



LOGOUT

WORLD'S BIGGEST CYBER AWARENESS CAMPAIGN

Who Am I ?

- Apurv Singh Gautam | Sc0rpion
- Network Penetration Tester, Security Enthusiast, Hacker, CTF Player
- Speaker at Null the Open Security Community, Pune
- From the Past 4 years in this field

Why Am I Doing This ?

- Have too much of free time 😊
- Want others to be aware
- Can't help everyone on Quora

CYBER SECURITY FUNDAMENTALS

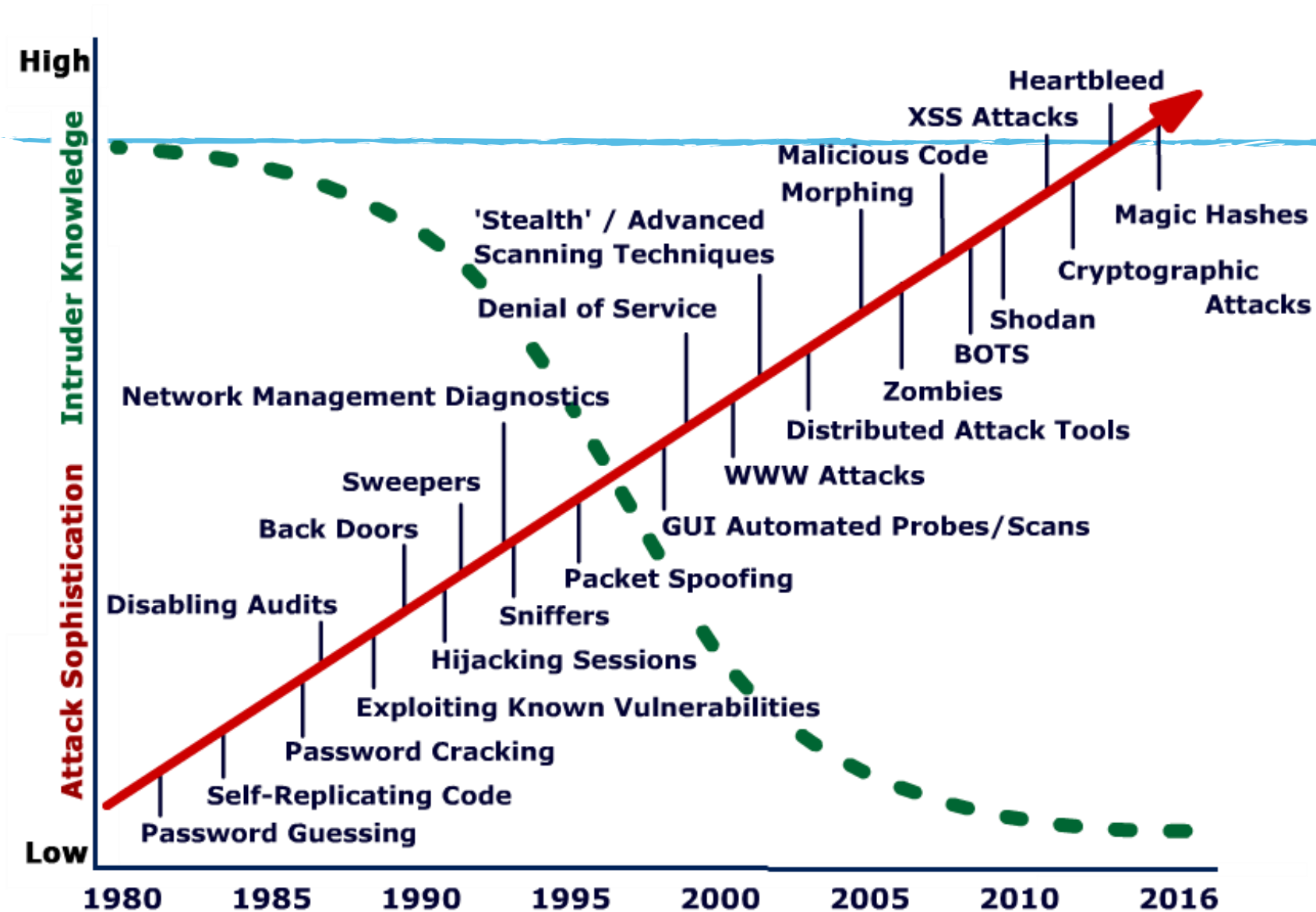


WHAT TO EXPECT??



NEED OF SECURITY

- Increasing awareness of technology but not Security
- Continuous Development & Competition in IT
- Increasing number of Cyber Criminals
- Increasing use of Network elements & applications
- Decreasing level of skill set



NEED OF SECURITY

- Any Security breach in the website of any person increases the risk of the public image
- Any Security breach in the website of any company increases the risk of company reputation
- Any Security breach in the government website may increase the risk on project management and government operations
- Any Security breach in the Military sector may jeopardise the safety of any country

What is HACKING??

- Hacking is an art of exploring various security breaches
- What people believe: It's an anti-social activity
 - : All the hackers are bad people
- The terms Hacker and Hacking are being misinterpreted and misunderstood with negative sidelines

COMMUNITIES OF HACKERS

- Hackers
- Crackers
- Phreaks
- Script Kiddies

TYPES OF HACKERS

- **White Hat Hacker** - They use their knowledge and skill set for good constructive intents. They find out new security loopholes and their solutions
- **Black Hat Hacker** - They use their knowledge and skill set for illegal activities and destructive intents
- **Grey Hat Hacker** – They use their knowledge and skill set for legal and illegal purpose. They are white hats in public but internally they do some black hat work

HACKING STRATEGY

- Reconnaissance (Information Gathering)
- Scanning
- Gaining Access
- Maintaining Access
- Covering Tracks

Cyber Crime is no more FUN...!!!

