What is Cyber Crime?
What is Cyber Security?
Why Cyber Security?
Beware! Pre-Installed Android Malware Found On 36 High-end Smartphones

📅 Friday, March 10, 2017  🌐 Wang Wei

Loki Trojan
<table>
<thead>
<tr>
<th>Galaxy Note 2</th>
<th>Galaxy Note 3</th>
<th>Galaxy Note Edge</th>
</tr>
</thead>
<tbody>
<tr>
<td>LG G4</td>
<td>Galaxy Note 3</td>
<td>Galaxy Tab S2</td>
</tr>
<tr>
<td>Galaxy S7</td>
<td>Galaxy Note Edge</td>
<td>Galaxy Tab 2</td>
</tr>
<tr>
<td>Galaxy S4</td>
<td>Oppo N3</td>
<td>Vivo X6 plus</td>
</tr>
<tr>
<td>Galaxy Note 4</td>
<td>Nexus 5</td>
<td>Nexus 5X</td>
</tr>
<tr>
<td>Galaxy Note 5</td>
<td>Nexus 5X</td>
<td>Asus Zenfone 2</td>
</tr>
<tr>
<td>Xiaomi Mi 4i</td>
<td>Lenovo S90</td>
<td>Oppo R7 plus</td>
</tr>
<tr>
<td>Galaxy A5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ZTE x500</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Xiaomi Redmi</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lenovo A850</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
WikiLeaks Exposed CIA's Hacking Tools And Capabilities Details

📅 Tuesday, March 07, 2017   ⌨️ Swati Khandelwal
Ransomware Hijacks Hotel Smart Keys to Lock Guests Out of their Rooms

Saturday, January 28, 2017  Mohit Kumar
This Ransomware Malware Could Poison Your Water Supply If Not Paid

📅 Thursday, February 16, 2017   📰 Swati Khandelwal
Yahoo Hacked Once Again! Quietly Warns Affected Users About New Attack

📅 Wednesday, February 15, 2017   ⚡ Mohit Kumar
Smart TV Maker Fined $2.2 Million For Spying on Its 11 Million Users

Tuesday, February 07, 2017  Swati Khandelwal
Police Arrest 5 Cyber Thieves Who Stole 3.2 Million From ATMs Using Malware

Friday, January 27, 2017   Mohit Kumar
Student Faces 10 Years In Prison For Creating And Selling Limitless Keylogger

📅 Saturday, January 14, 2017   ♂️ Swati Khandelwal
Los Angeles College Pays Hackers $28,000 Ransom To Get Its Files Back

19 Lakh rupees in Indian currency
Indian revenue is 3.46% affected by different Cyber attacks

Ref.: http://blog.kaspersky.com/Cyber-under-attack/
Cyber Attack Statistics

10,731 victims of virus/malware/spyware

Who’s least likely to behave securely online?

- 37% Women
- 29% Men
- 41% (average) of those aged 18-44

What puts victims at risk online?

- Occasionally download unknown files and web links on their:
  - 19% mobile devices
  - 23% computers

- Occasionally don’t download the latest software updates straight away on their:
  - 56% mobile devices
  - 40% computers

- Occasionally don’t install security software
  - 37%

- Occasionally turn off security software
  - 13%

Cyber Attack Statistics

What happens when victims get infected?

- 42% suffered an online security issue
- 9% lost files such as photos and important work
- 6% had credit card details stolen and goods bought in their name
- 5% had problems with online shopping
- 3% had their personal information accessed without permission
- 1% suffered damage to their reputation

Source:
Forget fingerprint authentication, retinal scanning or advanced facial recognition, etc..

“ It’s time for the Cardiac Authentication ”
Hacking Groups
The top 10 most notorious hacking groups are:

- Lizard Squad
- Anonymous (Legion)
- LulzSec
- Syrian Electronic Army

Src: https://hacked.com/hacking/
- Chaos Computer Club (CCC)
- Iran’s Tarh Andishan
- The Level Seven Crew
- GlobalHell
- TeaMpoisoN
- Network Crack Program Hacker Group

Src: https://hacked.com/hacking/
Cyber War

THE DIGITAL ERA
Categories of Cyber Crime
Computer As Target

- Use a computer to attack victim computer
- Attack on CIA of information or system
Computer As Weapon

- Fraud
- Gambling
- Pornography
- Piracy
- Harassment
Crimes in which computer systems are used as tools

- Cyber bullying/Stalking
- Data theft
- Pornography
- Theft of trade secrets and intellectual property
- Espionage on protected systems
- Data modification
- Financial fraud
- Identity theft and its misuse
- Financial fraud

Key Logger
Email Security

When did you create this Google Account?

