INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH & DEVELOPMENT

ISSN 2278 – 0211 (Online)

Mobile Security Trends

Jyothy Joseph
Assistant Professor, Computer Science Department
Al-Ameen College Edathala, Kerala, India
Shinto Kurian K.
Tech Mahindra, Smyrna, TN, USA

Abstract:
In the fast growing mobility revolutionary era, the importance of mobile devices (smart phone, tablet etc.) are drastically increased. Nowadays many of them relay mobile devices to do their personal and professional activities. Many of website activates are started switch to mobile apps. Majorly financial and e-commerce sector started recommending their customers to use the mobile apps. This changing trend increases the importance of mobile security requirements. This study helps to understand the current major mobile security trends and how it helps to provide better security on personal and professional life.

Key words*: Mobile security, Security Trend, Social Network Media, Encryption, Vulnerabilities*

1. Introduction

Mobility revolution is going for past few years; it is keep improving the new feel in communication environment. The concepts of mobile devices are drastically changing and it is on the way to replace the personal computers. As per the statistical analysis, 40 to 50 percent of global population expected to use the mobile devices by 2015. Nowadays mobile devices are providing a powerful computing platform, many of them are relaying mobile devices to handle their personal, commercial and financial dealings. So the importance of security is increased. Mobile security was a hot topic in 2013 and it is continuing as it is in 2014. Many studies are progressing and new security trends are releasing. New mobile security trends give a confidence to exploit the latest business opportunities. Implement a new business technique through the mobility feature is a security challenge. Present mobile security trends aims to overcome these challenges and safeguard the mobile devices from the malware attacks and cybercrimes which intending to make financial benefits in crookedly.

One of the biggest threats is the spams which are pushing to mobile devices through the social network Medias. The communication trend is switching from web to mobility, so the hackers also are changing their targets. Hackers are criminal business people and they are looking best business cases in mobile platform in crooked paths. Past few years the malware threats are multiplied. Below mentioned few of common spam messages, spreading through social network media.

- Looking for Business partners
- You got a lottery of XXXX dollars
- RBI security notification, verify your details
- XXXX Bank notification to verify your account details

Mobile devices should follow the latest security trends and equipped with latest security measures. Normally mobile devices are occupying huge volume of personal information. What will be the risk, if lost or hacked the device?How can save the personal data from threats? Below are few of common security trends follows in the mobile devices

- Antivirus protection
- Anti spyware protection.
- Follow the suggested password rules.
- Keep enable the feature to locate the device remotely
- Keep enable the feature to lock the device remotely
- Implement/enable the option to wipe out the data remotely
- Make sure operating system and software updates are up-to-date.
- Provide encryption options

This study is trying to list out the current mobility security trends which are aiming to safely live with new generation communication methodologies.

2. Research Structure

Many methodologies are available to define the workflow of a research topic. This study followed the analytical methodology as mentioned in below structure (Fig 1). Here doing a structured analysis of security usage and its implementation in the present mobile applications, then checking the present security trends. This study tries to gives an overview of present security flaws and security trends.