- Cyber crime controlled by IT ACT 2008 and respective IPC (constantly evolving)
- Complete control of Govt agencies over information stored, processed and transmitted over internet
- Upgradation of Investigating agencies with latest technology
- Service providers like ISPs, email service providers, etc are liable to share information with Govt agencies
- Upgradation of Forensic labs
- Stringent punishment for cyber crimes

Common Scenarios - Cyber Pornography

- Cyber pornography covers pornographic websites, pornographic magazines produced using computers and the Internet.
- Whoever publishes or transmits or causes to be published in the electronic form, any material which is obscene in nature falls under cyber pornography
- **Section 67:** Punishment for publishing or transmitting obscene material in electronic form
- **Punishment** – Imprisonment from 2 – 10 years with fine upto 10 lakhs

Common Scenarios – Identity Theft

- Identity theft is a term used to refer to fraud that involves stealing money or getting other benefits by pretending to be someone else.
- **Section 66C Punishment for identity theft.**

Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

- **Section 66D Punishment for cheating by personation by using computer resource**

Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

INTRODUCTION TO SOCIAL ENGINEERING

"Cause there's no PATCH for HUMAN STUPIDITY"

What is SOCIAL ENGINEERING??

In context of Information Security, it is the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

HACKER?

TECHNIQUE

- Human Interaction
- Respectable & Known Person or Entity
- Assembling all gathered information together

TYPES OF SOCIAL ENGINEERING

- Quid Pro Quo – Something for something
- Phishing
- Baiting
- Pretexting
- Diversion Theft

Phishing Email



Dear Gmail User,

As part of our security measures, we regularly update all accounts on our database system. We are unable to update your email account and therefore we will be closing your email accounts to enable the web upgrade.

You have been sent this invitation because our records indicate you are currently a user whose account has not been activated. We are therefore you sending this email so you can inform us whether you still want to use this account. If you are still interested please confirm your account by updating your details immediately because out system requires an account verification for the update.

To prevent an interruption with your Gmail services, please take a few moments to update your account by filling out the verification and update form immediately.

[Click here to verify your account](#)

Warning! Any account owner that refuses to update their account after receiving this email will lose their account permanently.

We appreciate your cooperation in this matter.

Sincerely
Gmail Member Services Team

From: PayPal Billing Department <Billing@PayPal.com>
Subject: Credit/Debit card update
Date: May 4, 2006 08:16:08 PDT
To: [REDACTED]
Reply-To: Billing@PayPal.com



Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension. This notification expires on 48.

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

Please follow the link below and login to your account and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

Sincerely,
Paypal customer department

<http://66.160.154.156/catalog/paypal/>

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, [log in](#) to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences [here](#).

LOGOUT

WEAKEST LINK??

No matter how strong your:

- Firewalls
 - IDS & IPS
 - Cryptography
 - Anti-Virus Software
-
- You are the weakest link in computer security. People are more vulnerable than computers.
 - "The weakest link in the security chain is the human element: - Kevin Mitnick

WAYS TO PREVENT SOCIAL ENGINEERING

- User Awareness
- Policies
- Third party Test
- Be Smart

Tips for avoiding a Social Engineering Attack

✓ **LIMIT PUBLIC INFORMATION:**

Limit the amount of personal information that you share online.

✓ **BE SKEPTICAL:**

Always question requests for sensitive information.

✓ **TRUST BUT VERIFY:**

Don't share information with people you don't know unless you can verify their identity.

✓ **CALL THEM BACK:**

Through the main switchboard if possible.

✓ **NO PASSWORDS OVER THE PHONE:**

Never share your password with anyone over the phone.





Students prone to Cyber Crime

REASONS:

- Prank
- Jealousy
- Revenge
- Ignorance
- Ex-relationships
- Curiosity
- Blackmailing
- Pornography

