

**Ministry of Electronics and Information Technology(MeitY)  
Government of India**



[www.isea.gov.in](http://www.isea.gov.in)

[staysafeonline.in](http://staysafeonline.in)

**Information Security Education and Awareness (ISEA) Project**

**Cyber Hygiene Practices**



# Information Security Education & Awareness

Ministry of Electronics and Information Technology  
Ministry of Communications and Information Technology  
Government of India



www.isea.gov.in

## Key Verticals of ISEA Phase-III



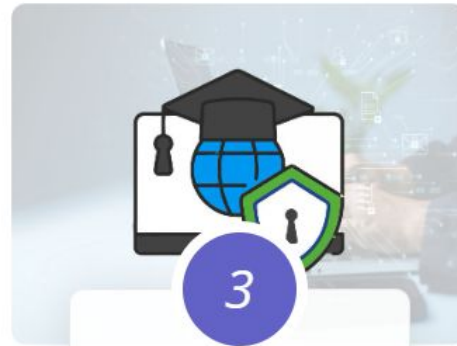
1

**Generating highly skilled & certified Cyber Security Professionals – CISOs**



2

**Grooming students towards products and solutions development in cyber security**



3

**Strengthening research & education in Information Security**



4

**Cyber Aware Digital Naagriks (Mass Awareness)**



5

**Common Infrastructure & Shared Resources**

# Cyber aware Digital Naagrik(stay safe online)

## Components

### 1. Mass Awareness activities

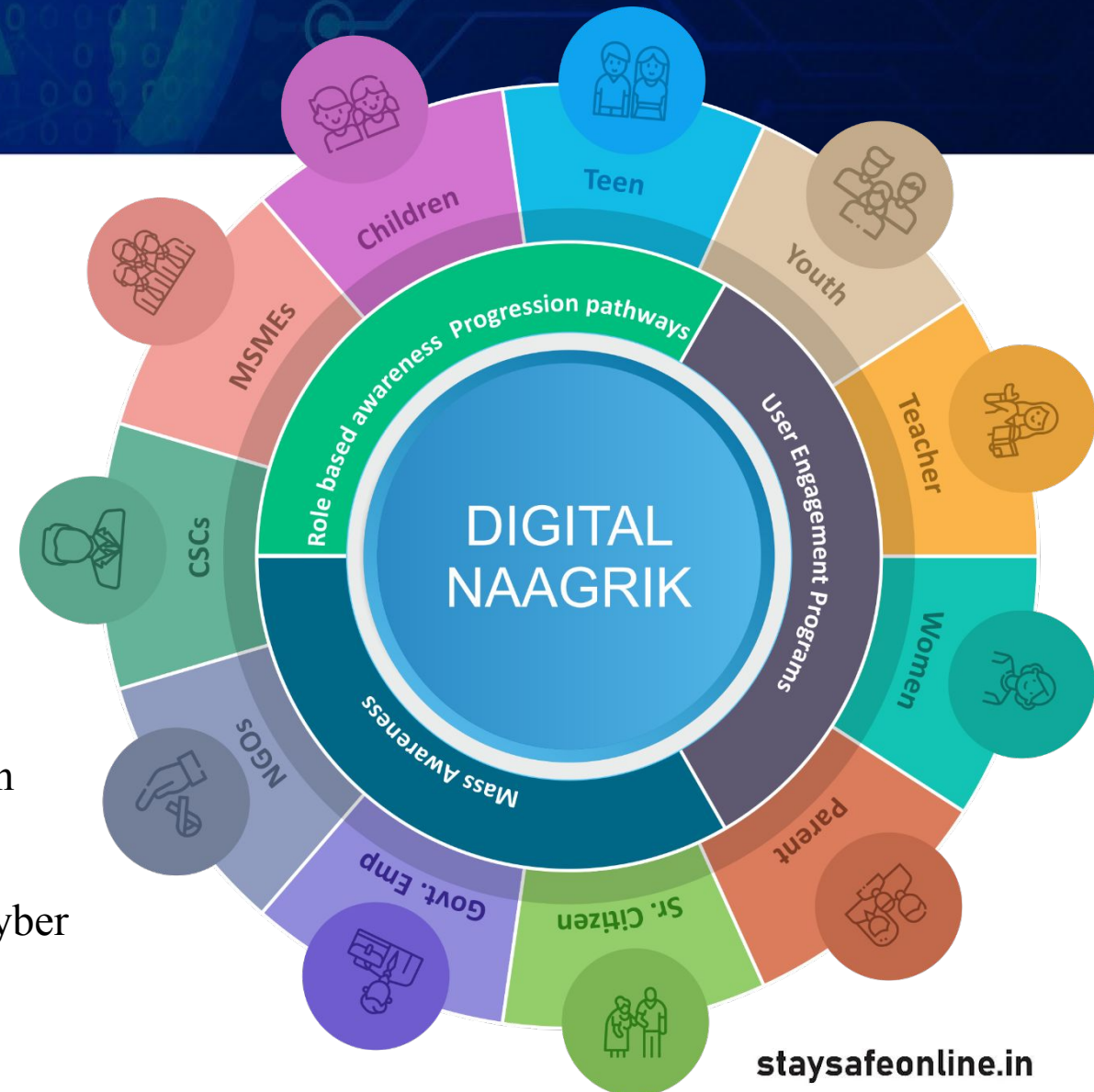
- Awareness workshops / Webinars
- Awareness weeks
- AIR/DD/ Community Radio programmes
- Educational TV Programs (Digi shala)/YouTube
- Mobile App (Cyber fitness/Awareness App)

### 2. Multilingual awareness content

- Website, Handbooks, posters, cartoon, videos, etc.
- Leverage Print, Electronic, Social media for dissemination

### 3. Role-based Awareness & Progression Pathways

- Interactive programs for Cyber Kid, Cyber Cadet, Cyber Women and Cyber Trainer
- User engagement: competitions, quiz, cyber clubs







Home / Awareness Resources

# Awareness Resources



Awareness  
Poster



Cartoon  
Storyboard



Cyber Security  
Tip of the Day



Do you Know ?



