**CAB240 Information Security - Semester 2, 2016.**Marking Criteria Sheet for Mobile Security Investigation

|  |  |  |  |
| --- | --- | --- | --- |
| Student Name: | YeongJe Park | Student Number: | N8923108 |

**Part I submission (due Friday 2 September)**

* Include your name, student number and news article titles in the appropriate spaces of this marking criteria sheet. Then include this page at the front of your submission.
* IMPORTANT NOTE: Keep a copy of your Part I submission. The Part II submission builds on this, so you must retain a copy to reference.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Report component** | **You have completed this component of the task outstandingly, with:** | **You have completed this component of the task well, with:** | **You have completed this component of the task satisfactorily, with:** | **Your attempt to complete this task is satisfactory in the following ways:** | **Your attempt to complete this component of the task is not satisfactory, as:** | **Mark:** |
| **5** | **4** | **3** | **2** | **1/0** |  |
| **Information security asset description** | Excellent description withcomprehensive details of:  □ the device hardware,  □ the operating system and version,  □ application software installed,  □ types of stored data | Very good description providing details for each of the following:  □ the device hardware,  □ the operating system and version,  □ application software installed,  □ types of stored data | Description providing some details for each of the following:  □ the device hardware,  □ the operating system and version,  □ application software installed,  □ types of stored data | Description providing some details for at least 3 of the following:  □ the device hardware,  □ the operating system and version,  □ application software installed,  □ types of stored data | Your description lacks details of the following aspects:  □ the device hardware,  □ the operating system and version,  □ application software installed,  □ types of stored data | /5 |
| **Overview of device usage** | Thorough overview of your use of the device; including evaluation of:  □ level of criticality of all items/applications and data, and  □ the sensitivity of the data items included in description with respect to CIA | Good overview of your use of the device; including evaluation of:  □ level of criticality of most items/applications and data, and  □ the sensitivity of most data itemsincluded in description with respect to CIA | Adequate overview of your use of the device; evaluating:  □ level of criticality of some items/applications and data, and  □ the sensitivity of someof the data items included in description with respect to CIA | Overview of your use of the device; evaluating either:  □ level of criticality of items/applications and data, or  □ the sensitivity of various data items included in description with respect to CIA | Overview of your use of the device does not cover:  □ the level of criticality of items/applications and data, or  □ the sensitivity of various data items included in description with respect to CIA | /5 |
| **Article 1 (O/S related) Name:** | | **iPhone vulnerability used to target journalists, aid workers** | | | | |
| **Article 1 summary:**  **Mobile device operating system** | Comprehensive article summary that correctly identifies and clearly explains the:  □ threat/s,  □ vulnerability and  □ security goal/s | Good article summary that correctly identifies and explains the:  □ threat/s,  □ vulnerability and  □ security goal/s affected | Satisfactory article summary that correctly identifies and describes the:  □ threat/s,  □ vulnerability and  □ security goal/s | Article summary identifies the:  □ threat/s,  □ vulnerability and  □ security goal/s affected | □ Inappropriate article, or  Article summary does not correctly identify:  □ threat/s,  □ vulnerability and  □ security goal/s | /5 |
| **Article 2 (App related) Name:** | | **Minimizing security risk of playing Pokemon Go** | | | | |
| **Article 2 summary:**  **Mobile device application** | Comprehensive article summary that correctly identifies and clearly explains the:  □ threat/s,  □ vulnerability and  □ security goal/s | Good article summary that correctly identifies and explains the:  □ threat/s,  □ vulnerability and  □ security goal/s affected | Satisfactory article summary that correctly identifies and describes the:  □ threat/s,  □ vulnerability and  □ security goal/s | Article summary identifies the:  □ threat/s,  □ vulnerability and  □ security goal/s affected | □ Inappropriate article, or  Article summary does not correctly identify:  □ threat/s,  □ vulnerability and  □ security goal/s | /5 |
| **Article 3 (User behaviour related) Name:** | | **The threat in downloading new mobile apps.** | | | | |
| **Article 3 summary:**  **User behaviour** | Comprehensive article summary that correctly identifies and clearly explains the:□ threat/s,  □ vulnerability and  □ security goal/s | Good article summary that correctly identifies and explains the:  □ threat/s,  □ vulnerability and  □ security goal/s affected | Satisfactory article summary that correctly identifies & describes:  □ threat/s,  □ vulnerability and  □ security goal/s | Article summary identifies the:  □ threat/s,  □ vulnerability and  □ security goal/s affected | □ Inappropriate article or  Article summary does not correctly identify:  □ threat/s,  □ vulnerability and  □ security goal/s | /5 |
| **Conclusion** | Excellent conclusion relating threats and vulnerabilities in the three articles to specific assets, features of user device, and/or usage | Good conclusion relating threats &vulnerabilities in at least 2 of the 3 articles to specific assets, features of user device and/or usage | Satisfactory conclusion relating threats and vulnerabilities in the at least two of the three articles to user device, assetsand/or useage | Attempts to relate threats and vulnerabilities in at least one of the three articles to the user device, assets and/or usage | Does not relate the threats and/or vulnerabilities in any of the articles to the user device or information assets | /5 |
| **Selected Articles:** | For all three articles,  □Comprehensive and correct reference details  □ Copies in appendix | For all three articles,  □Mostly correct reference details  □ Copies in appendix | For all three articles,  □References provided, but some details missing  □ Copies in appendix | For all three articles,  □References provided butmany details missing  □Copy in appendix | □Missing many important details OR  □ No reference details  □ No copies in appendix | /5 |
| **PART I total** | | | | | | /35 |

