for cell phones that can extract this information as well[10].

8.0   COUNTERMEASURES

Just like securing desktops, servers, systems, and other equipment, some basic steps to make mobile devices more resistant to attacks. Exactly what is included here is some basic guidance however, not a comprehensive set of all that can be carried out is pos- sible:

8.1   SETTING PASSWORDS

Setting passwords on all mobile devices is a requirement of all devices that will be mounted on a corporate network and/or store sensitive data for Digital media literacy. It is worth remembering that enabling certain features such as encryption will require the setting of any password before they will work.

8.2   STRONG PASSWORDS

Strong passwords are recommended on all devices. This task is of particular im- portance because many mobile devices allow to work with methods to

unlock the device aside from passwords. Many devices enabling to set PIN number codes, ges- tures, and regular alphanumeric passwords[11].

8.3   INSTALL ANTI MALWARE APPLICATIONS

Install anti malware applications to thwart the spread and infection of malware. Ideal- ly, the anti malware application should scan not only the device but also newly in- stalled applications and email for maximum effect[12].

8.4   USE ENCRYPTION

Use encryption on all devices whenever we can to protect both internal storage and secure digital cards. This really is an essential part of protecting data on a device in the event it is lost or stolen. Note that some older devices and elderly systems do not support encryption.

9.0   CONCLUSION AND DISCUSSION

A digitally media literate individual will possess a range of digital media skills, knowledge of the basic principles of mobile devices, and skills in using internet. The individual has the ability to engage in online communities and social networks while adhering to behavioral protocols. The individual is able to find, capture, and evaluate information[13]. For digitally media literate portable phones have taken the world by storm and have seen incredibly fast growth and adoption during the last several years for the digital media literacy[14]. Along with this expansion came a number of securi- ty issues to affect mobile devices. A chance to have a tiny and powerful device that is Internet linked and allows communication from anywhere at any time is alluring as well as a problem for companies. With the average person today possessing at least three mobile devices and using those devices for both personal and work purposes, the devices pose a problem for the workplace. Functioning systems such as Google's An- droid and the second-place Apple iOS are in several ways similar to but also totally different from traditional systems, offering securities challenge.

REFERENCES

NL Clarke, SM Furnell (2005) "Authentication of users on mobile telephones–A survey of attitudes and practices " .

P Gilster, P Glister (1997) "Digital literacy "

M Knobel (2008) "Digital literacies: Concepts, policies and practices".

S Furnell, N Clarke, S Karatzouni (2008) "Beyond the pin: Enhancing user authentication for mobile devices ".

SM Furnell, T Karweni (1999) "Security implications of electronic commerce: a survey of consumers and businesses".

M Becher, FC Freiling, J Hoffmann(2011) "Mobile security catching up? revealing the nuts and bolts of the security of mobile devices" .

M Knobel (2008) Digital literacies: Concepts, policies and practices

D Buckingham (2015) Defining digital literacy-What do young people need to know about digital media?

T Phan, L Huang, C Dulan(2002) "Challenge: Integrating mobile wireless devices into the computational grid ".

A Hoog – (2011) "Android forensics: investigation, analysis and mobile security for Google Android ".

I Burguera, U Zurutuza, S Nadjm-Tehrani (2011) "Crowdroid: behavior-based malware detection system for android ".

W Enck, M Ongtang, P McDaniel (2008) "Mitigating Android software misuse before it happens ".

A Hoog, K Strzempka (2011) "iPhone and iOS forensics: Investigation, analysis and mo- bile security for Apple iPhone, iPad and iOS devices ".

AP Felt, M Finifter, E Chin, S Hanna(2011) "A survey of mobile malware in the wild".