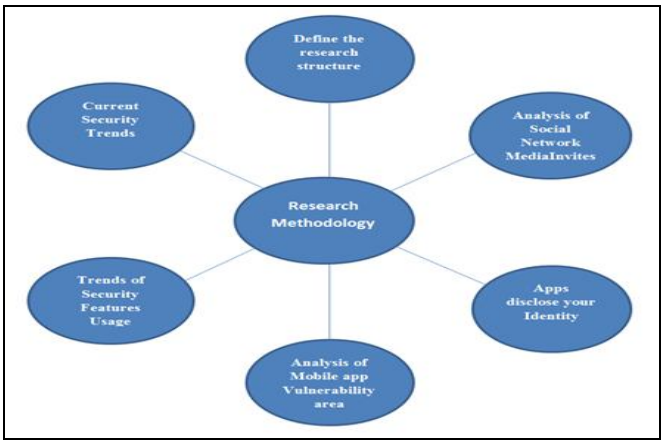


Figure 1: Research Methodology

- **Define the research Structure:** Here defining the analysis boundary and the flow. This analysis mainly focused the ways commonly originates the mobile security threat, then analyzing its critical impacts and major contributors. Then continue on the role of mobile device in the private or secured data, then focusing the present security trends. This analysis structure aims to give an overview of current mobile security trends and its importance.
- **Analysis of Social Network Media Invites:** Social network media is playing a vital role in mobile security. So its available security feature analysis helps to realize the present usage of personal data in social media. This analysis helps to take required precautions when responding to the social media invites.
- **Apps disclose your Identity:** Many of mobile apps are mandatorily asking few of personal specific identities for installing or configuring the application, also usage of few apps are capable to pick few other secured information through the mobile device. So this analysis helps to list out the major issue causing factors.
- **Analysis of Mobile App Vulnerability area:** This analysis helps to get an understanding on the major mobile app vulnerability area.
- **Trends of Security Features Usage:** Here trying to identify the mobile user's current approach on security features. It also helps to understand the majorly using mobile features and currently following security habits and culture.
- **Current Security Trends:** Here spotting, presently following or expecting major security features in mobile and its goodness.

2.1. Social Network Media Invites

Many of them experienced to receive the invite to join the social networks groups from knowing and unknowing contacts. Most of the social network groups or applications are restricting to use the contact number or e-mail id to register the network. Also many of the installable apps have the capability to access your contacts from mobile devises. Even though you registered a network using your minimum personal details, it is giving an option to choose other details from the given list. For instance, register in Facebook with minimum details, it is giving list of options to choose the place, School, College, company etc. The given list will be closely matching with actual one. How the social networks getting capability to list out specific persons details? It is through the contact details which available in that specific device or account. Present trend of social network apps are using Mobile and e-mail contacts to spread the message.

Usages of social network apps or sites through mobile devices are getting tremendous growth. As part of new advertisement trends, many of e-commerce apps and websites are suggesting to share the details in social network sites from customers identity. They providing the shortcut links to social network sites like Facebook, Twitter etc. But many of them are unsure the available security measures in that app or site. Social Network sties, Messaging/Game applications are challenging each other to push downloads messages and advertisements everyday to their users. Hackers are mainly utilizing social network sites, games, messaging apps and Video chatting apps to pull the secured information form the user without their knowledge. Recently Adaptive Mobile team (One of leading mobile security protecting team) had done a survey in North America, which explains (Table 1) the intensity of free

messaging apps to pull or push the secured information. The survey considered the android version of applications usage in February 2014.

Application	Inviting a contact	Inviting to entire contacts	Suggest to invite a friend	Suggest an invite to all friends	Suggest friends in advance	Difficult to skip the suggestion of friends	Not allowed to stop the invite
Glide	✔	✔	✔	✔	✔	✔	✘
Secrets	✔	✔	✔	✔	✔	✔	✘
Anyvideo	✔	✔	✔	✔	✔	✘	✘
Skout	✔	✔	✔	✔	✔	✘	✔
Pixer	✔	✔	✔	✔	✔	✘	✔
Hangtime	✔	✔	✔	✔	✔	✘	✔
Meow	✔	✔	✔	✘	✘	✘	✔
Tango	✔	✔	✔	✘	✘	✘	✔
Dice With Buddies	✔	✘	✘	✘	✘	✘	✘
Voxer	✔	✔	✔	✘	✘	✘	✘
Line	✔	✘	✔	✘	✘	✘	✘
ooVoo	✔	✘	✔	✘	✘	✘	✘
WhatsApp	✔	✘	✔	✘	✘	✘	✘
Viber	✔	✘	✘	✘	✘	✘	✘
WeChat	✔	✘	✘	✘	✘	✘	✘

