Kushal Adhikari

MOBILE SECURITY

Thesis

CENTRIA UNIVERSITY OF APPLIED SCIENCES

Information Technology

November, 2020

ABSTRACT

Centria University **of Applied Sciences**	**Date** October 2020	**Author** Kushal Adhikari

Degree programme

Information Technology

Name of thesis

MOBILE SECURITY

Instructor Kauko Kolehmain	**Pages** 30

Supervisor

Kauko Kolehmainen

Mobile security is one of the major problems in this generation. In this computerized era many people use computer and mobile phones in their daily life. This report tells about the mobile security, how cyber criminals hack the devices, and how to protect from such problems. And this report also talks about virus and to be aware of such virus. This report also talks about awareness, handling device safely, how to deal with unwanted application, how to use application and so on.

The aim of this thesis work is to illustrate the importance of security and its value. This thesis recognizes the security is not only a technical issue but a governance concern as well. Mobile security is importance in all level of organization. This thesis also discusses the procedures to be followed by organizations to ensure their information is safe and secure.

Key words

mobile devices, virus, hacker, advertisement, fake account, phishing, lost, theft.

ABBREVIATIONS

GDPR	General Data Protection Regulation
GPS	Global Positioning System
MAM	Mobile Application Management
MDM	Mobile Device management
OS	Operating Systems
SSL	Secure Socket Layer
UI	User Interface
UX	User Experience
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity

CONTENTS

1 INTRODUCTION 0
2 MOBILE SECURITY 2
2.1 Physical Security 4
2.2 Multi Users Logging 4
2.3 Secure Data Storage 5
2.3.1 Physical Controls 6
2.3.2 Technical Controls 6
2.3.3 Administrative Controls 6
2.4 Bluetooth attacks 7
2.5 Operating System Attacks 8
2.6 Application Level Threats 9
3 MOBILE OPERATING SYSTEMS 10
3.1 IOS Operating System 10
3.2 Android Operating System 11
4 USING INTERNET 13
5 SECURING MOBILE DEVICES 16
5.1 Use Strong Passwords 16
5.2 Utilize VPN (Virtual Private Network) 17
5.3 Encrypt Device 18
5.4 Install an Antivirus Application 19
5.5 Software Update 19
5.6 Use Secure Mobile URLs 20
6 MOBILE SECURITY STRATEGY TO DEVELOP AN APPLICATION 21
6.1 Architecture 21
6.2 Secure Software Development Lifecycle 22
6.3 Data Validation 22
6.4 Handle Identity Management 23
6.5 Mobile Application Management 24
6.6 Mobile Device Management 24
6.7 Design secure Application 25
6.8 Implement HTML5 content 26
6.9 Control External References 27
6.10 Promote Site Encryption 27

CONCLUSIONS

REFERENCES

Table

TABLE 1. Difference of HTML4 and HTML5 26

FIGURE

Figure 1. Flow of data transmission and potential locations 16
Figure 2. A VPN tunnel passing through the internet cloud 18

1 INTRODUCTION

The world has become narrow due to technologies. Single person can look information of the world while staying at home. The aim of this report is to be secure from hackers. How hackers hack the devices and how to be secure from such danger. The number of Mobile users is growing rapidly, and applications is launched hourly. Mobiles, laptops had replaced PCs, CPU. However, the shift to mobile is a major transition from the Personal Computers era, requiring enterprise IT to consider a new approach to secure data and minimizes the risk. Securing company content on mobile requires information technology to adopt new management tools and security strategies given the differences in the way mobile operators compared to PCs. However, those organization's that take a mobile first approach and address new requirements will enjoy the benefits that result, which include marked competitive differentiation and heightened innovation. This report provides the information of security in different type of devices. It says how to be secure from theft of information's of public organization, private organization, and personal information. There are different kinds of categories of attacks operating systems attacks, mobile app attacks, communication attacks and malware attacks.

So many systems, so little time. With so, many overlap and so little difference between many of the device types discussed in the preceding section in mobile devices. It can be confusing to tell just by looking at mobile device what security system should be applied in it. It is important to think about the operating system running on the device because that has a large impact on the type and availability of security products that should be applied to the devices. The operating system is the primary interface between the underlying hardware and the applications running on the device. Among other things, the operating system provides a generic mechanism for application developers to write a single application and run it on multiple hardware devices running the same operating system. For this reason, the operating system is the primary distinction that in this thesis to differentiate between mobile devices and everything else. Many mobile operating systems are available on the market today. Only a few of these have really taken off to the point where users are likely to see large numbers of users adopting them for use in the enterprise. Most vendors provide support for, at most, the top five operating systems on markets. Hackers are looking for small hole of the device. When they get chance they already get inside of the device and steals the private information. The best way to secure devices is awareness. Device users must make sure of logging out from all application after using it, do not open unknown links and complain to police in case of theft and lost. People faces scam calls, scam messages, adult advertisements, and adult scam links. Which had made bad environment while using device in public and with parents or with child. Different adult entertainment industries send different kinds of unrated pictures while using any webpage, applications. Such advertisements are not kid friendly. Advertisement blocking sites helps in some cases and increase in network security and also helps in some cases.

2 MOBILE SECURITY

Mobile security is to protect smartphones, tablets, laptops, and other computing devices. Mobile security is also known as wireless security. Mobile security has increased in recent years. To secure devices from thief, phishing, hacker mobile security is used. There are many organizations which have many data and data should be protected from hacker. Information should be private and should not be leaked. Company needs to protect their devices. The best way to protect company data is not to store the data in client devices. If somebody wants to know the data then they should need to get access permitted only over the network, there is no local copy to lose if a laptop or PDA is stolen or lost. This method also protects PCs in the office. This can be more convenient for a worker to work from local copy of data on a laptop transported from home or on a thumb drive, the high ability of broadband access and the maturity of remote access the technologies such as laptops and smart phones, which is much or less convenient. This approach provides better security while still letting people work in many locations and in many devices. (Symatec employee 2020.)

Many organizations have issued laptops as standard PC, a strategy that undercuts security. Only workers who need to work while travelling should be issued laptop. Then other workers can use PCs at home or at satellite offices. Companies that limit the use of mobile devices and discourage the use of locally stored data will still find exceptions that require local data storage on mobile devices, but these exceptions will be few and their small numbers will make them easier to manage. Mobile device has become one of the most important devices in these days 2020. Securing mobile phones are also important and useful in 2020. If device gets lost in taxi, restaurants which may cause problems, private information will be leaked, and it will be at risk. Those kinds of problem are very high nowadays. So, there are different kind of locking software which protects every device from theft and leaked of private information. (Saena 2020.)

