Cyber Security: Threats & Challenges

Presented at:
Indian Institute of Remote Sensing (IIRS), Dehradun

Speaker:
Yogesh Verma
Scientist/ Engineer, Space Applications Centre, ISRO, Ahmedabad

December 13, 2024

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**.

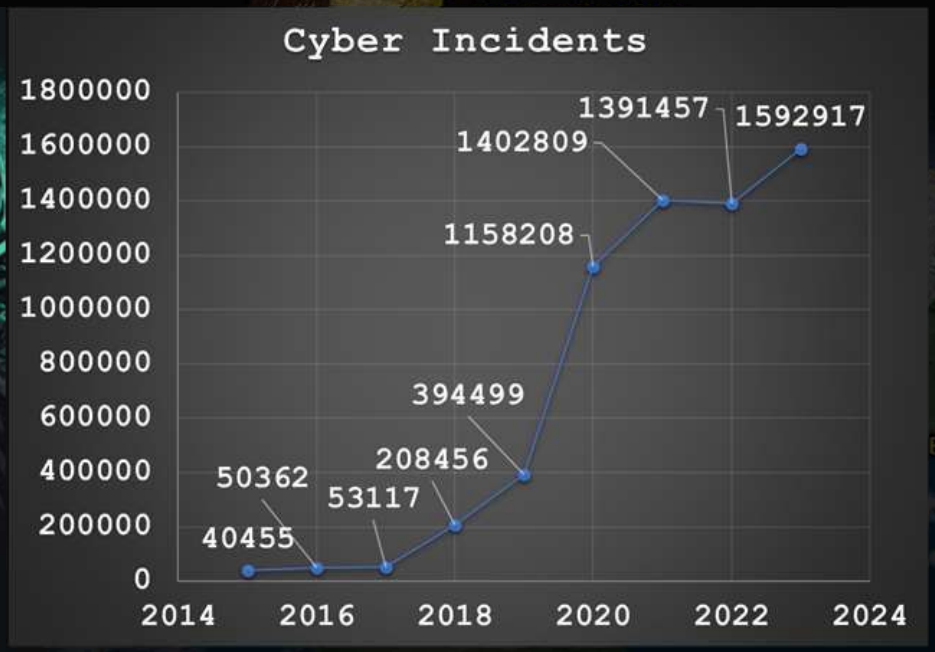
Confidentiality – restrict access to unauthorised users

✓ *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

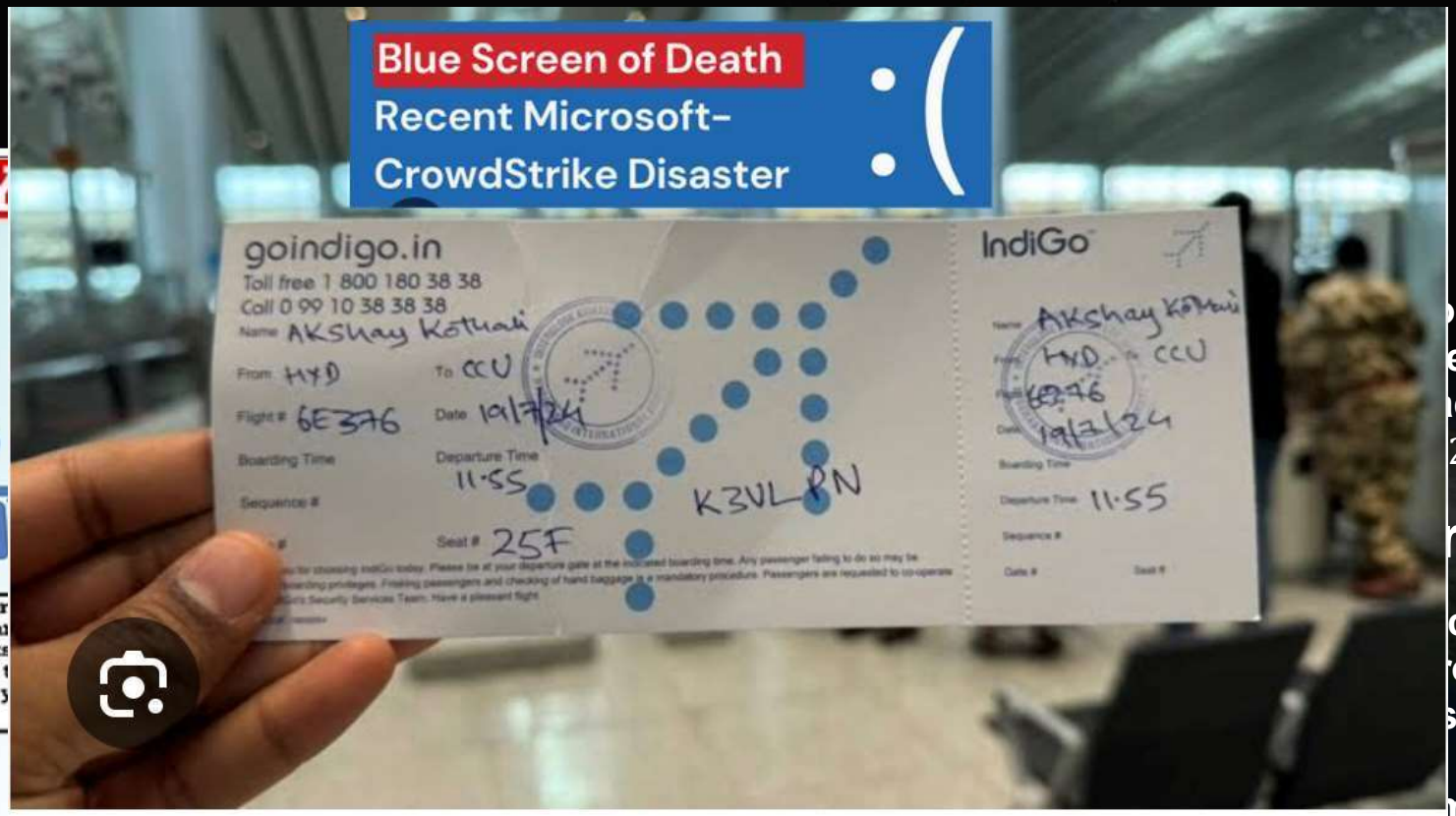
Availability – information can be accessed and modified by authorised users in an appropriate timeframe

Cyber Security Impact



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



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

Visit >

WHY

1 The inter up of ma networks internet website visit

Facebook, Ins in a massive g that was sent

onfiguration
ers and
ck after 7
21)

rs:

crore
ore
s

million (ad

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.