Table 1: Social Media Apps Invite

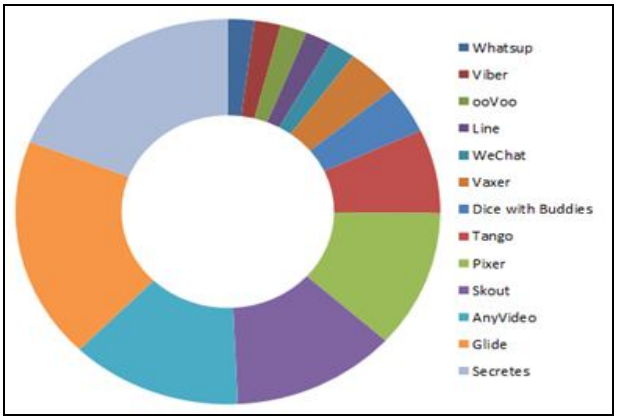


Figure 2 : Contact usage in different Apps

Many of your contacts affected from your mobile applications. Above doughnut diagram (Fig 2) explains the usage of your contacts to send invites from various mobile applications. They selected a broad cross-section of 15 Apps which represent the origin of the vast majority of Invites sent during this period.

2.2. Apps Disclose Your Identity

Mobile devices are capable to provide many of personal information. So the way of handling the device and the usage of various applications should be safe. When installing a new app, need to verify the app is actually required and it is providing the expected features. Below are the mainly available personal details from the mobile.

- Device identification number - IMEI, MEID, ESN or IMSI
- Location details
- Wireless device details
- Usage of device details
- Account information
- Installed Application details
- Application usage details
- SIM card details

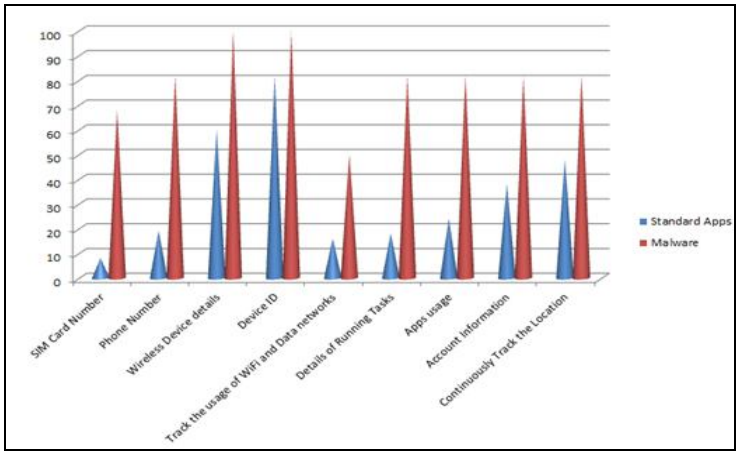


Figure 3: Secured data collection between a standard application and malware

Careless usage of social network apps and games pushes the malware to mobile devices. Malware are similar like a normal applications which monitor and track the device usage and collecting the secured information than a standard application and using for illegal purpose with abusive permission. An attacker can use the data for illegal activities. For instance, phone numbers use to spread the incorrect messages. Above cone graph (Fig 3) explain the secured data collection between a standard application and malware application. Fig-4 gives an overview of geographical malware population analysis.

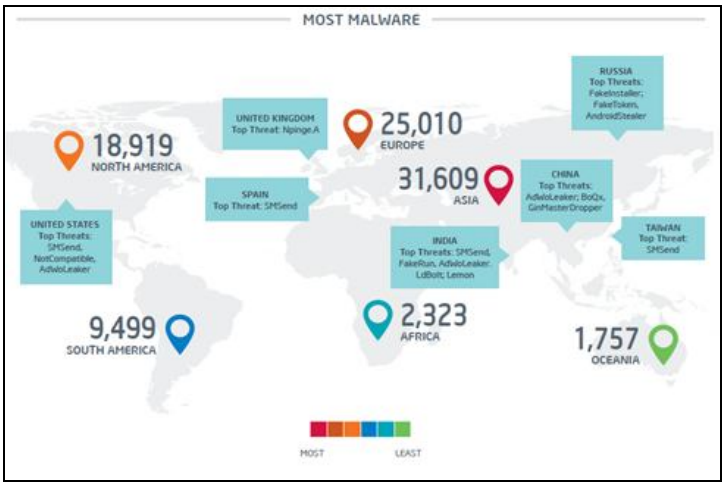


Figure 4: Malware population analysis

2.3. Mobile Apps Vulnerability Area

As the mobile devices are holding good amount of data the security features are getting highlighted. Cenzic service team did an analysis on Mobile application vulnerability. Below cone diagram (Fig5) explains their vulnerability categorization.