Fact Check -  
PIB



KBC-Kaun  
Banega  
CyberSafe



Warning Signs



Advisories



Brochures



Handbooks



Concept Video



Cyber Alert  
News



Cyber Security  
Tip Video



Reels/Shorts



# Awareness Quizzes



## Cyber Hygiene Security Practices

15  
Questions

10min  
Duration

Start



## Quiz on Cyber offences against Women

12  
Questions

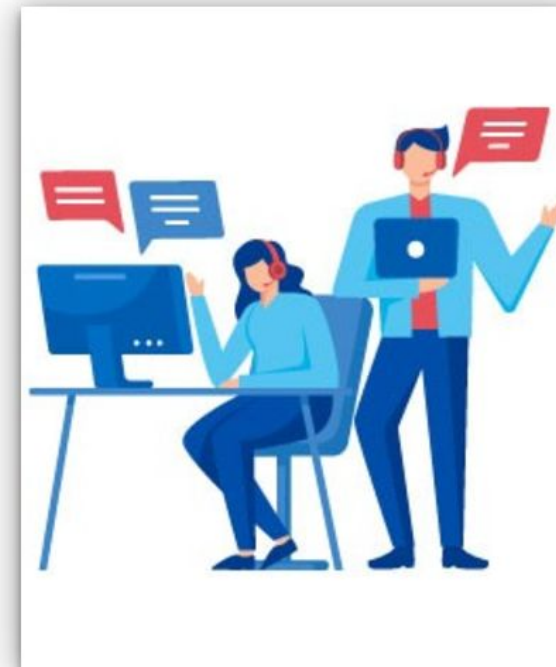
15min  
Duration



## Cyber Hygiene Practice Quiz for students

10  
Questions

10min  
Duration



## Cyber Hygiene Practices for Employees

10  
Questions

10min  
Duration

# Cyber Fitness Assessment



**Cyber Hygiene  
Fitness  
Understanding  
Threats**



**Safe e-mail and  
Internet Usage at  
Workplace**



**Test Your skills for  
recognizing and  
reporting threats**



**Role and  
contributions of  
employees to dela  
cyber security**



**Digital Parenting**



**Impact of Cyber  
Threats on**



**Tools to mitigate  
Social Engineering**

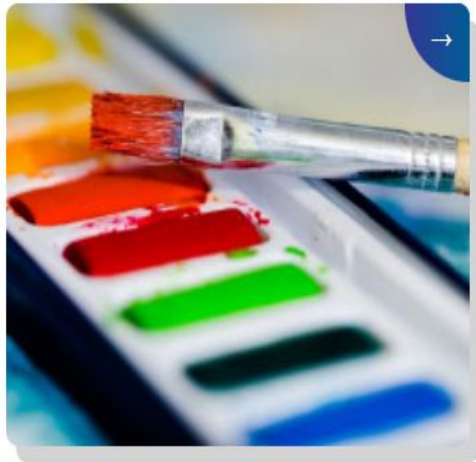


**Recognising and  
reporting Malware**

# National Level Competitions

Showcase your creativity and talent.

Competition Guidelines **UPDATED** . Give it a click to view.



Drawing/Painting



Cartoon Storyboard



Short Video



My Success Story: Thanks to Digital Naagrik



# Reinforce Cyber Hygiene, Cyber Security and Privacy for Digital Naagrik



Cyber Kid

[View](#)



Cyber Cadet

[View](#)



Cyber Girl

[View](#)



Cyber Yuva

[View](#)



Cyber Shikshak

[View](#)



Cyber Shakti

[View](#)



Cyber Parent

[View](#)



Cyber Varishth  
Naagrik

[View](#)



Employee

[View](#)



Cyber Pratinidhi

[View](#)

# Basics of Network Security: Threats and Defense Mechanisms

Protecting Ourselves in the Digital World

By Harpreet Bawa

# Why Network Security Matters?

Every 39 seconds a hacker attacks somewhere in the world

- Students → gaming ID hacked
- Teachers → email hacked
- Parents → bank fraud SMS