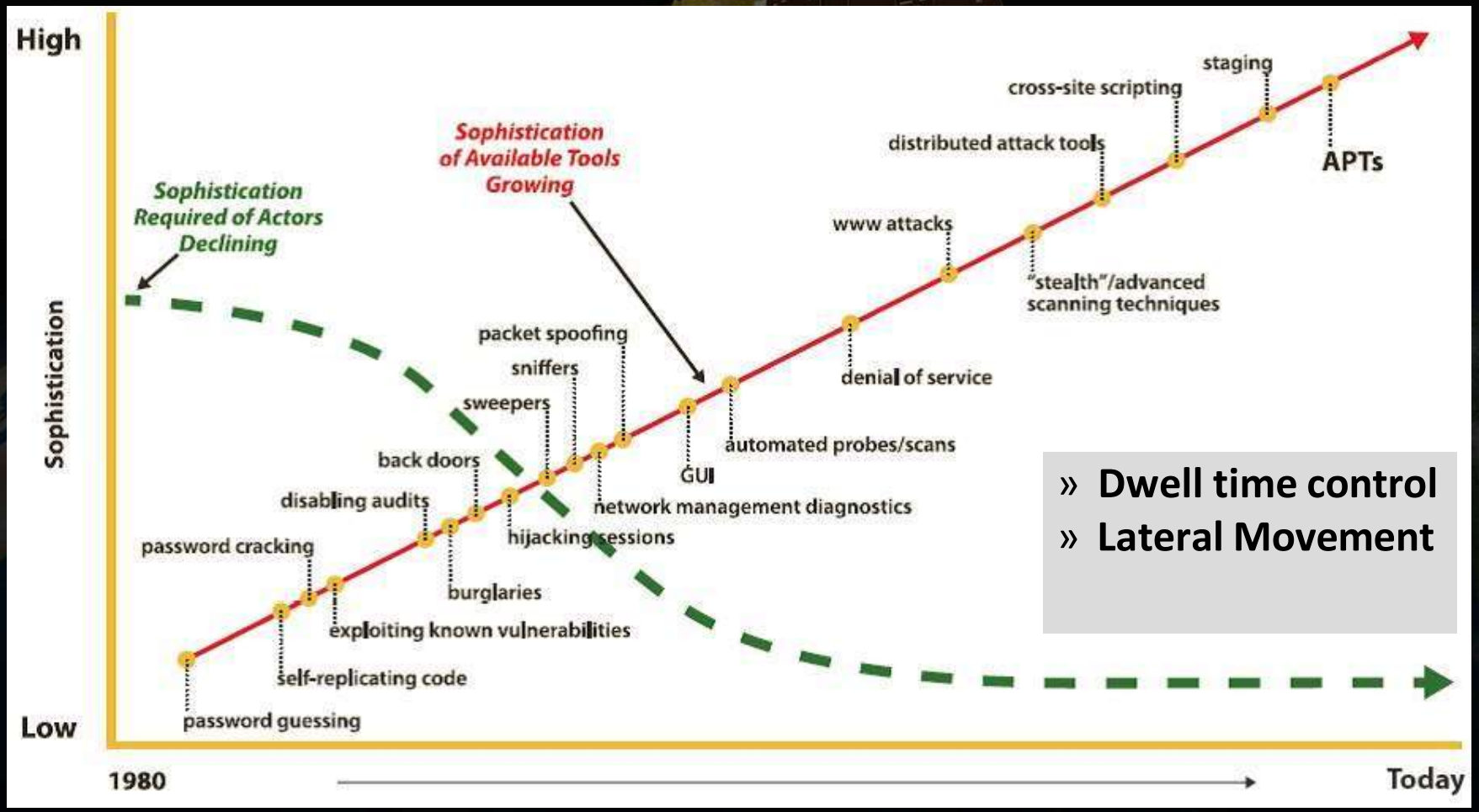
667% increase of targeted phishing attempts during COVID pandemic.

