INTERNET SAFETY

“safely navigate our brave new world!”
Introduction

- How are we currently addressing Internet Safety?
- What issues have we faced with the internet, and with devices that have internet capability (i.e. smart phones, ipads, ipods, and laptops?)
Why focus on internet safety?

Computer and Internet Use:

- 93% of youth are online and 68% of parents surveyed regulate web content, while 55% limit time on the computer (interesting note: more parents restrict TV viewing than internet content).

- Time spent using digital media by children aged 13-17 is now more than they spend watching television.

Src: According to the Pew Internet & American Life Project, 2007,
Why is Internet Safety Important?

Today, 8-18 year-old spending an average of 7 hours and 38 minutes (7:38) to using entertainment media across a typical day (more than 53 hours a week). Kaiser Family Foundation 2010
Student Safety?

• More than half of educated teens in the India have an **online profile** on a social networking site, and most have posted photos of themselves and their friends, among other personal information for the world to access or at least friends.

• Most of the children (including adults sometimes) doesn’t know what content to be posted on social media and to whom they need to share with.

• Set the privacy to your personal and be safe, live safe.
Law (IT ACT)

- A 2-10 years of imprisonment for publishing unwanted content on a targeted person or religion in social media.

- The chat group admin will also be liable if any unwanted activities happen which may cause damage to society.

- Creating a fake profile on a person and misusing the identity and fame is a severe punishable offence.
Public Service Announcement

TECHNOLOGY FLUENCY IS OUR RESPONSIBILITY!
Hacking Groups
The top 10 most notorious hacking groups are:

- Lizard Squad
- Anonymous (Legion)
- LulzSec
- Syrian Electronic Army
- Chaos Computer Club (CCC)
- Iran’s Tarh Andishan
- The Level Seven Crew
- GlobalHell
- TeaMp0isoN
- Network Crack Program Hacker Group

Src: https://hacked.com/hacking/
Chances to Cyber War?

THE DIGITAL ERA
Cyber Crimes in Top 20 Countries

1. United States of America 23%
2. China 9%
3. Germany 6%
4. Britain 5%
5. Brazil 4%
6. Spain 3%
7. Italy 3%
8. France 3%
9. Turkey 3%
10. Poland 3%
11. India 3%
12. Russia 2%
13. Canada 2%
14. South Korea 2%
15. Taiwan 2%
16. Japan 2%
17. Mexico 2%
18. Argentina 1%
19. Australia 1%
20. Israel 1%
All Other Countries 19%
Steps towards Cyber Safe INDIA

Cyber Security
Internet Safety is embedded in Technology Fluency

It’s our job to educate...

- Safe and responsible use of electronic communication.
- To keep personal information on the internet protected.
- To recognize and avoid unsolicited or deceptive communications received online and through texts and email.
- Recognize and report online harassment and cyber-bullying to adults and save the evidence.
- Recognize and report illegal activities on the internet.
Digital Communication

Virtual communities

- Gaming
- Social Networking
- Instant Messaging
- Microblogging
- Text messaging
- Social Messaging
- Video chats

Examples

- Wii, Playstation 3
- MySpace, Facebook
- GoogleTalk, IM, iChat
- Twitter
- Cellphones
- Facebook Status
- Skype, i-Chat
BEST PRACTICES – DO’S & DON'T’S on SECURED ELECTRONIC TRANSACTION
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.
Secure ATM banking (Contd.,)

- If you get a transaction slip, shred it immediately after use if not needed.

- If your ATM card is lost or stolen, report it to your bank immediately.

- When you deposit a cheque or card into your ATM, check the credit entry in your account after a couple of days. If there is any discrepancy, report it to your bank.

- Register your mobile number with the Bank to get alerts for your transactions.

- If your card gets stuck in the ATM, or if cash is not dispensed after you keying in a transaction, call your bank immediately.

- If you have any complaint about your ATM/Debit/Credit card transaction at an ATM, you must take it up with the bank.
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 & Don’ts

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.
Secure Mobile Banking Do’s & Don’t’s (Contd.,)

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 transfer funds without due validation of the recipient, as funds once transferred cannot be reversed.

• 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.
Secure Mobile Banking Do’s & Don’t’s (Contd.,)

• Never reveal or write down PINs or retain any email or paper communication from the bank with regard to the PIN or password.

• Be cautious while using Bluetooth in public places as someone may access your confidential data/information.

• Be careful about the websites you are browsing, if it does not look authentic, do not download anything from it.

• Download & Install application from trusted source.

• Install antivirus software & Update your mobile with latest version of applications & OS.
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
Secure your Debit/credit card
Password - Do’s

Do’s:

• Be creative and think of a password that is really different as well as difficult to guess.

• Mix upper and lowercase letters, and special characters like $, @, *, etc.

• Place punctuation or numbers randomly.

• Pick letters that are in different places on keyboard. Do not use sequences like ‘qwerty’.
Secure your Debit/credit card Password – Don’t’s

Don’t’s:

• Don’t use sequences of letters or numbers. E.g.: abcd1234, asdfg123 etc.

• Don’t use personal information like your name, date of birth, PAN number, etc.

• Avoid using the same password for several different accounts. Once hackers have guessed one password, they’ll often try to see if it works on other accounts.
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.
How to create a safe password to your computer?

- Keep alphanumeric passwords that are at least 8 characters long.

- You can use phrases in sentences such as "nature's wrath tsunami" to frame your passwords as they are easy to remember and difficult to crack.

- Do not use dictionary-based words, your spouse's name or your date of birth. These are easy to crack or guess.

- Do not keep the same passwords for multiple accounts.

- Do not write down your passwords.

- Change your passwords once in every three months.
Tips to secure your NetBanking

• Keep your Customer ID and Profile Password confidential and do not disclose it to anybody.

• Change your Profile Password as soon as you receive it by logging into your NetBanking account. Memorize your Profile Password, do not write it down anywhere.

• Avoid accessing internet banking from shared computer networks such as cyber cafes or public Wifi network like hotel/airport etc.

• Do not click on links in the emails or sites other than www.hdfcbank.com to access your NetBanking webpage.

• Always verify the authenticity of the Bank's NetBanking webpage by checking its URL as "https://netbanking.xyzbank.com" and the Lock symbol at the bottom corner of the browser.

• Disable "Auto Complete" feature on your browser.
Tips to secure your NetBanking (Contd.,)

• Uncheck "User names and passwords on forms", click on "Clear Passwords".

• Click "OK".

• Use virtual keyboard feature while logging into your internet banking account.

• Do cross check your last login information available on NetBanking upon every login to ascertain your last login and monitor any unauthorized logins.

• Always type in your confidential account information. Do not copy paste it.

• Always logout when you exit NetBanking. Do not directly close the browser.
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.
Tips to secure your Online Shopping (Contd.,)

• 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.
Any Questions?

vbrao@esflabs.com
+91 8019548656