

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



www.isea.gov.in

staysafeonline.in

Information Security Education and Awareness (ISEA) Project

Cyber Hygiene Practices

नेटवर्क सुरक्षा की मूल बातें: खतरे और रक्षा तंत्र

डिजिटल दुनिया में अपनी सुरक्षा

हरप्रीत बावा द्वारा



नेटवर्क सुरक्षा क्यों महत्वपूर्ण है?

हर 39 सेकंड में दुनिया में कहीं न कहीं एक हैकर हमला करता है।

- छात्र → गेमिंग आईडी हैक
- शिक्षक → ईमेल हैक
- अभिभावक → बैंक धोखाधड़ी एसएमएस

"अगर हम ऑनलाइन हैं, तो हम निशाना बन सकते हैं"

नेटवर्क सुरक्षा का परिचय

"नेटवर्क सुरक्षा का अर्थ है हमारे डिवाइस, खातों और डेटा को हैकर्स से सुरक्षित रखना।"

नेटवर्क सुरक्षा = उपकरणों की सुरक्षा, खातों, और डेटा की सुरक्षा हैकर्स से

- उदाहरण: सुरक्षित रहने के लिए घर के दरवाज़े बंद करने जैसा



छात्रों, शिक्षकों और अभिभावकों के लिए महत्व

- छात्र : घोटालों, साइबर धमकी (cyberbullying) से सुरक्षा
- शिक्षक : ऑनलाइन कक्षाओं और डेटा की सुरक्षा
- अभिभावक : सुरक्षित बैंकिंग, सुरक्षित ब्राउज़िंग.



सामान्य नेटवर्क खतरे – मैलवेयर

“दुर्भावनापूर्ण सॉफ्टवेयर जो (*Malicious software*) डिवाइस को नुकसान पहुँचाता है”

- प्रकार (Types): Virus, Worm, Trojan
- मामला: "एक निःशुल्क गेम डाउनलोड ने लैपटॉप से तस्वीरें चुरा लीं।"



उदाहरण – “एविलक्वेस्ट” मैलवेयर(**EvilQuest** Malware)
(2020)

- हैकर्स ने मैक (MAC) के लिए लोकप्रिय गेम का निःशुल्क पायरेटेड संस्करण फैलाया।
- जब उपयोगकर्ता गेम इंस्टॉल करते थे, तो उसमें गुप्त रूप से मैलवेयर इंस्टॉल हो जाता था।
- इस मैलवेयर ने सिस्टम को स्कैन किया, फोटो और दस्तावेजों सहित फाइलें चुरा लीं, और यहां तक कि उन्हें रैनसमवेयर की तरह एन्क्रिप्ट भी कर दिया।

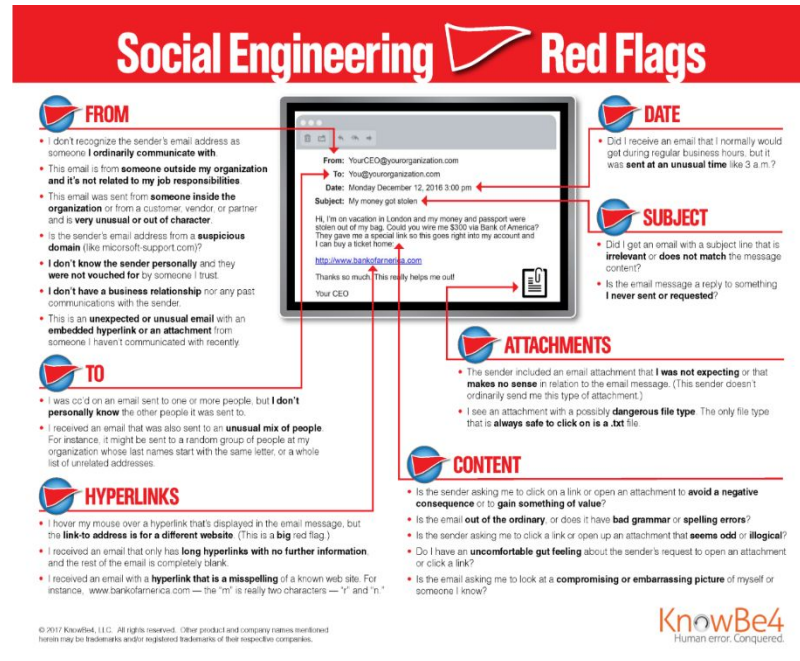
सामान्य नेटवर्क खतरे – फ़िशिंग

“लोगों को धोखा देने के लिए फर्जी संदेश/ईमेल”