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



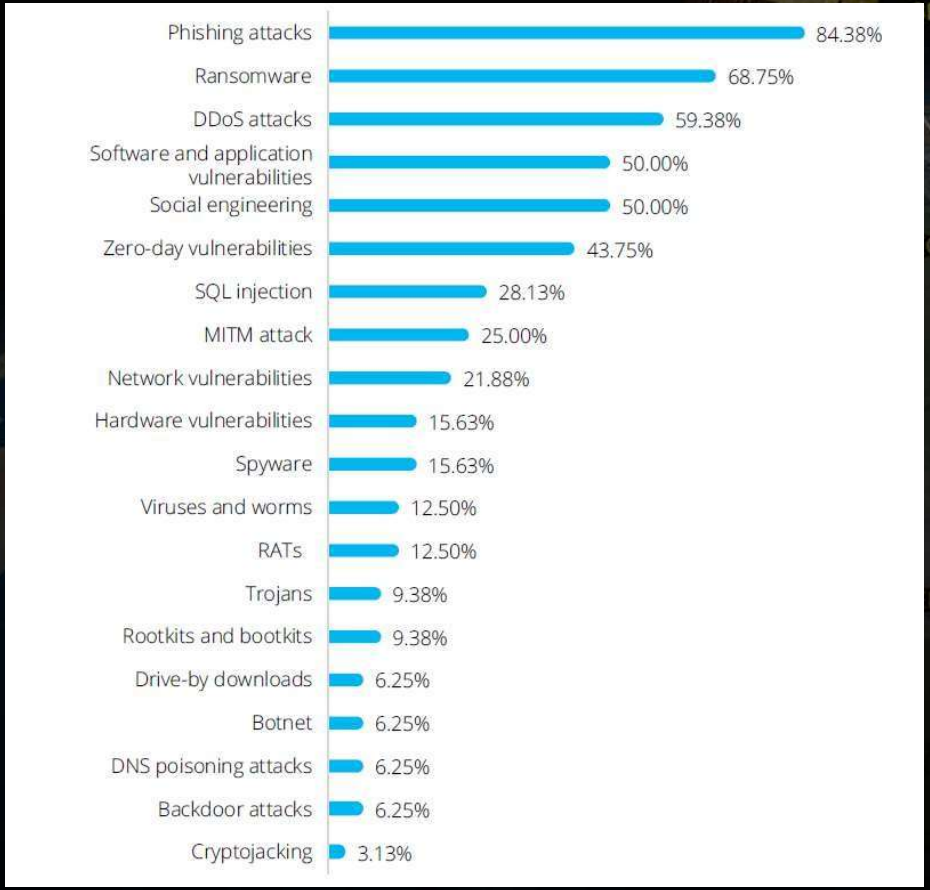
Source: SANS Institute

Top Cyber Security Threats-2024

Source: sprintzeal.com

Major Cyber Threat Pathways

Major Cyber Threats



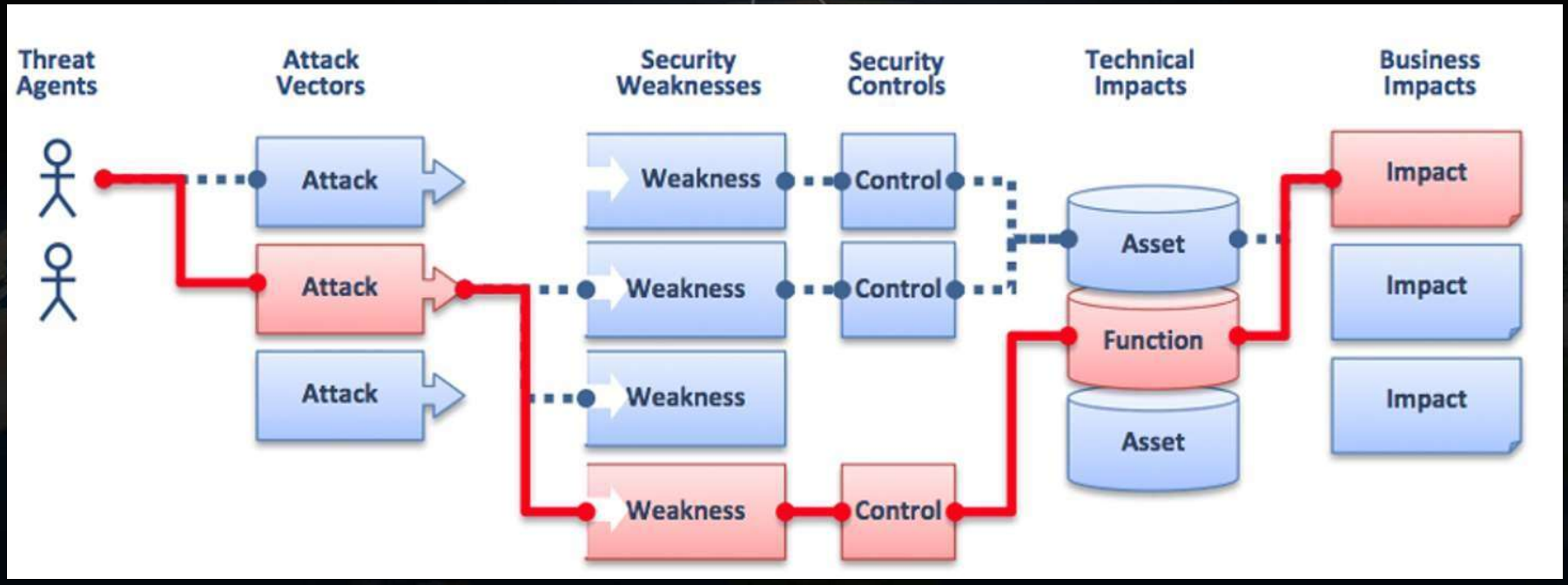
Majorly exploited by threat actors

Email	90.6%	Third Party and Open-Source Software	71.9%
Web Applications	65.6%	End Point Devices	62.5%
Cloud-based Pathways	59.4%	Software Supply Chain	59.4%
Individuals	53.1%	Mobile Devices	50.0%
Software, OS and Firmware Vulnerabilities	43.8%	Network File Servers	31.3%
Remote Access Portal	31.3%	Firewalls and Switches	28.1%
Network Application Servers	25.0%	IoT Devices	25.0%
Shared Databases and Directories	12.5%	Operational Technology	12.5%