**WATCH THIS HACKER
BREAK INTO
MY CELL PHONE ACCOUNT
IN 2 MINUTES**

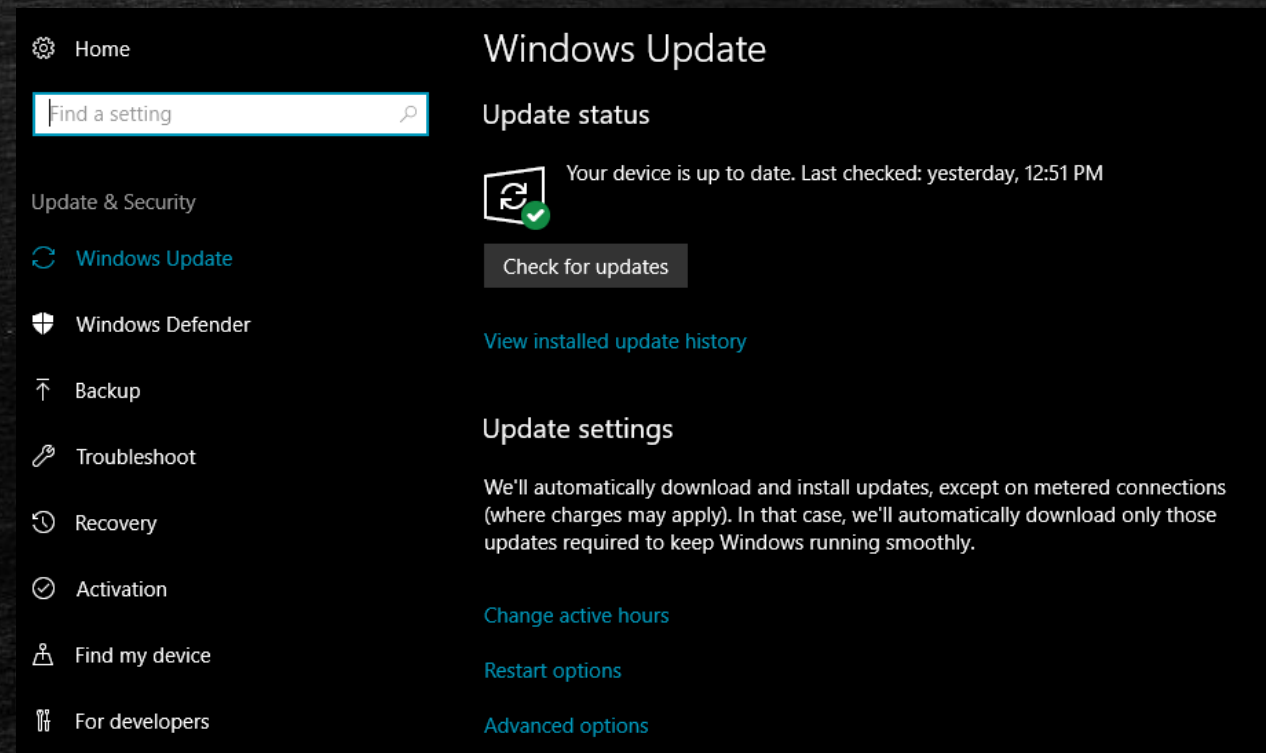
RANSOMWARE



CYBER SECURITY AWARENESS TIPS

Safe Computing Tips

- Keep your Computer Updated



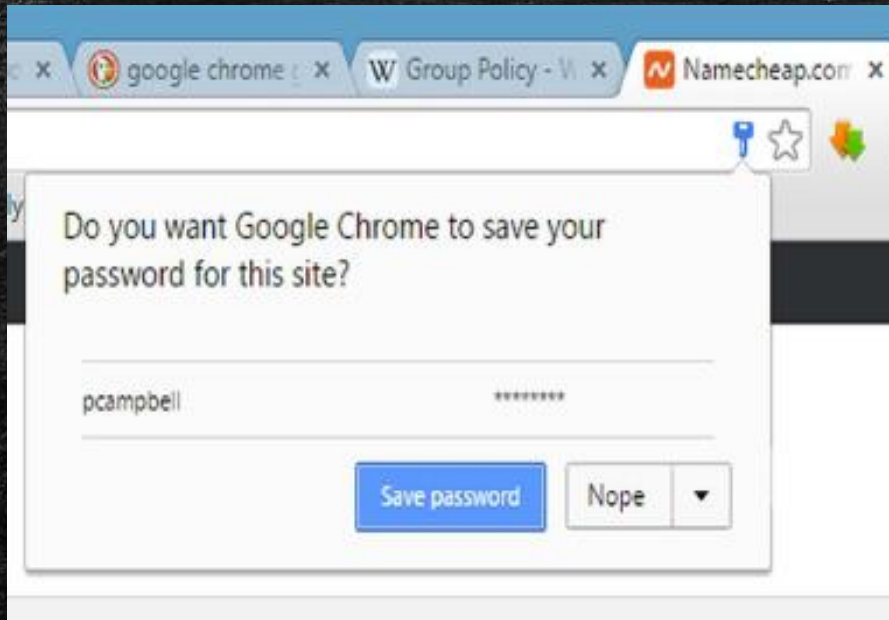
- Keep all the software up to date
- Do not use open Wi-Fi
- Lock the system when not in use
- Download Files Legally (Don't use Torrents :P)
- Backup on regular basis
- Use good Anti-Virus
- Use good Proxy/VPN