- उदाहरण: एसएमएस ‘आपका एटीएम कार्ड ब्लॉक हो गया है, यहां क्लिक करें’

“यदि यह लिंक आपके पास आए तो क्या आप इस पर क्लिक करेंगे?”

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

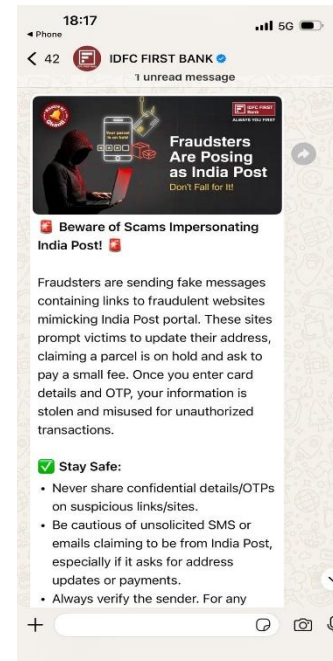
- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the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



18:17 5G

IDFC FIRST BANK

1 unread message

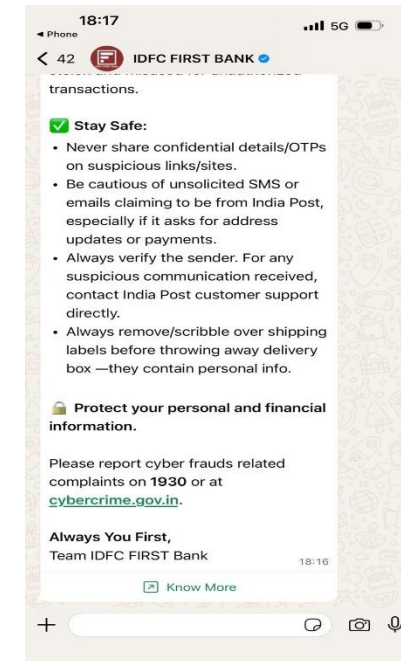
Fraudsters Are Posing as India Post
Don't Fall for It!

Beware of Scams Impersonating India Post!

Fraudsters are sending fake messages containing links to fraudulent websites mimicking India Post portal. These sites prompt victims to update their address, claiming a parcel is on hold and ask to pay a small fee. Once you enter card details and OTP, your information is stolen and misused for unauthorized transactions.

Stay Safe:

- Never share confidential details/OTPs on suspicious links/sites.
- Be cautious of unsolicited SMS or emails claiming to be from India Post, especially if it asks for address updates or payments.
- Always verify the sender. For any suspicious communication received, contact India Post customer support directly.



18:17 5G

IDFC FIRST BANK

transactions.

Stay Safe:

- Never share confidential details/OTPs on suspicious links/sites.
- Be cautious of unsolicited SMS or emails claiming to be from India Post, especially if it asks for address updates or payments.
- Always verify the sender. For any suspicious communication received, contact India Post customer support directly.
- Always remove/scribble over shipping labels before throwing away delivery box —they contain personal info.

Protect your personal and financial information.

Please report cyber frauds related complaints on 1930 or at cybercrime.gov.in.