Source – DSCI Survey 2023

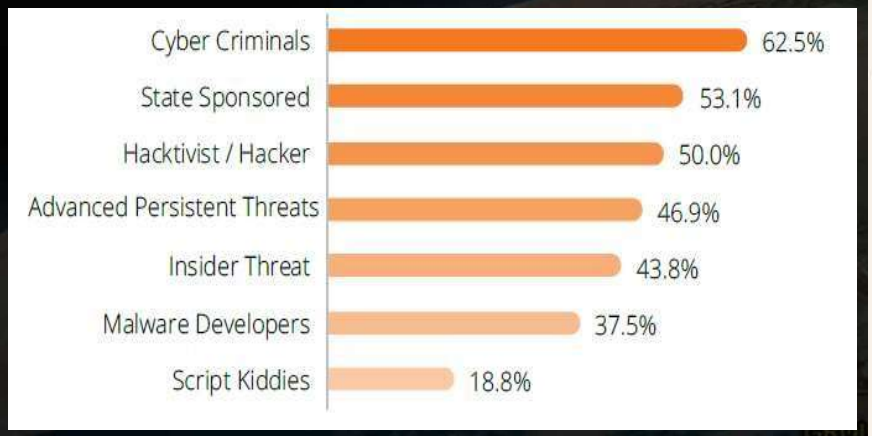
Threat Agents and Impact

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

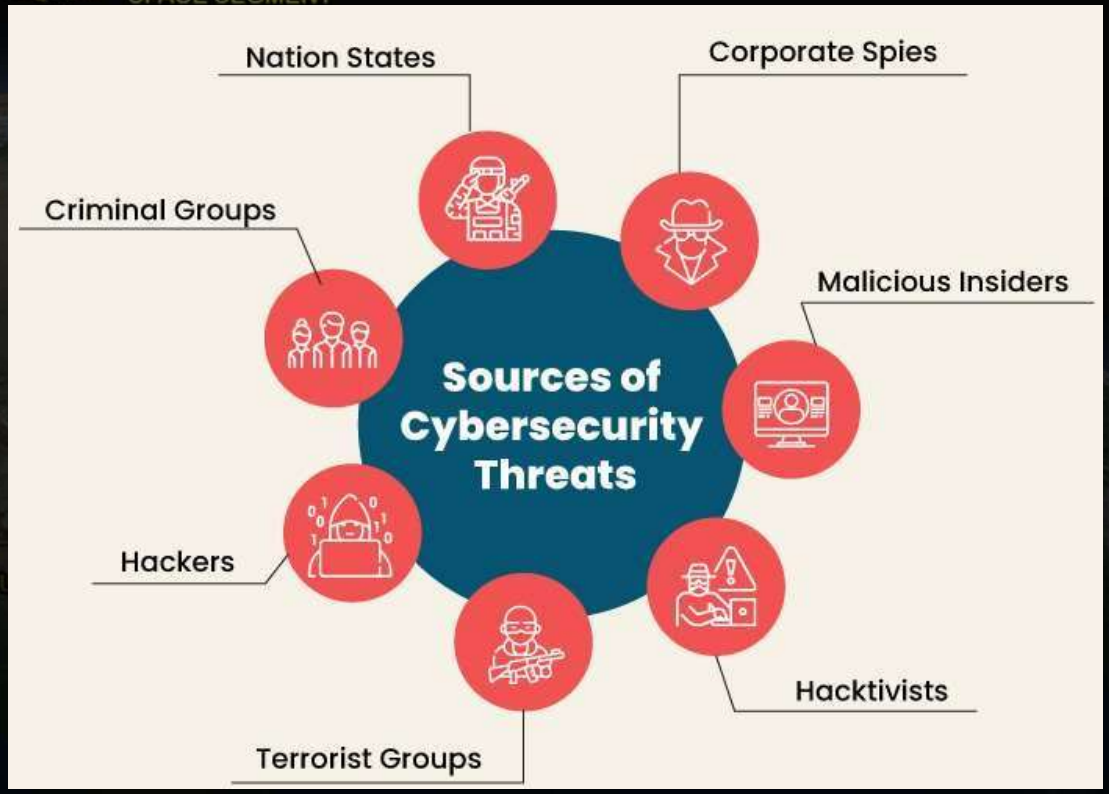


Risk = Likelihood x Impact

Sources of Cyber Threats



Source – DSCI Survey 2023



Cyber Security Challenges

Data Breaches

Unauthorised access or exposure of sensitive information.

Social Engineering Attacks

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

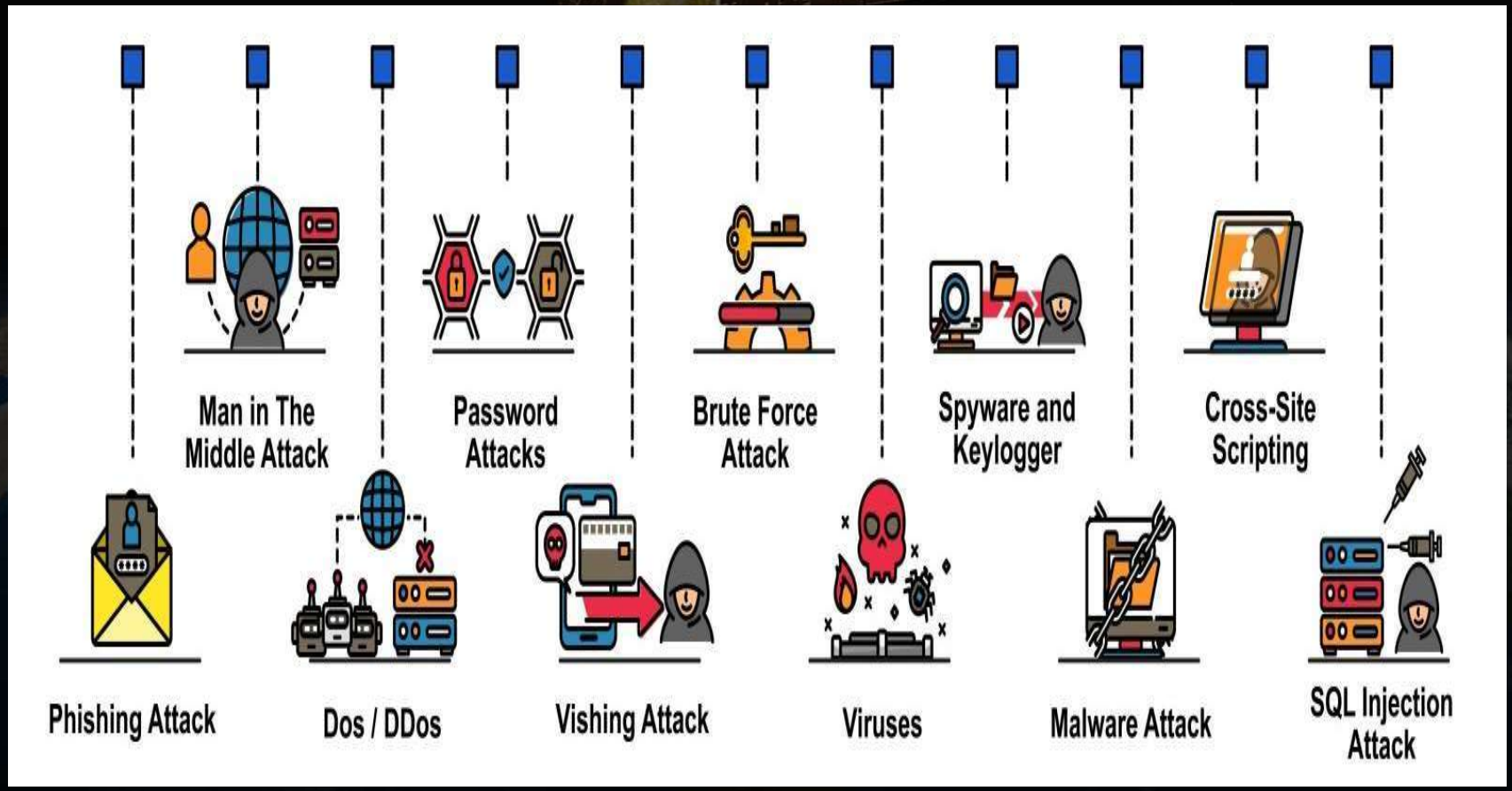
Malware Infections

Malicious software that compromises system integrity.

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.

Zero day attacks

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

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

NIC एनआईसी National Informatics Centre

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.