There is other kind software for application which can be locked by using passwords so if device gets lost also there will be no harm to the client or organization or to personal users. Malware attacks are also one of the problems. Hackers, thief, cyber criminals send different kind of SMS, links and opening such unknown links might be harmful to organization or to person. (Rouse 2012.)

IT department plays one of the important roles in securing mobile device. The job role of IT security analyst is to take responsibilities of maintaining top-notch security of all companies' information and data and to ensure said data remains protected from compromise. When a security incident does rise, it is a job of the security analyst to investigate and resolve the issue in a timely manner. To prevent security threats, the job requires regular security risks management, assessments, vulnerability scans and disaster recovery plans, while adhering to the security standards of the company. IT department must know how to secure, maintain, and install various security systems. They are also obligated to monitor external sources to find available security patches and to prioritize and make recommendations for implementation. And it is expected that IT security analysts demonstrate knowledge in the planning and creation of enterprise security documents and architecture. It is important to remain update with detailed knowledge of the IT security industry. This includes the awareness of new or updated security solutions, improves security processes and the development of new attacks and threat vectors. (IT Security Analyst 2020.)

Cyber security researcher check point has warned Android users in a blog on July 10, 2019, that as many as 25 million Android mobile devices have been hit with a malware called `Agent Smith´. The malware hides within installed application like WhatsApp, taking advantage of the vulnerabilities within the Android operating system. According to check point, this new breed of malware was able to copy popular application on the phone, but inject its own malicious code replacing the original application with the weaponized version. The hijacked application on the surface work fine but the malware is hidden from users. The malware then displays unwanted advertisement to users, which may not seem like a problem, but the same security flaws could be used to hijack banking, shopping and other privacy data, according to Aviran Hazum, head of check points analysis and response team for mobile devices. Hypothetically nothing is stopping them from targeting bank application changing the functionality to send your bank credentials to third party. The user would not be able to see any difference, but the attacker could connect to your bank account. (Rajagopal 2019.)

Cyber security industry is rapidly growing every day. Although more resources are being deployed to counter cyber-attacks, the nature of the industry still has a long way to go before we can catch up with these threats. It is important for us to define what the current information security and cybersecurity industry looks like. 95 percentage of breached records came from only three industries in 2016 Government, retail, and technology. The reason is not necessarily because those industries are less diligent in their protection of customer records. They are just very popular targets because of the high level of personal identifying information contained in their records. A Clark school study at the University of

Maryland is one of the first to qualify the near constant rate of hacker attacks of computers with internet access every 39 seconds on average, affecting one in three Americans every year and the non-secure usernames and passwords we use that give attackers more chance of success. 64 percentage of companies have experienced web-based attacks. 62 percentage experience phishing and social engineering attacks. 59 percentage of companies experienced malicious code and bonnets and 51 percentage experienced denial of service attacks. (Milkovich 2019.)

2.1 Physical Security

For securing mobile phones physically users need to logout from the public devices, after using any applications or after opening any documents and never keep passwords in remember mode. Close all the application and make sure to shot down the devices. The devices may get lost or theft in such case contact to police as soon as possible. Nowadays it is possible to lockdown the phone. Lost device can be located from GPS. Set up lock screen message, suspend your device, wipe all data from your device. Currently there are no mainstream technical solutions that help to prevent device from losing. Technology is advancing day by day and when it comes new and innovative physical security measures, however these current measures have been slow to market, and it is not adopted by public masses. Fourth line defines the consists of mobile device recovery and dealing with the loss of data. Identifying the loss of device as quick as possible is the top priority in getting the device back. The sooner you know it is lost you can take action to secure it. Try remote tracking of the device. When the device gets drop in water then there is chance of damaging device. In such case there is no good solution so, always backup the data. There is waterproof device in the market which helps in such cases. Handling device carefully and awareness helps to protect device physically. (Mooney II 2013.)

2.2 Multi Users Logging

Mobiles phones are used for different proposes while any friend ask for some propose and he/she may steal your information so, it is better to not to share mobile phone to third party. While using company's mobile or any device make sure it is protected properly. There are many applications which can lock the folders which have important documents so there is more security while using such folder lock application. For the personal devices never keep weak password. Never share device with other. Do not use personal phones, computers in the work of organizations. Organizations may have strong security systems, and which can hamper your personal devices. The security systems of organizations may also erase the important files, pictures of device. Device used for companies are used by many staff. In such case never open any personal accounts in such devices. If any application must open after opening, make sure to close application and can delete history. Each application needs different security model so, the data from one does get exposed to the other, because if there is one user profile, the device may or may not be able to support the distinction. (Mobile Application Security, page 4.)

2.3 Secure Data Storage

Mobile phones need to secure data. passwords, credit card details may steal so do not share phones and make sure to logout the such data. After using any means of application, data, documents make sure to close them and remove all the important personal information. Companies use internet for business and can have benefits. But it can also increase the risk of scams and security threats. Back up your business´s data and website. This can help to recover any information which is loose. It is essential that you back up your important data and information regularly. Backing up does not cost much and it is easy to do. (Business, 2019) Large companies with successful security policy know their data. They know where the data is stored and how it is used. Mapping data flow enables companies to better assess weak points. Additionally, large companies employ discovery tools that enable them to make sure data is accessible by only authorized devices or personnel. These capabilities allow large companies to be GDPR complaint as well as fulfil other privacy/transparency standards. Also, they use the cloud in some manner, whether it is for data storage or as a software platform. However, unless the cloud is created and run internally, large companies do not control the security measures of the cloud. Rather, the Cloud Service Providers (CSPs) do. This lack of control makes most IT department nervous; consequently, they use cloud security tools for encrypting data before it is uploaded to the cloud, protecting/ monitoring endpoints, ranking data by risk level, and tracking data movement within the cloud. The variety of tools available continues to expand, offering companies greater control over cloud data security. Software testing help offer lists of tested and emerging software solutions for the cloud. (RSI Security 2019.)

2.3.1 Physical controls

Physical controls are designed to protect storage resources and the data they contain from physical, as opposed to logical, access by unauthorised persons. This physical controls come in many forms, but this may include guards or other security personnel monitoring data centres and storage resources to prevent unauthorized access. CCTV monitoring with video retention, Access control such as biometric readers or smart card readers to prevent unauthorized access, along with anti-pass-back turnstile gates that permit only one person to pass through after authentication, internal environment monitoring using systems such as temperature sensors and smoke detectors, alternative power sources such as backup generator. (Rubens 2019.)