This report will show basic definition about hardware, software and data on mobile device. Furthermore, it is also contained some stories about iPhone and informational security issues under three articles. These articles include Operating system, Application and User behaviour in the world.

First of all, people could easily identify and use various hardware in our life. There are some types of hardware devices such as input and output devices, CPU, memory, cameras, batteries, Touch ID sensors and so on. Input device transmits data and instructions to mobile devices while output device send data and instructions to visual effects from mobile devices. For instance, input device shows a tablet pencil, keyboard, and scanner while output device shows a printer, monitor. The CPU is the most important element on mobile device. The CPU executes interpretation and arithmetic operation to show results after users enter data or command. Apple mobile phone which this reporter personally belonging have A8 chip for CPU. The memory device save information and data on mobile device. This device shows 16GB and 64GB under iPhone 6+.

Secondly, a mobile operating system is essential program and foundation to manage software and hardware for running devices. Every mobile devices should have an OS to execute program and application. If there is a device without OS, it will be an inefficient machine. Furthermore, the operating system provides also reliable security for better mobile system. When unknown user access the system, this OS will strictly limit to access. There are well-known two OS for mobile like iOS and Android. These OS combines some features of computer operating system with other good features for devices. OS could also upgrade to new version for better system and new technology when company launch or update a new mobile OS version. For instance, if the Apple releases new software to provide better features, people will be received new version notifications on iPhone. Now, the newest iOS is 9.3.5 version on iPhone. These OS could offer smaller features than OS for computer. But, people can use simply actions like watching movies, web surfing and playing game by using phone or tablet. Company for making OS try to create better OS to use easily and provide improved quality of technology. Thus, people could choose useful OS version.

Thirdly, there are a number of type of applications on mobile device. When people purchase an iPhone, it can be seen some installed application software such as a Bluetooth, camera, map, Wi-Fi, music player, cellular, notepad. Therefore, some useful applications exist already on mobile device before people buy device. These applications have each valuable features. For example, a map application could be the method to help finding destination. Another representative popular application is a Bluetooth which could provide function to share data and connect with other devices. Furthermore, in terms of iPhone, the Safari which is a software for internet provides powerful security by OCSP(Online Certificate Status Protocol) and certificate verification warnings when user do web surfing. People could install other application such as game, video and other useful materials for education through installing application store without any fee.

Lastly, it has been beneficial for user who use smartphone or tablet which enable information collectively, therefore they can find the data conveniently. For example, by utilising mobile devices, people could store their private data such as contact, photos, video, calendar, books data which can be essential element for living. People could also download a number of data from internet without connecting computer. If people want to watch movie or read some novels, they can directly install them on their mobile devices from smartphone web.

In terms of hardware for iPhone 6+, it is considered that the most important thing is A8 chip which is the part of CPU. The A8 chip is foundation of iPhone as if there is no this chip, it cannot be used critical functions of iPhone. This processor could provide the Secure Enclave which is great function for information security. Attackers could not compulsory decrypt the encrypted data in iPhone by hacking skills. If they want to decrypt their data, they should know password to open iPhone. But, if hackers could not decrypt code in succession, the iPhone will be locked and deleted these data. Furthermore, their defence function will be removed by only Apple company. So, the Secure Enclave technology could protect criticality data by satisfying confidentiality, integrity and availability. There is also useful hardware feature for Touch ID sensor by utilising fingerprint. It could provide more safer and helpful technology to access mobile devices. People could also use this sensor for payments by scanning fingerprint. It could show good merits in respect of confidentiality.