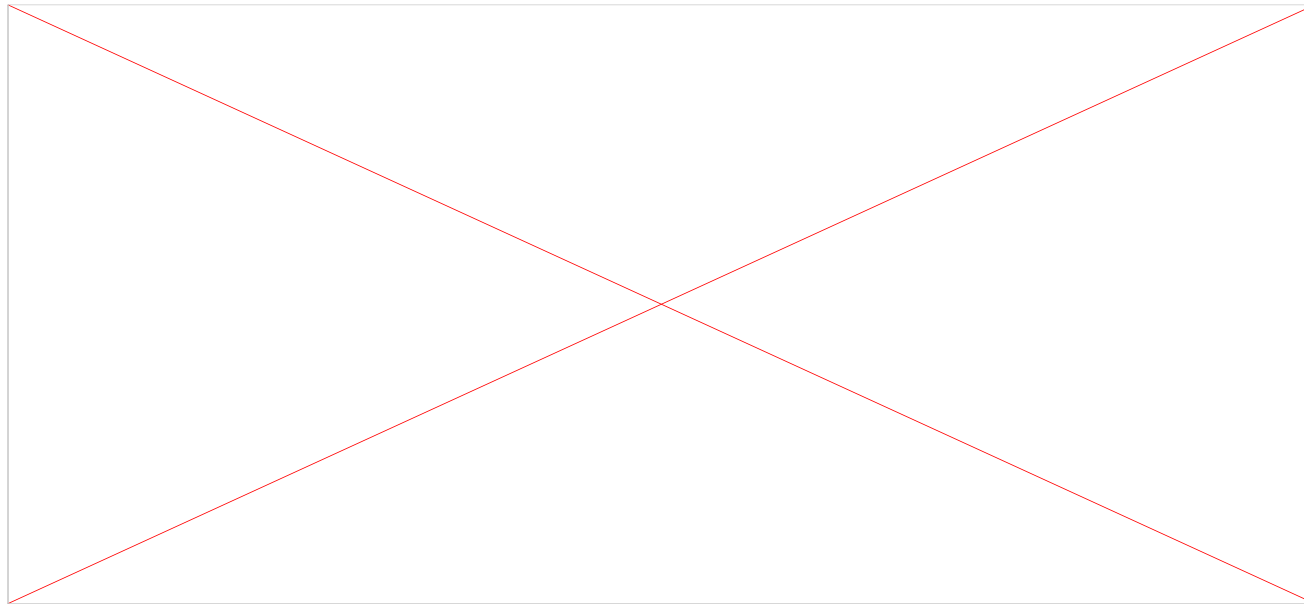
*"If we are online, we are/can be a target."*

# Introduction to Network Security

“Network Security means protecting our devices, accounts, and data from hackers.”

Network Security = Protecting devices, accounts, and data from hackers

- Analogy: Like locking doors at home to stay safe



# Importance for Students, Teachers & Parents

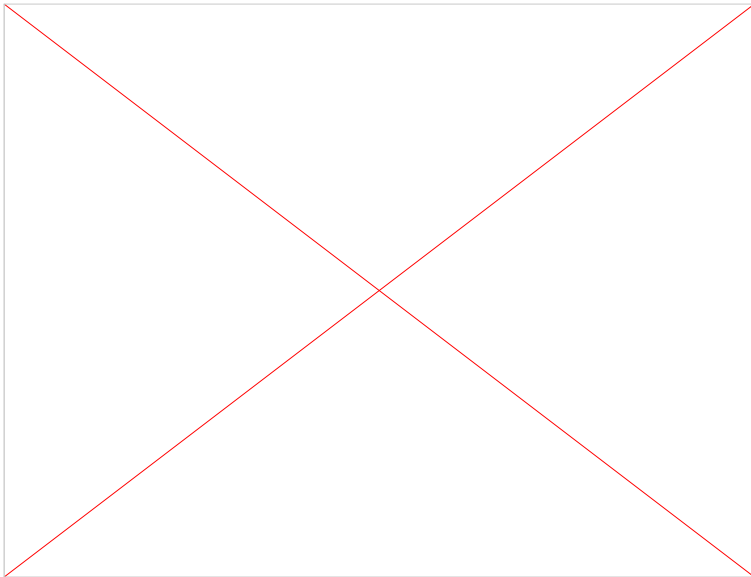
- **Students:** protect from scams, cyberbullying.
- **Teachers:** safeguard online classes, data.
- **Parents:** safe banking, safe browsing.



# Common Network Threats – Malware

*“Malicious software that harms devices”*

- **Types:** Virus, Worm, Trojan
- **Case:** “A free game download stole photos from a laptop.”



## Example – The “EvilQuest” Malware (2020)

- Hackers spread a free pirated version of popular games for Mac.
- When users installed the game, it secretly installed malware.
- This malware scanned the system, **stole files including photos and documents**, and even encrypted them like ransomware.

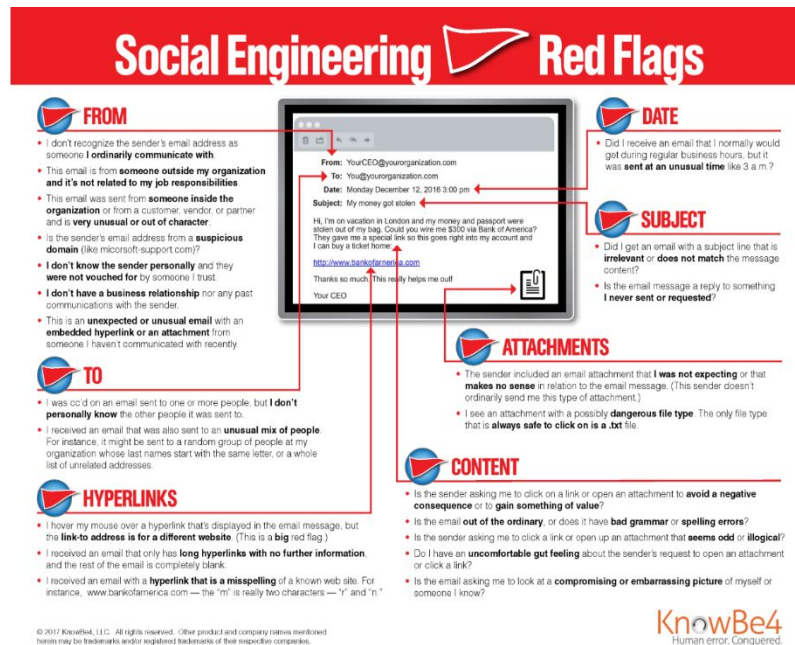
# Common Network Threats – Phishing

“Fake messages/emails to trick people”

