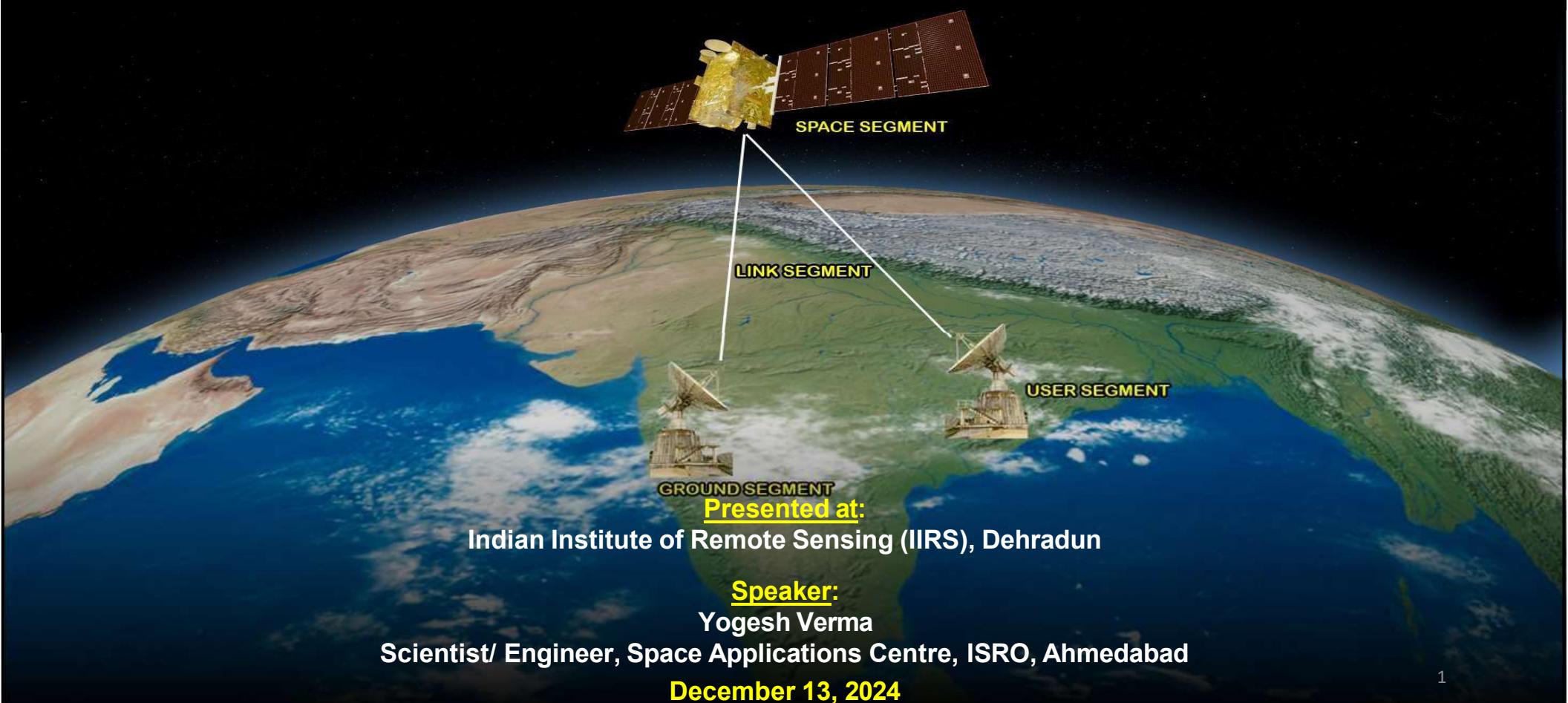


Cyber Security: Threats & Challenges



Overview

- Cyber Security
- Threat Vectors
- Attack Modus Operandi
- Challenges
- Security Measures
- Q&A

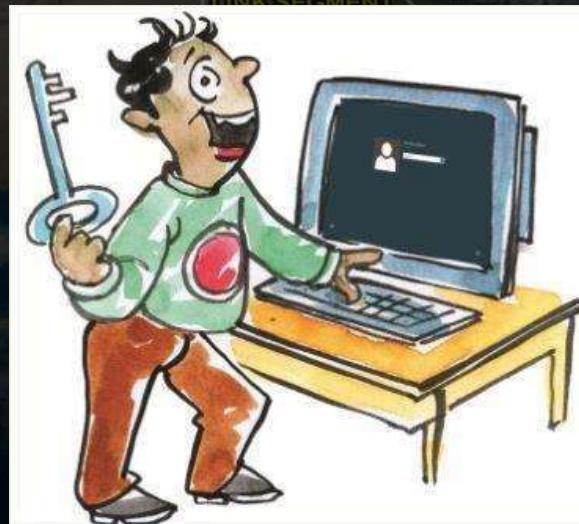


Cyber Security

- **What we need? - Healthy Security Posture** for organisation and user's assets
against relevant security risks in the cyber environment.



Physical Security



System Security



Cyber Security

CIA Triad

Baseline standard for evaluating & **implementing information security**.



Confidentiality – restrict access to unauthorised users
✓ *Encryption, IDs and passwords, MFA and additional defensive strategies.*

Integrity – data or information not altered during its transmission *or at rest* in an unauthorised manner

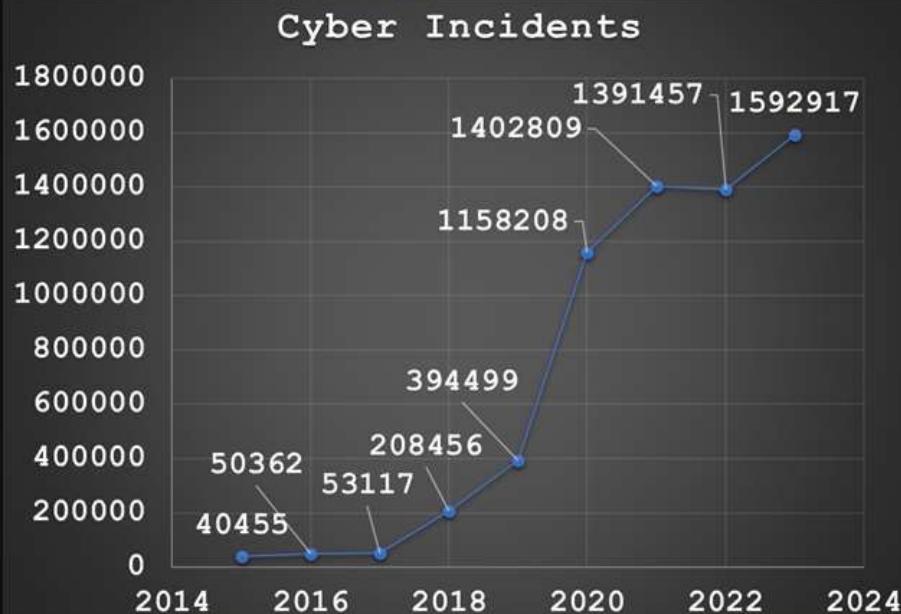
Availability – information can be accessed and modified by authorised users in an appropriate timeframe

Cyber Security Impact

GOVT
AGENCIES
UNDER
ATTACK

Cyberattacks on Indian government agencies more than doubled in 2022

India, US, Indonesia, and China accounted for nearly 40% of the total cyberattacks on government agencies in 2022



Source: Cert-In, NCRP, I4C Portal

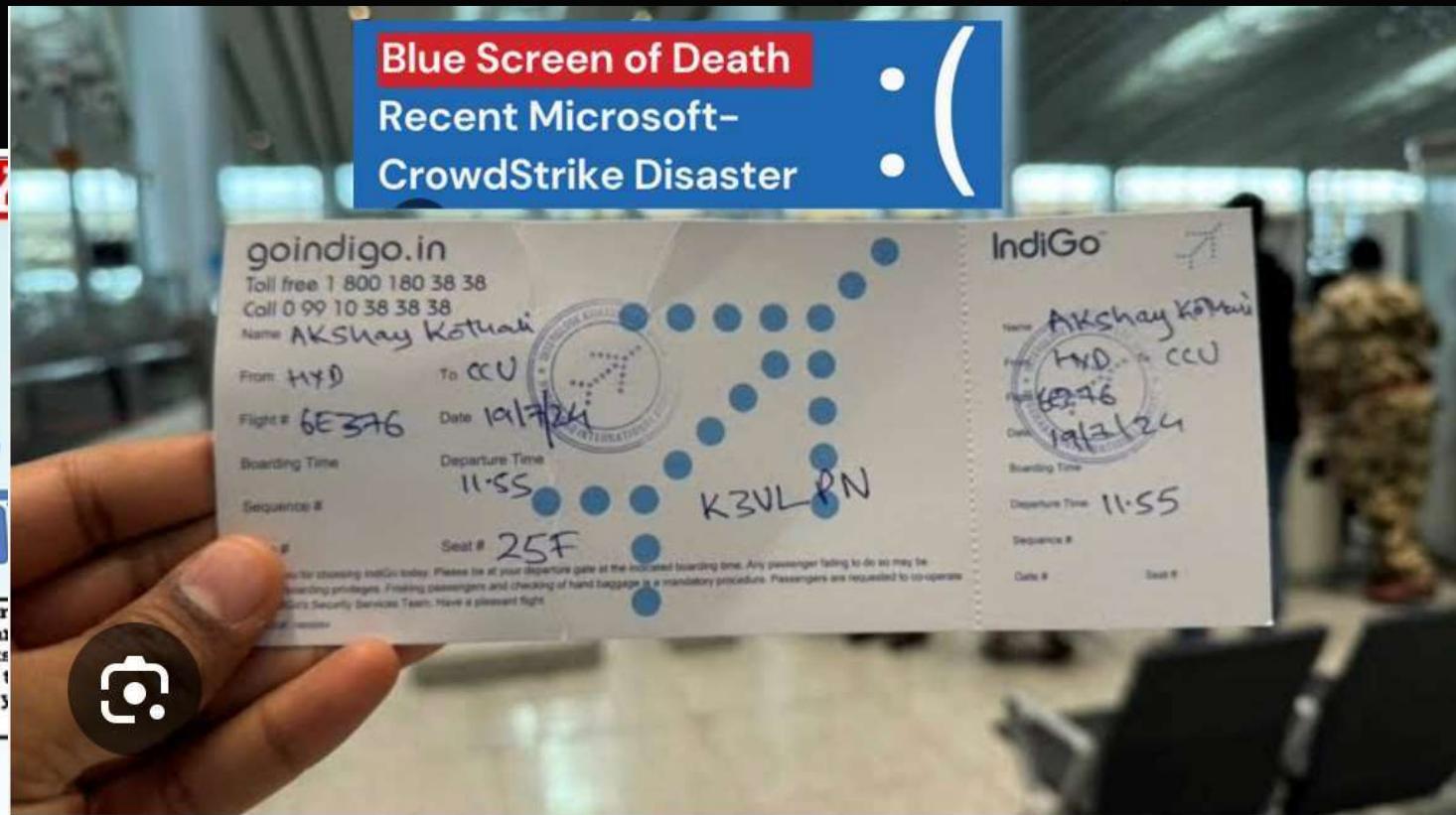


- 6000 complaints reported daily
- Rs. 60 Crore reported loss by Indian Victims daily
- 35% of reported amount more than 50 Lakhs
- 60,000 daily calls on 1930

WHY



① The inter-
up of man-
networks
internet
website
visit



Facebook, Ins
in a massive g
that was sent t

'My first hand-written boarding pass': Flyer shares unique ...