- **Infrastructure:** The infrastructure securities are comparatively high in web applications but that level security is not available for mobile applications. Many of the secured mobile applications are not validating the security certificates to make

sure the app is providing the information to right place. This vulnerability allow an attacker to stand in the middle of the transactions and attack the secured information

- **Privacy Violation:** Privacy is one of the major concerns rising in the mobile apps. The mobile devices having private information, the leakage of private information causing to get involve your identity in many places without your knowledge.

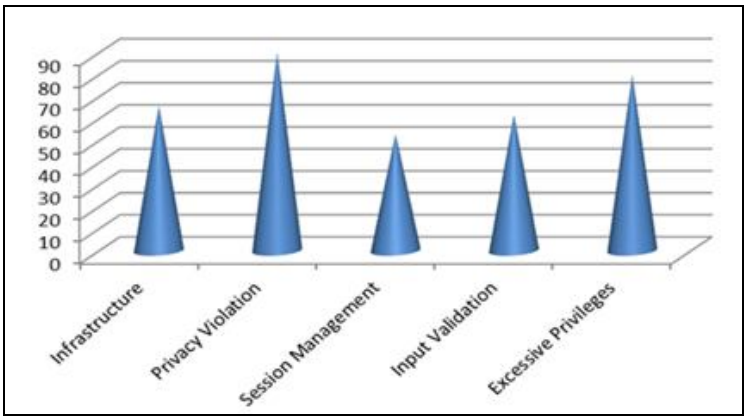


Figure 5: Mobile App Vulnerability Categorization

- **Input Validation:** Many of mobile applications not doing the proper input validation and recommended encryption mechanism. When using those kinds of apps to pass the sensitive data it is building a risky atmosphere.
- **Session Management:** Many of mobile applications are not properly maintain the session management; it is causing the application vulnerability. After the application usage, if the sessions are not properly closing that gives a way to hackers or malware applications to use that particular session for crooked functionalities.

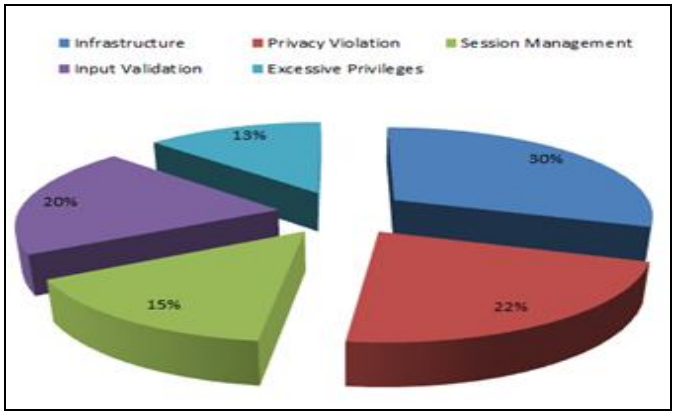


Figure 6: Mobile Apps Vulnerability Population

- **Excessive Privileges:** Excessive privileges stems from developers giving their apps more power than is necessary to complete its function. Mobile app developers should be careful on infrastructure, Privacy Violation, Session Management, Input validation and exclusive privileges. Above pie chart (Fig 6) explain application vulnerability population percentage.

2.4. Trend of Security Feature Usage

Many of security features are available in current available mobile devices. But many of them are not utilizing well or they might not be aware about those features or they might not require those feature. Below analysis disclose the people attitude towards privacy and security feature in mobile devices. This data is collected by Enterprise Risk Survey from four countries based on an online survey conducted in more than 1000 working people from each country.

2.4.1. Private data in Mobile device

Majority people are storing many of their personal or secured information in mobile device, the below table (Table 2) and cone diagram (Fig 7) helps to understand the secured data usage in mobile device from different area. More than 60% of people, at least maintain few of secured data in mobile. This helps to realize the importance and usage of mobile in personal life.