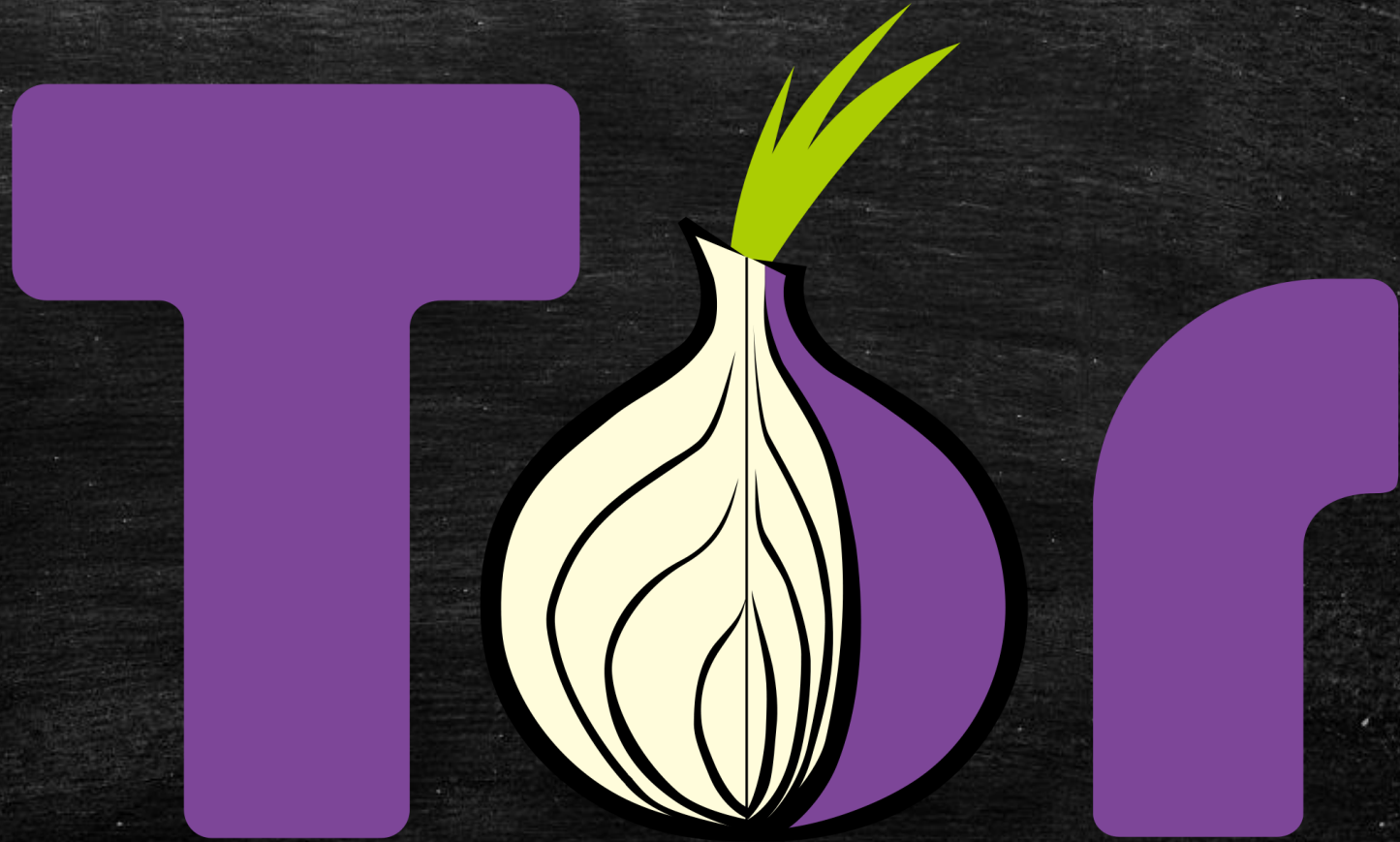
- Cover Mic and Camera with Tape



- Don't store password in browser



- Use TOR



Internet Surfing Tips

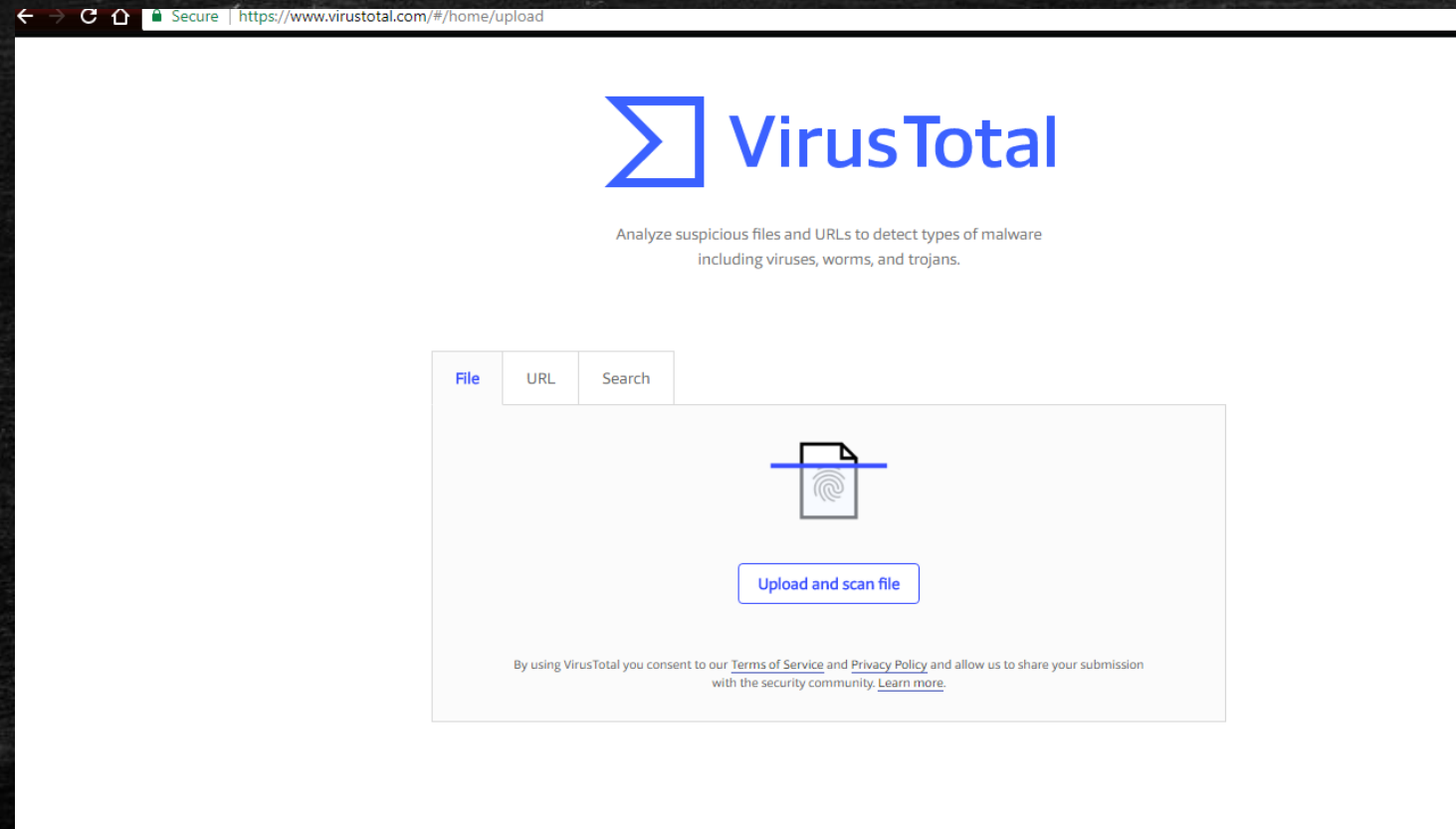
- Use private browsing in Chrome/Firefox
- Check for green lock and HTTPS in URL
- Keep your browser Up to Date
- Never click on unknown links
- Turn on Do Not Track feature in the browser
- Delete your profile from sites which you don't use (<http://backgroundchecks.org/justdeleteme/>)
- Use Sandboxie



- Use DuckDuckGo browser
- Use Panoptick (https://panoptick.eff.org/)



- Use VirusTotal for checking files
(<https://www.virustotal.com/#/home/upload>)