2.3.2 Technical Controls

Many organizations set controls to protect data storage resources and data from unauthorized access while forgetting to secure the management system themselves. This could enable an attacker to set themselves up with access credentials or elevate their privilege, enabling them to access data that they should not. There is by no means a comprehensive list of technical controls. Endpoint protection for all mobiles, laptops and other devices that can access data to minimize the risk of malicious software being installed that could compromise data storage. Special measures to protect data storage that contain credit information and other valuable information. Database security best practices includes database hardening, the use of database firewalls, database activity monitoring and other database security tools. (Rubens 2019.)

2.3.3 Administrative Controls

Administrative controls come down to the policy, planning and procedures. All of which play an important role in data storage security. Security policies for data should include where different types of data can be stored, who can access it, how it is encrypted and when it should be deleted. For a risk management runs analysis and identify security risks within your agency to determine the probability and magnitude of occurrence and how you are going to offset that risks. For a new worker, decides who gets access to what, and ensure you are disabling accounts when an employee leaves the agency. Know how you are going to handle business continuity and recovery after losing office space to an unanticipated fire, tornado, or environmental hazard. Where the employees going to work, what minimum applications do they need to continue business. (Rubens 2019.)

StockX was hacked, exposing millions of customers data. It was not system updates as it claimed. StockX was mopping up after data breach, TechCrunch can confirm. The fashion and sneaker trading platform pushed out a password reset email to its users. Thursday citing "system updates" but left users confused and scrambling for answers. StockX told users that the email was legitimate and not a phishing email as some had suspected but did not say what caused the alleged system update or why there was no warning. An unnamed data breached seller contacted TechCrunch claiming more than 6.8 million records were stolen from the site in May by hacker. The seller declined to say how they obtained the data. The stolen data contained names, email address, scrambled passwords, and other profile information. (Whittaker 2019.)

2.4 Bluetooth Attacks

It is easy stole data from Bluetooth. Hacker may steal information with some software. users need to turn off Bluetooth after your personal use. Bluetooth means of transferring data. It is a wireless means of communication. It helps to contact between two devices through which file, sound, music can transfer to each other. It has both positive and negative effects. In positive it helps to transfer data. In negative it also transfers virus; hacker can send any kind of application through which they can stole personal information. A new Bluetooth attack vendor that allows attackers to take control of device, access corporate data and networks, penetrate air gapped networks, and spread malware to adjacent devices. The attack does not require the target device to be paired to the attacker's device, or even to be set on discoverable mode. The attack vector which the researchers are calling Blue Borne, leverages eight zero-day vulnerabilities, four of them critical. It affects mobile, IoT operating systems including Android, iOS, Windows, and Linux.8.2 millions of Bluetooth product are using in worldwide. The Bluetooth attack vector requires no user interaction, is compatible to all software versions, and does not require any preconditions or configuration aside of the Bluetooth being active. Bluetooth enabled devices are constantly searching for incoming connections from any devices, and not only those they paired with. This means a Bluetooth connection can be established without pairing the device at all they added. This makes blue borne one of the most potential attacks found in recent years and allows an attacker to strike completely undetected. Blue Borne can be used to lunch remote code execution and man in the middle attacks and it could be used for wide variety of malicious objectives, including cybercrime, data theft. (Goldman 2017.)

2.5 Operating System Attacks

Operating system can be vulnerable and suffered from malicious attacks due to running a lot of applications during that are suffering or downloading applications from the internet. A malware writer can take advantage of these features to develop malicious applications. Automatic updates will eventually install the patches you need. But the automatic updates tend to roll out slowly, leaving your PC vulnerable during critical time between the public release of patch and the moment when you install it**. (**Brandt 2009.)

Authentication refers to identify each user of the system and associating the executing programs with those users. It is the responsibility of the operating system which ensures that a user who is running a program is authentic. System generally identifies users by passwords, user card/key, fingerprint. One-time passwords provide additional security along with normal authentication. In one-time password system a unique password is required every time user tries to login into the system. Once a one-time password is used then it cannot be reused. For banking transaction, commercial application one-time passwords are used mostly. Operating system processes and kernel do the designated task as instructed. If a user program made these processes do malicious tasks, then it is known as program threats. One of the common examples of program threat is a program installed in a device which can store and send user credentials via network to some hacker. Trojan horse is a program which traps user login credentials and store them to send malicious user who can later login to device and can access system resources. Trap door is a program which is designed to work as required, have a security hole in its code and perform illegal action without knowledge of user. Virus is also very dangerous to device. It is a small code embedded program. They are highly dangerous, and it can delete, modify, and can crash system. (Operating System Security 2020.)

2.6 Application Level Threats

Application level threats appear to be mostly discussed threats in the world. As mobile device can execute downloaded applications, applications can be a target vector to be breach the security of the device and the system it connects to a corporate network. The threats can be due to malicious applications, particularly those downloaded from a third-party application store. Web level threats are not specific to mobile devices, the security and privacy risks to mobile devices due to web level threats are real. One key web level threat is phishing, which uses email or other social media applications to send an unwanted user links to a phishing website designed to trick users into providing sensitive information such as user credentials. When combined with social engineering, phishing is one of the top seven security threats identified by Karspersky lab for the 2015-2016. (Chen 2016.)

3 MOBILE OPERATING SYSTEMS

Mobile operating system is an operating system which is specifically designed to run on a mobile device such as mobile phones, smartphones, and other handholding devices. Mobile operating system is the software platform on top of which other programs can run on your device, such as thumb wheel, keyboards, WAP, synchronization with application, email messages and more. There are many popular operating systems like; Android operating systems, Bada (Samsung electronics) BlackBerry Operating system, iPhone OS/iOS (Apple), MeeGo Operating system (Nokia and Intel), Palm OS (Garnet OS), Windows Mobile and many more. When you purchase the device the manufacturing companies will have the operating systems for that specific device. And those operating systems will work differently. Android is the most popular mobile operating system. Also, Android had highest number of vulnerabilities in 2019 compare to another operating system. Many mobile operating systems offer a native web browser application, which allows users to search the internet and visit webpages. Mobile operating system also offers application stores, which allow users to download and interface with mobile application. Several mobile operating system also have native GPS application that allows user to search locations, follow step-by-step directions and in some cases shares location with different devices. In some cases, the application adds new features and improve user interface for websites that are accessible via a web browser, but other application brings new functionality to the mobile devices. Most mobile operating system other than Android are tied to specific hardware with little flexibility. Users can jailbreak or root devices, hardware which allows them to install another OS or unlock restricted applications. (Beal 2020.)