Visit >

e: Fortune Inc.

Cyber Security Facts

Every **39 seconds** there is a cyber attack. **~2200** attacks every day.

3 Lakh new malware is created **every day**.

New Phishing website emerges every 20 seconds.

Trojans account for **58%** of all computer malware.

74% of the breaches confirmed were due to human factor or error.

94% of malware is delivered via Phishing Email.

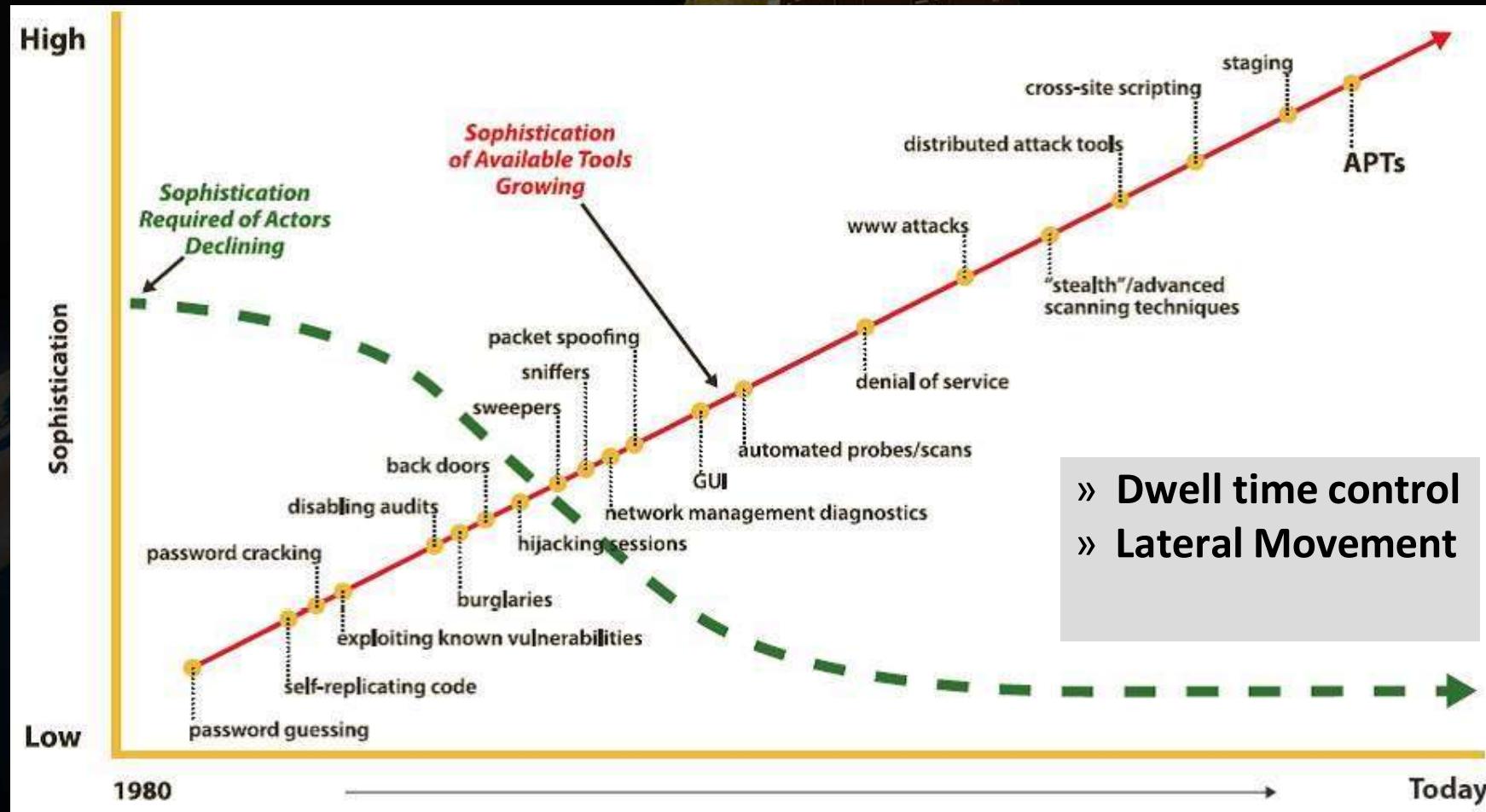
667% increase of targeted phishing attempts during COVID pandemic.

32% of all information breaches involve Phishing

74% of phishing websites are HTTPS

Sources: Statista, Techcircle, Electric.ai, Getstra.com, jumpcloud, DataProt, Cert-In

