Qs

Must Ask following Qs if someone force you to download and install some application:-

- Do I need this app when already known and worldwide used similar apps are available?
- What special feature this app has which is not in other widely used apps?
- Why someone who you know or do not know is asking to shift / install another app?
- How many downloads are there of such an app and who has developed it?
- What all permissions is the app asking and does it really commensurate with what it is offering like:-
  - ✓ Why it need access to files?
  - ✓ Why it needs access to location service?
  - ✓ Why it needs access to microphone?
  - ✓ Why it needs to backup / read SMS?
  - ✓ Why it is asking for accessibility options?

Download Applications Only From Reputable Sources

Best Practices

1 Be selective in adding friends on Facebook. Make sure they are trustable and you know them personally before adding them

2 Register a complaint if you think you are becoming a victim of cyberbullying or harassment

3 Install and maintain firewall software and be aware of mobile security

4 Never post photos of yours Spouse / Parents / Siblings

5 Keep your personal information private: Your Full Name, Home Address, Phone Numbers, Birthday etc.

6 Do not reveal your location details on Social Networking Platforms

7 Do not be part of unknown / unverified SMN groups / discussion forums

8 Never click on any link until you are not sure about its source

9 Always use strong passwords and never share it with others.

10 Never connect your mobile or laptop to public / free / unsecured WIFI networks available at restaurants/ transports / airports etc.

Are You The Target?

Protect Yourself & Your Family

Mobile Phone Hacking Threats

1 **Web Based**

Compromise of personal / private data by visiting malicious websites

2 **App Based**

Leakage of personal / private data to hackers through installation of malicious / crafted Applications

3 **Network Based**

Loss of personal / private data through network based attacks including by connecting to public / free WIFI

4 **Physical**

Installation of malicious code by hackers / vendors through physical access to phones / computers

Security Risks and Threats - Internet / Social Media

1 Identity Theft

Use of another person's personal information to commit fraud or other crimes

2 Cyberbullying

It is a form of harassment using electronic means, typically by sending messages of an intimidating or threatening nature. One may face cyberbullying due to careless use of internet / social media

3 Injection of malicious codes into a website

Malicious codes have been injected into few websites like pornography etc. Visiting such sites may hack your devices

4 Impersonation

Attacker posses as a legitimate individual of an institution to lure a person into providing his personal information including banking details

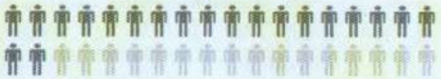
5 Malwares

Software intentionally designed to gain unauthorized access to computers / mobile phones. Such software are normally hyperlinked to web pages. Careless clicks may lead to their installation and loss of personal data

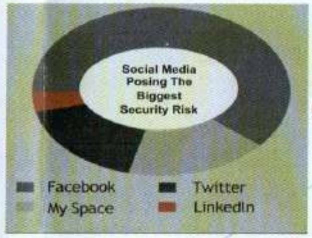
6 Stealing data through Adware

Adware are advertising software that generates revenue for its developer. Individuals having bad intentions can use such software to steal your information

Above 50% users don't bother about privacy settings



Rise in Social Media usage in last few years



Over 90% of the users affected through Spam

What You Compromise From Hacked Mobile Phone?

1 Your complete contact list

2 Your personal data including photographs, videos and audios

3 Yours emails, passwords and security patterns

4 Your SMS, messages / chats on different SMNs

5 Your browsing behavior: web history

6 Your banking / financial details

7 Access to your camera and microphone