Always You First,
Team IDFC FIRST Bank

18:16

[Know More](#)

सामान्य नेटवर्क खतरे - मैन-इन-द-मिडिल (MITM)

“आपके डिवाइस और इंटरनेट के बीच हैकर”

- **वास्तविक जीवन का उदाहरण:** “एक लड़के ने कैफे में मुफ्त वाई-फाई का इस्तेमाल किया, बाद में उसे पता चला कि उसका सोशल अकाउंट हैक हो गया है।”

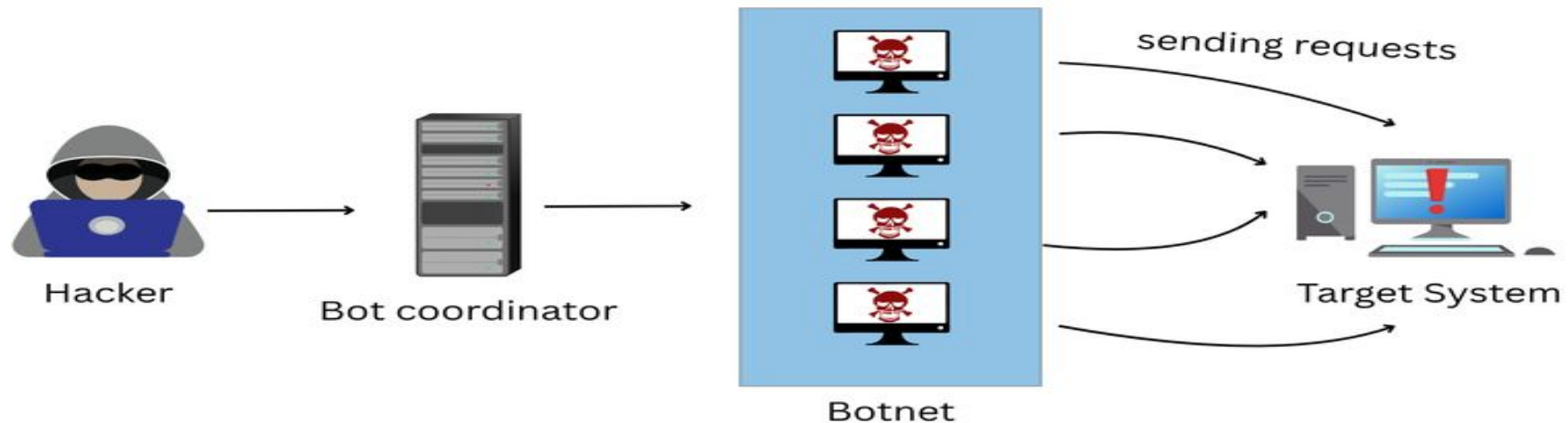


सामान्य नेटवर्क खतरे - डिनायल ऑफ़ सर्विस(DoS)

सरल परिभाषा: "ओवरलोड द्वारा वेबसाइटों को क्रैश करना।"

- वास्तविक जीवन का उदाहरण: परीक्षा के दौरान रिजल्ट वेबसाइट क्रैश हो जाना

How is Botnet Used for DDoS Attack



Reference: UniNets

सामान्य नेटवर्क खतरे - सोशल इंजीनियरिंग

“मशीनों को नहीं, लोगों को धोखा देना”