- **Example:** SMS ‘Your ATM card is blocked, click here’

“Would you click this link if it came to you?”

## Social Engineering Red Flags



**FROM**

- I don't recognize the sender's email address as someone I **ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like microsoft.support.com)?
- **I don't know the sender personally** and they were **not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink** or an **attachment** from someone I haven't communicated with recently.

**DATE**

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

**SUBJECT**

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something I **never sent or requested**?

**ATTACHMENTS**

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

**CONTENT**

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary** or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

**TO**

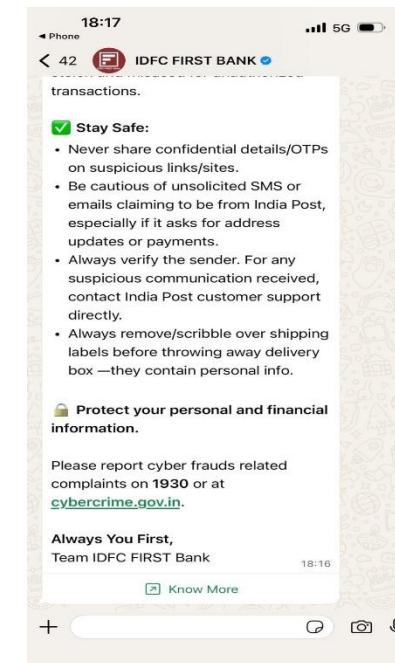
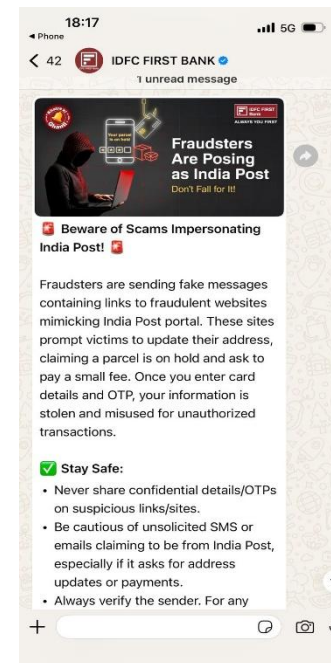
- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

**HYPERLINKS**

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big red flag**.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, [www.bankofamerica.com](http://www.bankofamerica.com) — the "m" is really two characters — "i" and "n."

© 2017 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

KnowBe4  
Human error. Conquered.



# Common Network Threats – Man-in-the-Middle

*“Hacker between your device & internet”*

- **Real Life example:** “A boy used free café Wi-Fi, later found his social account hacked.”

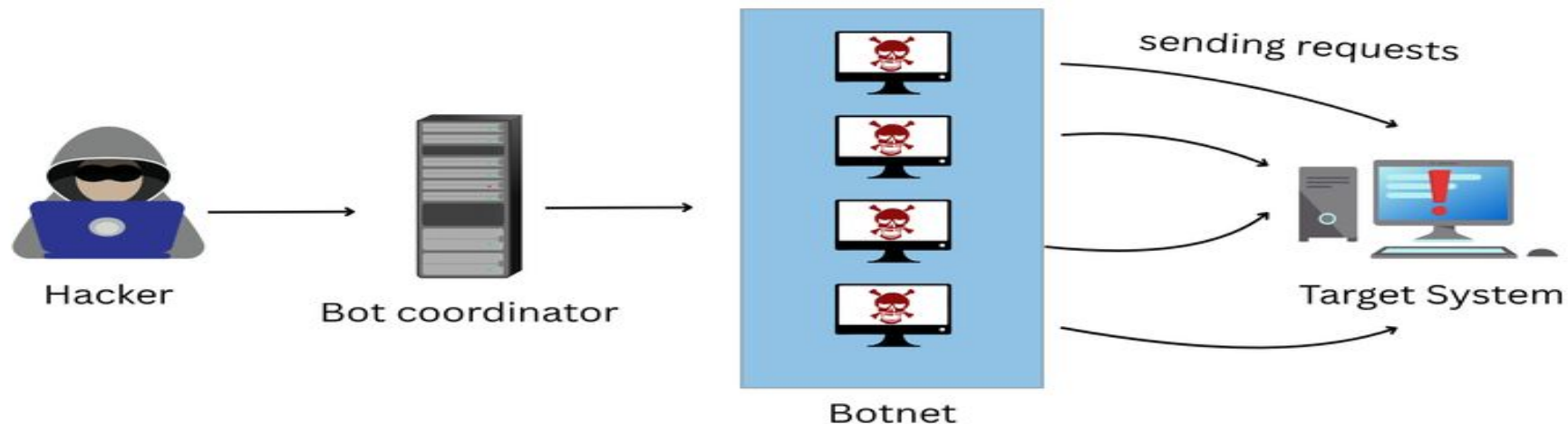


# Common Network Threats – Denial of Service (DoS)

Simple definition: “Making websites crash by overload.”

