Research Paper Management

A Study Of Mobile Internet Users In India

Dr.Arjun Waykar Associate Professor, Department of Economics, Vivekanand College, Mantha (Maharashtra)

Mr.Yashwant Waykar Assistant Professor, Department of Management Science Dr.B.A.M.University, Aurangabad.- 431001

ABSTRACT

Mobile broadband is the marketing term for wireless Internet access through a portable modem, mobile phone, USB wireless modem, tablet or other mobile devices. The mobile Web refers to the use of browser-based Internet services from handheld mobile devices, such as smartphones or feature phones, through a mobile or other wireless network. Traditionally, access to the World Wide Web has been via fixed-line services on laptops and desktop computers. Nowadays, you can also use internet on your mobile phones using a Wi-Fi or 3G connection.

Mobile devices face an array of threats that take advantage of numerous vulnerabilities commonly found in such devices. These vulnerabilities can be the result of inadequate technical controls, but they can also result from the poor security practices of consumers. Cyber-crime rate is increasing continuously in India during last 8-10 years as the number of internet users are increasing. Several security measures are suggested for safe & secure usage of mobile internet. Few of the important security measures are continuously passwords must be changed, download apps from trusted websites, install quality antivirus etc.

KEYWORDS –Mobile Internet, security, cyber-crimes, and internet

Mobile Internet' refers to access to the Internet via a cellular telephone service provider. It is wireless accesses that can handoff to another radio tower while it is moving across the service area. It can refer an immobile device that stays connected to one tower, but this is not the meaning of "mobile" here. Wi-Fi and other better methods are commonly available for users not on the move. Cellular base stations are more expensive to provide than a wireless base station that connects directly to an internet service provider, rather than through the telephone system.

A mobile phone, such as a smartphone, that connects to data or voice services without going through the cellular base station is not on mobile Internet. A laptop with a broadband modem and a cellular service provider subscription that is traveling on a bus through the city is on mobile Internet.

A mobile broadband modem "tethers" the smartphone to one or more computers or other end user devices to provide access to the Internet via the protocols that cellular telephone service provider may offer.

Mobile broadband is the marketing term for wireless Internet access through a portable modem, mobile phone, USB wireless modem, tablet or other mobile devices. The first wireless Internet access became available in 1991 as part of the second generation (2G) of mobile phone technology. Higher speeds became available in 2001 and 2006 as part of the third (3G) and fourth (4G) generations. In 2011, 90% of the world's population lived in areas with 2G coverage, while 45% lived in areas with 2G and 3G coverage. Mobile broadband uses the spectrum of 225 MHz to 3700 MHz.

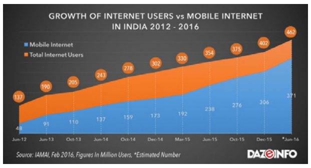


Fig.1. Growth of internet users Vs Mobile internet in India 2012-2016

From Fig.1. , it can be understood that the Mobile internet's popularity and usage in India is increasing drastically as compare to the normal internet users. As mobile internet was only 48 Million in Jun 12 out of 137 Million total internet users in India. The share of mobile internet user was very less as compare to other internet users. The rise of Mobile internet users can be clearly seen in fig.1 in the Blue color segment. Out of 462 Million internet users 371 Million users prefer Mobile internet for performing different activities over the internet. Several surveys predicted the huge rise can be seen in the upcoming years in the Mobile internet usage.

Purpose of Internet Access in Urban India -

80% -	Online Communication
74% -	Social Networking
30% -	Entertainment
13% -	Online Shopping
11% -	Online Ticketing

A survey by IMRB I-Cube 2015, which was performed to identify the purpose of mobile internet access in Urban & rural India. In the earlier part of this paper we have monitored that the mobile internet is increasing with vast pace. we can observe very interesting figures regarding mobile internet usage. Out of total surveyed users it was identified that 80% mobile internet users in urban India use internet for online communication purpose. Mobile internet can be used on the go anywhere in India, people are using for different types of communication as official with email, personal etc. It is also observed that 74% users use mobile internet for social Networking such as Facebook, Twitter, LinkedIn , whatsapp etc. Mobile users tend towards using internet for performing more of social networking & communication over the information downloading related academic or other. It gives slight inclination of users for wasting of time on internet more on social networking than on academic & other related activities.

Mobile internet is definitely a significant move in the right direction as far as the convenience of the customer as well as the banker are concerned but it must be applied with adequate precaution to avoid falling prey to unscrupulous elements poaching the internet.

Application-Based Threats
Downloadable applications can present many types of security issues for mobile devices. "Malicious apps" may look fine on a download site, but they are specifically designed to commit fraud. Even some legitimate software can be exploited for fraudulent purposes. Application-based threats generally fit into one or more of the following categories:

Malware is software that performs malicious actions while installed on your phone. Without your knowledge, malware can make charges to your phone bill, send unsolicited messages to your contact list, or give an attacker control over your device.

Spyware is designed to collect or use private data without your knowledge or approval. This stolen information could be used for identity theft or financial fraud.

Privacy Threats may be caused by applications that are not necessarily malicious, but gather or use sensitive information than is necessary to perform their function.

Vulnerable Applications are apps that contain flaws which can be exploited for malicious purposes. Such vulnerabilities allow an attacker to access sensitive information, perform undesirable actions, stop a service from functioning correctly, or download apps to your device without your knowledge.