Secondly, the most vital software is operating system compared with others on mobile devices. According to the iPhone, iOS software will be often released for new features and emerging security issues by the Apple. So, users of Apple product could upgrade new iOS version without payment for better use. The iOS could show a strong security system and people believe this OS could protect our information without security program. But, the iOS vulnerabilities show some important security issues for jail-breaking when users access to products based on iOS without permission. Jail-breaking is offering download apps on apple store to unauthorized users and detour the essential security of iOS. The jail-breaking iPhone will be faced with many Trojan and malignant code virus compared to non jail-breaking mobile since when users could install free apps, these some apps could be covered dangerous virus. So, hackers could easily attack jail-breaking mobiles to access and get data.

There are a great number of application on iOS. In particular, there are also sensitivity application such as contact, calendar, photo, mail box and so on as these application have personal and communication information. These application could be locked code to protect information in respect to confidentiality and integrity. There is also significant application for banking task. Nowadays, many people use mobile bank for banking operation as it could provide convenience service and save time in our life. This bank application contain very important information such as personal, bank account, card number and particulars of payment information. To prevent hacking mobile bank is essential action as if this application was attacked, money in bank account will disappear. So, bank application offers security program, password, touch fingerprint to protect their information. These security solutions show security goals for confidentiality and integrity.

Lastly, there are a lot of stored data on iTunes which is a useful program for Apple products when people used iPhone or other Apple products for some years. Many data could be automatically saved by this program on computer. So, when people changed new iPhone, they could recover their old data such as photos, music, contact, apps and communication with message from iTunes. Especially, photos are considered more essential data to people than others since these photo could show good and bad memory with family, friends and others. There are also sensitive data on iPhone since people used to write difficult information to remember and important data. For example, if they change phone number or new bank account, they could not instantly remember as these information are new and hard to remember. So, notepad on mobile had various personal data.

Semester 2 2016

**Mobile Security Investigation**

**Title**: iPhone vulnerability used to target journalists, aid workers

**Author:** Kelly, Heather

**Reference details (if online article, give URL and date accessed):**

Kelly, H. (2016, Aug 25). iPhone vulnerability used to target journalists, aid workers.*CNN Wire Service* Retrieved from http://gateway.library.qut.edu.au/login?url=http://search.proquest.com/docview/1813993584?accountid=13380

**Brief summary:**

The Apple released new software for iOS 9.3.5 after people discovered a malware. This malware allowed hackers to do everything on iPhone by utilising remote control. When the Apple chased unknown spyware, they could find NSO group which is selling software to governments. The Citizen Lab team and Lookout started to analysis these problems. According to the investigation team, when people click text link, their iPhone have automatically installed the malware and approved all of functions such as every applications, records of calls and messages, calendar and so on to attackers.

**Information asset.**

There are a lot of information assets in this article. For example, attackers could get individual information such as name, phone and ID number, date of birth and stored data on iPhone when people got malware to their iPhone by clicking text link.

**Threat.**

This threat shows deliberate human action by a hackers and an external threat. The attackers could spray text link with virus to access to user's iPhone. The iPhone could be unwittingly downloaded malware when people click text link on message or web. This security goals are confidentiality and integrity. According to the confidentiality, hackers could get people personal or saved information on iPhone. In terms of integrity, they could also edit and delete their stored information on virtual.

**Vulnerability.**

The vulnerability was known as "Trident". This vulnerability could provide hackers access to iPhone. After they got access to iPhone, they could control everything on iPhone system. For instance, attackers could intercept emails and messages, recognize passwords, calendar and contract data.

**Security incident / attack.**

The news story shows vulnerability about previous iOS version. Therefore, the Apple distributed new iOS version for 9.3.5 to solve their problems. Before it was released, hackers could access to iPhone by virtual without consent when people click text link with malware. Attackers could also control their iPhone to gain and abuse information. According to the this article, many people were exposed to unknown spyware as they usually click text link to search information or connect websites.

To protect malware on iPhone people can update new operating system software for iOS 9.3.5. The Apple released better iOS for security system compared to last version.

Semester 2 2016

**Mobile Security Investigation**

**Title**: Minimizing security risk of playing Pokemon Go

**Author:** [Hudson, Laura](http://search.proquest.com.ezp01.library.qut.edu.au/indexinglinkhandler/sng/au/Hudson,+Laura/$N?accountid=13380)

**Reference details (if online article, give URL and date accessed):**

Hudson, L. (2016, Jul 14). Minimizing security risk of playing pokemon go. *International New York Times* Retrieved from http://gateway.library.qut.edu.au/login?url=http://search.proquest.com/docview/1803635387?accountid=13380

**Brief summary:**

Nowadays, Pokemon Go is the most famous application game on mobile device as Poketmon Go shows special technology by utilising augmented reality. After this game was launched, many people could play Pokemon Go by approving to access Google or Facebook account. Some critics said that this company could invade players’ private life when people play this game to catch pokemons.