- **Real Life example:** Result website crashing during exams

## How is Botnet Used for DDoS Attack



Reference: UniNets

# Common Network Threats – Social Engineering

“Tricking people, not machines”

- **Example:** Fake bank call asking for OTP

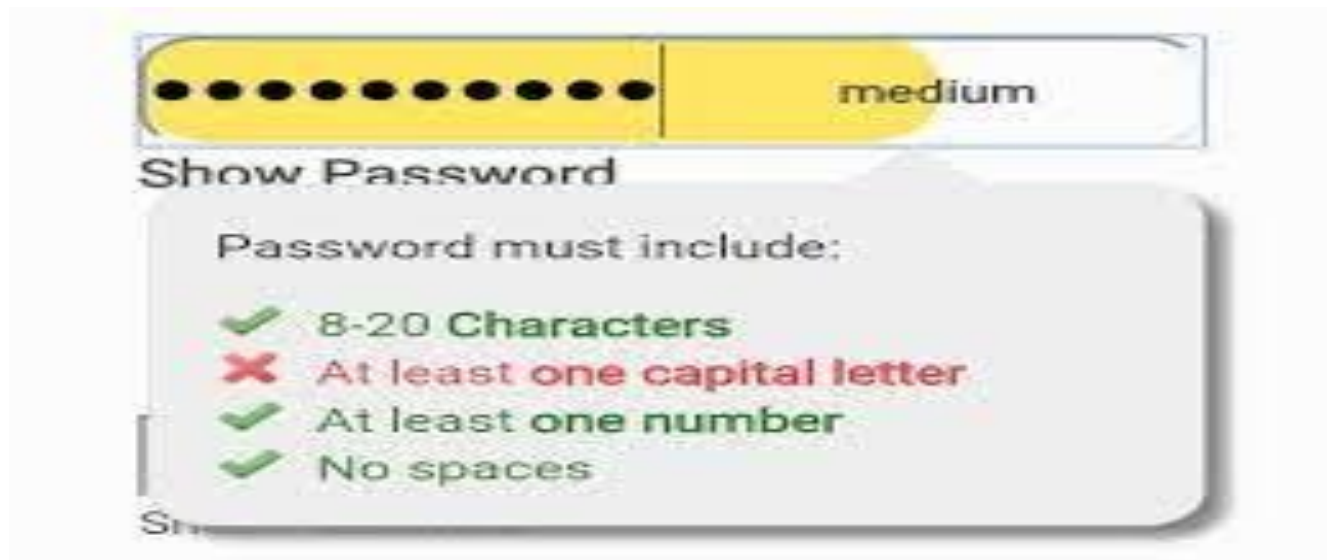


shutterstock.com · 2011026575

# Defense Mechanisms & Best Practices

## 1. Defense - Strong Password:

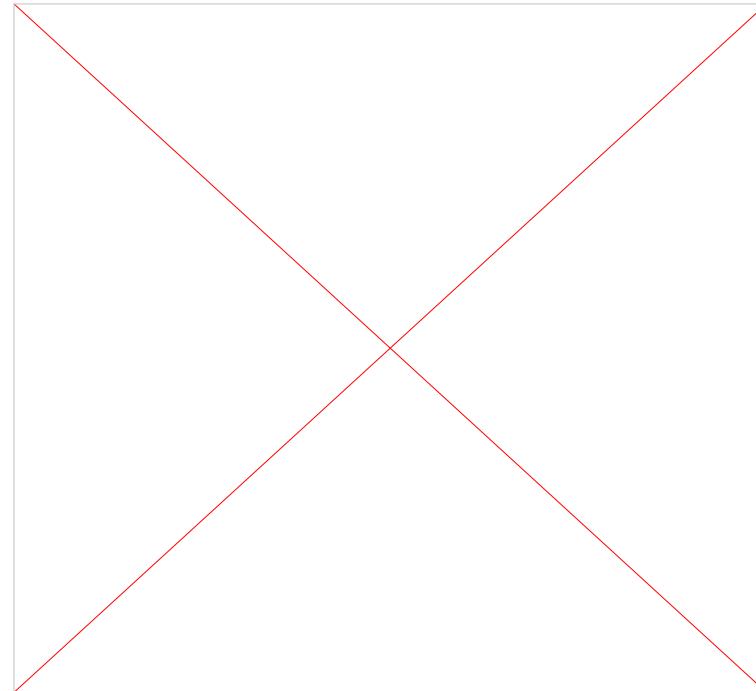
- Use long, unique, mixed passwords
- Fun fact: “123456 is still the most common password”.
- Weak vs strong password examples



# Defense Mechanisms & Best Practices


## 2. Defense - Firewalls & Antivirus:

- Firewall = Gatekeeper (blocks suspicious traffic)
- Antivirus = Doctor (detects & removes malware)