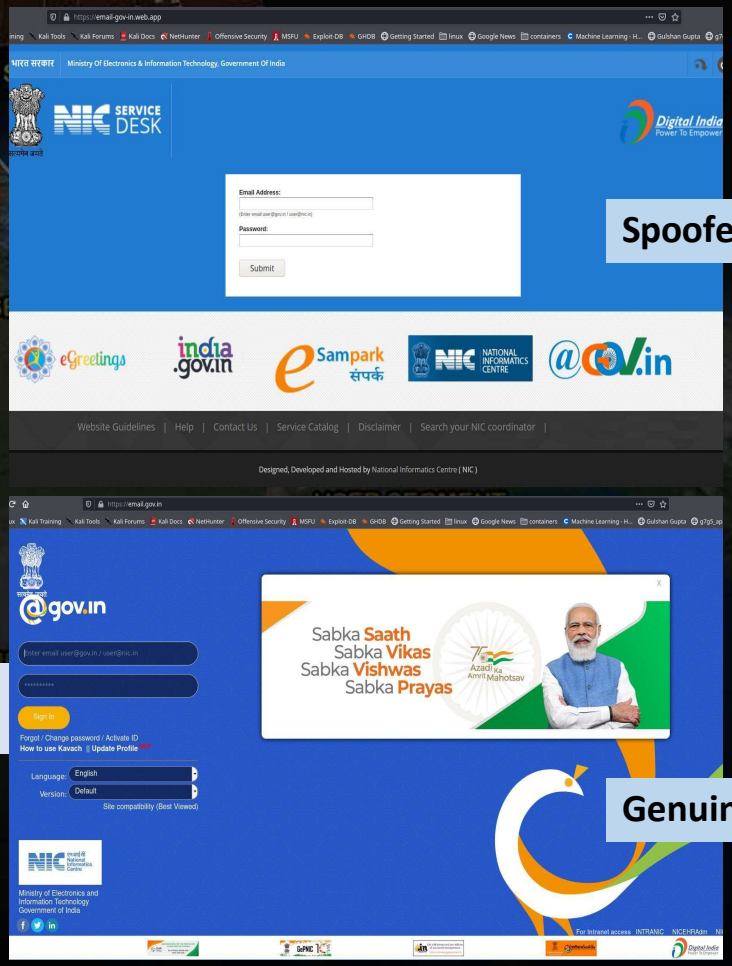
99%

Activate a new quota here

Thank You,

@GOV.IN

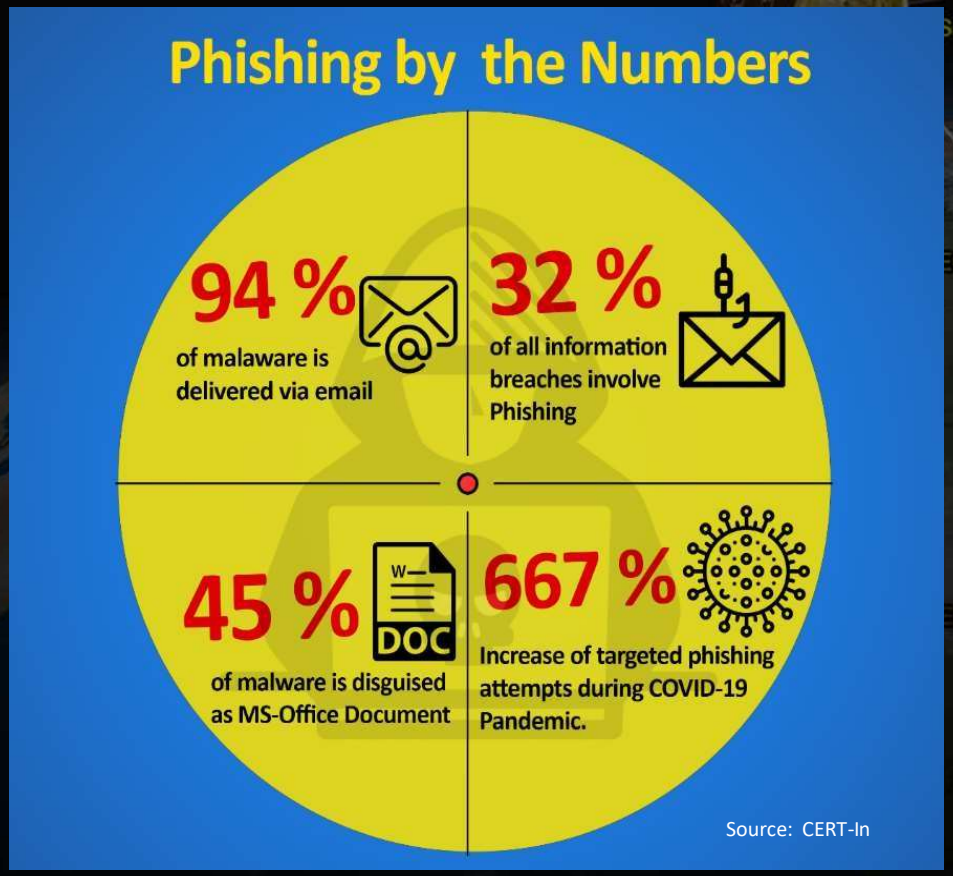
https://email-gov-in.web.app/.

