

Crimes associated with the Cellphones



Omveer Singh, GCFA
Additional Director / Scientist 'E'

Cyber Forensics Lab
Indian Computer Emergency Response Team (CERT-In)
Department of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India
New Delhi

Cellphone v/s Computers

- Most of the cyber crimes being carried out using computers can easily be carried out using a cellphone or smartphone
- Advanced cellphones have the facility of e-mails & internet
- Smartphones are having most of the features of a small computer
- Portability and easy connectivity of cellphones makes it a versatile tool in the hands of criminals

Cellphones and Crimes

- 3 ways to link a cellphone with the crimes:
 - It can be used as a **communication tool** in the process of committing a crime
 - It can be used as a **data storage device** - digital evidence associated with a crime
 - It can be used as a **device** to carry out a crime
 - SMSing, Vishing, Phishing
 - Harassment

Some Common Cyber Crimes

- Cyber bullying – calls, SMS, chats
- Cyber stalking
- Cyber harassment
- Cyber frauds
- Identity theft
- Net extortion
- Charity frauds
- Credit card frauds
- Nigerian / 419 frauds

Cellphone Spams

- Unwanted SMS, MMS
- Unwanted marketing calls
 - Credit cards
 - Insurance
 - Loan offers
 - Investments
 - Charity
 - Subscription for services
 - Real Estate

Cellphone Stalking

Repeated use of cellphones to a targetted person in –

- Making threatening SMS / calls
- Sending obscene SMS / MMS / images
- Making abusive / excessive phone calls
- Harassment over SMS / calls

Charity Frauds

- Preys on the kindness of the society
- Take advantage of sympathies for the victims of national tragedies & natural disasters
 - floods, droughts, earthquakes, sunami, cyclones, etc.
- Seek donation for the charities for the victims through SMS, e-mails & internet

Mobile Phones: Traditional Crimes

- Mobile devices (handset) theft
- Phone calls between accomplices
- Phone calls to harass
- Phone Cloning
 - subscribers' information, stolen from a mobile phone service provider, was used to create cloned phones in Korea in late 2004

Mobile Phones: Cyber Crimes

- Data stored in mobile phones
 - Call logs, contacts, SMS, images, etc.
- SMSing (SMS + Phishing)
- SMS - containing a link to a site that downloads a Trojan horse, is circulated via cellphones
- Cloning of SIM Cards

Theft of mobile phones

- Financial loss
- Free calls till disconnection
- Money from resale of mobile phones
- SMS to contacts in phonebook -
 - in distress abroad;
 - kindly transfer money in my friends bank account

Rechipping of Mobile phones

- Existing ESN (CDMA) / IMEI (GSM) No. is replaced by a new one on the stolen handset to change its identity; almost impossible to trace
- Using a combination of keys / buttons (ESN) or by connecting to a computer and using relevant software, chip is reprogrammed
- Easy resale of stolen cellphones
- Can be used by criminals to make anonymous & unidentifiable free calls

Cloning of a mobile phone

- At present almost impossible
- Programmed to impersonate a mobile phone owned by a legitimate subscriber
- It's ESN No. and Mobile Phone No. is installed in the cloned mobile phone (CDMA) or SIM Card is cloned
- Fraudulent calls, made on the cloned mobile phone, are billed to the legitimate subscriber

Subscription frauds

- User subscribe a mobile phone with false / fake identity documents
- May use and pay the bills under complete anonymity
 - Big headache for security agencies during investigation of crimes
- May make free calls till disconnection due to non payment

Cellphone Camera

- Taking other's photos without consent
- Making obscene MMS
- Capturing photos of other's payment cards – credit / debit card (for fraudulent use later, on-line financial frauds, cloning)

References

- Wikipedia – The Free Encyclopedia
<http://en.wikipedia.org/>
- “Forensic Analysis of Mobile Phones” by Paul McCarthy
<http://www.mobileforensicsworld.org>
- Collecting Electronic Evidence After a System Compromise” by Matthew Braid, SANS Security Essentials.
- “Computer Forensics – An Overview” by Dorothy A. Lunn, SANS Institute; Course Contents : SANS SEC508
- “Computer Forensics and Investigations” by Bil Nelson, et al