**Information asset.**

This information assets show detail of user’s account such as photos, email, stored papers, location of players and so on. Niantic company which is made Pokemon Go could access and gain players’ information when people play this game. Thus, this company could gain the great amount of data about players in the world.

**Threat.**

This threat source shows internal threat related with deliberate human action. Company could be saved a number of personal information about users on database system. So, these employees could expose or copy stored information on database system when they abuse their data to make money by selling. This may compromise the security goal Confidentiality; the personal information such as phone number, moving route and stored document are revealed without approval.

**Vulnerability.**

The vulnerability is permitting for access of user’s account on Google or Facebook to play Pokemon Go. So, user's private information will be exposed to their company. This company could be stored a lot of information on their database system.

**Security incident / attack.**

The article shows that information about users of Pokemon Go is always exposed to Niantic company. This company could gather user’s information by people playing this game. The company could recognize and analysis various personal information on database system, so that players will be exposed their privacy in their life. These information show location of user, E-mail, photos and sensitive elements. If system manager mistake or abuse managing database, it will make great information asset issues.

Therefore, this company should provide service to play Pokemon go without approving to access Google and Facebook account to protect user’s data. People could play this game without anxiety about their personal information.

Semester 2 2016

**Mobile Security Investigation**

**Title**: The threat in downloading new mobile apps.

**Author:** [Chowdhary, Sudhir](http://search.proquest.com.ezp01.library.qut.edu.au/indexinglinkhandler/sng/au/Chowdhary,+Sudhir/$N?accountid=13380); [Sen, Monalisa](http://search.proquest.com.ezp01.library.qut.edu.au/indexinglinkhandler/sng/au/Sen,+Monalisa/$N?accountid=13380)

**Reference details (if online article, give URL and date accessed):**

Chowdhary, S., & Sen, M. (2016, Jul 11). The threat in downloading new mobile apps.*Financial Express* Retrieved from http://gateway.library.qut.edu.au/login?url=http://search.proquest.com/docview/1802682316?accountid=13380

**Brief summary:**

This article shows that people in India provide their personal information to download free apps. These people were exposing privacy risks by trading their information. Nearly half of people approved access to individual and mobile data to exchanges free apps. Indian used to use more Smartphone to access internet than computer. According to the survey from Symantec shows that mobile wallets, e-commerce and banking apps were the most famous apps in India. Therefore, they used to usually face mobile security issues. To protect their information there are some methods.

**Information asset.**

In India, people usually agreed access for their information assets to download free applications. Information assets describe private information on Smartphone such as contacts, photos, mails, date of birth and financial data. So, These assets will be easily disclosed to hacker.

**Threat.**

This case is one of external threats. Indian people were faced with unexpected danger by virus attacks when they download free application. Hackers could hide malignant code on free application to hack their Smartphone. This may compromise the security goal is confidentiality since when people download free apps, their personal information will be exposed by approving.

**Vulnerability.**

People in living India are trading private information to install free applications on Smartphone. They think that installing free apps is more important than their personal information. In addition, they usually visited unofficial app stores to download apps without payment. According to the this situation, they did not have concept about significance of information security. Thus, various individual information will be exposed simply to hackers in India.

**Security incident / attack.**

This news shows that Indian people did not have idea about importance of information security since they used to download free apps by offering their information. So, their private information could be disclosed on internet. Hackers could easily gain information about users of smartphone. Some incidents show abuse of bank account details or credit card and leaking or hacking of private data.

The Symantec recommend some methods to protect themselves. Firstly, Use difficult passwords and lock patterns. Secondly, check settings and updates usually. Thirdly, install apps from official stores. Lastly, use helpful security.

In conclusion, there have recently coming out many security issues about mobile devices in our society as most people use mobile devices such as smart phone and watch, tablet. These devices are useful tool for busy lives. People could do every things by using mobile devices. For example, people could communicate well through those of applications with other people, and safely accessing to private banking accounts. Furthermore, people could also enjoy entertainment such as watching TV, listening music, playing games, social media. Many people usually spend time by using the functions above of mobile devices. Due to this mobile`s popularity, some hackers are trying to inject virus on website, application, text link and mail to users. To prevent individuals` leakage from hackers, a number of solutions have been represented.