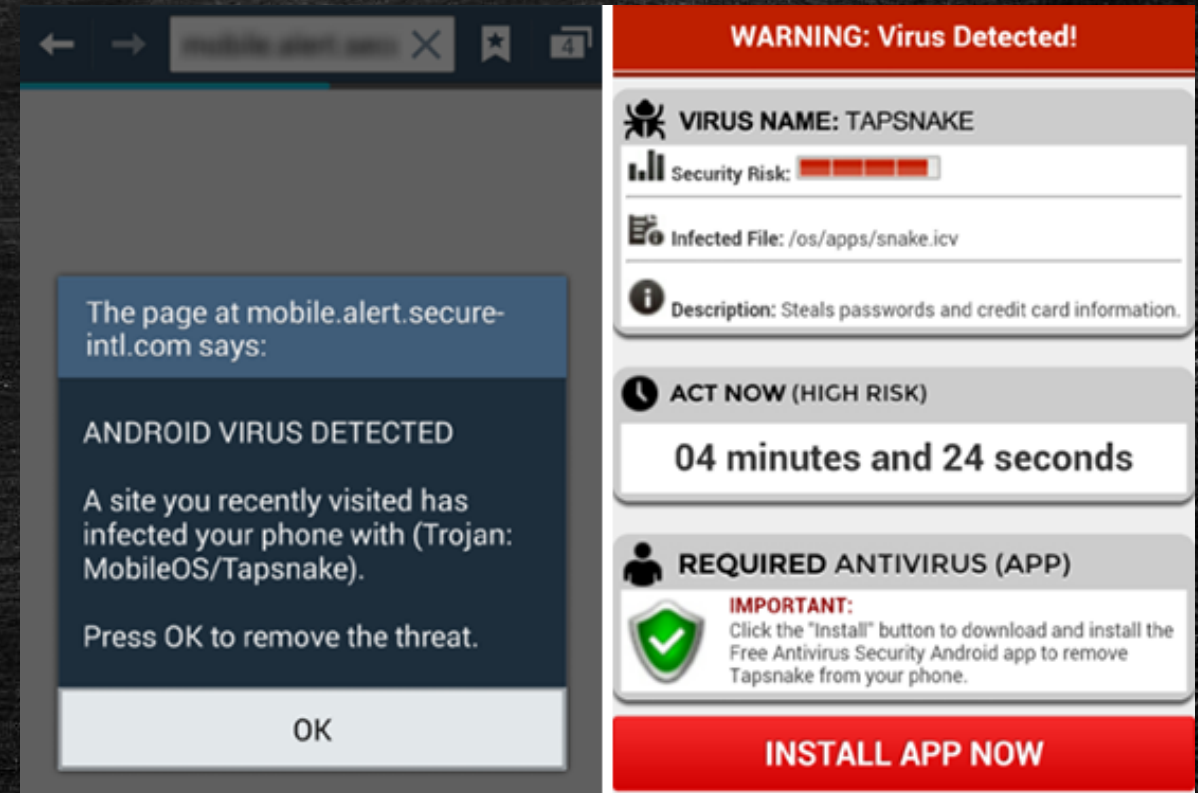
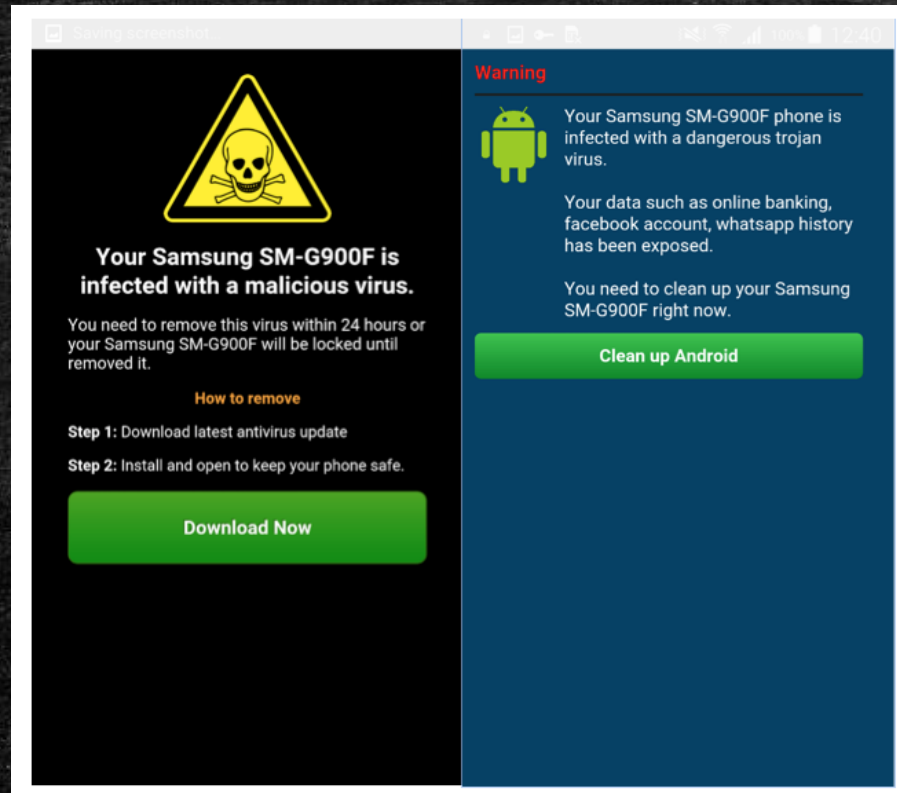


Mobile Security Tips


- Lock your phone using screen lock
- Do not connect to unknown Wi-Fi networks
- Do not connect your phone using USB to unknown devices
- Always update OS as soon as it releases
- Use Lock Apps for Files and Media
- Use Guest Mode
- Keep sensitive files on authentic Cloud Storages


-
- Do not Jailbreak or Root your smartphone
 - Download apps from authorized app stores only
 - Use Privacy options and disallow any permissions that is not necessary
 - Do not accept calls from weird numbers (VoIP Calls)
 - Schedule Routine Scans
 - Don't react to Scarewares and Adwares

Scarewares




Beware of these kind of APPS !!