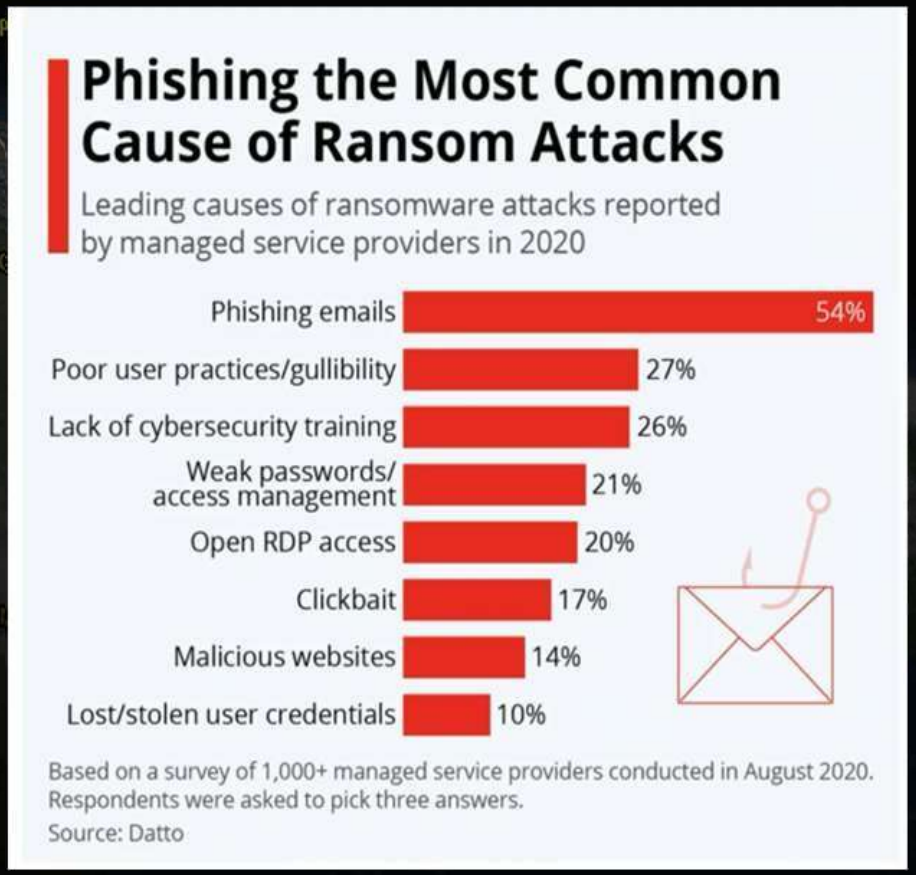


Spoofed Login page

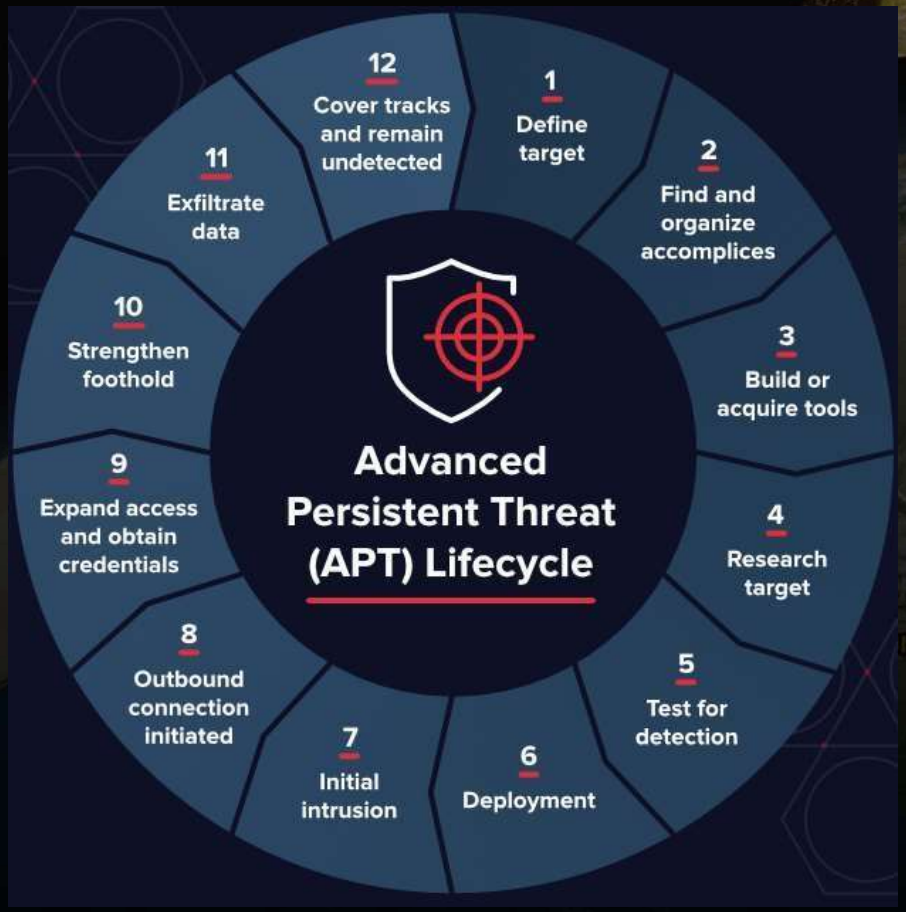
Genuine Login page

Phishing Attack Numbers





Advanced Persistent Threats

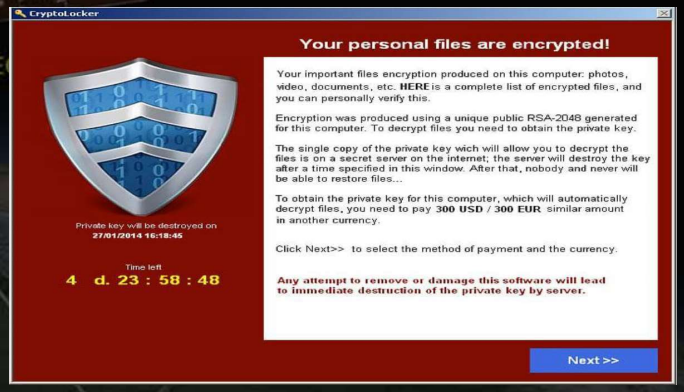


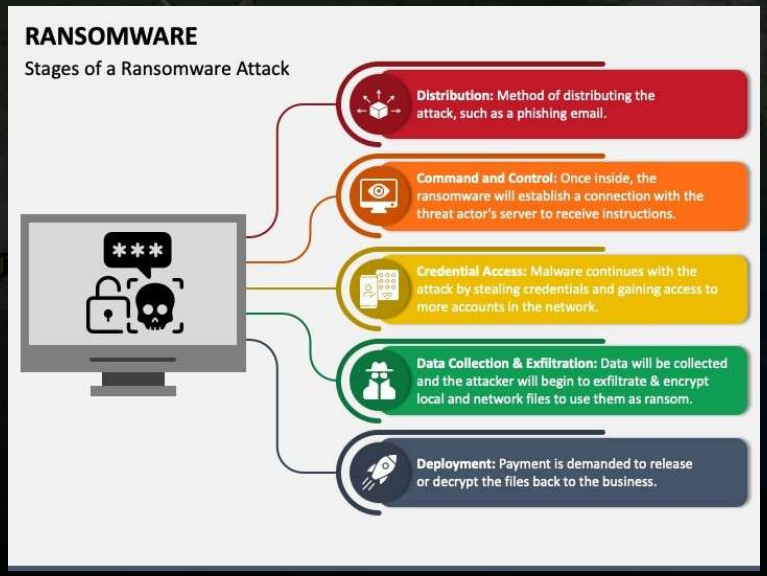
- **APT:**
  - Nation or state-sponsored group.
  - Dwell time, **204 days**. (APAC)
  - **Advanced:** Full spectrum of intelligence gathering techniques
  - **Persistent:** Continuous monitoring and interaction
  - **Threat:** Specific objectives and well funded
- **Approach:**
  - Self-destructing 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?