3.1 IOS Operating System

iOS has been a very advanced and sophisticated mobile operating system ever since it was first released in 2007. Building on the unique capabilities of Apple hardware, system is designed to maximize the security of the operating systems on Apple devices without compromising usability. System security encompasses the boot-up process, software updates and the ongoing operation on the operating system. Secure software requires a foundation of security built into hardware. That is why Apple devices running iOS, iPadOS, macOS, or watch operating system have security capabilities designed into silicon. Apple provides layers of protection to ensure that application is free of known malware and have not been tampered with. Additional protections enforce that access from application to user data is carefully mediated. Apple devices have encryption features to safeguard user data and enable remote wipe in the case of device theft or loss. Apple devices include boot and runtime protections so that they maintain their integrity during ongoing operation. These protections vary significantly between iOS, IPadOS, and macOS devices based on the very sets of capabilities they support and the attacks they must therefore thwart. Privacy is one of Apple´s USPs, so it is added plenty of privacy enhancing features to iOS 13. On location sharing, users can choose to share your location to an app just once then require the app to ask you again next time it wants permission. For continuous sharing, Apple says it will provide reports on background tracking and that it will shut the device on wi-fi and Bluetooth tracking. Apple has its own sign in with Apple log-in to rival social logins using Facebook and Google accounts within apps and on the web. Apple says it´s the sign-in without the tracking and it uses Face ID on the device. There is also a neat looking Hide my email function for sign-ups where Apples creates a new unique and random email that forwards to our main account, one per app so they can be easily disabled. (Apple Platform security 2020.)

3.2 Android Operating System

Android operating system is one of the most widely used operating system in these days. IT is easy to use so it is popular. Android operating system is mainly divided into four main layers: the kernel, libraries, application framework and applications. Its kernel is based on Linux. Linux kernel is used to manage core system service such as virtual memory, networking, drivers, and power management. Android operating system follows a variety of security mechanisms. When a developer installs an application a new user profile with that application is created. Each application run with its own instance of Dalvik VM. So, application cannot access shared data or resources when they require permission. All Android applications are signed so users know that the application is authentic. The signing mechanism allows developer to control which application can grant access to other applications on the system. Mobile security applications for googles android platform help protect Android smartphones and mobile devices from malware threats as well as unauthorized access following accidental loss or theft of the device. Additional security features frequently offered by android mobile security application include securing data on the device, VPN connectivity for protecting data in transit, scanning website for potential phishing schemes or other fraudulent activity, helping users locate their deice if stolen or loss. Android mobile security applications are available from google as well as known third party security vendors such as lookout, Avast, Kaspersky, Symantec and Qihu. Android seeks to be most secure and usable operating system for mobile platforms by repurposing traditional operating system security controls to protect application and user’s data, protect system resources and provides application isolation from the system, other application and from the users. Also, it provides security features like; robust security at the OS level through the Linux kernel, mandatory application sandbox for all application, secure interposes communication, application signing and app-defined and user granted permissions. Android have one of the best security features. The android platform takes advantages of the Linux users-based protection to identify and isolate app resources. To do this, android assigns a unique user ID (UID) to each Android apps and runs in its own process. Android uses this UID to setup a kernel-level App Sandbox. Application signing allows developers to identify the author of the app and to update without creating complicated interfaces and permissions. Every app that runs on the android platform must be signed by the developer. As part of the Android security model, Android uses Security-Enhanced Linux (SELinux) to enforce mandatory access control over all process, even processes running with root/superuser privileges. Verified Boot strives to ensure all executed code from a trusted source rather than from an attacker or corruption. It establishes a full chain of trust, starting from a hardware-protected root of trust to the bootloader to the boot partition and other verified partitions. (Stroud 2020.)

4 USING INTERNET

Internet is widely used in this world. Internet has connected the people. Mostly people use internet through their phones. Internet has both good and bad effects. Using internet correctly helps users to get out of trouble. While using internet users needs to keep personal information professional and limited, keep the privacy setting on, practice safe browsing, make sure the internet connection is secure, be careful while downloading any application. While purchasing through online purchase from secure sites, be careful while posting any information or any pictures. Be careful with the person you meet online. Use secure network like VPN. VPN and fibric optic networks are not perfect inherently secure. Hence, a company sharing its business between two or more office locations must allocate extra resources to protect its IT network. For the security measure and the protection of sensitive company data, two complementary devices are required; layer 2 encrypts are hardware security modules. Scheme for the protection of an internal network with multiple locations.
Private does not automatically indicate protected or confidential. The word private just means the opposite of public. This also applies for a virtual private network VPN, which creates a kind of an internet via a public network by integrating external sites into the company network. Private in the context of a VPN hence means just that the private network will be logically separated from the public network. However, there is often no explicit protection against illicit access as encryption is not mandatory. The same sort of privateers applies to fibre optic networks; data might be illicitly tapped by organizations willing to invest some effort to get after it. Hence, managing a company based in multiple locations implies protecting sensitive data in transit. Mobile VPNs which provide mobile devices with access to network resources and software applications on a network, when they contact via wireless or wired networks. Mobile VPNs are used in environments where workers needs to keep application sessions open at all times throughout the working day, as they connect to different wireless network., encounter gaps in coverage or suspend and resume their device to preserve batery life. A conventional VPN cannot survive such events because the network tunnel is distrupted, causing application to disconnected, fail or the computing device may crash. Mobile VPNs are adopted by professionals. They are commonly used in public safety, home care, industries, hospital setting and other service management. (Mobile Security Technologies Control, page 38.)

A basic home wireless network connecting an internal point, such as a cable from your internet service provider, to a router to allow multiple devices to connect network very quickly. To enhance the security of home or outdoor wireless network you must be very careful. For the better secure of your device do not connect to any Wi-Fi networks. Keep strong password for your hotspot. Increase the wi-fi security of your home by activating network encryption. Turn off the wi-fi bottom of your device when you are not using device. Do not access personal bank accounts or sensitive data on unsecured public networks, do not leave our laptops, phones unattended in a public place. Even you are working on a secure network, that will not stop someone from sneaking a peek at our device. Do not shop online using public wi-fi. Do not turn off automatic connectivity. Most of the devices have automatic connectivity settings, which allow seamlessly connect from one hotspot to the next. This is a convenient feature, but it can also connect devices to networks which is ordinarily not use. Keep these setting turn off, especially while travelling to unfamiliar places. (Rijnetu 2020.)

Despite all the security improvements and architectural changes that have occurred within mobile applications, some categories of classic vulnerabilities show no sign of diminishing. Despite many security flaws having been known about for decades, we are continuing to repeat those flaws in new platforms without having implemented the established fixes and improvements that have also been known about for some time, these include defects in business logic, failure to properly apply to access controls and other design issues. Another important point is that 20-30-year-old problems are not magically going away because users have gone mobile. They have become more prevalent due to accessibility to coding and lack of formalized security training and education. Even in a word of bolted together application components and everything as a service, these timeless issues are likely to remain widespread. Vulnerabilities are commonly associated with applications that are installed on mobile devices. However, it is important to recognize that vulnerabilities can exploited at all levels in the mobile device stack.