According to the operating system issues, the iOS was known highly security OS in the world and people have believe that this OS protect their information from hackers. But, before iOS 9.3.5 version was made by Apple, last iOS version had vulnerability which is called "Trident". It is considered highly serious problem for information assets since attackers could access every information and functions on iPhone. Hackers could send and spread text link which are illegally hacked to unspecific people. This text link was covered vicious virus by attackers to hack and access iPhone. If people click this link, their iPhone will be infected by hazardous virus. The hacker could control and access their iPhone on virtual. So, they could know many information such as personal, bank account, contact, conversation information and so on. Then, they could also abuse or sell these information for pecuniary benefits. After the Apple recognize this vulnerability, they release new version for iOS to solve problem.

Secondly, in terms of application, there are a great number of application on iOS. Users for iPhone could download easily various applications on apple store. About 2 months ago, the Pokemon Go application was released in some countries. This application is new augmented reality game. Many people could spend a lot of time by playing this game to catch Pokemon and increase trainer level. So, this app has been the most famous game on mobile device in the world. But, the vulnerability of app shows that people should permit for access to their Google or Facebook account if people want to play Pokemon GO. When people are trying to play this game, the company could have right to access their account of google or facebook. So, users could be exposed their private information to this company. Furthermore, when people play this game, they should also permit their location since this game is based on augmented reality. They could also know personal information and moving route of players. This company should change regulation about permitting their information as it is very sensitive information in our society.

Some information asset issues could be made by the user behaviour. For instance, if people did not set up their mobile password to access, other people could access to mobile device without password. So, they could have some personal or other information by accessing other mobile device. Especially, there is very serious user behaviour about using mobile devices in India. Most people in India install usually free apps by offering their personal information. Hackers could simply attack their mobile phone to inject virus in India. Indian does not have idea about important of individual information. It is really serious vulnerability on information security. They could be faced exposing their information when they download free apps. To prevent exposing personal information they should change their idea about information security.

Nowadays, people could simply face some security issues as mobile device is one of the most essential products in our life. This report shows basic definition of hardware, software and data on mobile device. Furthermore, There are information security issues related to operating system, application and user behaviour from article.

**Appendix**

**1) iPhone vulnerability used to target journalists, aid workers**

**Author:**Kelly, Heather

[ProQuest document link](http://gateway.library.qut.edu.au/login?url=http://search.proquest.com.ezp01.library.qut.edu.au/docview/1813993584?accountid=13380)

**Abstract:**

Human rights activist Ahmed Mansoor first received a suspicious text message on August 10.

**Links:**[Check if fulltext is available at QUT](http://sf5mc5tj5v.search.serialssolutions.com.ezp01.library.qut.edu.au/?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ProQ%3Anorthcentralnews&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.genre=unknown&rft.jtitle=CNN+Wire+Service&rft.atitle=iPhone+vulnerability+used+to+target+journalists%2C+aid+workers&rft.au=Kelly%2C+Heather&rft.aulast=Kelly&rft.aufirst=Heather&rft.date=2016-08-25&rft.volume=&rft.issue=&rft.spage=&rft.isbn=&rft.btitle=&rft.title=CNN+Wire+Service&rft.issn=&rft_id=info:doi/)

**Full text:**

One of the most significant iPhone hacks to date was outed with a simple text message.

Security researchers on Thursday announced they had discovered a new piece of iPhone malware that allowed attackers to see virtually everything on your iPhone. They traced the previously unknown spyware back to an Israeli-based company called the NSO Group. NSO openly sells software that it says can track a person's mobile phone -- and many of its clients are governments.

At the same time on Thursday, Apple released a software update for iOS 9.3.5 that patches the vulnerabilities. The company recommends anyone using an iPhone update their iOS immediately. For users running the beta of iOS 10, the latest seed also patches the exploits.

Researchers said it appeared governments had used NSO's software to target journalists and human rights workers. They used fake domains to try and disguise themselves as legitimate groups like the Red Cross, news organizations, and large tech companies.

Human rights activist Ahmed Mansoor first received a suspicious text message on August 10. The next day he got another, this time with a link promising information on detainees in UAE jails. No stranger to hacking attempts, the well-known dissident forwarded the messages to a researcher at Citizen Lab in the University of Toronto's Munk School of Global Affairs.

Citizen Lab teamed up with mobile security company Lookout to investigate. Together they confirmed the discovery of an advanced piece of spyware that took advantage of three previously unknown iOS security holes. By clicking on the text link, Mansoor would have unwittingly installed the malware and allowed the sender full access to his communications.