- उदाहरण: फर्जी बैंक कॉल ओटीपी मांग रहा है

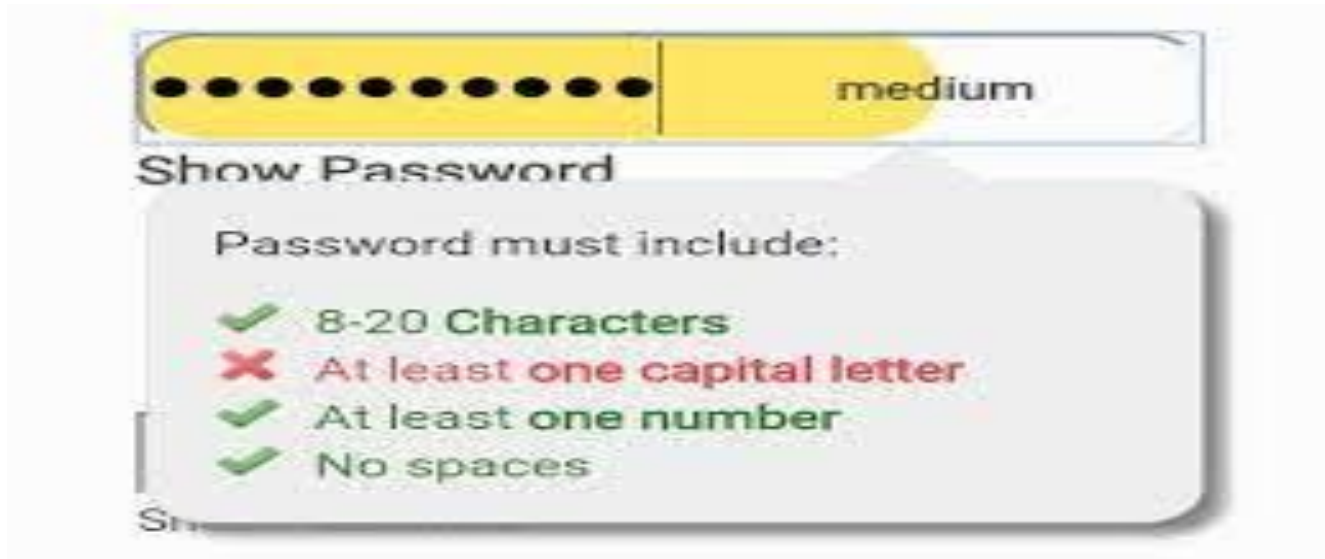


shutterstock.com · 2011026575

रक्षा तंत्र और सर्वोत्तम प्रथाएँ (Best Practices)

1. रक्षा - मजबूत पासवर्ड:

- लंबे, अनोखे और मिश्रित पासवर्ड का इस्तेमाल करें
- मज़ेदार तथ्य: "123456 अभी भी सबसे आम पासवर्ड है"।
- कमज़ोर बनाम मज़बूत पासवर्ड के उदाहरण



रक्षा तंत्र और सर्वोत्तम प्रथाएँ (Best Practices)


2. सुरक्षा - फ़ायरवॉल और एंटीवायरस

- फ़ायरवॉल = गेटकीपर (संदिग्ध ट्रैफ़िक को ब्लॉक करता है)
- एंटीवायरस = डॉक्टर (मैलवेयर का पता लगाता है और हटाता है)

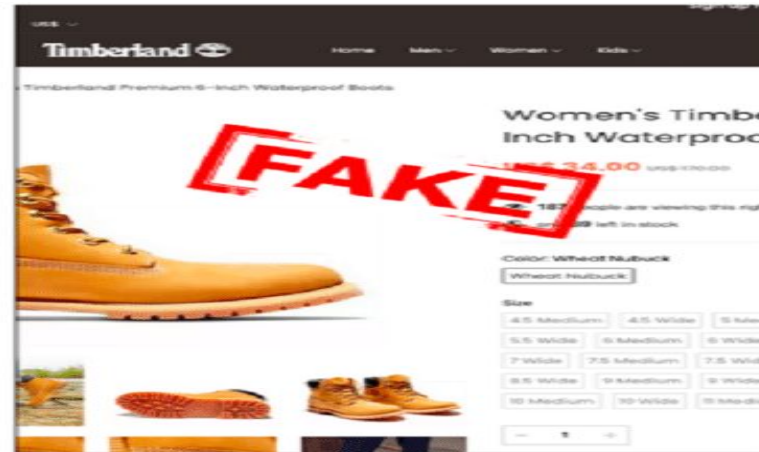


रक्षा तंत्र और सर्वोत्तम प्रथाएँ (Best Practices)

3. रक्षा - सुरक्षित ब्राउज़िंग आदतें:

- HTTPS की जाँच करें 
- अज्ञात लिंक/डाउनलोड से बचें
- पायरेटेड ऐप्स का इस्तेमाल न करें