Although the mobile phone vendors try to ensure application security through requiring application to be signed to be downloaded from the official application stores, misuse of certificates means that even application downloaded from vendor stores or enterprise sites are not guaranteed to be free from malware. Even legitimate application often requests more permission then needed to perform their function, which can expose more data than necessary. Large numbers of mobile devices are not kept update with operating system releases. Outdate operating systems mean devices are vulnerable to security threats that are patched in the later versions. When the users jailbreak or root devices, they work around the built-in restrictions of the device. While users feel that jailbreaking gives them freedom and more access to the device’s capabilities, jailbreaking also eliminates many controls that provide security. Portable devices are easily lost or stolen. When an employee loses physical control of their mobile device, they also lose control of the data on that device. If the device is not appropriately protected with passwords and encryption, any data on that device may exposed. No matter how well you publicize your safe mobile computing politics, there will be employees who find them too inconvenient to follow. Organization need tools to enforce policies rather than relying on employees' good will. The large number of mobile devices used in an organization makes monitoring and managing them difficult. It is not easy to understand the status of all mobile devices. There is no single standard for mobile devices, especially when you allow bring your own device (BYOD) rather than supplying the devices. Because of the variety of devices and operating systems, it is difficult to apply controls consistently to ensure the safe of all of them. Users often reply on public Wi-Fi to stay connected when they work outside the office. These unsecured Wi-Fi networks can allow malware to be installed on devices or eavesdroppers to intercept data. (Prescient solutions 2018.)

5 SECURING MOBILE DEVICES

In a mobile world, there can often be little or no control over the device. The latest mobile devices are designed to offer abilities beyond voice and email, and to provide board internet and network connectivity like 3G, 4G, long term evolution, Wi-Fi, Bluetooth, and wired connection to a personal device. However, the increasing number of ways to transmit data also create several potential ways that the device can be exploited. When a device downloads a new application from online application store, there is a hazard that the software contains malware able to damage private and corporate data on the device. A device connected through Wi-Fi can be exploited and used in main-in-the middle attacks as in FIGURE 1. Flow of data transmission and potential locations. Security threats can occur in multiple places along the varying paths of data transmission. (Securing your mobile business with IBM work light, page 9.)

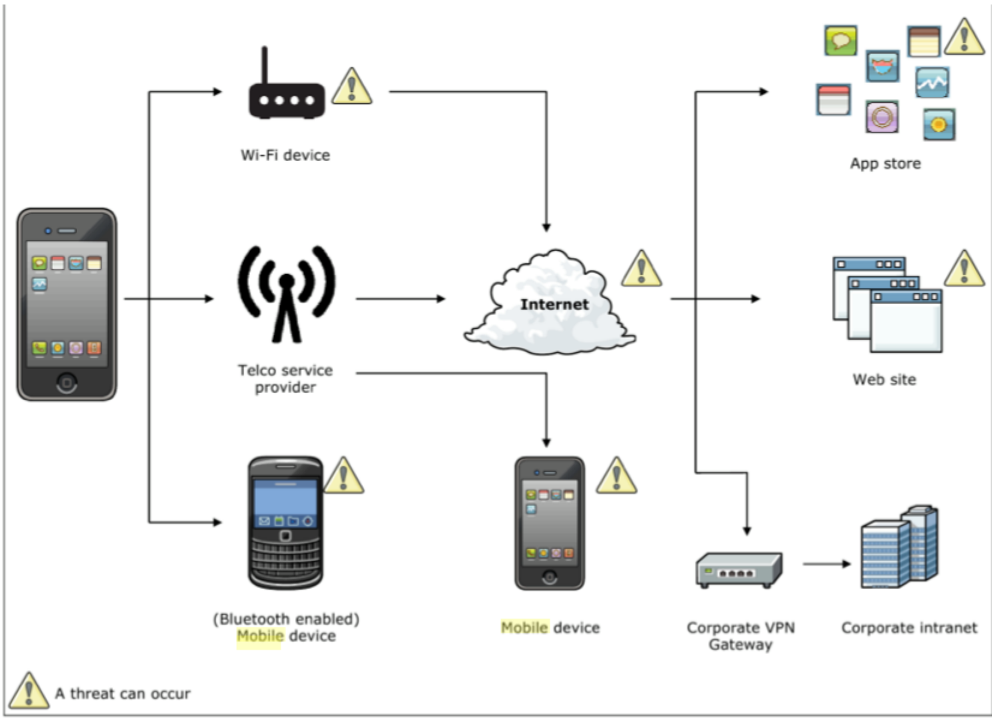

FIGURE 1. Flow of data transmission and potential locations

5.1 Use Strong Passwords

The first place to start is to create strong passwords these are passwords that are difficult for hacker to guess. You should not use any personal information. Consider how easily a hacker might be able to obtain this sort of personal information; much of it can be found through online searches or through online sources or through browsing social networking accounts. If you decide to use personal information to form your password or user ID, a hacker may be able to deduce what is based on what he or she knows about you personally or from information you have posted online. Shorter passwords and user ID are easier to crack because of their simplicity. Long and nonsensical passwords are stronger than logically consistent and short passwords because hackers do not always attempt to personally deduce targeted account information. Often, hackers will utilize type of program known as a password cracker or password attacker. These programs use algorithms based on common password patterns to guess a user's login information. Use uppercase letter, lowercase letter, numbers, symbols help to make strong passwords. (Mobile Security, 2020.)

5.2 Utilize VPN (Virtual private network)

VPN is a private network that at some point utilize public resources, most commonly the internet. It is a system that allows for the authentication and encryption of data between two endpoints. This allows to maintain security and privacy of a leased network, while enjoying the case and speed benefits made available by the internet. When the VPN tunnel is created, different types of users and resources can be accessed through the tunnel. Mobile devices, such as PDA´s are able to access company e-mail servers so they can keep in touch with clients and business associates; server to server sharing can take place, and sales records can be uploaded to a company database on the fly. This access and the security that is required is provided using strong encryption. (Juniper Networks Secure Access SSL VPN, page xiii, xiv.)