Country	No Private data	Few Data is private	Near half data is private	More than half data is private	Full Data is Private	Conclusion
USA	29%	24%	17%	10%	20%	Nearly **71%** of people having the private data in their mobile.
UK	45%	25%	11%	6%	13%	Nearly **55%** of people having the private data in their mobile.
Germany	31%	38%	14%	11%	6%	Nearly **69%** of people having the private data in their mobile.
India	40%	32%	13%	5%	10%	Nearly **60%** of people having the private data in their mobile.

Table 2: Data percentage Mobile Device

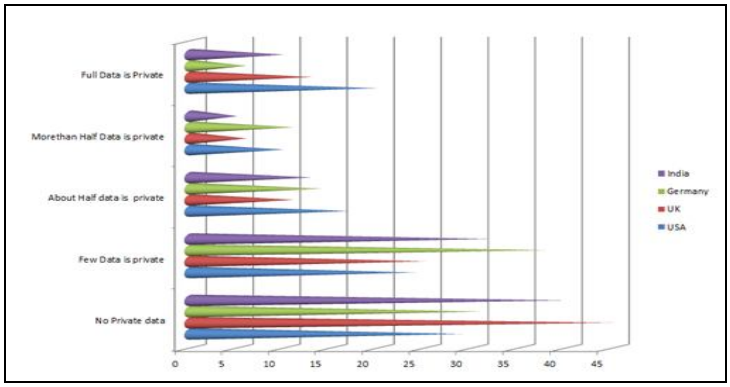


Figure 7: Data in Mobile Device

2.4.2. Usage of Mobile device

Presently the mobile phones takeover many personal computers' activities. Many of them primarily relay their mobile device to work, financial activities and entertainment. This is causing to increase the importance of security awareness. Emails and contacts, together cover major data stored in the phone. Below table (Table 3) and bar diagram (Fig 8) helps to understand the usage percentage of mobile devise for various functionalities in different countries.

USA				**UK**			
Details	**1st Rank %**	**2nd Rank %**	**3rd Rank %**	**Details**	**1st Rank %**	**2nd Rank %**	**3rd Rank %**
Work Email	12	15	15	Work contacts	24	17	13
Personal Contacts	18	14	8	Work email	13	16	16
Work Contacts	14	15	10	Personal contacts	18	14	9
Login Details	16	10	10	Login details	13	10	9
Work Files	9	11	14	Work files	9	10	13
Personal Email	10	10	11	Work applications	4	8	12
Photos	10	7	9	Personal email	5	9	8
Work Applications	5	8	12	Photos	6	7	5
Notes	2	4	5	Notes	3	5	9
Social Media Data	2	4	4	Social Media Data	4	3	4
Music	2	2	3	Music	3	2	3

GERMANY				INDIA			
Details	**1st Rank %**	**2nd Rank %**	**3rd Rank %**	**Details**	**1st Rank %**	**2nd Rank %**	**3rd Rank %**
Work contacts	21	16	13	Personal contacts	17	24	16
Work files	17	16	14	Work email	13	16	18
Work email	12	18	15	Social Media Data	12	17	13
Personal contacts	13	10	9	Work contacts	11	12	9
Work applications	6	9	13	Personal email	9	8	11
Login details	9	9	9	Work files	10	9	10
Personal email	10	8	6	Photos	7	6	9
Photos	4	7	7	Login details	3	4	5
Notes	2	4	8	Notes	4	3	6
Social Media Data	3	3	6	Work applications	2	3	4
Music	3	2	2	Music	2	2	4

Table 3: Usage of Mobile functionalities

Below bar diagram (Fig 8) explain the ranking analysis of various mobile functionalities. Email and contacts emerges bigger importance in all the regions. Login details (user id and password) also get higher importance. This analysis suggesting these three features are required higher protection.