The combination of the vulnerabilities, together known as "Trident," gives the attacker access to an iPhone's camera, microphone and location. It can intercept text messages and emails, download calendar and contact data, and see passwords stored in the iPhone's keychain. It can record phone calls and messages from WhatsApp and Viber, and access communication apps including iMessage, Gmail, Facebook, Skype, and Line.

"We were made aware of this vulnerability and immediately fixed it with iOS 9.3.5. We advise all of our customers to always download the latest version of iOS to protect themselves against potential security exploits," said Apple spokesman Fred Sainz in a statement.

NSO Group denied any knowledge of this specific hack.

"The company sells only to authorized governmental agencies, and fully complies with strict export control laws and regulations," NSO spokesman Zamir Dahbash said in a statement. "The agreements signed with the company's customers require that the company's products only be used in a lawful manner. Specifically, the products may only be used for the prevention and investigation of crimes."

Credit: Heather Kelly

**Subject:**Human rights; Computer viruses; Researchers

**Publication title:**CNN Wire Service

**Publication year:**2016

**Publication date:**Aug 25, 2016

**Year:**2016

**Section:**BUSINESS

**Publisher:**CNN Newsource Sales, Inc.

**Place of publication:**Atlanta

**Country of publication:**United States

**Publication subject:**General Interest Periodicals--United States

**Source type:**Wire Feeds

**Language of publication:**English

**Document type:**News

**ProQuest document ID:**1813993584

**Document URL:**<http://gateway.library.qut.edu.au/login?url=http://search.proquest.com.ezp01.library.qut.edu.au/docview/1813993584?accountid=13380>

**Copyright:**Copyright 2016 Cable News Network. Turner Broadcasting System, Inc. All Rights Reserved.

**Last updated:**2016-08-25

**Database:**ProQuest Central

**2) Minimizing security risk of playing Pokemon Go**

**Author:**Hudson, Laura

[ProQuest document link](http://gateway.library.qut.edu.au/login?url=http://search.proquest.com.ezp01.library.qut.edu.au/docview/1803635387?accountid=13380)

**Abstract:**

Niantic has said the expansive permission requests were "erroneous" and that Pokemon Go did not use anything from players' accounts other than basic Google profile information. Niantic also said it was working on a fix to change the permissions to a level that would be "in line with the data that we actually access."

The flap highlights how clicking "yes" to whatever requests pop up when installing an app on a mobile device can compromise privacy, sometimes in insidious ways. In disclosures, some apps say they will hand over data to law enforcement officials or other private parties to respond to legal requests, for example, or even on their own volition.

"A number of these games are not only making money on the front end by selling you the game or things within the game, but they are also collecting data about your habits and what you're doing on your phone, and selling that to third-party marketers," said Andrew Storms, vice president of security services at the security company New Context. "You're pretty much giving the rights to all your information to this company."

**Links:**[Check if fulltext is available at QUT](http://sf5mc5tj5v.search.serialssolutions.com.ezp01.library.qut.edu.au/?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ProQ%3Aafricannews&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.genre=unknown&rft.jtitle=International+New+York+Times&rft.atitle=Minimizing+security+risk+of+playing+Pokemon+Go%3A+Developer+moves+to+fix+expansive+access%2C+but+its+request+isn%27t+uncommon&rft.au=Hudson%2C+Laura&rft.aulast=Hudson&rft.aufirst=Laura&rft.date=2016-07-14&rft.volume=&rft.issue=&rft.spage=15&rft.isbn=&rft.btitle=&rft.title=International+New+York+Times&rft.issn=&rft_id=info:doi/)

**Full text:**

The game's developer made expansive permission requests -- in error, it says, and it uses only basic data -- but many apps make similar requests.

Pokemon Go has attracted hordes of players within days of its release. The mobile game has also attracted concerns about just how vulnerable our personal data can be in the hands of seemingly benign applications.

In the past few days, security bloggers noticed that the game, which is free to download and made by Niantic Inc. in partnership with the Pokemon Company and Nintendo, requested permission not only to use a player's smartphone camera and location data but also to gain full access to the user's Google accounts -- including email, calendars, photos, stored documents and any other data associated with the login.

Critics quickly called the game a "huge security risk" that was invading people's privacy, and Senator Al Franken, a Minnesota Democrat, expressed concerns on Tuesday about the issue.

Niantic has said the expansive permission requests were "erroneous" and that Pokemon Go did not use anything from players' accounts other than basic Google profile information. Niantic also said it was working on a fix to change the permissions to a level that would be "in line with the data that we actually access."