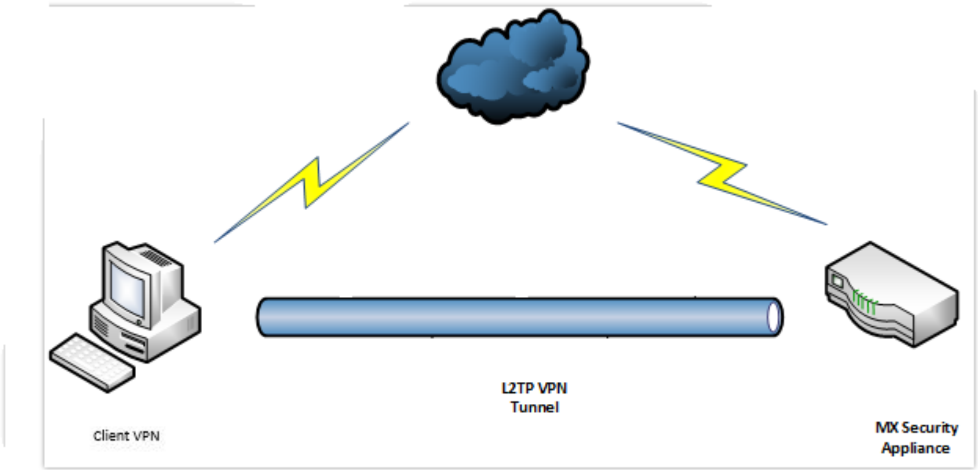

FIGURE 2. A VPN tunnel passing through the internet cloud

5.3 Encrypt Device

To encrypt the device there are many steps to follow. Fully charged the battery, and leave connected to power. Open the setting then tap the security bottom in the personal section to display the security screen. Tap the encrypt phone bottom or the encrypt tablet bottom. The encrypt phone screen or the encrypt tablet screen appears. Some devices have encrypted button and encrypt device screen instead. Read the information and then tap the encrypt phone button or the encrypt tablet button. The confirm our PIN or confirm your password appears on the screen. Type password or PIN then click continue button. The encrypt? Screen appears, warning you that encryption is irreversible and that your device will restart several times during the encryption process. Tap the encrypt device button and device starts encryption process. You will see the encryption screen with a process as it works. When the type password to decrypt storage prompt appears, type your Pin or passwords and ap the done button. Android then decrypts your data, the lock screen appears, and you can type your PIN or passwords to unlock the device as usual. (Androids Tips and Tricks, Page 115.)

5.4 Install an Antivirus Application

The recommendation is for device to install an antivirus application and update its malware signatures often. Possible antivirus application is F-secure mobile security, the McAfee mobile security and Trend micro's mobile security. Like antivirus application available for desktop, computers but on a smaller scale, mobile application are available to help protect devices from known viruses. The trend is for device malware to increase due to, among other reasons, the sophistication level of the devices that allows for malware development, the fact that mobile device is not physically limited as desktops are, and the potential for damage pinging the radar of the malware authors- this suggestion would appear to be common sense, nut these products are relatively new and the average user is not even aware the antivirus solutions exist for mobile platforms. (Advances in Computers, Page 234,235.)

5.5 Software Update

Most software needs to be updated to meet the new requirements of usage and platforms, bugs remaining in the application, security issue and new purposes. Software upgrade can cost some money for the user. Software upgrade are always scheduled and usually road mapped beforehand. If you bought your software recently, and an upgrade is released soon after that, the most personal finance software companies will offer the upgrade to the latest version free. Software update helps to repair security issues and replace with new and secure version. It helps to cover the security issues and hacker cannot pass through the new updated software. It includes security patches. It also helps to protect data in case of hacker try to enter through your device. (Symanovich 2020.)

Securing software is also one of the important roles for mobile security. One of the most dangerous attacks on web application is SQL injection: attackers inserting malicious SQL into dynamic SQL statement. It is easy for attackers to find free tools like SQL map or SQL ninja. SQL injection is easy to prevent. simply need a parameterize your SQL statements, making it clear to the SQL interpreter which parts of a SQL statement make up the command and which parts are data. Encode data before using it helps to prevent from attack. Validate Input Data before you use it or store it. All data from outside your program or service, especially data from clients, is evil and needs to be validated: files, parameters, HTTP headers, cookies. it does not matter if the client or the other system validated the data. You need to validate it again. Build security Testing into Development with the velocity of development increasing in Agile and DevOps, it is not possible for security auditors or penetration testers to keep up. Security checks need to be included in code reviews, and security testing needs to be automated and included in continuous integration and continues delivery pipelines. Make sure that you have good automated unit and integrated test coverage for security features and controls and critical business: code that handles money. Private data, trade secrets, and admin functions. This must include both positive and negative tests. Other system level security tests and checks can be automated in CI/CD using tools like Gaunt It, BDD security and Zapper. These tools make it easy to run security tests and provide clear pass/fail feedback. Static analysis checking using tools like Find bugs and PMD, also needs to be part of a developer´s toolbox, integrated into your IDE and into the CI/CD pipeline to catch security mistakes and other coding problems. It´s your code so, it´s your job to make application, software, program safe and secure. (Bird 2015.)

5.6 Use Secure Mobile URLs

Many organizations are introducing new login pages optimize for mobile web browsing. Adding additional login pages and domains where users are asked to enter credentials gives the users a confusing experience that could be detrimental to anti-phishing education. For example, some organization are using third parties to host their mobile sites. These sites stem from their parties to host their mobile sites. These sites stem from that third party’s domain, not the organizations. furthermore, some organization are creating and hosting their own sites but are using different extensions, such as .mobi. new mobile URLs are confusing to users. Common mobile URLs that could be used are isecpartners.mobi, mobile-isecpartners.com, mobilevendor.com/isecpartners. To mitigate this risk, host the login page under the base “.com” URL and use an “m.” prefix. (Mobile issue and Development Strategies, page 13.)

6 MOBILE SECURITY STRATEGY TO DEVELOP AN APPLICATION

For any organization that are developing mobile applications should have a mobile security strategy. Strategy should be developed prior to any actual corporate mobile access deployment. IT must develop a strategy to provide mobile workers with secure access to resources. A good security strategy involves tools and best practices that do not hinder the end user experience. IT professional should look at mobile threat detection functions of different mobile threat defence tools when selecting one. Mobile threat detection is one of the key features of mobile threat defence, and it is driven by the analytics engine that monitors and tracks user behaviour to compare it against historical data. The engines use AI capabilities, such as machine learning to improve pattern recognition and behaviour monitoring on devices, application and more. IT professionals does not blacklist everything so, the users can only download and access whitelisted, work related applications. When old mobile security measures fail, IT professionals needs to take actions to contain the breach. This process could involve a reset of passwords for any account with suspicious activity or a confirmed breach on mobile device. (Powers 2019.)