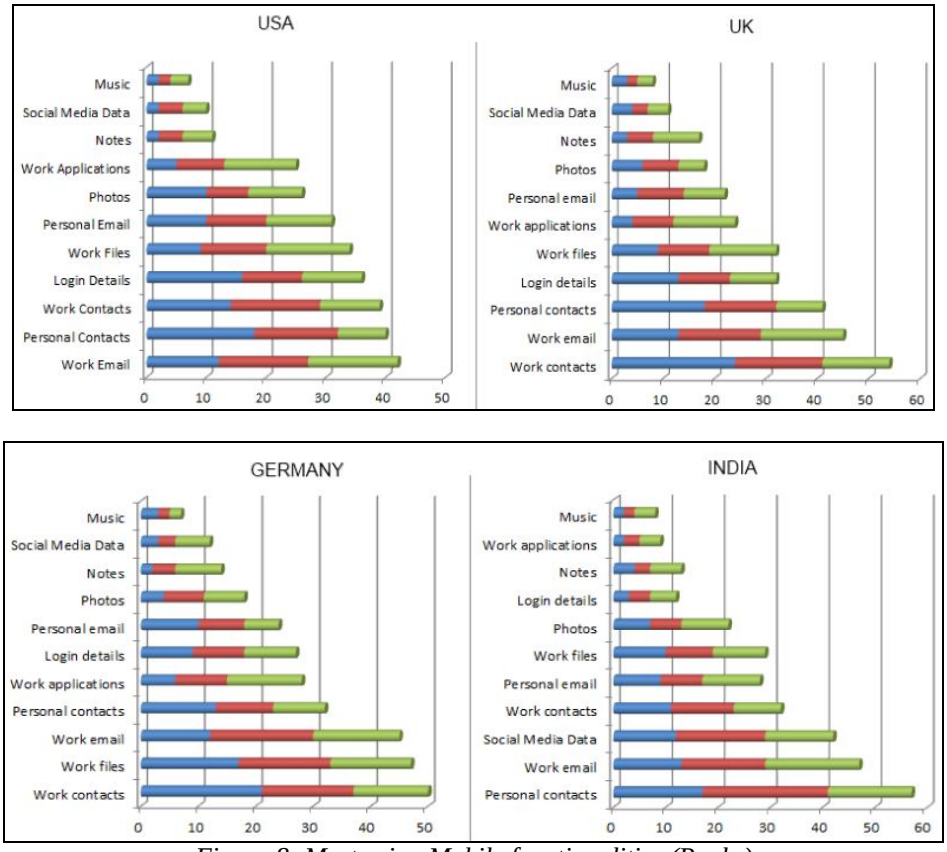
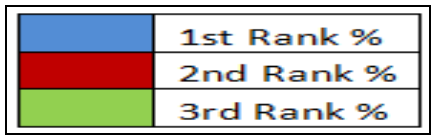


Figure 8: Most using Mobile functionalities (Ranks)



2.4.3. Security Culture in Workplace

Many of organizations are using the mobile device for work purpose. Most of the places have defined the security policies. But few places are not using the policies or some of them are not aware the policies. Below table (Table 4) and doughnut chart (Fig 9) helps to understand the importance and usage of security features.

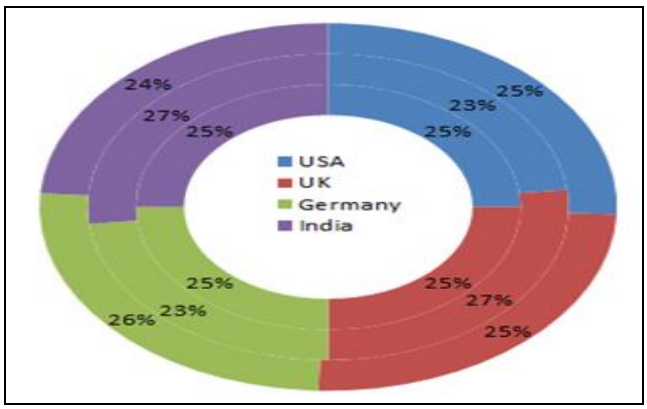


Figure 9: Security culture in work place

#	USA	UK	Germany	India	Comments
Relax	3	3	3	3	Not using any formal policies
Moderate	26	30	26	30	Few policies are available but everyone is not aware and not forcing to use
Strict	70	68	70	65	Policies are defined and using well

Table 4: Security Policy Usage level

2.4.4. Change in Security Habits

Present days, many of them are using mobile devices in their day-to-day activities. But many of them not bring the security features into their usage culture. Below table (Table 5) and area chart (Fig 10) explain the security habits in different regions of people. Around more than 60% of people are not following any security habits.