The flap highlights how clicking "yes" to whatever requests pop up when installing an app on a mobile device can compromise privacy, sometimes in insidious ways. In disclosures, some apps say they will hand over data to law enforcement officials or other private parties to respond to legal requests, for example, or even on their own volition.

"A number of these games are not only making money on the front end by selling you the game or things within the game, but they are also collecting data about your habits and what you're doing on your phone, and selling that to third-party marketers," said Andrew Storms, vice president of security services at the security company New Context. "You're pretty much giving the rights to all your information to this company."

So what can be done to minimize the security risks that come with some apps? Here's a refresher on how to safeguard private information.

Read the fine print Ari Rubinstein, a Silicon Valley security engineer, recommends paying close attention to the scope of access that apps request during installation -- or to look up the details online -- and say "no" if the demands make you uncomfortable.

If you are unsure about the permissions you have already granted, check them on iOS by clicking on Settings and scrolling down for a list of apps that you can examine and change individually. On Android, click Settings and click Apps under the Device Settings, then choose an app and select Permissions.

Permissions are not the only things to worry about; you also need to know what kinds of data an app is collecting from your phone. Information about those is typically contained in an app's privacy policies, which are often available within the settings of an app, or searchable online.

If you cannot find the disclosures, or you are unable to understand their legalese, consider holding off until you learn more.

As for Pokemon Go, while the game may not be digging through emails, it is capable of tracking your location. And like those of many apps, its privacy policy allows it to give any data it has about you to law enforcement officials or private parties in response to legal requests or even to whatever it may deem an unethical or legally actionable activity. It can also share nonidentifying information about you with other companies for what it says are "research and analysis, demographic profiling, and other similar purposes."

Regularly audit third-party apps Because apps often use platforms like Facebook and Google to authenticate accounts, Mr. Rubinstein suggests regularly checking the access you have granted through the settings of these systems.

With Facebook, go to your account settings and click on Apps to examine and revoke access. With Google, go to Privacy and Security Settings and click on Connected Apps and Sites to see or change the apps connected to your account.

"Most likely users have apps that they never use that put them at a similar risk" to that from the Pokemon app, he said.

**Company:**Niantic Inc

**Publication title:**International New York Times

**First page:**15

**Publication year:**2016

**Publication date:**Jul 14, 2016

**Year:**2016

**Publisher:**International New York Times

**Place of publication:**Paris

**Country of publication:**France

**Publication subject:**General Interest Periodicals--France

**Source type:**Newspapers

**Language of publication:**English

**Document type:**News

**ProQuest document ID:**1803635387

**Document URL:**<http://gateway.library.qut.edu.au/login?url=http://search.proquest.com.ezp01.library.qut.edu.au/docview/1803635387?accountid=13380>

**Copyright:**Copyright International New York Times Jul 14, 2016

**Last updated:**2016-07-13

**Database:**ProQuest Central

**3) The threat in downloading new mobile apps**

**Author:**Chowdhary, Sudhir; Sen, Monalisa

[ProQuest document link](http://gateway.library.qut.edu.au/login?url=http://search.proquest.com.ezp01.library.qut.edu.au/docview/1802682316?accountid=13380)

**Abstract:**

[...]the smartphone is often the first and only device used for accessing the internet.

**Links:**[Check if fulltext is available at QUT](http://sf5mc5tj5v.search.serialssolutions.com.ezp01.library.qut.edu.au/?ctx_ver=Z39.88-2004&ctx_enc=info:ofi/enc:UTF-8&rfr_id=info:sid/ProQ%3Abankinginformation&rft_val_fmt=info:ofi/fmt:kev:mtx:journal&rft.genre=unknown&rft.jtitle=Financial+Express&rft.atitle=The+threat+in+downloading+new+mobile+apps&rft.au=Chowdhary%2C+Sudhir%3BSen%2C+Monalisa&rft.aulast=Chowdhary&rft.aufirst=Sudhir&rft.date=2016-07-11&rft.volume=&rft.issue=&rft.spage=&rft.isbn=&rft.btitle=&rft.title=Financial+Express&rft.issn=&rft_id=info:doi/)

**Full text:**

People download apps every day, but the truth is that consumers in India are trading their personal information in exchange for free apps, exposing themselves to privacy risks. Nearly one in two Indians have granted access to contacts and mobile data in exchange for free apps; close to 40% have granted access to their camera. That's not all. Victims lost an average of a day's time dealing with mobile security issues, according to the India findings from Symantec's Norton Mobile Survey that sheds light on the security gaps and the privacy risks smartphone and mobile apps present.