उदाहरण: नकली बनाम असली शॉपिंग वेबसाइट

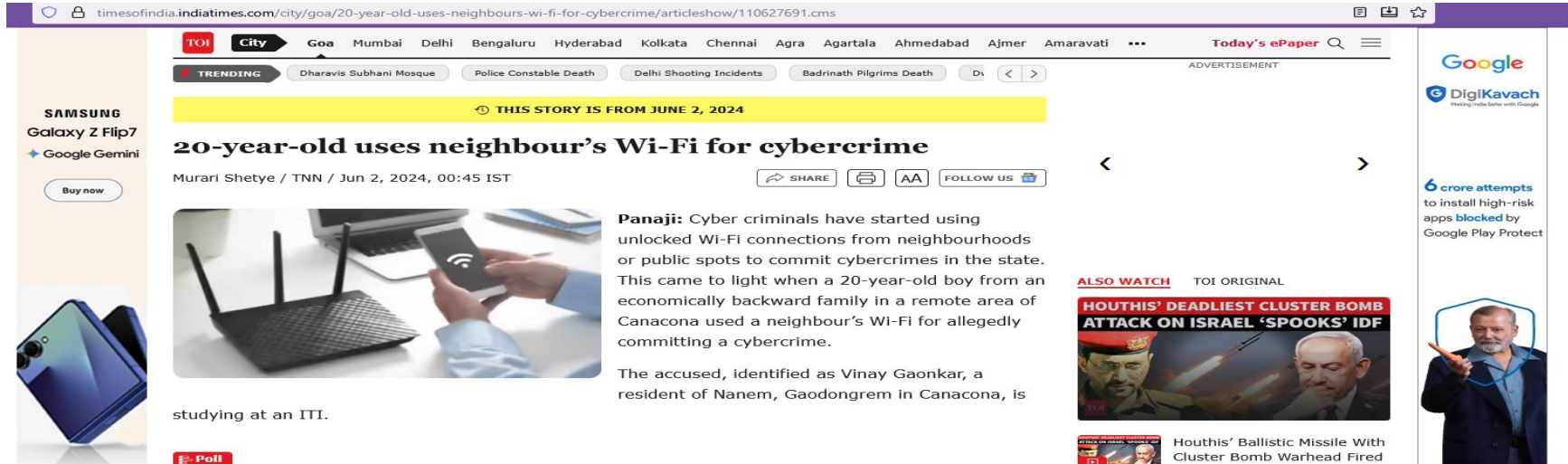


रक्षा तंत्र और सर्वोत्तम प्रथाएँ (Best Practices)

4. रक्षा - सुरक्षित वाई-फाई:

- डिफॉल्ट राउटर पासवर्ड बदलें
- WPA2/WPA3 का इस्तेमाल करें
- वाई-फ़ाई को खुलेआम शेयर न करें

“वास्तविक जीवन की कहानी: एक पड़ोसी अवैध गतिविधि के लिए वाई-फाई का दुरुपयोग कर रहा है।”