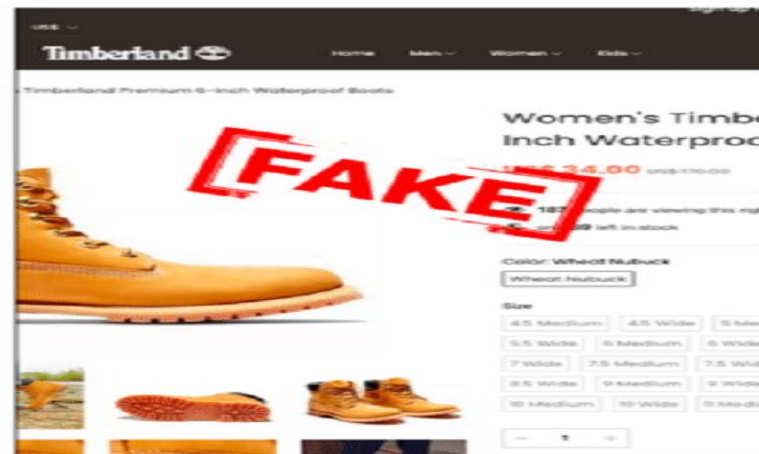
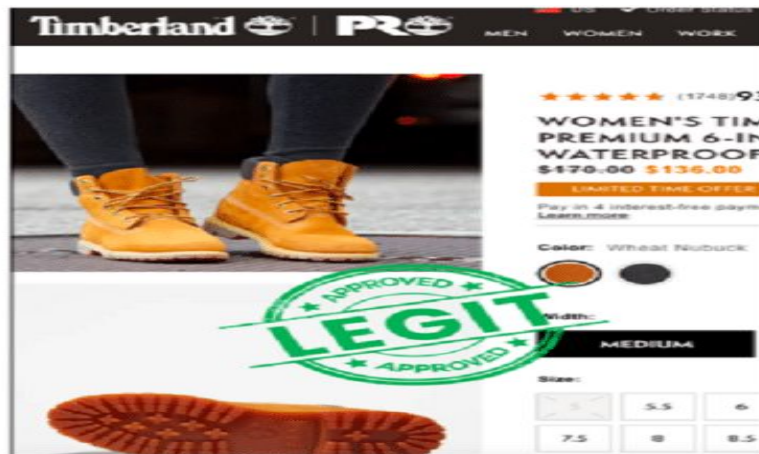