The Norton study reveals that two out of three Indians (65%) now access the internet more often on a mobile device than on a PC. In fact, the smartphone is often the first and only device used for accessing the internet. "In today's mobile-first world, mobile devices are like digital warehouses storing our most personal moments and information, such as photos and videos, conversations with friends and family, health and fitness details, financial data and more," says Ritesh Chopra, country manager, India, Norton by Symantec.

Highlighting the increased dependency and usage, respondents reported that they check their device an average of 41 times a day. While making calls continue to be the primary use of a smartphone, applications for internet browsing, communication and social media are just as important. "The report identified that the most concerning security issues for Indian mobile users were virus attacks, followed by threats involving fraudulent access or misuse of credit card or bank account details, and hacking or leaking of personal information," Chopra says (see interview).

**Where mobile meets money**

The survey reveals that mobile wallets, mobile banking and e-commerce apps were among the top five apps used by the Indian users. Mobile devices are increasingly important to how we shop and pay-both online and in-store. Close to 50% of consumers accept that they shop online more than ever before. While 68% of the users worry about the security threats of online shopping, 42% say they have in fact experienced a security problem, threat or nuisance as a

result of using their devices for online shopping. Yet, only 26% of online shoppers believe that threats are increasing. Ironically, a whopping 50% believe that online risks are reducing.

Interestingly, within India, users in Delhi (71%) indulge more frequently in mobile banking than those in Mumbai (63%). When it comes to mWallet, 52% of users believe their mWallet has come under threat as a result of using other apps on their devices, especially social media apps which are perceived to pose the greatest threats, according to 27% respondents. This is not surprising as, on an average users find it safe to hold over Rs 19,000 across their mWallet accounts at any given time. In terms of losses, the victims felt that security problems had taken up an average of over 24 hours to resolve.

**Stay safe, be aware**

There are many steps consumers can take to protect themselves. Norton recommends the following best practices:

\* Use strong passwords and lock screen patterns: Lock screen security is important, as it makes it more or less impossible for a thief to access your information. Also, use different passwords for different apps and change them often.

\* Be vigilant: Being aware of SMS phishing scams is another measure. It's not just emails you have to watch out for these days- phishing scams come in the form of text messages as well.

\* Review settings and updates regularly: Keeping your phone or tablet's software updated is important. If your mobile device isn't regularly updated, it's vulnerable to threats.

\* Download apps from official app stores: Third-party app stores may not put apps through the same rigour as official app stores such as the Google Play Store or Apple's App Store.

\* Depend on reliable security

Solutions: Consider using a security software such as Norton Mobile Security, it helps to use discretion when installing apps. Norton Mobile Insight, a proprietary intelligence tool, crawls over 200 app stores globally to determine and provide dynamic analysis of app behaviour. It protects against Android apps that leak personal information from devices, change settings and require high battery or data usage.

Without doubt, mobile apps bring many benefits but a user needs to be careful and employ security measures when using them.

Copyright 2016 The Indian Express Online Media Pvt. Ltd., distributed by Contify.com

Credit: Sudhir Chowdhary, Monalisa Sen

**Subject:**Electronic commerce; Social networks; Fraud; Mobile commerce; Internet; Personal information; Smartphones

**Location:**India

**Publication title:**Financial Express

**Publication year:**2016

**Publication date:**Jul 11, 2016

**Publisher:**Athena Information Solutions Pvt. Ltd.

**Place of publication:**New Delhi

**Publication subject:**Business And Economics

**Source type:**Newspapers

**Language of publication:**English

**Document type:**News

**ProQuest document ID:**1802682316

**Document URL:**<http://gateway.library.qut.edu.au/login?url=http://search.proquest.com.ezp01.library.qut.edu.au/docview/1802682316?accountid=13380>

**Copyright:**Copyright 2016 The Indian Express Online Media Pvt. Ltd., distributed by Contify.com

**Last updated:**2016-07-11

**Database:**ProQuest Central

**Reference List**

Kelly, H. (2016, Aug 25). iPhone vulnerability used to target journalists, aid workers.*CNN Wire Service* Retrieved from http://gateway.library.qut.edu.au/login?url=http://search.proquest.com/docview/1813993584?accountid=13380

Hudson, L. (2016, Jul 14). Minimizing security risk of playing pokemon go. *International New York Times* Retrieved from http://gateway.library.qut.edu.au/login?url=http://search.proquest.com/docview/1803635387?accountid=13380

Chowdhary, S., & Sen, M. (2016, Jul 11). The threat in downloading new mobile apps.*Financial Express* Retrieved from http://gateway.library.qut.edu.au/login?url=http://search.proquest.com/docview/1802682316?accountid=13380