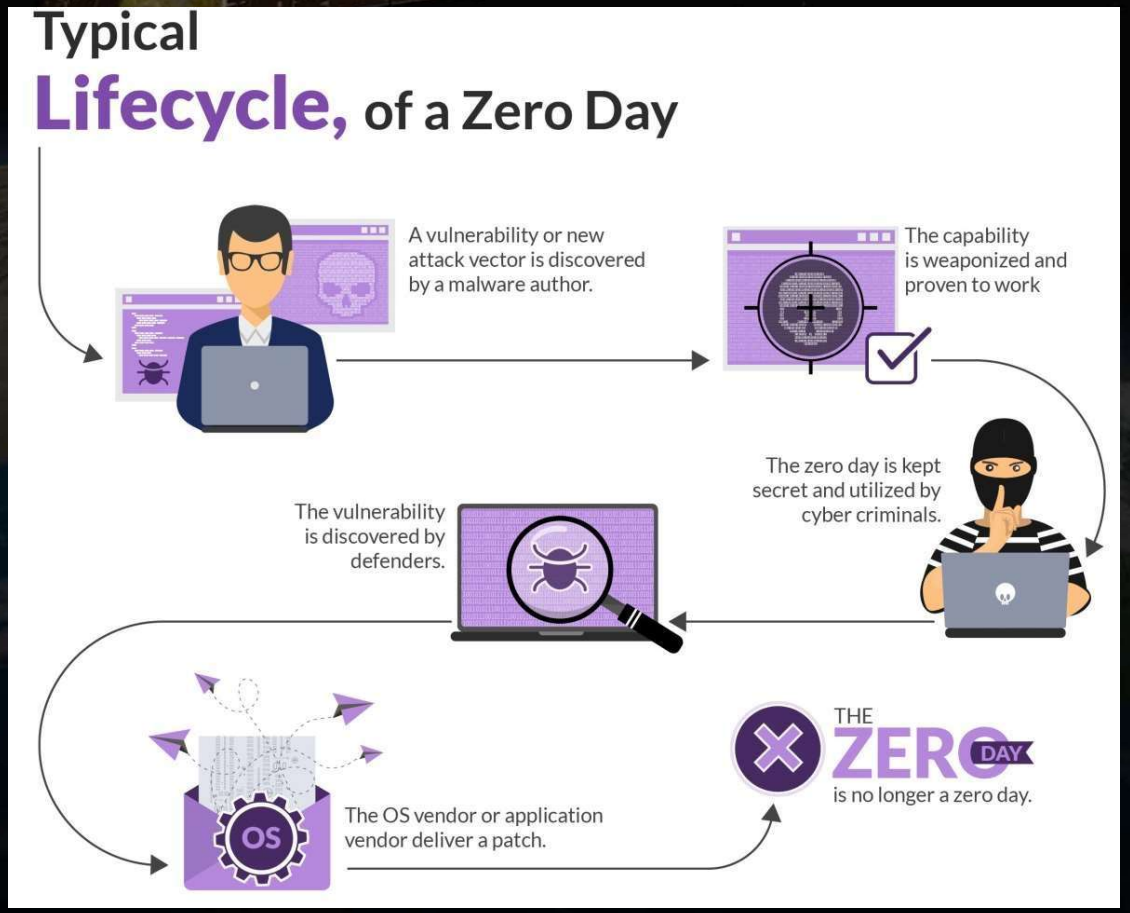
Vulnerability or attack vector is **known only to attackers**, so that it work without intervention from defenders. No patch available.

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



Hindustan Times

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

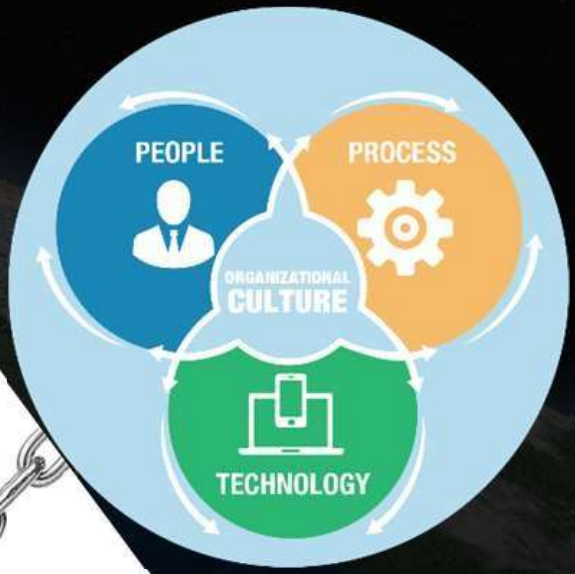
A 73-year-old man in India fell victim to a deepfake scam after receiving a call from someone impersonating his former colleague and asking for money. The scammer used deepfake technology to create a video call in which the impersonator's face and voice matched the victim's former colleague. The victim 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.

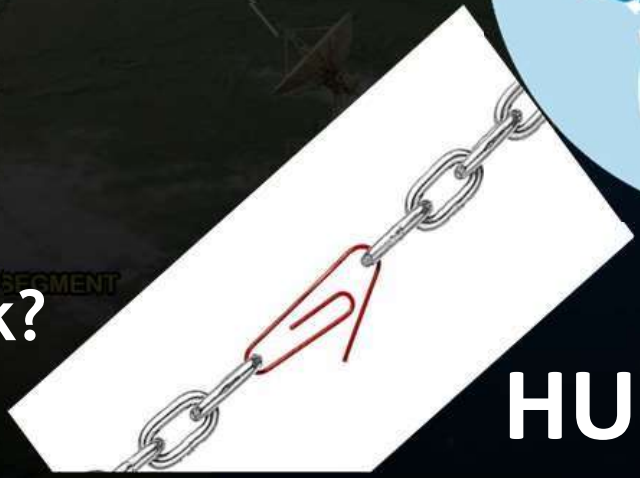
- **Deepfake Scam It is AI-based technology** used to produce or alter video content so that it presents something that didn't, in fact, occur.
- Deep learning neural networks are used to manipulate video (faces) & audio (voice) by morphing & merging. Voice is overlaid and lips are synced.
- **AI Voice 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?**





HUMANS

Can You Read This?

I cnduo't bvleiee taht I culod aulaclty uesdtannrd waht I was rdnaieg. Unisg the icndeblire pweor of the hmuan mnid, aocdcrnig to rseecrah at Cmabrigde Uinervtisy, it dseno't mttaer in waht oderr the lterets 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 sitll raed it whoutit a pboerlm. Tihs 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 ipmorantt!

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

Root Cause of The Problem?

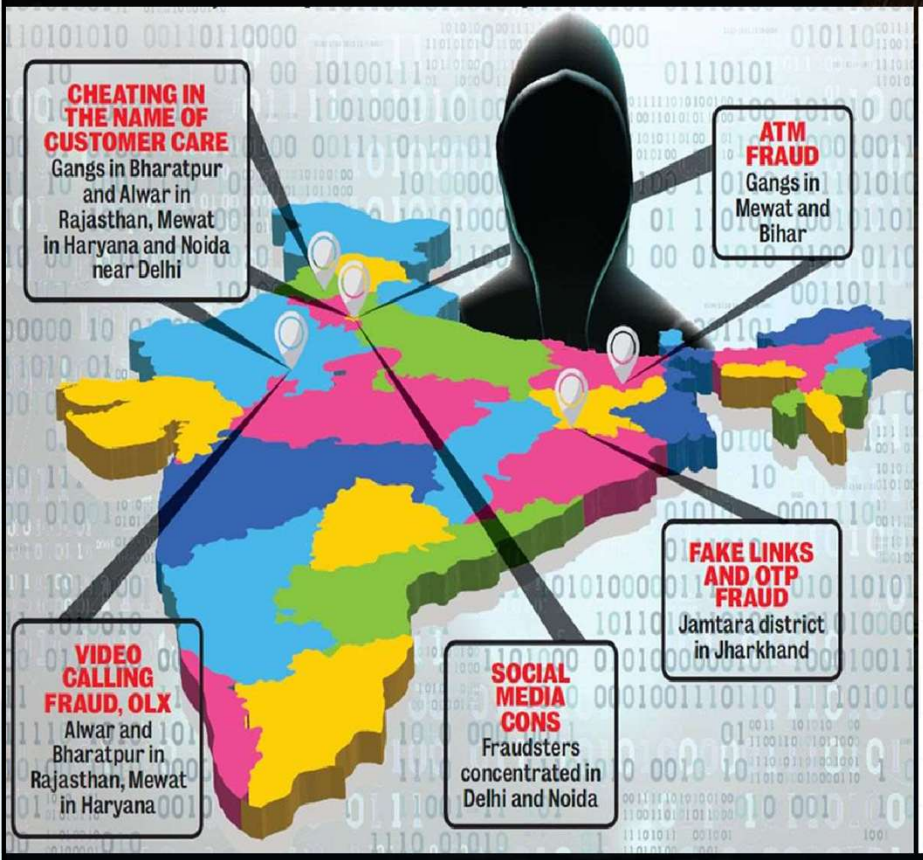
- ➢ Human reaction?
- ➢ [CRITICAL VULNERABILITIES EXPOLITED BY SCAMSTERS]