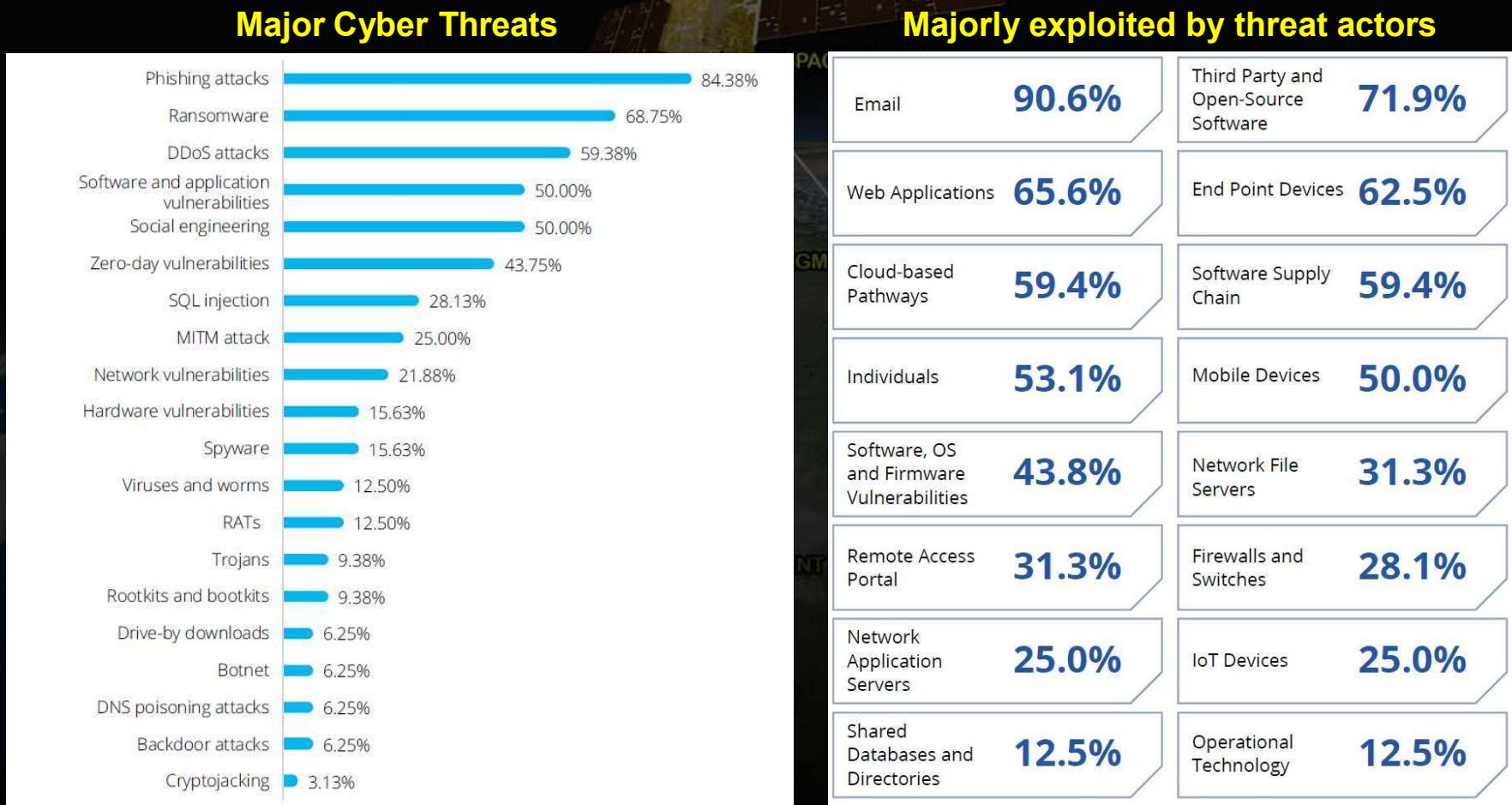
Evolution In Technology & Cyber Threats



Top Cyber Security Threats-2024



Major Cyber Threat Pathways

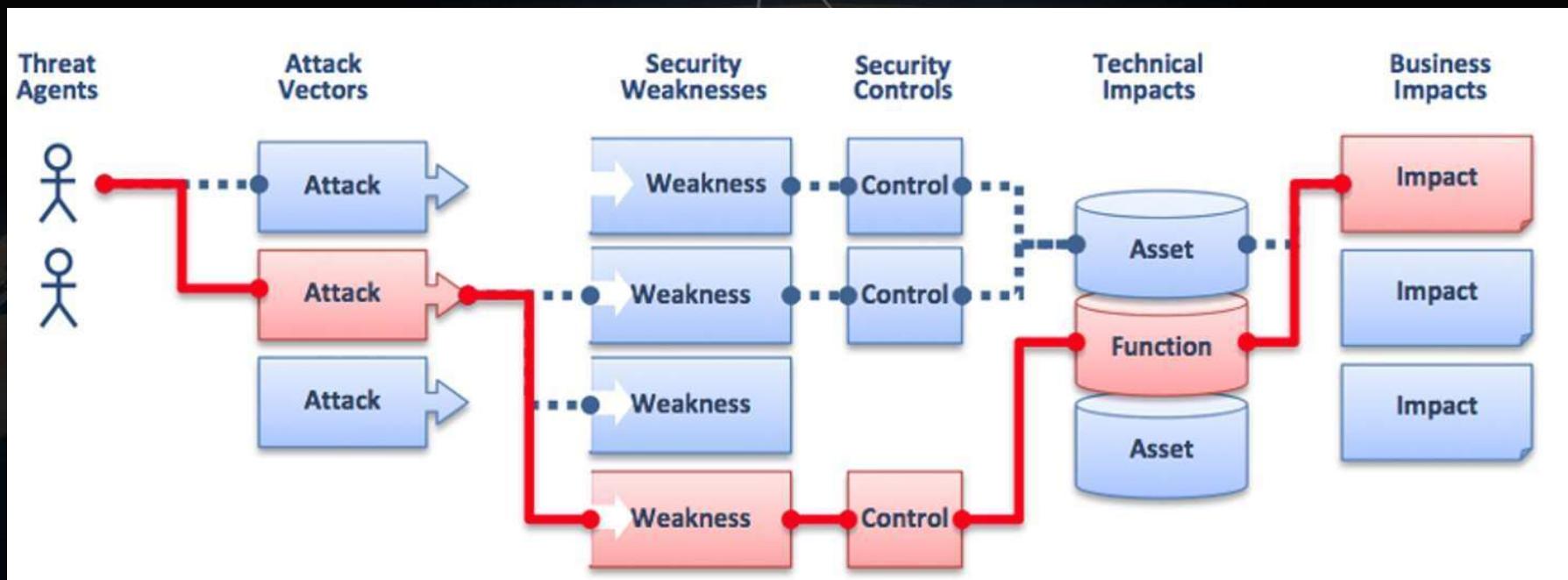


Source – DSCI Survey 2023

10

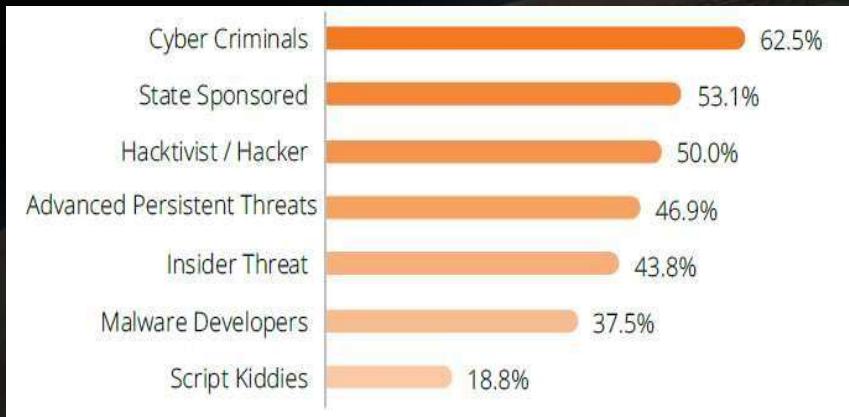
Threat Agents and Impact

- **Threat:** Any **malicious act** that **attempts to gain access** to a end-point, network **without authorisation or permission** from the owners.

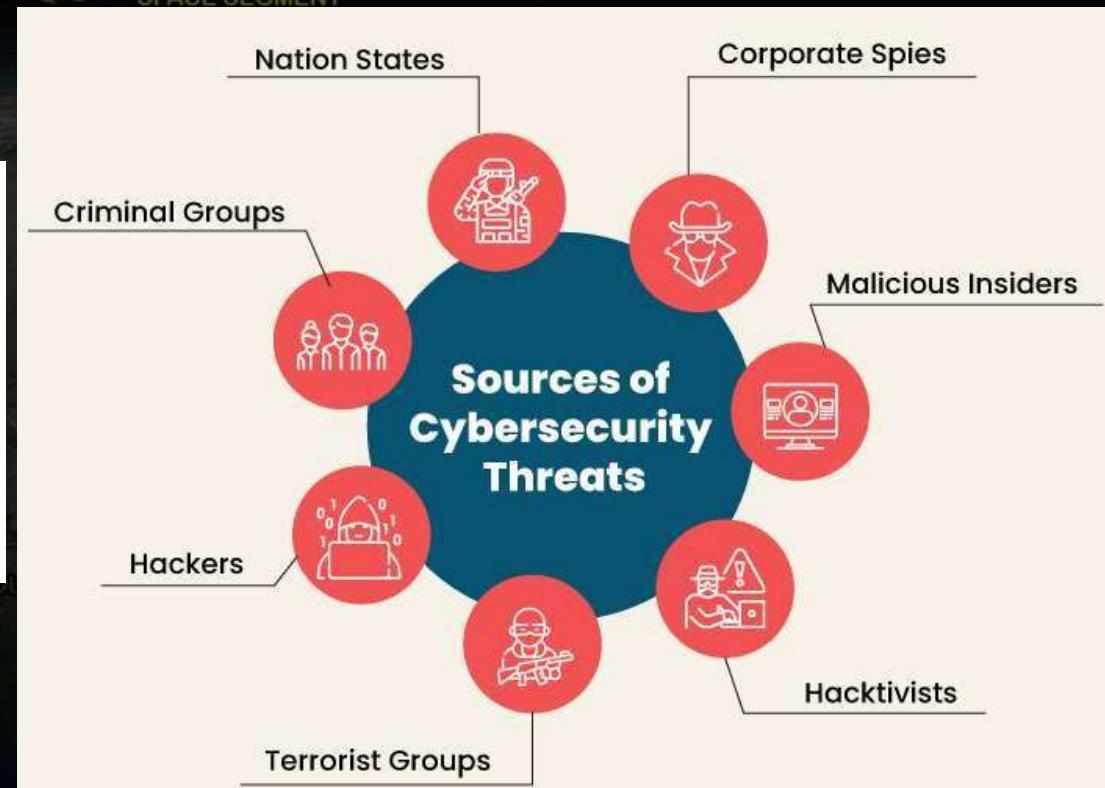


$\text{Risk} = \text{Likelihood} \times \text{Impact}$

Sources of Cyber Threats



Source - DSCI Survey 2023



Cyber Security Challenges

Data Breaches

Unauthorised access or exposure of sensitive information.

01

Malware Infections

Malicious software that compromises system integrity.

03

Social Engineering Attacks

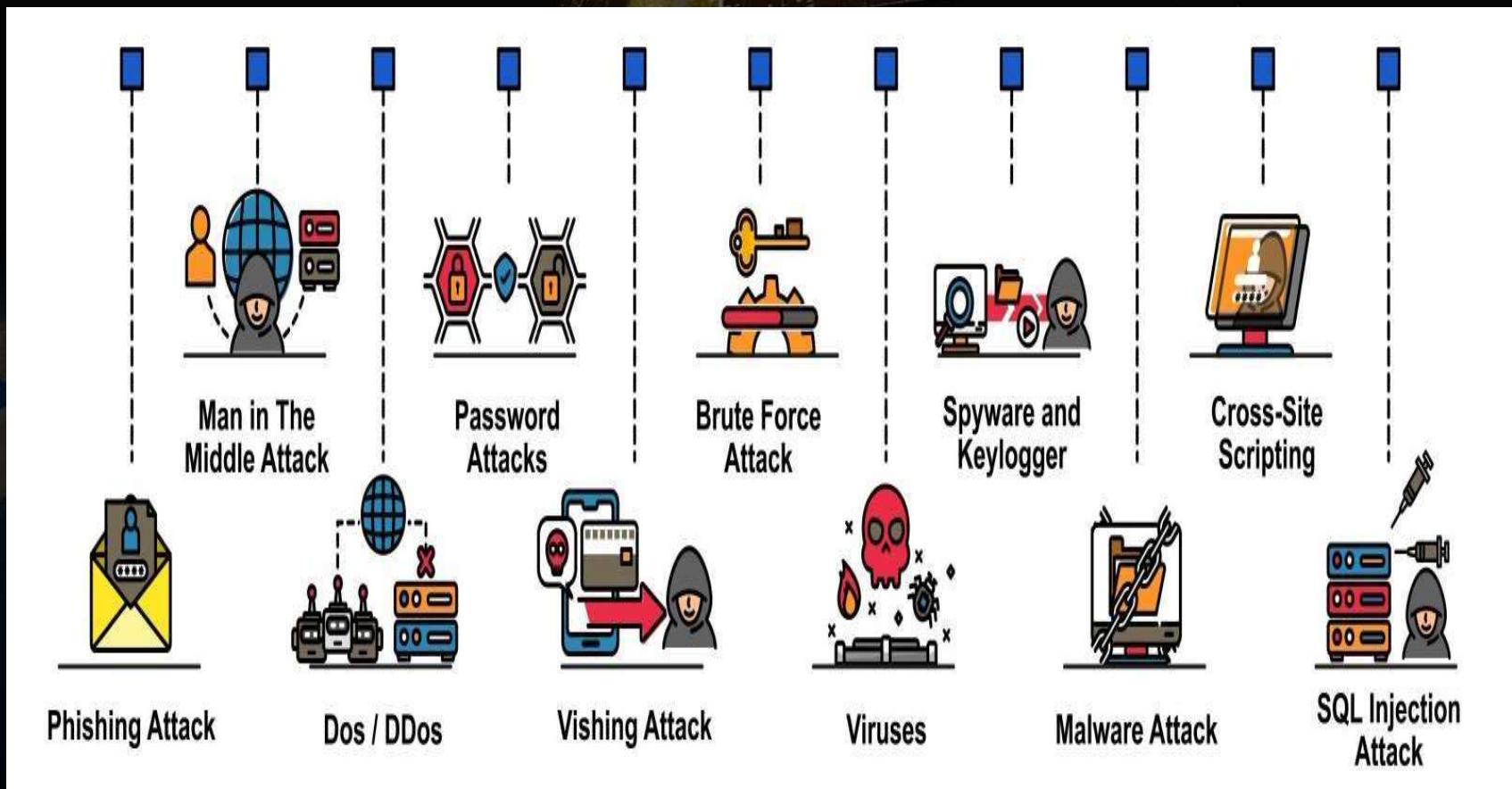
Social Engineering deceptive tactics to trick individuals into sharing confidential data.

