An Ethical Guide to Hacking Mobile Phones – By Ankit Fadia

1. Security Threats

Bluetooth Hacking

- Introduction
- Working
- Case Studies
- Types of Bluetooth Threats
- The Bluejack Attack
- OBEX Push
- Bluespamming
- Bluetoothing
- Modifying a Remote Mobile Phone's Address Book
- Fadia's Hot Tools for Bluejacking
- Countermeasures
- The BlueSnarf Attack
- OBEX Pull
- Fadia's Hot Tools for Bluesnarfing
- Countermeasures
- The Blue Backdoor Attack
- The BlueBug Attack
- Fadia's Hot Tools for Bluebug Attacks
- Short Pairing Code Attacks
- Default Pairing Code Attacks
- Random Challenge Response Generators
- Man-In-Middle Attacks
- Privacy Concerns
- Brute Force Attacks
- DOS Attacks
- Cracking Pair Codes
- Blueprinting
- Fadia's Hot Picks for popular Blueprinting Tools
- Bluetooth Wardriving
- Fadia's Hot Picks for popular Bluetooth Hacking Tools
- Vulnerable Mobile Phone Handsets
- Countermeasures
- Live Attack Logged Data

Mobile DOS Attacks

- Introduction
- Working
- Different Types of DOS Attacks
- Case Studies
- Bluesmacking (Ping of Death)
- Fadia's Hot Picks for popular Bluesmacking Tools
- Ping Flooding
- Jamming
- Malformed OBEX Message Attack
- Failed Authentication Attack
- Extreme Bluejacking
- Malformed SMS text Message Attack
- Local Malformd SMS text Message Attack
- Malformed MIDI File Attack
- Malformed Format String Vulnerability
- Vulnerable Mobile Phone Handsets
- Countermeasures
- Live Attack Logged Data

2. Viruses and Worms

- Introduction
- Working
- Case Studies
- Types of Malicious Files
- The Cabir Worm
- The Mabir Worm
- The Lasco Worm
- The Commwarrior MMS virus
- The Skulls Trojan
- The MOS Trojan
- The Fontal Trojan
- The Hobbes Trojan
- The Drever Trojan
- The Locknut.A Trojan
- The WinCE Duts Virus
- The Onehop Trojan
- The MGDropper Trojan
- The Appdisabler Trojan
- The Dampig File Dropper
- The Doomboot Trojan

- Car Viruses
- Mobile Phone Platforms
- Fadia's Hot Picks for popular Mobile Antivirus Tools
- Countermeasures
- Live Attack Logged Data

3. Security Tips and Tricks

Nokia

- Secret Codes
- Restore Factory Default Settings
- Unlocking the Phone
- Default Passwords
- Activating Half Rate
- Unlocking the Service Provider Lock
- Telephone Programming Tips
- Bypassing the PIN prompt
- Increasing the Battery Life
- Use your mobile phone to snoop on other people
- Crashing a Nokia Phone
- Cheat Codes
- Quick SMS Typing
- Quick Reboot
- Making FREE Phone Calls
- Sending FREE Text Messages
- Spoofing Your Phone Number

Motorola

- Secret Codes
- Restore Factory Default Settings
- Unlocking the Phone
- Default Passwords
- Telephone Programming Tips
- Increasing the Battery Life
- Use your mobile phone to snoop on other people
- Crashing a Motorola Phone
- Finding the Distance from Radio Base Station
- Quick Reboot
- Making FREE Phone Calls
- Sending FREE Text messages
- Spoofing Your Phone Number

Samsung

- Secret Codes
- Restore Factory Default Settings
- Unlocking the Phone
- Default Passwords
- Telephone Programming Tips
- Increasing the Battery Life
- Use your mobile phone to snoop on other people
- Crashing a Samsung Phone
- Finding the Distance from Radio Base Station
- Quick Reboot
- Making FREE Phone Calls
- Sending FREE Text messages
- Spoofing Your Phone Number

Sony-Ericsson

- Secret Codes
- Restore Factory Default Settings
- Unlocking the Phone
- Default Passwords
- Telephone Programming Tips
- Increasing the Battery Life
- Use your mobile phone to snoop on other people
- Crashing a Sony-Ericsson Phone
- Finding the Distance from Radio Base Station
- Quick Reboot
- Making FREE Phone Calls
- Sending FREE Text messages
- Spoofing Your Phone Number

Cingular/AT&T Wireless Security Tricks

Sprint PCS Security Tricks

DoCoMo Japan Security Tricks

Blackberry Mobile Phone Tricks

Vodafone

4. Appendix

- Security Test: A Comparison of various Handsets
- GSM VS CDMA
- iMode
- More Resources on the Internet