6.1 Architecture

A good mobile application architecture ensures that components have multiple responsibility layers. Or, a good mobile application architecture is the one that will enforce assumptions and good programming patterns like SOLID or KISS. Meeting all these conditions allow you to accelerate development and make future maintenance much easier. This way, it saves time and money. However, a wisely selected architecture together with platform-specific technology like Swift for iOS or Kotlin for Android will be best for resolving complex business problems in the most effective way for mobile projects. It will allow to avoid many problems causing the quirks of hybrid technologies. This will be a time and money saving approach in the long term. Good architecture must be so abstract as it can be applied to the platforms such as iOS or Android. One of the most crucial features of a good architecture is responsibility layer separation. The architecture should be flexible and robust enough to support devices, application and any back-end infrastructure and associated networks. The mobility revolution puts incredible power in the hands of the end user, but that power depends on access to back-end information systems. This means that for the existing systems, a new application architecture needs to be built around them. Where the organization issues mobile devices, the devices should be exclusively used for work, and no work at all should be allowed on personal devices. (Mobile Security and Privacy, page 26.)

6.2 Secure Software Development Lifecycle

Mobile application should be subject to regular source code reviews throughout the secure software development lifecycle to detect and remove any code vulnerabilities as early and as often as possible. Consider security when building, planning for test cases. Use code scanning tools such as Coverity, code sight and Application scan sources. Perform a gap analysis to determine what activities, policies currently exist in the organization and their effectiveness. Setup a software security initiative by establishing realistic and achievable goals with defined metrics for success. Processes for security activities should be formalized during software security initiative setup. To secure software conduct a security risk assessment and create a risk profile. When measuring security risks, follow the security guidelines from relevant authoritative sources. Employ a combination of use and misuse cases. The security should foresee possible threats to the software and express them in misuse cases. After the code is complete review it again and search for holes and then bring it to practice. (Mougoue 2016.)

6.3 Data Validation

Develop and enforce sound application security process to prevent unauthorized code manipulation. When developing mobile application developers should undertake mobile security awareness training. Code analysis through a combined approach of static and automated software analysis and expert review by trained professionals. The network centric position of mobile application development requires specialized understanding and expertise. Implement appropriate session management as the form factor for mobile often means application use long lasting tokens for authentication, authorization as well as session management. Minimum cryptography settings for mobile devices should be defined and enforced. Make sure that device encryption is enabled on the device. While some device manufacturers enable encryption by default, other require that encryption is enabled in the device encryption is enabled in the device setting. If the device is owned by person, then personal device encryption should be used. If the device is owned and managed by an organization, then enterprise encryption is recommended. Data confidentialities consider what the data confidentiality setting should be for mobile device application. Environmental and biometric sensors in the device such as acceleration, ambient temperature, fingerprint, geolocation, humidity, proximity, sound, video, image capture etc should comply with the organization data capture policies and their use should be selectively controlled by mobile device management. Application penetration testing should be subjected to a multilevel approach. Test the application to ensure it complies with policies and best practices, but since it is a mobile application, also test network functionally and APIs or servers the application may connect to. The mobile application should be subject to application penetration testing before being loaded to an application stores and before going outside. (Man, HO Au, Kim-Kwang, Raymond 2011.)

6.4 Handle Identity Management

User authentications require confirmation of the user's identity as described in a corporate directory service before giving access to secured data or software. Two factor authentications are recommended for confidential data, such as a username, password combination plus a successfully answered challenge question or positive fingerprint identification. There are single-factor authentication example password or PIN, multi factor authentication example token code or a smart card, and multistep authentication example single factor plus code sent to a user out of band. Usually multifactor authentication I multistep authentication involves the user receiving a code via SMS or an application such as duo and entering it alongside their PIN, password, the phone could be considered as something you have thus qualifying this as two factor authentication. However, the code that is used as well as the credentials used to access the account, device which receives the code, in the second step. Two factor authentication refers specially and exclusively to authentication mechanisms where the two authentication elements fall under different categories with respect to some something you know; you have and something you are. Multistep authentication that requires two physical keys, two passwords, or two forms of biometric identification is no two factors, but two steps are still valuable. Device authentications confirm the unique identity of the physical device; it must meet security and configuration requirements, independent to any of its users. Device access control protect physical access to the device by requiring successful reorganization of a policy-defined password, pattern swipe, biometric scan, voice, or facial recognition. A well thought out mobile device management strategy is a key ingredient for a successful mobility deployment. Ideally the organizations IT section should be at least aware of every smartphone and tablet used in an organization, from activation to retirement. Accomplishing this requires a cohesive plan for mobile device management. It is advised that assets are defined, and hole mobile application use these assets.

Include capability for over the air device wipe that erase all application and data of the device, device lock block device access and remote device configuration. (Mobile Security Strategy, page 29.)

6.5 Mobile Application Management

Mobile application management describes software and services responsible for providing and controlling access to internally developed and commercially available mobile application used in business setting on the companies. Decide on relevant acceptable use policies to help set expectations. Make sure employee are clear on which applications are blacklisted and which they can access. Consider an enterprise application store, which provides a central online location for distributing, downloading, and tracking policy compliant mobile application use by employees. Use mobile application management tools to transparently install and configure business or security application, especially if you allow bring your own device; you cannot always count on employees to do it correctly on their own. Establish a way to track application downloads and ongoing usage, monitor to detect outdated or disabled application and enforce the removal of blacklisted application. (Mobile Security Strategy, page 28.)

6.6 Mobile Device Management

Mobile device management describes a management approach for controlling, monitoring, and optimizing mobile devices. The intent of mobile device management is to get an accurate data to control and monitor mobile devices in companies' environment and to establish a database for registered mobile devices and their users. A comparison to local device management, which typically supports technical engineers to control and monitor stationary IT infrastructure shows the similarities and differences between the two approaches. However, in terms of mobile device management and under consideration of local device management, device management comprises many aspects and functionalities. Mobile operating system support MDM solutions typically consist of a client/server architecture. A mobile client is installed in mobile devices to communicate with the server and exchange relevant data. It indicates the supported operating systems for mobile device management. The roaming status helps the technical engineer to determine, which mobile network is used in currently. Roaming itself is a technology that allows the user to set or receive phone calls or use mobile data transmission, no matter in which mobile network they are located. To monitor and regulate roaming costs, mobile device management software vendors set up control mechanisms to control the roaming status. Battery status delivers information about the battery consumption or the charge level for each mobile device. It helps to indicate whether the battery could be damaged or not. Hence, it is often used for inventory management. Global positioning system (GPS) is widely used functionality to locate mobile device. It is often used to find stolen or lost mobile devices. It allows an exact localization of users or mobile devices and could therefore be used in many scenarios. Network information shows connections to mobile networks, information exchange via virtual private networks or mobile data usage. Such information supports the technical engineer by analysing possible security or network lacks. Detailed statistics about mobile application helps to determine possible security risks. If an organization wants to apply defined security standards, they must consider mobile applications. Applications black/white listings in mobile application management are further steps to secure mobile networks. (Mobile Device Management, page 44,45.)