04

Insider Threats

Risks posed by authorised individuals with malicious intent.

Cyber Threats & Attacks



Cyber Security Attacks

Deep fake technology

Using AI/ML to create fake audio, video or image content.

01

Zero day attacks

Vulnerability or attack vector is known only to attackers, so that it work without intervention from defenders.

02

03

04

Ransomware attacks evolution

Encrypting data and demanding payment.

Advance Persistent Threat (APT)

Sophisticated targeted attacks.

Social Engineering Attack Techniques

Steal info
on click of a link



False sense of trust (Call by CEO to give some info)

False promise to lure a victim into trap to steal info

Is it a Phishing Email?

From: Remya Mohan Muthadath [mailto:md-nhm@gujarat.gov.in]

Sent: Monday, November 08, 2021 8:35 AM

To: 'noreply@gov.in' <noreply@gov.in>

Subject: Mail Notice!

Importance: High

Sensitivity: Personal



WARNING: Mail Quota Exceeded

Your account has reached its storage limit. You may no longer be able to receive mails. Use the link below to activate a free new quota.

99%

[Activate a new quota here](#)

Thank You,



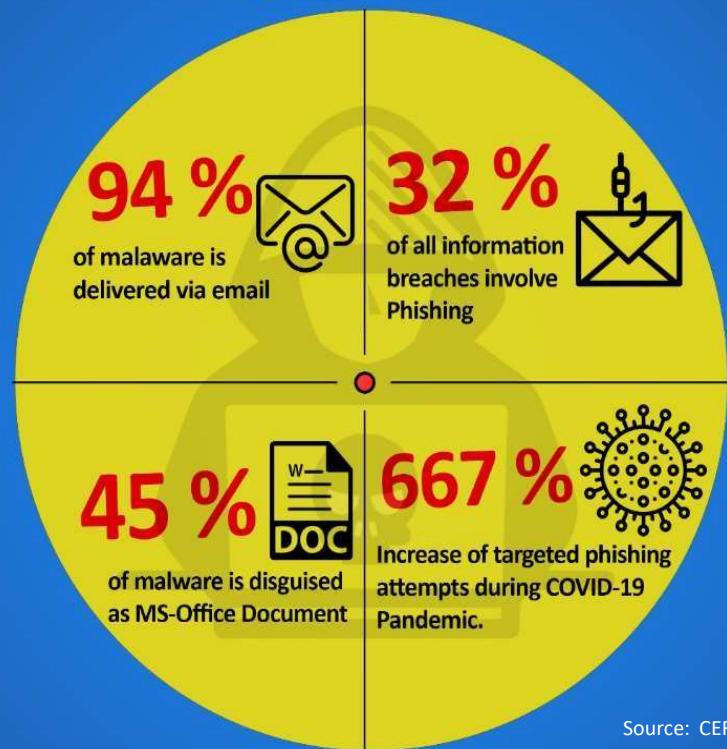
@GOV.IN

<https://email-gov-in.web.app/>.

The image shows two side-by-side screenshots of login pages for the National Informatics Centre (NIC).
The top screenshot, labeled "Spoofed Login page", shows a fake version of the NIC login interface. It features a blue header with the NIC logo and "Digital India" branding. Below the header is a login form with fields for "Email Address" and "Password". The footer contains links to "eGreetings", ".india.gov.in", "Samprak", and "@GOV.in". A banner at the bottom right promotes "Sabka Saath Sabka Vikas Sabka Vishwas Sabka Prayas" and "Azadi Ka Amrit Mahotsav".
The bottom screenshot, labeled "Genuine Login page", shows the official NIC login page. It has a similar blue header with the NIC logo and "Digital India" branding. The login form is identical. The footer includes links to "Website Guidelines", "Help", "Contact Us", "Service Catalog", "Disclaimer", and "Search your NIC coordinator". It also features the same promotional banner for the Azadi Ka Amrit Mahotsav.
A large blue arrow points from the "Activate a new quota here" link in the email body to the URL "https://email-gov-in.web.app/" displayed below it, highlighting the phishing attempt.

Phishing Attack Numbers

Phishing by the Numbers



Phishing the Most Common Cause of Ransom Attacks

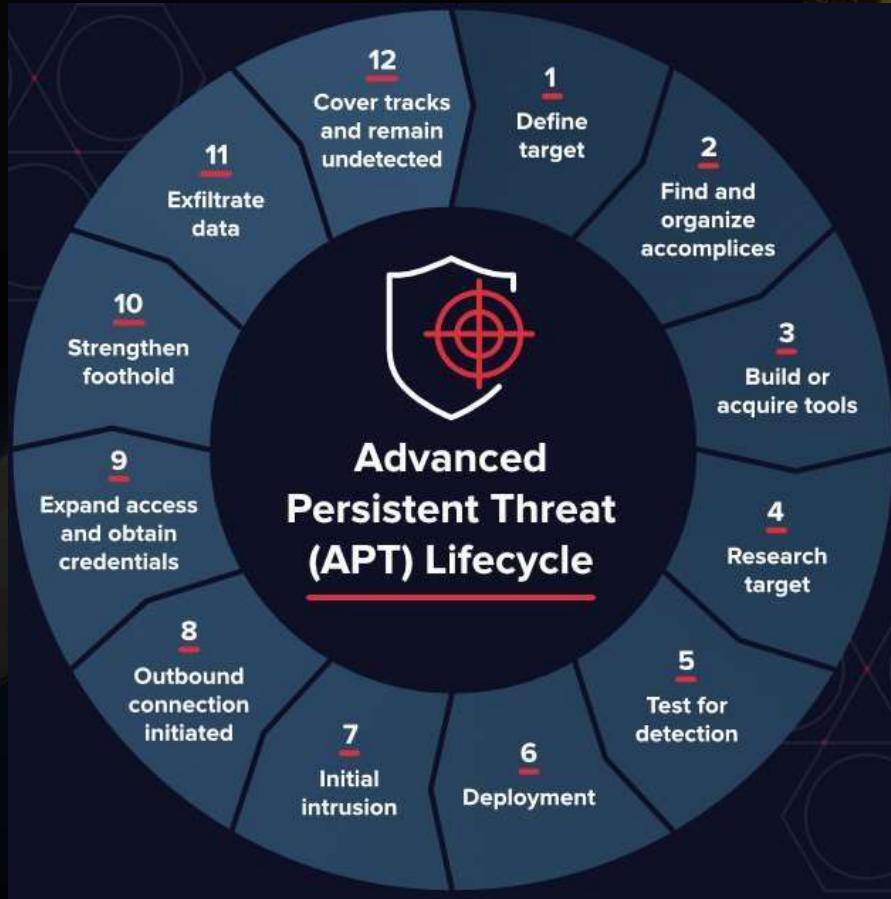
Leading causes of ransomware attacks reported by managed service providers in 2020



Based on a survey of 1,000+ managed service providers conducted in August 2020. Respondents were asked to pick three answers.

Source: Datto

Advanced Persistent Threats



- » **APT:**
 - » SPACE SEGMENT
 - » Dwell time, **204 days**. (APAC)
 - » **Advanced:** Full spectrum of intelligence gathering techniques
 - » **Persistent:** Continuous monitoring and interaction
 - » **Threat:** Specific objectives and well funded
- » **Approach:**
 - » Self-destructing malware and sniffers
 - » File size is small and file names don't raise red flags
- » **Targets:** .mil, .gov sites, defense, CEOs, etc.

Ransomware Attack?

- Encrypts a victim's files or locks the system's screen.
- Attack Vectors:
 - Improperly secured RDP
 - Phishing emails
 - Software flaws
 - Malicious websites or SMS
- In exchange for releasing the data, cybercriminals seek ransom money from their victims.
- **Offline backup** is the protection solution.

Source: checkpoint.com



What is Zero Day Attack?