 **Indian Browser**
Version 0.3 may request access to




Contacts

- find accounts on the device




Location

- access approximate location (network-based)
- access precise location (GPS)




Phone

- read phone status and identity



Storage

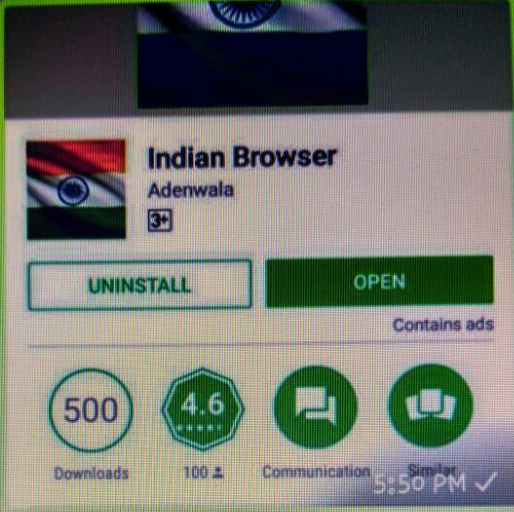
- write/delete internal storage
- read the contents of your internal storage



Other

- draw over other apps
- set wallpaper
- have full network access
- prevent phone from sleeping
- pair with Bluetooth devices
- run at startup
- install shortcuts
- receive data from Internet
- enable Bluetooth
- view network connections
- view Wi-Fi connections

You can disable access for these permissions in Settings. Updates to Indian Browser may automatically add additional capabilities within each group. [Learn more](#)



Indian Browser
Adenwala
3+

UNINSTALL **OPEN**

Contains ads

500 Downloads 4.6 100+ Communication

5:50 PM ✓

Jitna INDIA k log h plzzz apna uc brouser ko delete kr de kuu ki wo china ka brouser h ..
aur same function india ke brouser me bhi h uska naam india brouser h download kr le
pllllll isko itna sher kre ki kisi indian k mobile me uc brouser na hooo

5:52 PM ✓

720 x 938 pixels 80.1 kB 64% 770 / 829

Password Protection Tips

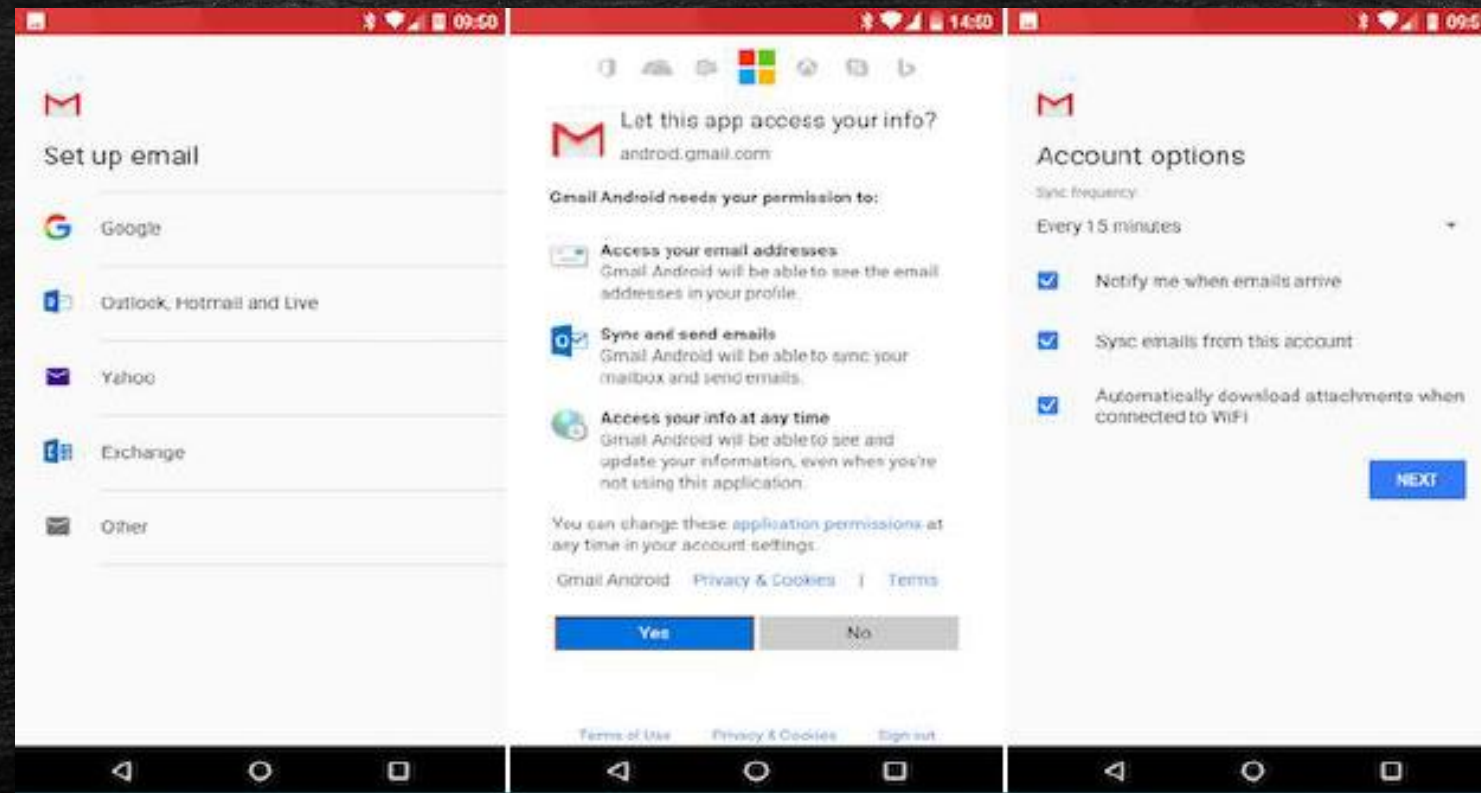
- Use different passwords for each account
- Always log off from your accounts
- Avoid entering password on computer that you don't control
- Beware of keyloggers
- Use complex password (Take help of password generators)
- Use reliable password vaults (KeepPass, PassPack)
- Use two-factor authentication
- Don't write true answers during security questions