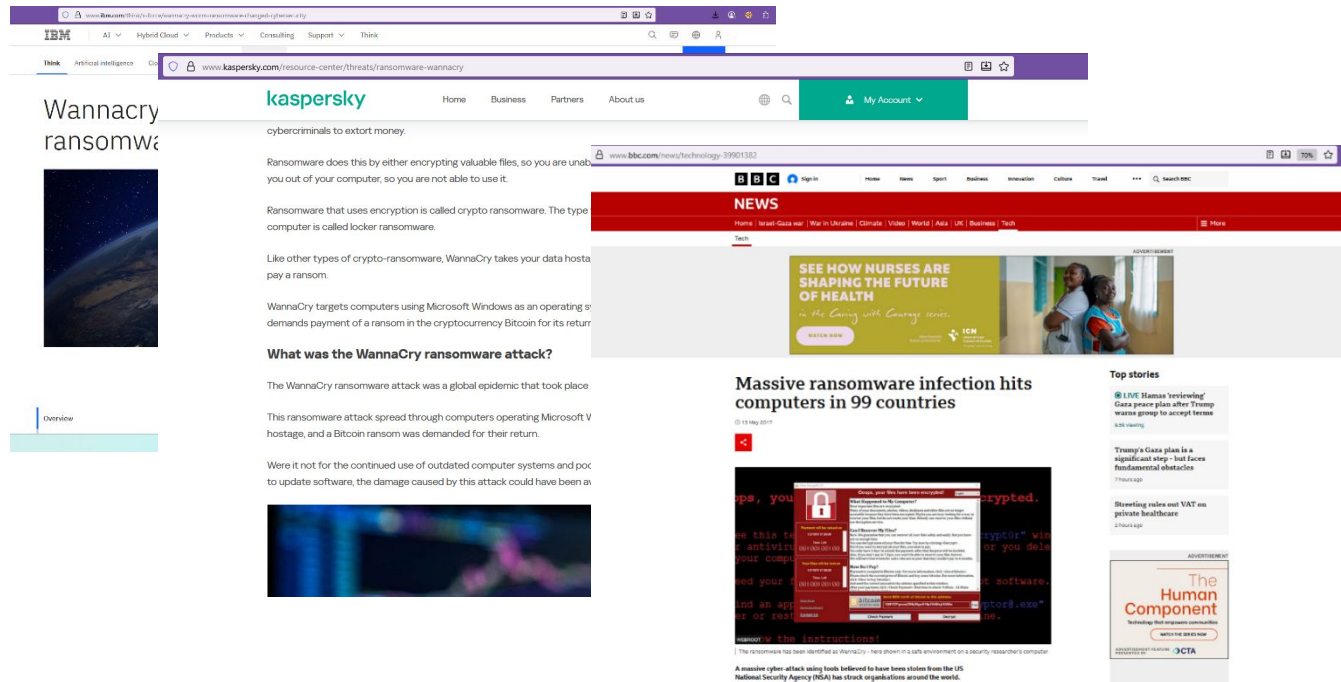
The screenshot shows a news article on the Times of India website. The article is titled "20-year-old uses neighbour's Wi-Fi for cybercrime" and is dated June 2, 2024. The article text states: "Panaji: Cyber criminals have started using unlocked Wi-Fi connections from neighbourhoods or public spots to 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 near a Wi-Fi router. There are also advertisements for Samsung Galaxy Z Flip7 and DigiKavach, and a "Poll" button.

रक्षा तंत्र और सर्वोत्तम प्रथाएँ (Best Practices)

4. रक्षा - बैकअप और अपडेट:

- बैकअप रैंसमवेयर से डेटा बचाते हैं
- अपडेट सुरक्षा खामियों को दूर करते हैं

मामला: अपडेट न होने के कारण WannaCry का प्रसार हुआ



The collage consists of three main parts:

- Top Left:** A screenshot of a Kaspersky article titled "Wannacry ransomware". The article discusses how ransomware works, mentioning encryption and the use of Bitcoin for ransom payments. It also includes a section titled "What was the WannaCry ransomware attack?" which describes the global impact of the attack.
- Top Right:** A screenshot of a BBC News article titled "Massive ransomware infection hits computers in 99 countries". The article reports on the widespread nature of the attack, which affected a significant portion of the world's computers.
- Bottom Center:** A screenshot of a ransomware payment screen. The screen displays a message in Hindi, asking for a ransom payment of 100 Bitcoins. It includes a countdown timer and a warning that the user's files will be deleted if the ransom is not paid.

रक्षा तंत्र और सर्वोत्तम प्रथाएँ (Best Practices)

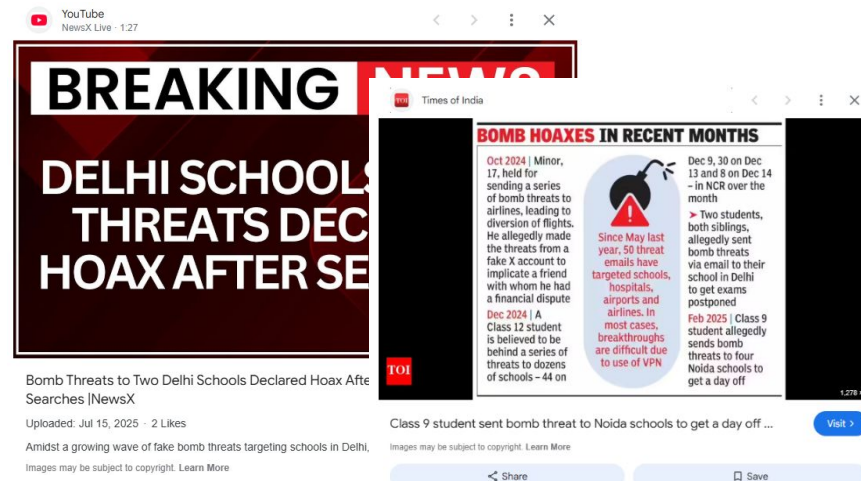
5. रक्षा - छात्रों के लिए साइबर स्वच्छता :