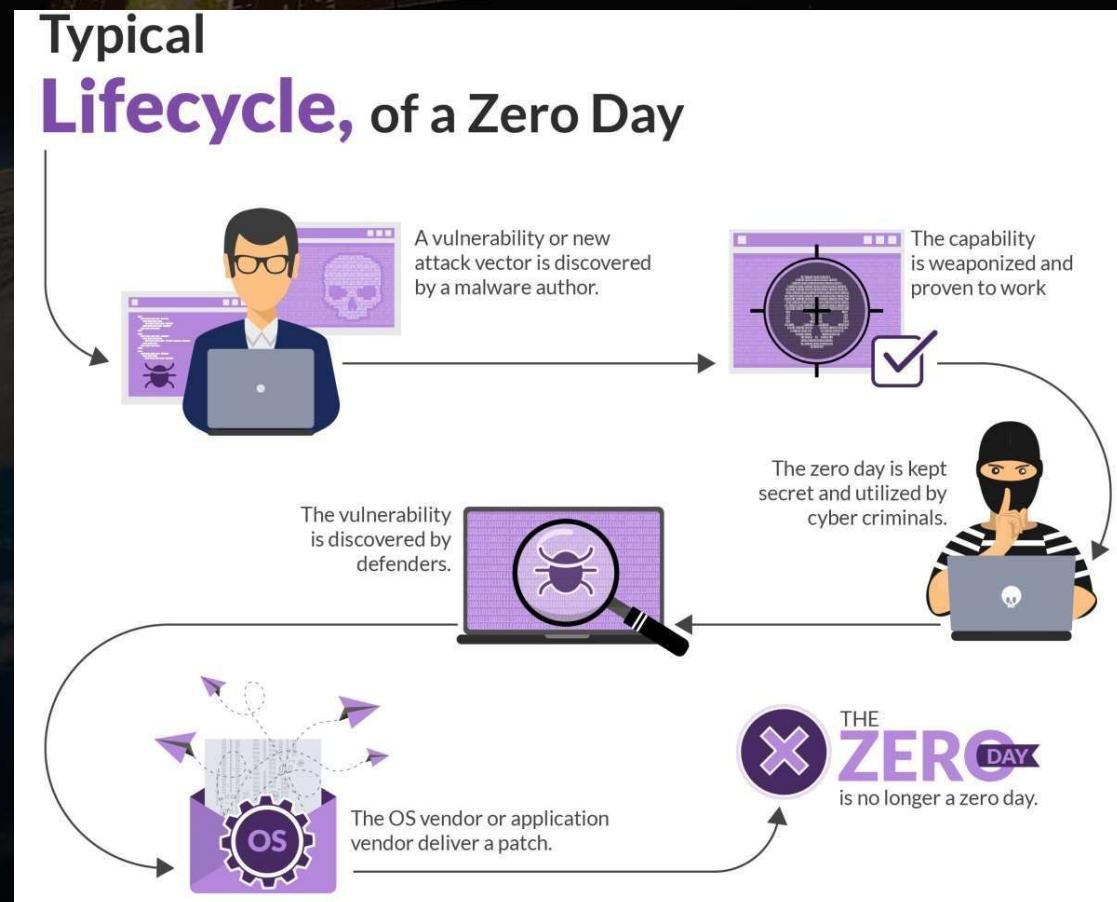
Vulnerability or attack vector is **known only to attackers**, so that it work without intervention from defenders. No patch available.

At least **66 zero-days** have been found to be in use in 2021, which is **almost double** the number of such attacks recorded last year.

Source: MIT Technology Review Report, 2021

97 exploited as zero-days in 2023.

- Source: Mandiant report, 2023



Home / India News / Kerala man loses ₹ 40k to AI-enabled deep-fake fraud

Kerala man loses ₹40k to AI-enabled deep-fake fraud

Jul 18, 2023 01:01 AM IST



By Vishnu Varma

A 73-year-old man in India fell victim to a deepfake scam after receiving a call from someone impersonating his former colleague and asking for money. The scammer used deepfake technology to create a video call in which the impersonator's face and voice matched the victim's former colleague. The victim transferred money before realizing he had been tricked. Police have traced the money to an account in Maharashtra and are investigating further. This is the first reported case of a deepfake scam in India.



- **Deepfake Scam** It is **AI-based technology** used to produce or alter video content so that it presents something that didn't, in fact, occur.
- Deep learning neural networks are used to manipulate video (faces) & audio (voice) by morphing & merging. Voice is overlaid and lips are synced.
- **AI Voice Cloning** to Scam even a few seconds of the person's voice is enough to capture the "essence of that person's voice & then create entirely original statements & conversations with the same frequency, intensity, harmonic structure, tone & inflection"
- **Conclusion:** Deepfaking is becoming a serious cyber crime !! Make sure you understand the difference between the real and fake ones!

Cyber Attacks : Modus Operandi

How We Protect Information?

- People

- Training, education, awareness, repetition

- Process

- Governance, oversight, policy, reporting

- Technology

- Firewalls, IDS/IPS, SIEM, Anti-malware
 - Strong passwords, Logging/monitoring

- Which is the weakest link?



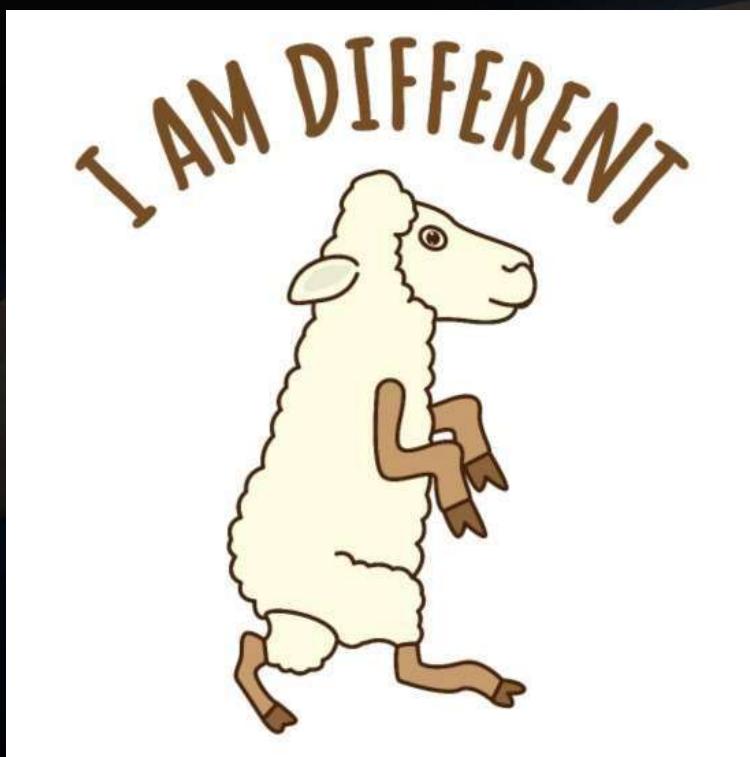
Can You Read This?

I cn duo't bvleiee taht I culod aulacly uesdtannrd waht I was rdnaieg. Unisg the icndeblire pweor of the hmuun mnid, aocdcnrig to rseecrah at Cmabrigde Uinervtisy, it dseno't mttaer in waht oderr the Iterets in a wrod are, the olny irpoamtnt tihng is taht the frsit and lsat ltteer be in the rhgit pclae. The rset can be a taotl mses and you can stil raed it whoutit a pboerm. Tihis is bucseae the huamn mnid deos not raed ervey ltteer by istlef, but the wrod as a wlohe. Aaznmig, huh? Yaeh and I awlyas tghhuot slelinpg was ipmorant!

- **HUMANS** are product of evolution.
- Majority of the human brains will REACT similarly under a given situation.

Root Cause of The Problem?

- Human reaction?
- [CRITICAL VULNERABILITIES EXPOLITED BY SCAMSTERS]

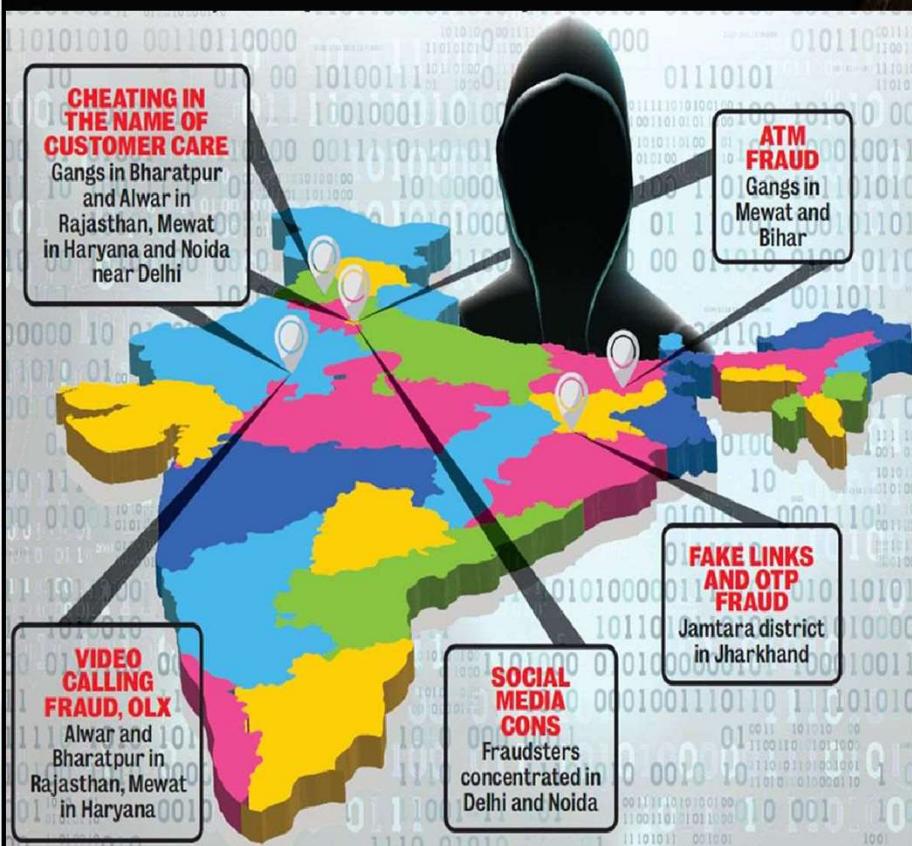


Criminals deceive the human mind by manipulating emotions.