6.7 Design Secure Application

Before any mock-ups are created or any lines of code are written, your entire design team should collaborate on the security essentials for new project. During this time, it is important to review common threats that are aimed at websites and mobile applications and the best practices for protecting against them. The goal of UI and UX should be to only display information and tools that user can see. This concept of access control must be emphasized by all members, including those who work at the database and network layers. When designing an interface, always assume that a hacker will do whatever it takes to manipulate your website or application and expose a flaw. Elements that allow external input, such as search fields and common boxes, are especially vulnerable and should secured before any code is published and released. Web designers use an element known as cookie to track an individual’s session from single computer. A cookie is a small piece of text that identifies the person on a website and allows them to view account information without having to log in each time they open their browser. While this approach does offer a level of convenience, designers should consider adding login limitations for the sake of security. For example, by setting up 24-hour automatic logout timer on a website or mobile application, you can ensure your users security even if their computer or phone is stolen.

6.8 Implement HTML5 content

HTML types and how they work in different ways

HTML4	HTML5
DOCTYPE declaration too lengthy and refers to an external resource.	DOCTYPE declaration is simple and in one line, for example: <!DOCTYPE html>
No multimedia supporting tags. Third party plugins used.	Introduces dedicated tags for multimedia like <audio>, <video>
Applet tag that was used to display applets in browser was removed.	Object tag was added to display applet types items.
The acronym(<acronym>) tag had been removed.	A new tag<abbr> introduced in place of acronym
HTML4 is complete with compatible with almost all web browsers.	HTML5 being a newer version is not compatible with all the browsers.

TABLE 1. Difference of HTML4 and HTML5

The latest version of the Hyper Text language known as HTML5 and is supported by popular web browsers like google chrome and Mozilla Fire Fox. This update HTML represents a major shift forward and incorporates several new elements that can boost your sites security. Thanks to HTML5, web and mobile designers no longer must rely on the Adobe Flash platform to add native support for audio and video content to their projects. Flash was found to have number of security vulnerabilities that could allow hackers to extract source code elements and access back-end servers. Although HTML5 is considered to the web standard today. It still has certain limitations when it comes to online security. If your website relies on JavaScript code for interactive elements, then you remain at risk for cross-site scripting (XSS) attacks. (Bocetta 2018.)

6.9 Control External References

Most website and mobile applications have dedicated space set up for advertisements. Although UI and UX designers primary focus is on the internal elements they are creating they also need to consider the external references that end up in the project. Designers need to keep in mind that these ad blocks will often point to external HTML sources that could contain links and other interactive content. As a result, they represent vulnerabilities to a variety of common attacks and should be controlled as much as possible. Otherwise your user's data could be put in danger and damage the company's reputation in the process. (Bocetta 2018.)

6.10 Promote Site Encryption

A business owner should encrypt their data to protect their customers personal data and a costumer will want to see the identity of the business owner so they can make an educated trust decision. A business owner therefore must also consider how they want their business to be perceived by their potential customers and how much they trust they believes they need from them to supply their personal information. This will vary depending on brand and industry. Generally, all websites should have some level of encryption on them. When you take information from your website visitors like name, address, card details, you are in position where you are responsible for managing data and should therefore be responsible for encrypting your website, application and data received through it. Most internet users will recognize the padlock symbol at the top of a web browser as a sign of a secure website. It indicates that the current URL address is equipped with a secure socket layer (SSL) certificate for encrypting all communication between the browser and the sites web server. With a valid SSL certificate, your users can be assured that password entry and credit card payments are secure and cannot be hacked by others on the local network. With so much focus on internet privacy in the news, its critical to offer your userbase this kind of protection. As a UI and UX designer, you may want to go beyond and padlock icon and create another way of emphasizing your sites security measures. For example, you could add security seals from PayPal and credit card companies to indicate that your company or organization is trustworthy manager of financial transactions. (Bocetta 2018.)

CONCLUSIONS

This report concludes that devices are danger until it is secured by security management and through personal management. Computers and other electronical devices are very important in 2020. About 70 percentage of people use internet from their mobile phones and 68 percentage of people use desktop or laptop. Mobile phones, computers are mainly for communication and to store the materials which is very important in this generation. Online service is used daily, which is private or public. Private documents, mails or banking usernames and passwords are very important. They should be secure from cyber criminals, thief and from hacker.

The literature review and all the collected information denotes that every single user who are using mobile device should have knowledge of security and privacy. People who are working from mobile devices should be more careful. And such organization should focus on security.

Lack of awareness may hamper in privacy. Be aware about malicious webpage, application. Turn off all applications, logout and make sure to close Bluetooth to be secure. Install anti-virus, check security updates, keep strong passwords and update. The companies who are developing mobile devices and mobile application should also focus on securities. Such companies should make strategy in security while making any application or device. The best way to protect devices is the same way to protect yourself from illness. And be aware of threats and implement securities as soon as possible makes everything secure.

REFERENCES

Apple platform security 2020. IOS operating System. Available: https://support-apple.com/guide/security/welcome/web. Accessed May 2020. Accessed May 2020.

Brandt 2009. Available: Operating system Attacks, tutorials point simply as learning, operating system security. Accessed May 2020.

Google 2020. Available: Business.gov.au/risks-management/cyber-security/how-to-protect-your-business-from-cyber-security-thrats.Business.gov.au. Accessed May 2020.

Google 2020. Available: www.bebopedia.com/term/mobile dvicesecurity.html. Accessed May 2020.

Milkovich 2019. Available: www.cybinsolutions.com/cyber-security-facts-stats/. Accessed May 2020.

Mougoue 2016. Available: Securing software's. Accessed May 2020.

Paul Rubens 2019. physical controls of the device, administrative controls, administrative controls. Available: Secureplanet.com/cloud/data-storage-security.html. Accessed June 2020.

Prescient Solutions 2018. Challenges for Securing Devices. Available: www.prescientsolutions.com/blog/8-mobile-security-challanges-you-need-to-manage/. Accessed June 2020.

Raymone 2017, Available: techrepublic.com. Accessed April 2020.

Rich Campagna, Subby Iyer, Ashwin Krishnan 2020. Available: www.zednet.com/ article / whose-responsibility is mobile device management/Mobile device security for dummies. Accessed June 2020.

Sam Bocetta 2018. Six ways to design a more secure Application. Available: blog.fluidui.com. Accessed July 2020.