# Defense Mechanisms & Best Practices

## 3. Defense - Safe Browsing Habits:

- Check for HTTPS 
- Avoid unknown links/downloads
- Don't use pirated apps

*Example: Fake vs real shopping website*

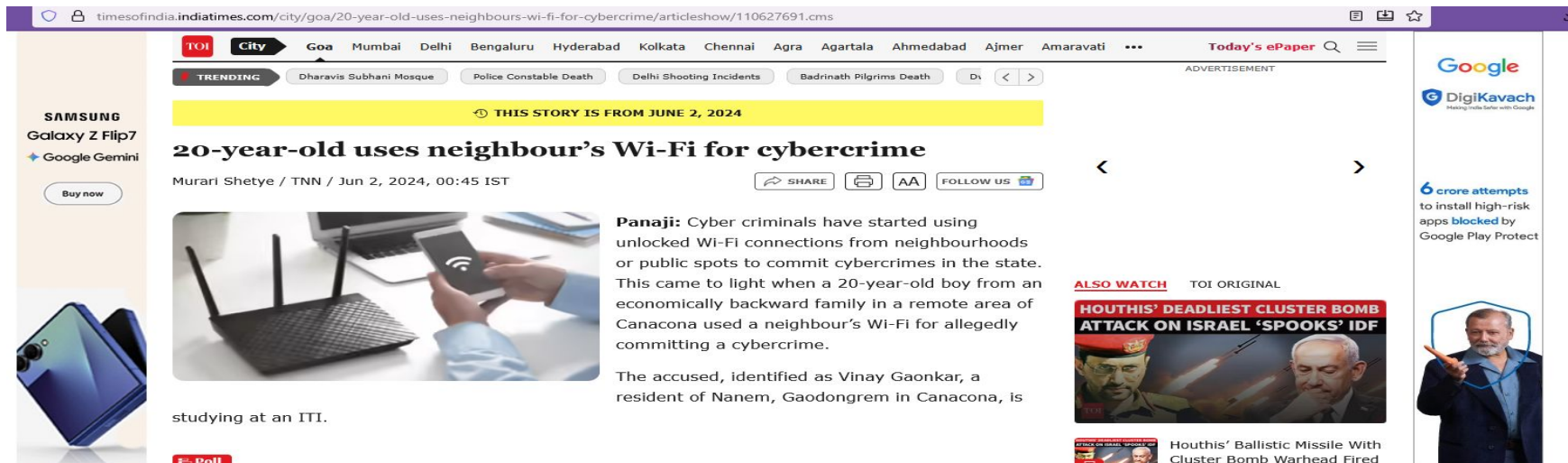


# Defense Mechanisms & Best Practices

## 4. Defense – Protect WIFI:

- Change default router password
- Use WPA2/WPA3
- Don't share Wi-Fi openly

*“Real life Story: A neighbour misusing Wi-Fi for illegal activity.”*



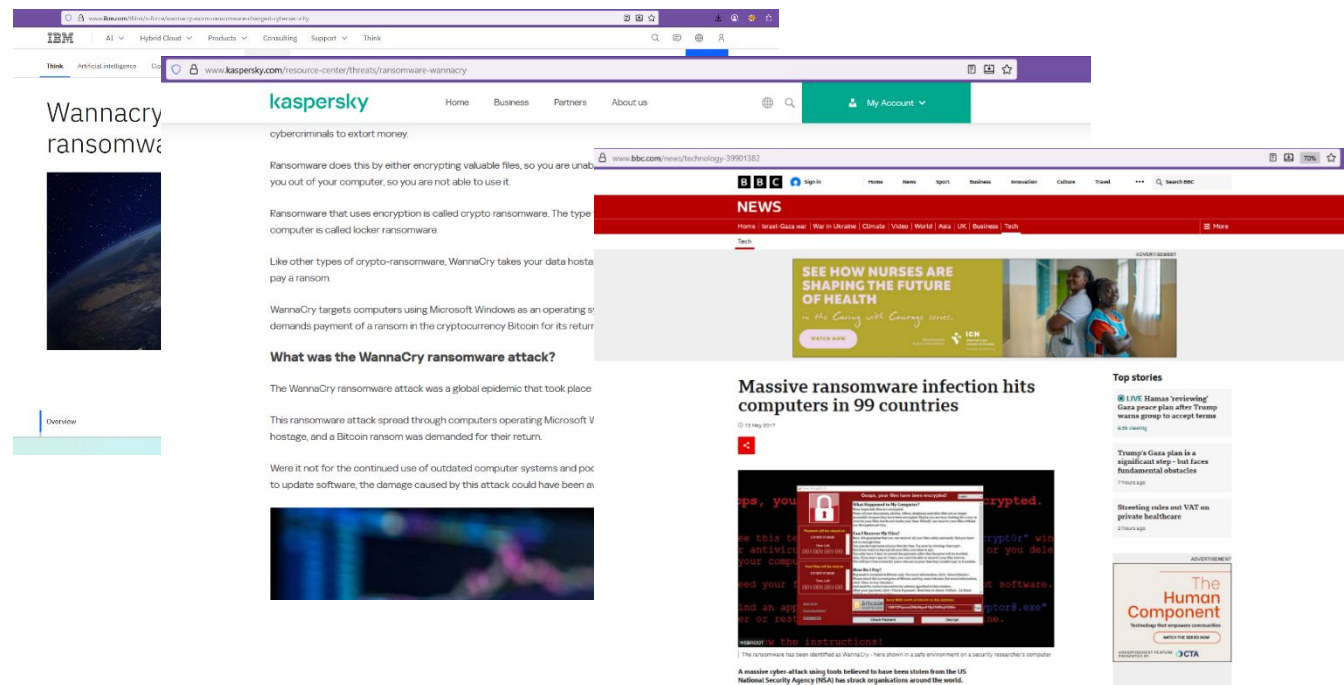
The screenshot shows a news article on the Times of India website. The article is titled "20-year-old uses neighbour's Wi-Fi for cybercrime" and is dated June 2, 2024. The author is Murari Shetye. The article text states: "Panaji: Cyber criminals have started using unlocked Wi-Fi connections from neighbourhoods or public spots to commit cybercrimes in the state. This came to light when a 20-year-old boy from an economically backward family in a remote area of Canacona used a neighbour's Wi-Fi for allegedly committing a cybercrime. The accused, identified as Vinay Gaonkar, a resident of Nanem, Gaodongrem in Canacona, is studying at an ITI." The article includes an image of a person using a smartphone next to a Wi-Fi router. There are also advertisements for Samsung Galaxy Z Flip7 and Google Gemini on the left, and a Google DigiKavach advertisement on the right. A "Poll" button is visible at the bottom left of the article content.

# Defense Mechanisms & Best Practices

## 4. Defense - Backups & Updates:

- Backups save data from ransomware
- Updates fix security holes

*Case: WannaCry spread because of no updates*



The collage consists of several overlapping screenshots:

- Top Left:** A Kaspersky article titled "Wannacry ransomware" with a sub-header "cybercriminals to extort money". The text explains that ransomware encrypts files, making them unusable. It distinguishes between crypto-ransomware (like WannaCry) and locker ransomware. It notes that WannaCry targets Windows computers and demands Bitcoin. A section titled "What was the WannaCry ransomware attack?" describes it as a global epidemic that spread through outdated Microsoft Windows systems. A small image shows a view of Earth from space.
- Top Right:** A BBC News article titled "Massive ransomware infection hits computers in 99 countries". The article includes a date of 01 May 2017 and a small image of a ransomware screen with a red lock icon and the word "encrypted".
- Bottom Right:** A "Top stories" section from BBC News, featuring a headline about Hamas' ceasefire plan and another about Trump's Gaza plan. Below this is an advertisement for "The Human Component" by CTA.