Exploiting emotions leads to computer frauds and cyber crimes:

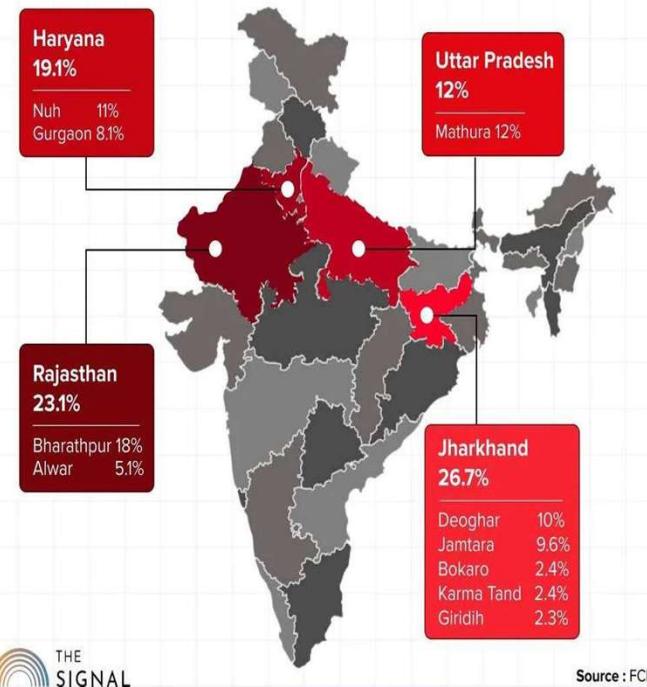
- Trust (Calling from bank, link for payments)
- Greed (Winning Lottery, Inheritance, free or extremely lucrative deals)
- Panic (Card or account blocking, account hacked being misused)
- Fear and Fear of Missing Out (offer expiring in minutes)
- Threat (someone injured or hospitalised, near and dear one is danger)
- Disruption (RFID Tags, Demonetisation, Car key Fobs)

Crime Hotspots in India



India's Cybercrime Hotspots

These districts make up 80% of India's reported cybercrimes

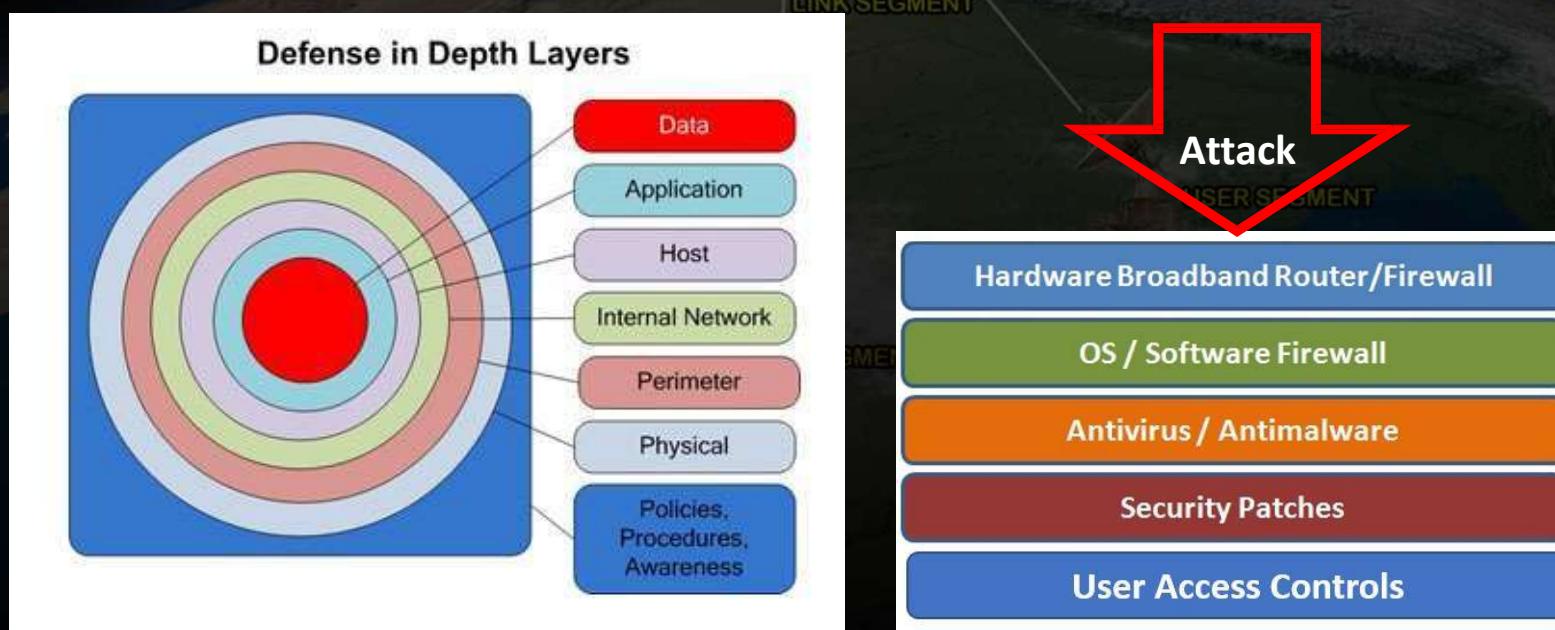


- Jamtara, JH
- Mewat, HR
- Bharatpur & Alwar, RJ
- Noida, Delhi
- Motohari, Bihar

10 Districts account for 80% of cyber crime cases in the country

Security Measures

**Defense in depth is the Best line of control that
Uses multiple layers of defense to address technical, personnel and
operational issues.**



Attack Surface

SPACE SEGMENT

Network insecurities

Open ports

Weak protocols

Software bugs

Insufficiently secured in-house-developed applications

Vulnerable commercial programs (e.g., WordPress, etc.)

Physical security loopholes

Rogue or dissatisfied current and former employees

Openly displayed login credentials (e.g., username-password combinations on sticky notes, etc.)

Social engineering-prone people

Reused or recycled passwords

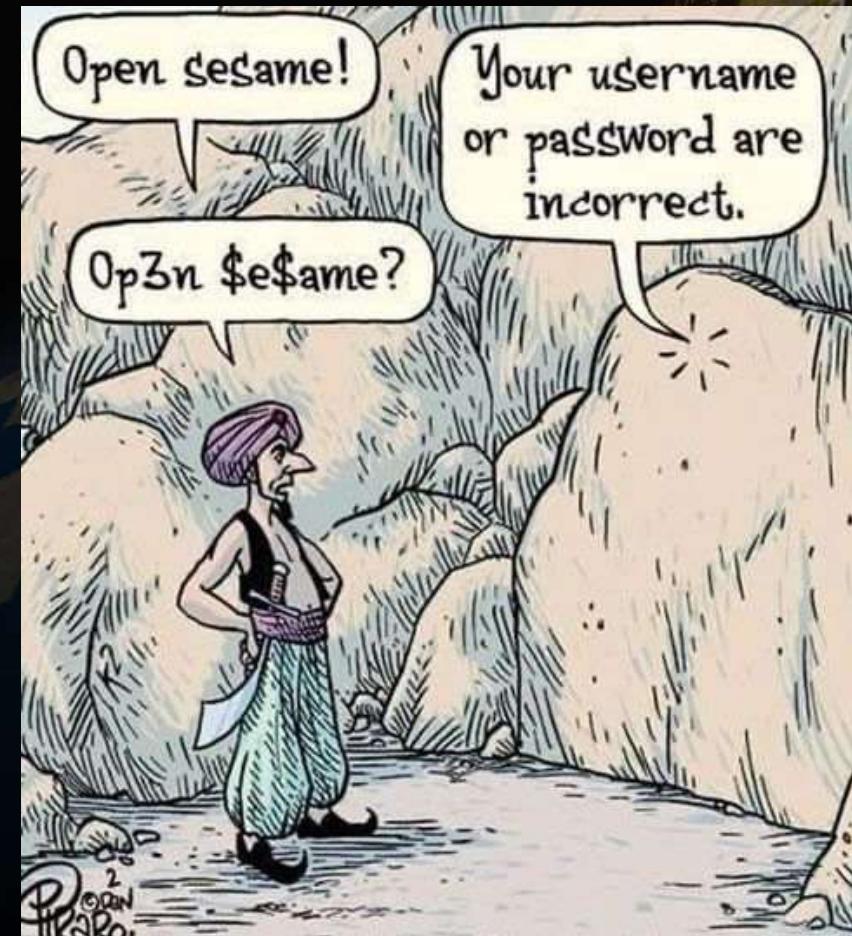
Unmonitored use of social media and unprotected personal devices

Secure Coding Practices



- » Design as per **security policies**
- » Default **deny**
- » Adhere **least privilege policy**
- » **Sanitise data**
- » Practice **defense in depth**
- » **Static/dynamic code analysis** to eliminate security flaws
- » Adopt a **secure coding** guidelines
- » **Threat modeling**
- » **Risk Management**

Guess the Story?



SPACE SEGMENT

» MORAL OF THE STORY

» ALI BABA 40 CHOR

» DON'T SHARE your password

» DON'T SHARE In Public

» UPDATE Password regularly

» KEEP Strong Password

» AUTO-LOCK Your System

» KEEP IDENTITY Safe

SEGMENT

USER SEGMENT

Enable MFA



Enabling MFA makes you significantly less likely to get hacked.

And That is Why...

You should enable **Multi-Factor Authentication**. This will help to **protect your account** if your password was stolen or leaked in a data breach.

Multi-Factor Authentication (MFA)

Double your Login protection / Lock down your login

IS ALL ABOUT YOU

Something you know, or
“knowledge factor.”



who **YOU** are

- fingerprint scanners
- voice verification
- facial recognition

Something you know, e.g:
“Password”

Something you have, or
“possession factor.”



what **YOU** know

- security questions
- passwords and passphrases
- PINs

Something you possess, e.g:
“Mobile phone”

Something you are, or
“inherence factor.”



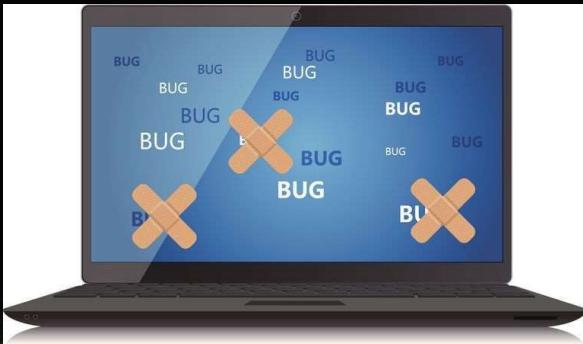
what **YOU** own

- SMS authentication
- application-based authenticators
- hardware tokens

Something you are, e.g:
“Fingerprint”



Update Software



- Update **Operating System** on your devices.
- Update your **applications**- especially web browsers.



Use Official USBs



**USB Drives may contain malware- Report to IT team.
Use Official drives in systems.**

Google Search Scam

Some of the **top search results** in Google are phishing links.