Email & Chatting Tips

- Use encrypted emails like Proton Mail, Mailvelope
- Use end-to-end encrypted chat applications like Telegram, Signal, Wickr, CHatSecure
- Delete unused accounts
- Don't fill out your full information on social sites
- Use temporary mails for services you do not trust (Temp-Mail, Guerrilla Mail)
- Use Mail2Tor for sharing sensitive information

- Read all the permission that third party application want to access in your email account



Social Media Tips

- Check privacy settings. Do not show anything which is sensitive
- Limit your Bio information
- Avoid sharing account details
- Choose friends wisely over the internet
- Think before you share something online (status, pics, videos)
- Use different passwords for each social media account
- Restrict friend requests
- Access Control (who can see what)



अथवा प्रमाणित करें।

इसरायल या जमीनी अरबों से 11:00 सुबहों से दोपहरी 2:30 से इसरायल-पलुस्तिन और अरबों के बीचों में घंटों भीषण होठों को सहता पड़ा। राजधानी की एक पब्लिक लाइव को निगरान या सीक्योरिटी को इसे निगरान कर लिया गया। मस्जिदों पर सारे इसरायल या इसकी टोनों का 11वीं की रात से इसने हवाई को बॉलिंग के साथ भीषणता का इसरायल किया। इसने के विधि बिना ही इसरायल उसे अरबों को घंटों और बॉलिंग के पदों पर उसे भीषण या इस की अरबों की अरबों से। बॉलिंग को निगरान या इसरायल से सारे को और सीक्योरिटी से होठों के निगरान रिपोर्ट दर्ज करता। पुलिस से निगरान को अरबों की इसकी से उसके

पा के नाम से विराजित कर लिया।
दुर्गेश्वर मोदीजी यहाँ मुलाठी दुर्ग के बालक कि टाटोलीयन विद्यापीठ स्थापित के किए लीक्यो की दुर्गेश्वर पा पा के दुर्गेश्वर ह। सोलस ने अकाल अकाली के नाम से काली आईदी की ह। यहाँ भी अल्लोरी केनालुका पा मुनीजी की अल्लोरी बरौदो की कोरी चीन मुनी ह। दुर्ग यहाँ के सोलस पावर लुपन में विराजित के जान लीक्यो की दो बा पकड़ा भी जान मुनी ह। हा बा बा पावर लुपन के अल्लोरीकी के मानने यहाँ बापकन सुत जान बा। विरा लुपन ने लुपन की बालक कि सोलस में सोलस की बरौदो पा कंडरकर की लीक्यो लीक्यो की। दुर्ग मुनी की उरी पावरल सोलस का बरौदन पा बा बा लुपन करन बा। लोक दुर्ग विरा लुपन ने उरी विराजित में ले लिया। सब लीक्यो लुपन की लीक्यो कर बा बा।



मानवाधिकार-बाल अधिकार आयोग से भी शिकायत
 लखनौ में बताया कि पोलियोवायरस से इलाज के दौरान 1997 में मरवाया गया था।
 1997 में मरवाया गया था।
 1997 में मरवाया गया था।

टो बार पकड़ा गया, सोशल साइट पर शीएब से खन गया आकाश अवस्थी

साथ में दिया गया एक प्रस्ताव, जोकि
जहाँ से आया है, वहाँ से ही आया है
ने एनडीए सरकारों और एनडीए का
अधिकार और भी बढ़ाया है।

[illegible][illegible]

- 20) अजयन लोको को न ले
कुछ विचारक लेते और न
ले पावते हैं।
- 21) एक विचारक अपने का
पुस्तक को अपनी जेब
में डाल ले।
- 22) विचारक काले घाते के
विचारक में कोई चीज
न हो ले काले काले है।
- 23) रोज़ अपनी पुस्तक को
विचारक लेता का लेते
और कोई किन्तु अनुचित
के विचारक न लेते काले
- 24) अजयन लोको को न ले

[illegible][illegible]