- सोशल मीडिया पर ज़्यादा शेयर (Overshare) न करें
- गेमिंग चैट में सावधानी बरतें
- बुलडिंग या धोखा धड़ी की रिपोर्ट करें



केस स्टडी – दिल्ली-एनसीआर के स्कूलों को भेजे गए फर्जी धमकी भरे ईमेल

1 मई, 2024 को, दिल्ली-एनसीआर के 80-100 से ज़्यादा स्कूलों (प्रमुख स्कूलों सहित) को उनके आधिकारिक ईमेल पतों पर बम की धमकी भरे ईमेल मिले। ईमेल में दावा किया गया था कि परिसर में विस्फोटक रखे गए हैं, जिससे अभिभावकों और छात्रों में दहशत फैल गई; कई स्कूल जल्दी बंद कर दिए गए, कक्षाएं रद्द कर दी गईं और छात्रों को घर भेज दिया गया। धमकी भरे ईमेल एक ही आईपी एड्रेस पर मिले, जो एक रूसी डोमेन (mail.ru) से आया था। जाँच (डॉग स्कवाँड, बम निरोधक इकाइयाँ, पुलिस) के बाद, स्कूल परिसर में कुछ भी संदिग्ध नहीं मिला। धमकियों को अफवाह घोषित कर दिया गया।



The screenshot shows a YouTube video player with a NewsX Live broadcast. The main headline reads "BREAKING NEWS DELHI SCHOOLS THREATS DEC HOAX AFTER SE". Below it, a sub-headline says "Bomb Threats to Two Delhi Schools Declared Hoax After Searches | NewsX". The video is uploaded on Jul 15, 2025, and has 2 likes. A secondary article from Times of India is also visible, titled "BOMB HOAXES IN RECENT MONTHS". This article reports on a series of bomb threats in October 2024, a Class 12 student in December 2024, and a Class 9 student in December 2025 who allegedly sent bomb threats to Noida schools. A red warning icon with a bomb is used to highlight that since May of the previous year, 50 threat emails have targeted schools, hospitals, airports, and airlines, and that breakthroughs are difficult due to the use of VPNs.

केस स्टडी: मोबिक्विक डेटा उल्लंघन (भारत)

- मार्च 2021 में, डिजिटल भुगतान/वॉलेट सेवा मोबिक्विक ने बताया कि लगभग 11 करोड़ उपयोगकर्ताओं का डेटा एक हैकर फ़ोरम/डार्क वेब पर बिक्री के लिए उपलब्ध पाया गया।
- लीक हुए डेटा में संवेदनशील उपयोगकर्ता विवरण शामिल थे: लिंक किए गए मोबाइल फ़ोन नंबर, केवाईसी दस्तावेज़, आधार कार्ड नंबर, क्रेडिट कार्ड की जानकारी।
- **व्यक्तियों पर प्रभाव:**
 - पहचान की चोरी का जोखिम
 - फ़िशिंग / फ़र्जी कॉल
 - वित्तीय धोखाधड़ी
- **हमारे लिए सबक:**
 - अनोखे और मज़बूत पासवर्ड का इस्तेमाल करें
 - ध्यान रखें कि आप किन ऐप्स पर अपना निजी डेटा सुरक्षित रखते हैं
 - स्टेटमेंट और ओटीपी की नियमित निगरानी करें
- **संदेश:**
 - यहां तक कि विश्वसनीय ऐप्स में भी समस्याएं हो सकती हैं; आपकी सतर्कता ही आपकी पहली रक्षा पंक्ति है