Scammers also invest in **search engine optimization** techniques & work hard to rank their scam sites in the top search results.

Fraudulent Medicare or health insurance websites. Criminals may also target your healthcare information by creating fake websites that ask you to "verify" your **Medicare number**.

Fake **customer support websites**, Scammers pretend to be from technical support companies and get you to give them **remote access to your computer**.

1

Search Result Shows Brand

Title displays correct brand name

2

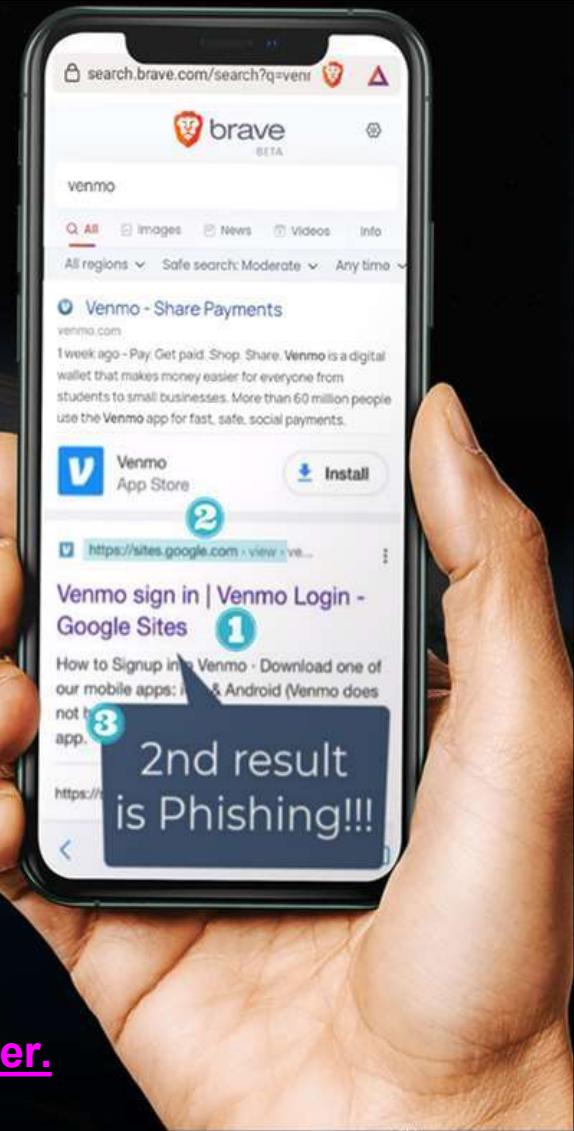
URL Mismatch

Title says Venmo but URL is a generic sites.google.com

3

2nd Result for Organic Search

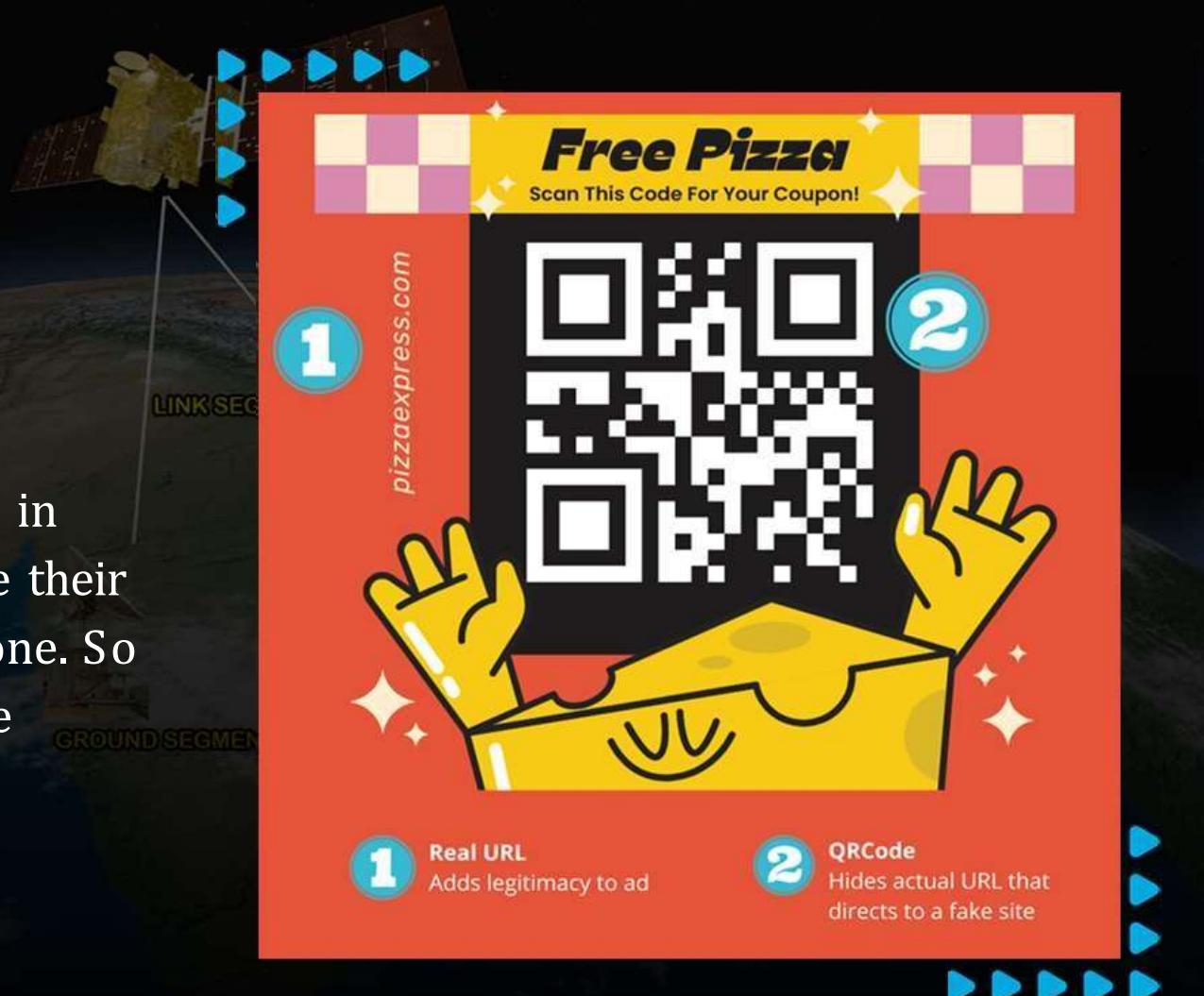
Even top search results can be manipulated for fake sites



QR Code Scam

Who thought a QR code could be dangerous?

They are everywhere, especially in restaurants. Criminals can place their own sticker over the legitimate one. So that when you scan it, you will be **redirected to a fake site.**



Exercise:1 ऐया आप का ईमेल या मोबाइल से कभी Data Breach हुआ ह? Check it out

12 BILLION Accounts were stolen from hacked sites & apps So even if you have a **STRONG PASSWORD**, it may still not be enough. **Check if yours account was leaked at**

<https://haveibeenpwned.com>

The image contains two side-by-side screenshots of the Have I Been Pwned website. Both screenshots show a search bar at the top with the placeholder "Your-email-ID" and a blue button labeled "pwned?".

Screenshot 1 (Top): The background is green. It displays the message "Good news — no pwnage found!" and "No breached accounts and no pastes (subscribe to search sensitive breaches)". Below this, there's a section titled "3 Steps to better security" with three steps: 1. Protect yourself using 1Password to generate and save strong passwords for each website. 2. Enable 2 factor authentication and store the codes inside your 1Password account. 3. Subscribe to notifications for any other breaches. Then just change that unique password.

Screenshot 2 (Bottom): The background is red. It displays the message "Oh no — pwned!" and "Pwned in 1 data breach and found no pastes (subscribe to search sensitive breaches)". Below this, there's a section titled "3 Steps to better security" with the same three steps as the first screenshot.

The image shows the main page of the Have I Been Pwned website. At the top, there's a navigation bar with links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main heading is "';--have i been pwned?" with a subtitle "Check if your email or phone is in a data breach". Below this is a search bar with the placeholder "email or phone (international format)" and a blue "pwned?" button.

On the right side, there are several statistics:

Category	Value
646	pwned websites
12,441,647,441	pwned accounts
115,587	pastes
227,248,018	paste accounts

Below the statistics, there are sections for "Largest breaches" and "Recently added breaches", each listing several breached datasets with their respective counts and logos.

आप पासवड कितना Secure है? Check it out at

passwordmonster.com

info@passwordmonster.com

How Secure is Your Password?

Take the Password Test

Tip: It's often better to have longer passwords than shorter, more complex ones

Show password:

Indiadigital234!

Weak

16 characters containing:

Lower case

Upper case

Numbers

Symbols

Time to crack your password:

1 hours

Review: Oops, using that password is like leaving your key in the lock. Your password is weak because it contains a female name, a common password, a sequence of characters and a dictionary word.

Your passwords are never stored. Even if they were, we have no idea who you are!

Almost Everything Google know about you...Seriously – Everything !! (since 2 decades)

Especially if you use Google's products like; Android, Gmail, Google Drive, Google Maps, YouTube, Google Search

<https://myactivity.google.com/myactivity>

Activity controls

The data saved in your account helps give you more personalized experiences across all Google services. Choose which settings will save data in your Google Account.

Safe with Google
You control what data gets saved to your account. [Learn more](#)

Web & App Activity
Saves your activity on Google sites and apps, including associated info like location, to give you faster searches, better recommendations, and more personalized experiences in Maps, Search, and other Google services. [Learn more](#)

Subsettings

Include Chrome history and activity from sites, apps, and devices that use Google services

Include voice and audio activity. [Learn more](#)

Auto-delete (On)

Deleting activity older than 3 months

Manage all Web & App Activity

Cancel Next

Some activity may not appear yet

My Google Activity

The activity you keep helps Google make services more useful for you, like helping you rediscover the things you've searched for, read, and watched.

You can see and delete your activity using the controls on this page.