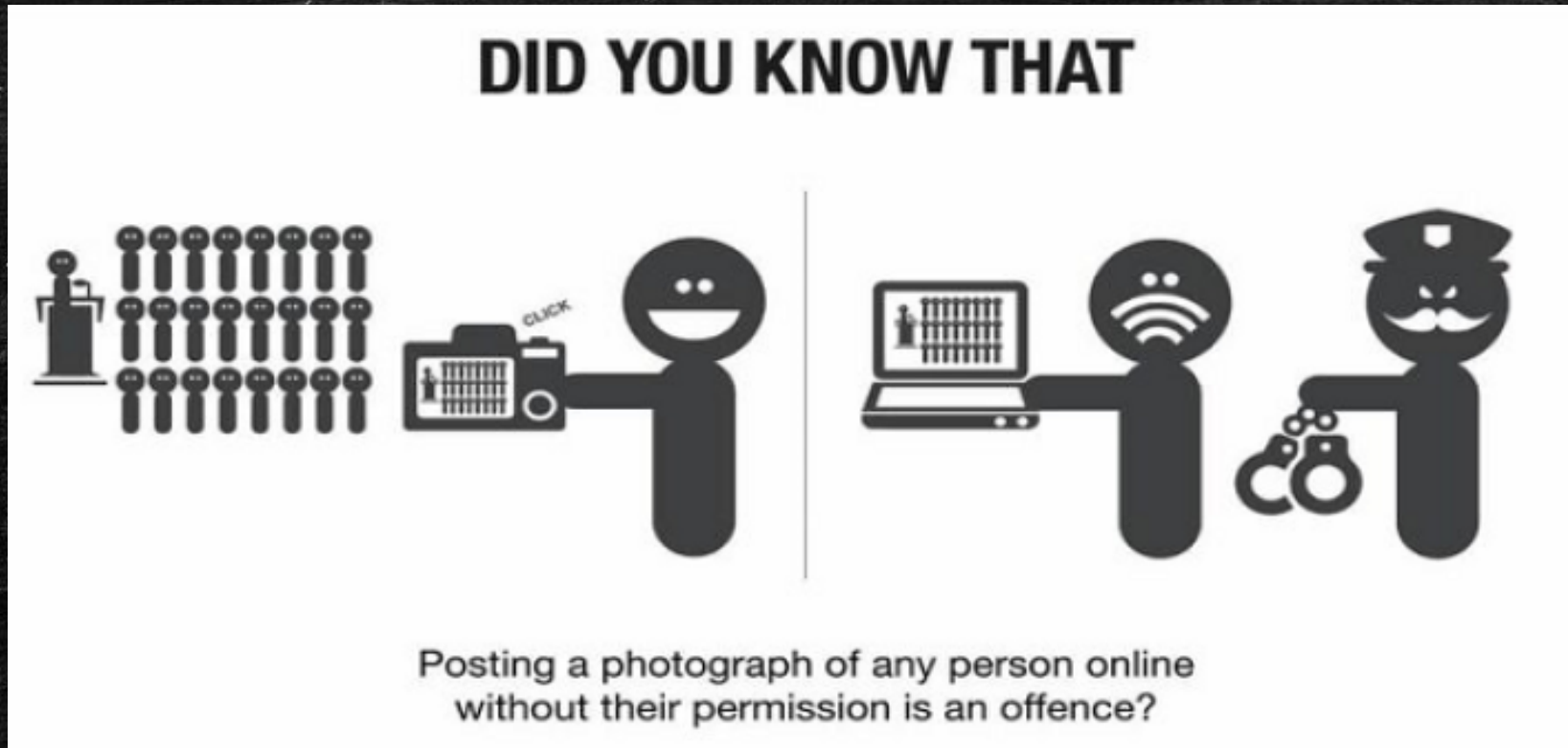
BLUE WHALE GAME





Did you Know that ?

- According to IT Act 2008 Section 66A Identity theft will result in 3 years jail and 5 lakh



Banking Tips

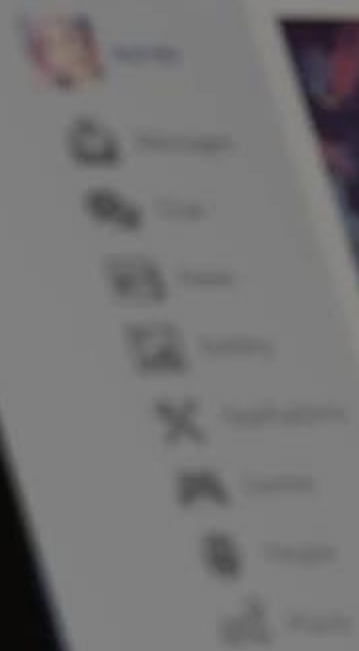
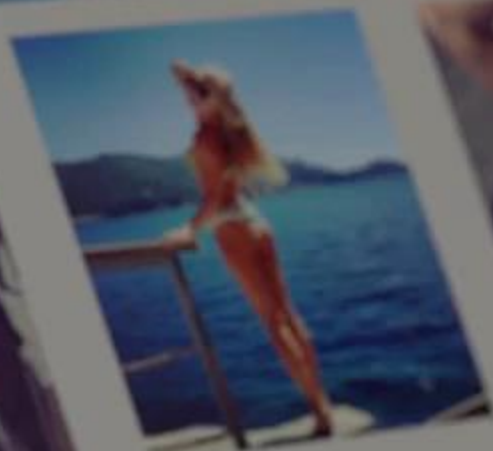
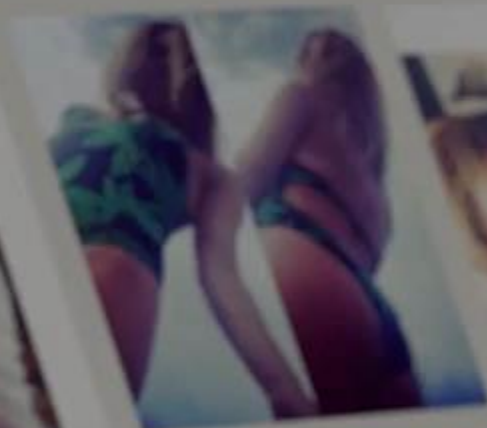
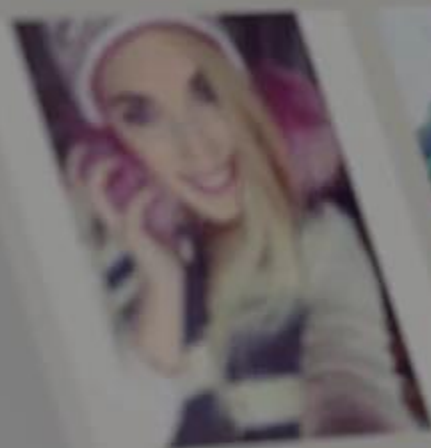
- Use Online Virtual Keyboard provided by the Banking website
- Never check "Remember Me" on banking websites
- Never use banking services on public Wi-Fis or cyber café.
- Always use 2 Factor Authentication
- Create a really strong password for Banking
- Change your password and ATM Pin regularly
- Beware of Shoulder Surfing





Preventing Online Scams

- Always check URLs of the sites you visit
- Always write the URL yourself instead of clicking on the link
- For suspicious links check the links on AVG ThreatLabs, Kaspersky VirusDesk, Scanurl, PhishTank, etc
- Never believe in any offers saying “you won something”. No one is giving free money
- Never click on unknown ads or pics
- Use pop-up blockers
- Try to avoid and make a distance with people having malicious intents



ANY
QUESTIONS



THANK YOU !!

- Email – apurvsinghgautam@gmail.com
- Social Handle – apurvsinghgautam
(LinkedIn, Twitter, Quora)

Thank You!