Web-based Threats
Because mobile devices are constantly connected to the Internet and frequently used to access web-based services, web-based threats pose persistent issues for mobile devices:

Phishing Scams use email, text messages, Facebook, and Twitter to send you links to websites that are designed to trick you into providing information like passwords or account numbers. Often these messages and sites are very different to distinguish from those of your bank or other legitimate sources.

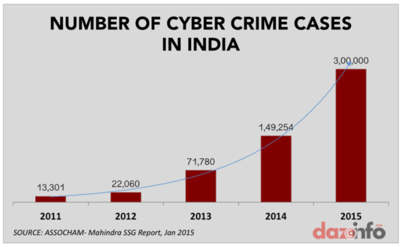
Drive-By Downloads can automatically download an application when you visit a web page. In some cases, you must take action to open the downloaded application, while in other cases the application can start automatically.

Browser exploits take advantage of vulnerabilities in your mobile web browser or software launched by the browser such as a Flash player, PDF reader, or image viewer. Simply by visiting an unsafe web page, you can trigger a browser exploit that can install malware or perform other actions on your device.

Network Threats
Mobile devices typically support cellular networks as well as local wireless networks. Both of these types of networks can host different classes of threats:

Network exploits take advantage of flaws in the mobile operating system or other software that operates on local or cellular networks. Once connected, they can install malware on your phone without your knowledge.

Wi-Fi Sniffing intercepts data as it is traveling through the air between the device and the WiFi access point. Many applications and web pages do not use proper security measures, sending unencrypted data across the network that can be easily read by someone who is grabbing data as it travels.



SOURCE: ASSOCHAM- Mahindra SSG Report, Jan 2015

Fig.2. Cyber Crimes in India
From Fig.2, it can be identified that the cyber-crimes cases are increasing continuously over the years. As per the survey it can be interpreted that there has been tremendous growth in cyber-crime case from 2014 (149254) to 2015(3, 00,000). It is a major cause of concern for the internet users. As safety is the crucial issue in usage of internet. There are several security loop holes were identified in the habits & overall usage structure of Indian internet users.

Classifications Of Cyber Crimes: Cyber Crimes which are growing day by day, it is very difficult to find out what is actually a cyber-crime and what is the conventional crime so to come out of this confusion, cyber-crimes can be classified under different categories which are as follows:

1. Cyber Crimes against Persons:
There are certain offences which affect the personality of individuals can be defined as:

- Harassment via E-Mails:
- Cyber-Stalking:
- Dissemination of Obscene Material:
- Defamation:
- Hacking:
- Cracking:
- E-Mail Spoofing:
- SMS Spoofing:
- Carding:
- Cheating & Fraud:
- Child Pornography:
- Assault by Threat:

2. Crimes Against Persons Property:
As there is rapid growth in the international trade where businesses and consumers are increasingly using computers to create, transmit and to store information in the electronic form instead of traditional paper documents. There are certain offences which affects persons property which are as follows:

- Intellectual Property Crimes:
- Cyber Squatting:
- Cyber Vandalism:
- Hacking Computer System:
- Transmitting Virus:
- Cyber Trespass:
- Internet Time Thefts:

3. Cybercrimes against Government:
There are certain offences done by group of persons intending to threaten the international governments by using internet facilities. It includes:

Cyber Terrorism:
- Cyber Warfare:
- Distribution of pirated software:
- Possession of Unauthorized Information:

4. Cybercrimes Against Society at large:
An unlawful act done with the intention of causing harm to the cyberspace will affect large number of persons. These offences includes:

- Child Pornography:
- Cyber Trafficking:
- Online Gambling:
- Financial Crimes:

Forgery:

- Therefore following safety tips are proposed by cyber cell Mumbai for usage of mobile banking in India.
- Don'ts
- Please do not click photographs without permission by your mobile phones. You are invading the privacy.
- Do not send obscene/pornographic text, images. SMS.
- Do not send obscene/pornographic text, MMS
- Do not receive from or reply to sms/mms of strangers.
- Do not transmit obscene/ pornographic material, as it is an offence under Information Technology act –2000. punishment is 5 yrs imprisonment and 1lac rupees fine.
- Do not keep your Blue tooth open to all; you may receive obscene/pornographic text, images and viruses.
- Do not give your mobile numbers while chatting on INTERNET to avoid "STALKING".
- DO not handover your mobile phone to unauthorized service center, to avoid CLONING.

Do's

- Note down your IMEI number.
- Security pin code should be used to avoid misuse of your mobile phones.
- Mms/sms received should be checked before opening the message.
- Delete obscene/pornographic text, images. SMS/MMS. From your mobile phones.
- Anti-virus software should be loaded in the mobile phone.
- Mobile phone keypad should be locked after every use.
- Use your mobile phone when necessary

Conclusion –

Mobile internet usage is found to be at the higher side in last few years and the figures of mobile internet users shall rise continuously in coming years as well. All smartphones, as computers, are preferred targets of attacks. These attacks exploit weaknesses related to smartphones that can come from means of communication like SMS, MMS, Wi-Fi, Bluetooth and GSM , the de facto global standard for mobile communications. There are also attacks that exploit software vulnerabilities from both the web browser and operating system. Finally, there are forms of malicious software that rely on the weak knowledge of average users. Several security measures are suggested for safe & secure usage of mobile internet. Few of the important security measures are continuously passwords must be changed, download apps from trusted websites, install quality antivirus etc.

References –

1. http://www.legalindia.com/cyber-crimes-and-the-law/
2. http://cybercellmumbai.gov.in/html/news/do-and-dont-for-mobile.html