#	USA	UK	Germany	India
Yes	43%	33%	40%	35%
No	57%	67%	60%	65%

Table 5: Security feature usage in each region

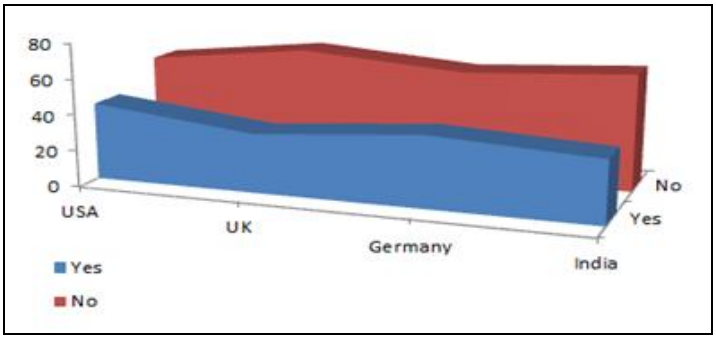


Figure 10: Security Habits

2.5. Current Security Trends

- **Biometric Reader:** This is one of the advanced security measure, it helps to identify the device owner based on the person's physical feature like finger print or eyes. This feature is helping to protect the device from unauthorized device access. Few of physical features are unique in each person and difficult to mimic, this advantage is utilizing in biometric reader.
- **Encryption:** Encryption will help to keep the sensitive data in secured way. Few of latest mobiles are providing encryption feature along with operating system itself. This option will help to provide an additional security on top of PIN or passcode.

It is keeping your personal data in encrypted format in device itself. Many software are available to configure the security feature in user defined way.

- **Avoid Public Wi-Fi Networks for secured transactions:** Keep the mobile Wi-Fi connectivity settings as secured to avoid the automatic connections on public networks. Many of open networks are not using WPA (Wireless Protected Access) or WPA2 password, so it might not be secure. Make sure the secured information only passing through secured Wi-Fi or else your phone's data network (2G/3G/4G).
- **Use Websites for secured transactions:** Many of websites are configured with security certificate and the security indicator (https) is visible to users. But many of mobile apps are not having this security configuration also it is not visible in apps. If you're doing a secured transaction and you are not sure the mobile apps security, it's advisable to use the respective website through your mobile browser instead of mobile app. Federal Trade Commission (FTC) was recognized similar critical security flaw in few of famous mobile apps.
- **Antivirus/spyware Protection:** Antivirus software helps to protect the device from mobile virus (spread from one vulnerable device to another), worms (self-replicating nature, that does not alter files but resides in active memory and duplicates itself), Trojans (malicious or harmful code to loss or theft of data), spyware (gather the information using the device utilities like camera, voice recorder etc without knowledge) and other malwares.
- **Remote Locking/password change:** This feature helps to lock the device or change the password from remote location when the device is stolen or lost.
- **Remote Wipe:** This feature helps to erase the secured data from remote location when the device is stolen or lost. There are options available to copy the required data before the remote wipe.
- **Locate/Track the device:** Software and services are available to track the mobile device. For enabling the same needs to sync the device with the service. GPS services are commonly using to track the device.
- **Device Scream:** This feature helps to setup an alarm via text commands or from your online management account. It's a helpful feature when the device is lost.

3. Conclusion

Usage of latest security features in the mobile devices will be helpful to keep the private data in secured way. To avoid mobile security threats, advisable to keep update the latest security features, also keep follow the latest security trends. If the mobile device is holding any kind of financial information, highly recommend tofollows above mentioned security trends.

4. References

1. 'AdaptiveMobile surveys' https://www.adaptivemobile.com/
2. 'Federal Trade Commission (FTC)' https://www.consumer.ftc.gov/
3. 'Mcafee mobile security Report' https://www.mcafeemobilesecurity.com
4. 'Application Vulnerability Trends Report' https://www.cenzic.com/
5. 'Top Ten Reviews' https://www.mobile-security-software-review.toptenreviews.com/
6. 'Mobile Enterprise Risk Survey Report' https://www.absolute.com/