Web & App Activity Location History YouTube History

On On On

Google protects your privacy and security. [Manage My Activity verification](#)

Search your activity

Filter by date

Web & App Activity Location History YouTube History

Off Off Off

Some activity may not appear yet

Pause Location History

Pausing Location History may limit or disable personalized experiences across Google services. For example, you may not see recommendations based on places you've visited or helpful tips about your commute.

This setting will be paused on all sites, apps, and devices signed in to this account.

This setting does not affect other location services on your device, like Google Location Services and Find My Device.

Your location may still be saved in your Google Account when using other Google sites, apps, and services. For example, location data may be saved as part of activity on Search and Maps when your Web & App Activity setting is on, and included in your photos depending on your camera app settings.

Pausing this setting doesn't delete any of your past data. You can see or delete your data and more at [maps.google.com/timeline](#).

Visit [account.google.com](#) to change this and your other Google Account settings and learn about the data Google continues to collect and why at [policies.google.com](#).

Cancel Pause

Choose an auto-delete option for your Web & App Activity

Auto-delete activity older than 3 months

Don't auto-delete activity

Regardless of your choice, you can always manually delete any time

COMMON QUESTIONS

What's Web & App Activity?

How long is right for me?

How else can I control my data?

Cancel Next

आप के
है?

नाम/आधार पर कितने मोबाइल नंबर और लिंक चलता

The screenshot shows the TAF COP platform. On the left, there are two cards: one orange card showing '599936 requests received' and one green card showing '18963 requests resolved'. The main right section has a heading 'TAF COP' with a SIM card icon. Below it, a sub-instruction reads: 'Know the number of connections issued in your name by logging in using your mobile number'. A large input field for a '10 digit Mobile number' is followed by a CAPTCHA input field containing 'G T W N L S J'. Below these are 'Enter Captcha' and 'Validate Captcha' buttons. An 'OTP' input field with a 'Resend OTP' link and a 'Login' button are at the bottom.

SANCHAR SAATHI ABOUT CITIZEN CENTRIC SERVICES KEEP YOURSELF AWARE FAQs IN SOCIAL MEDIA AUTHORIZED LOGIN

TAF COP

Know the number of connections issued in your name by logging in using your mobile number

599936
requests received

18963
requests resolved

10 digit Mobile number

G T W N L S J

Enter Captcha

Validate Captcha

OTP

Resend OTP

Login



india.gov.in



SANCHAR SAATHI

ABOUT

CITIZEN CENTRIC SERVICES

KEEP YOURSELF AWARE

FAQs

IN SOCIAL MEDIA

AUTHORIZED LOGIN

Welcome : 919

707 2:31



 Not My Number

 Not Required

 Required

Mobile numbers registered in your name : 1

Request Number

Track

9199XXXX8707

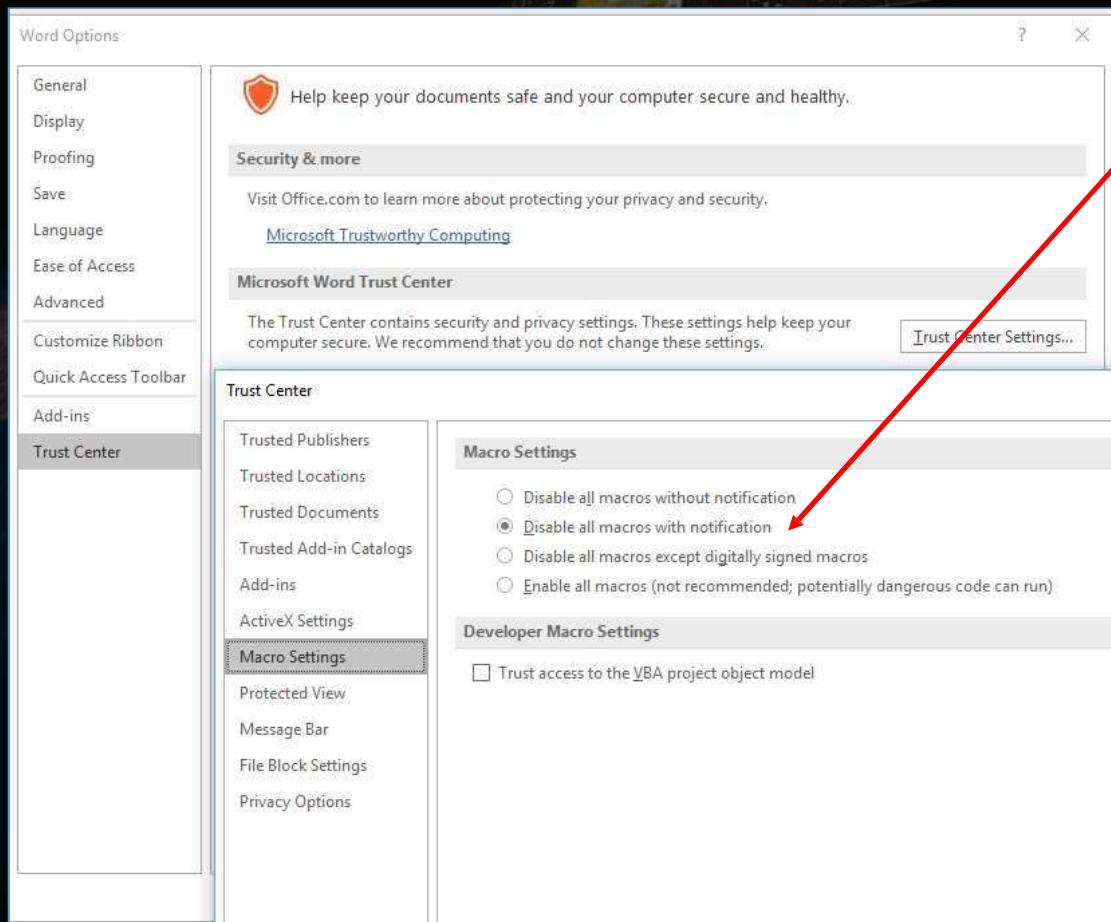
Not My Number

Not Required

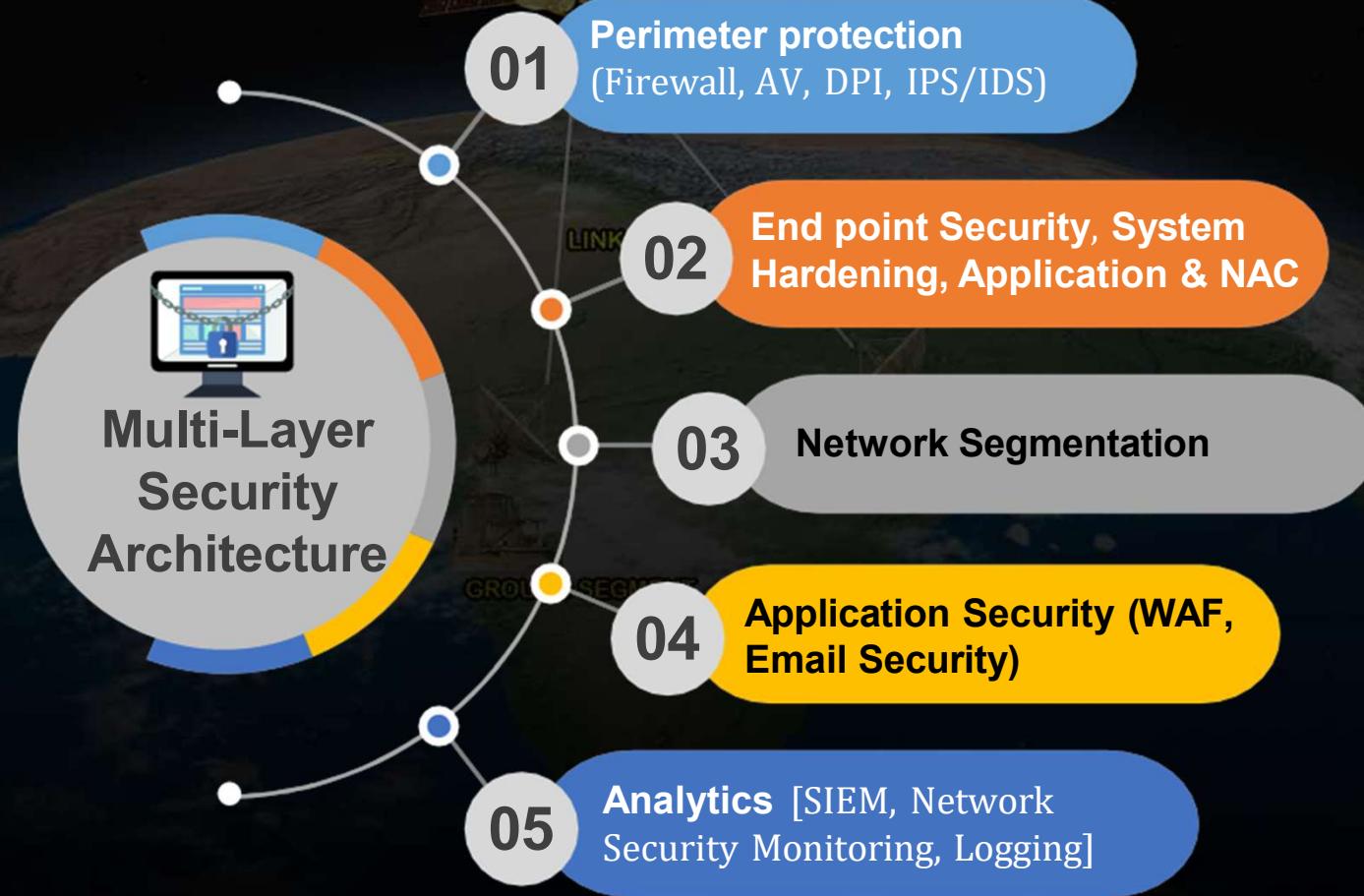
Required

Report

Exercise:5 Microsoft Office- Keep All macros disabled



Security Controls



Security Controls



Cyber Awareness Activities & Incident Reporting

06

01

Principle of Least privilege

VAPT, Mock Drills, Inter-Centre Audits, 3rd Party Audits

05

02

Air-Gapped Networks

Patch Management

04

03

Secure Code Practices