साइबर सुरक्षा चेकलिस्ट

- ❑ मज़बूत वाई-फ़ाई पासवर्ड
- ❑ 2FA का इस्तेमाल करें
- ❑ डिवाइस को नियमित रूप से अपडेट करें
- ❑ महत्वपूर्ण फ़ाइलों का बैकअप लें
- ❑ बच्चों को ऑनलाइन सुरक्षा के बारे में शिक्षित करें

प्रमुख टेकअवे

- ❑ खतरे वास्तविक हैं, लेकिन बचाव आसान है
- ❑ जागरूकता ही सबसे अच्छा बचाव है
- ❑ अपनी डिजिटल दुनिया को अपने घर की तरह बंद करें

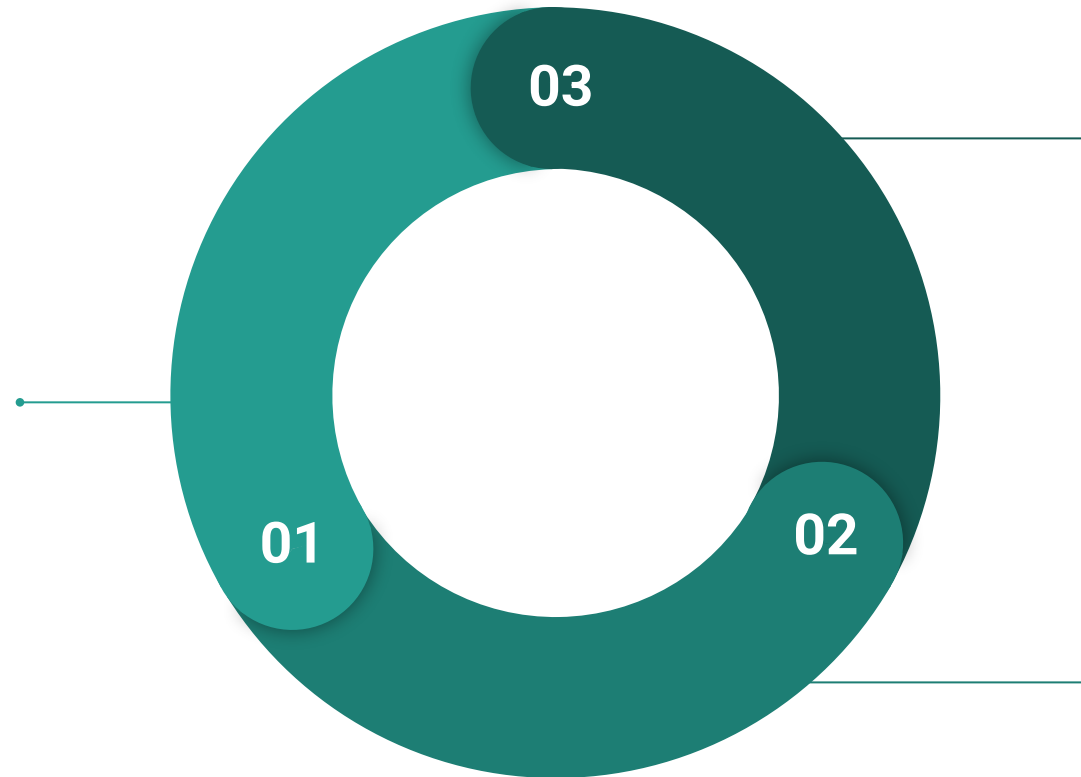
समापन

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](http://www.cybercrime.gov.in)

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





www.isea.gov.in

staysafeonline.in



ISEA Whatsapp Number for Incident Reporting

+91 9490771800



Join our WhatsApp and Telegram Channel at

ISEA - Digital Naagrik



To Share Tips / Latest News, mail us to

isea@cdac.in



[c/InformationSecurityAwareness](https://www.youtube.com/c/InformationSecurityAwareness)



[/company/information-security-awareness/](https://www.linkedin.com/company/information-security-awareness/)



[/infosecawareness/](https://www.facebook.com/infosecawareness/)



[/InfoSecAwa](https://twitter.com/InfoSecAwa)



[/infosec_awareness/](https://www.instagram.com/infosec_awareness/)



[/Informationsecuritytips/](https://www.pinterest.com/Informationsecuritytips/)