# Defense Mechanisms & Best Practices

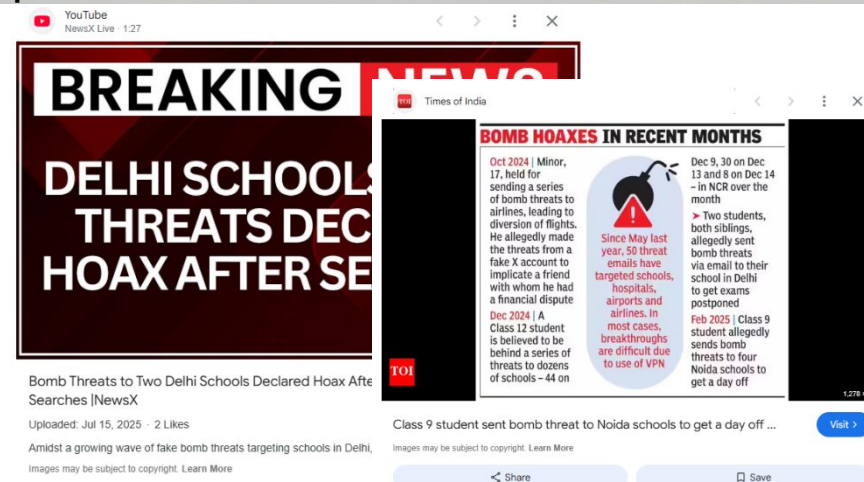
## 5. Defense - Cyber Hygiene for Students:

- Don't overshare on social media
- Be careful in gaming chats
- Report bullying



# Case Study – Hoax Threat Emails to Delhi-NCR Schools

- On **May 1, 2024**, over **80-100 schools across Delhi-NCR** (including prominent schools) received **bomb threat emails** sent to their official email addresses.
- The emails claimed explosives had been planted on premises, leading to panic among parents & students; many schools shut early, classes cancelled, students sent home.
- The threat emails were traced to a single IP address, from a Russian domain (mail.ru).
- After investigations (dog squads, bomb disposal units, police), nothing suspicious was found at school premises. The threats were declared **hoaxes**.



# Case Study: MobiKwik Data Breach (India)

- In **March 2021**, digital payment / wallet service **MobiKwik** reported that data of nearly **110 million** users was found on sale on a hacker forum/dark web.
- The leaked data included sensitive user details: linked mobile phone numbers, KYC documents, Aadhaar card numbers, credit card information.
  
- **Impact on individuals:**
  - Risk of identity theft
  - Phishing / fake calls
  - Financial fraud
- **Lessons for us:**
  - Use unique, strong passwords
  - Be careful which apps you trust with personal data
  - Regularly monitor statements & OTPs
- **Takeaway message:**

Even trusted apps can have issues; your vigilance is your first line of defense.

# Cybersecurity Checklist



- Strong Wi-Fi password
- Use 2FA
- Update devices regularly
- Backup important files
- Educate kids about online safety

# Key Takeaways



- Threats are real, but defense is simple
- Awareness is the best protection
- Lock your digital world like your home

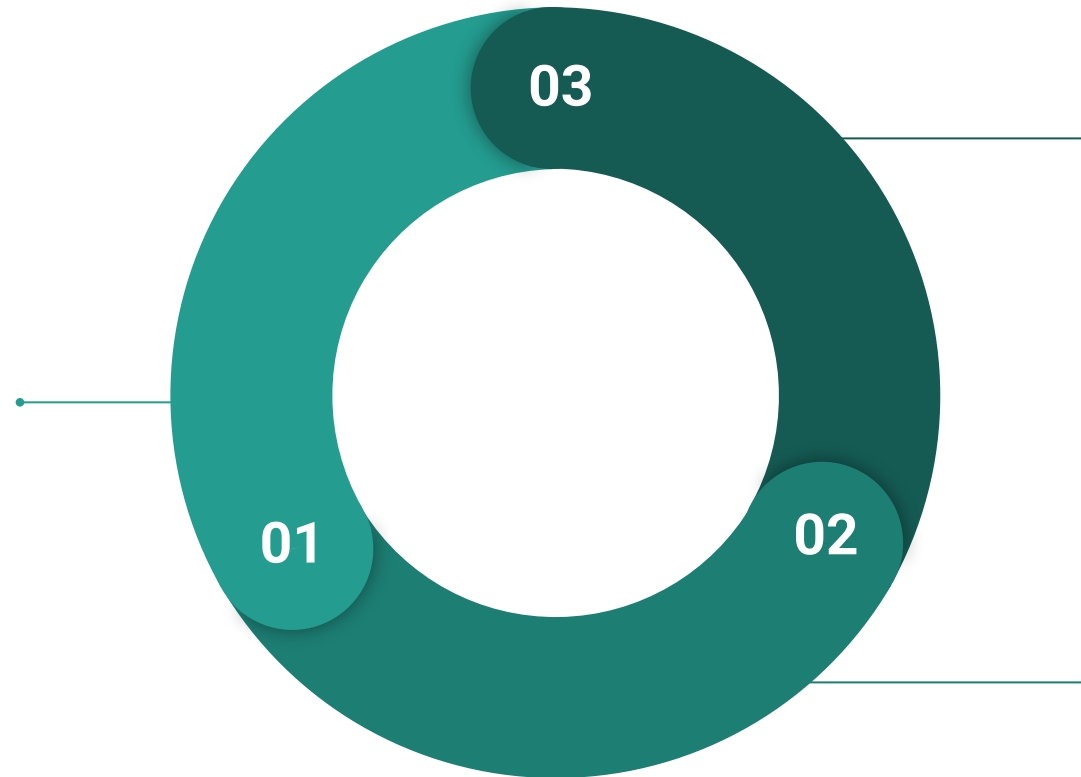
# Closing

Stay Safe, Stay Secure!

*Thank you for joining*

Call 📞 1930  
(Helpline number)

to register any  
complaint about  
cybercrime.



You can also file  
your complaint 📄  
online through  
**www.cybercrime.  
gov.in**

You can also file  
your complaint at  
the **nearest  
police station**