Month ▼ Year ▼

Next

Try a different question
Welcome to 10 Minute Mail! This is your temporary e-mail address:

a2561183@mvrht.net

YOU HAVE 0 MESSAGE(S).
Def:

“Operating System is an interface between user and Hardware”
A kernel is the central part of an operating system. It manages the tasks of the computer and the hardware - most notably:

- Memory
- CPU time
Microsoft Windows (or simply Windows) is a meta family of graphical operating systems developed, marketed, and sold by Microsoft.
Types of OS

Linux OS

Server operating System
Flavours Of Red Hat

Client Operating System
Fedora, Ubuntu etc.
Types of OS

- OS X 10.11 (El Capitan)
- OS X 10.10 (Yosemite)
- OS X 10.9 (Mavericks)
- OS X 10.8 (Mountain Lion)
- Mac OS X 10.7 (Lion)
- Mac OS X 10.6 (Snow Leopard)
- Mac OS X 10.5 (Leopard)
- Mac OS X 10.4 (Tiger)
- Mac OS X 10.3 (Panther)
- Mac OS X 10.2 (Jaguar)
- Mac OS X Server 1.0 (Hera)
- Rhapsody Developer Release (Gazelle/Titan1U)
- Public Beta (Kodiak)
An operating system performs basic tasks such as,

- Controlling and allocating memory
- Prioritizing system requests
- Controlling input and output devices
- Facilitating networking and managing file systems
The main functions of operating systems are:

- Program creation
- Program execution
- Input / Output operations
- Error detection
- Resource allocation
- Accounting
- Protection
Important Cyber Safety Actions

1. Install OS/Software Updates
2. Run Anti-virus Software
3. Prevent Identity Theft
4. Turn on Personal Firewalls
5. Avoid Spyware/Adware
6. Protect Passwords
7. Back up Important Files
BEST PRACTICES - DO'S & DONT'S on
SECURED ELECTRONIC TRANSACTION & E-Commerce
How to Secure your ATM banking?

- **Memorize your PIN.** Do not write it down anywhere and certainly never on the card itself.

- Do not share your PIN or card with anyone including Bank employees not even your friends or family. Change your PIN regularly.

- Stand close to the ATM machine and use your body and hand to shield the keypad as you enter the PIN.

- Do not take help from strangers for using the ATM card or handling your cash.

- Do not conduct any transaction if you find any unusual device connected to your ATM machine.

- Press the 'Cancel' key and wait for the welcome screen before moving away from the ATM. Remember to take your card and transaction slip with you.
How to Secure your Mobile Banking?

• While talking to the Phone Banking officer, never disclose the following
  • 4 digit ATM/IVR PIN
  • OTP
  • Net Banking password
  • CVV (Card Verification Value)

• Ensure that no one see you entering you PIN (personal identification number).

• Avoid giving verification details to the Phone Banking officer while in public places.

• The Phone Banking channel is meant to be used by the account holder only. Do not transfer the line or hand over the phone to any other person after you complete self-authentication.
Secure Mobile Banking Do’s & Dont’s

Do's:

• **Password protect** the mobile phone. It is recommended to set the maximum number of incorrect password submissions no more than three.

• Choose a **strong password** to keep your account and data safe.

• **Review your account statements** frequently to check for any unauthorized transactions.

• Change your **Profile Password** regularly.

• Report a lost or stolen phone immediately to your service provider and law enforcement authorities.
Dont's

• Never give your PIN or confidential information over the phone or internet. Never share these details with anyone.

• Don’t click on links embedded in emails/social networking sites claiming to be from the bank or representing the bank.

• Don’t store sensitive information such as credit card details, mobile banking password and user ID in a separate folder on your phone.

• Don’t forget to inform the bank of changes in your mobile number to ensure that SMS notifications are not sent to someone else.
Tips to Secure your Debit/credit card Password

When you receive your Card PIN, change it immediately.
Also never use the following for your PIN:

• Your kids’ or loved ones’ date of birth

• 1234 or 4321, 9876 or 6789 – easy to guess

• Digits of your mobile number

• Your date of birth or anniversary

• First or last 4 digits of your card number
How to Secure your Computer?

• Use licensed software. Software purchased from untrustworthy sources could have virus or trojans that could corrupt your files and reveal your confidential data.

• Protect your computer accounts with strong passwords.

• Update your computer with latest security patches for your operating system, browser and email client.

• Use anti-virus, anti-spyware and personal firewalls.

• Observe click discipline while browsing through different websites. You may land up clicking on to malicious link that could download malicious code / software or virus on to your computer.

• Downloading software from non-trustworthy sites including torrent sites may lead to infecting your computer with virus.
Tips to Secure your Online Shopping

• Always shop or make payments through trusted/reputed websites.

• Do not click on links in emails. Always type the URL in the address bar of the browser.

• Before entering your private details, always check the URL of the site you are on!

• If you are a frequent online shopper, signup for Verify by Visa and Master Card secure code program.

• Check your account statements regularly and bring any fraudulent transaction to the notice of the bank.

• Check for PAD LOCK symbol on the webpage before starting to transact.

• Do not click on links in emails or on referral websites to visit the online shopping site. Always type the URL in the address bar.
• Do not enter your confidential account information such as Credit Card Numbers, Expiry Date, CVV values, etc. on any pop-up windows.

• Use One Time Password (OTP) received on the mobile phone instead of static Visa and Master Card secure code password as OTP are more secure.
Thank you