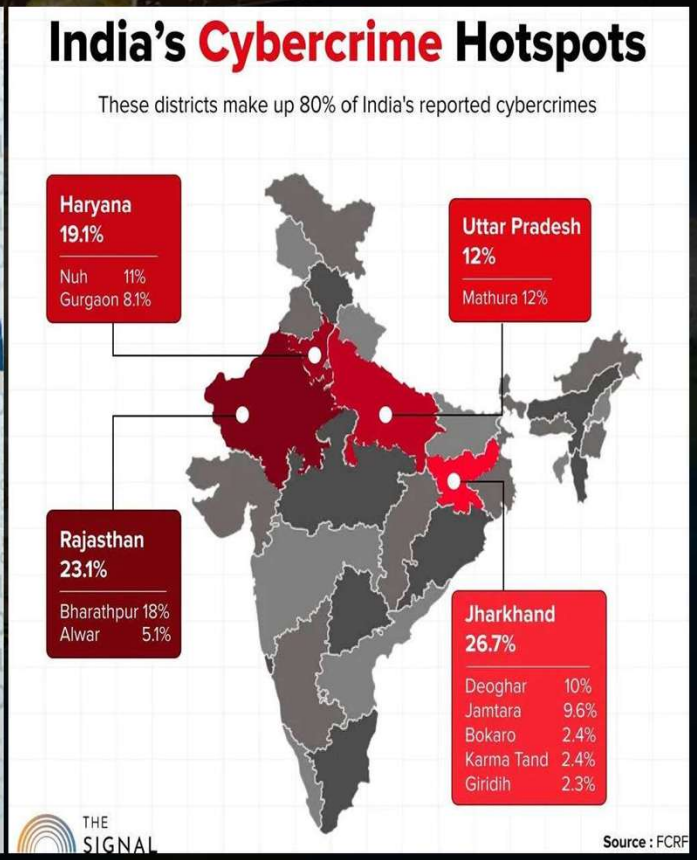
Criminals deceive the human mind by manipulating emotions.

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





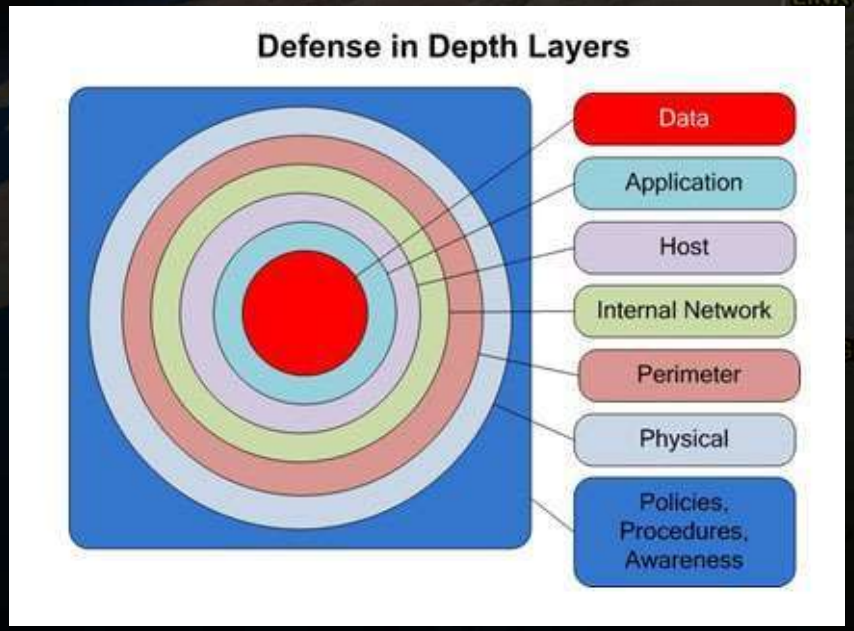
- ❑ Jamtara, JH
- ❑ Mewat, HR
- ❑ Bharatpur & Alwar, RJ
- ❑ Noida, Delhi
- ❑ Motohari, Bihar

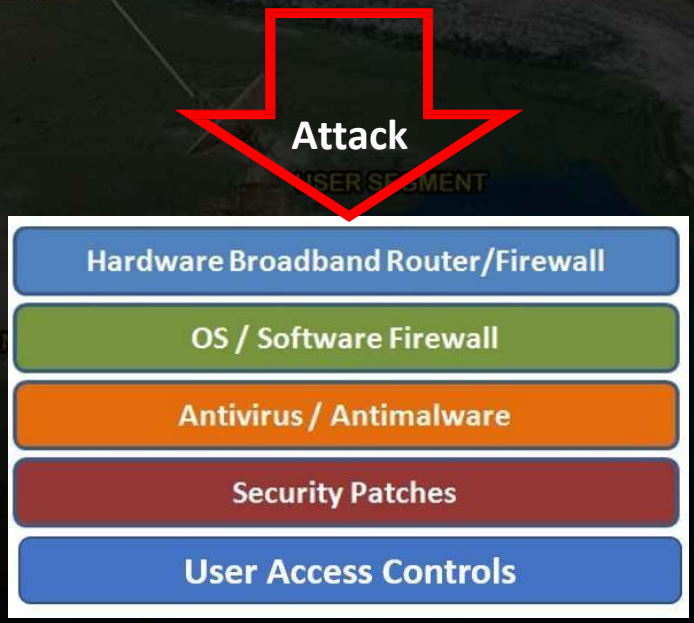
10 Districts account for 80% of cyber crime cases in the country

Security Measures

Defense in depth is the Best line of control that

Uses multiple layers of defense to address technical, personnel and operational issues.





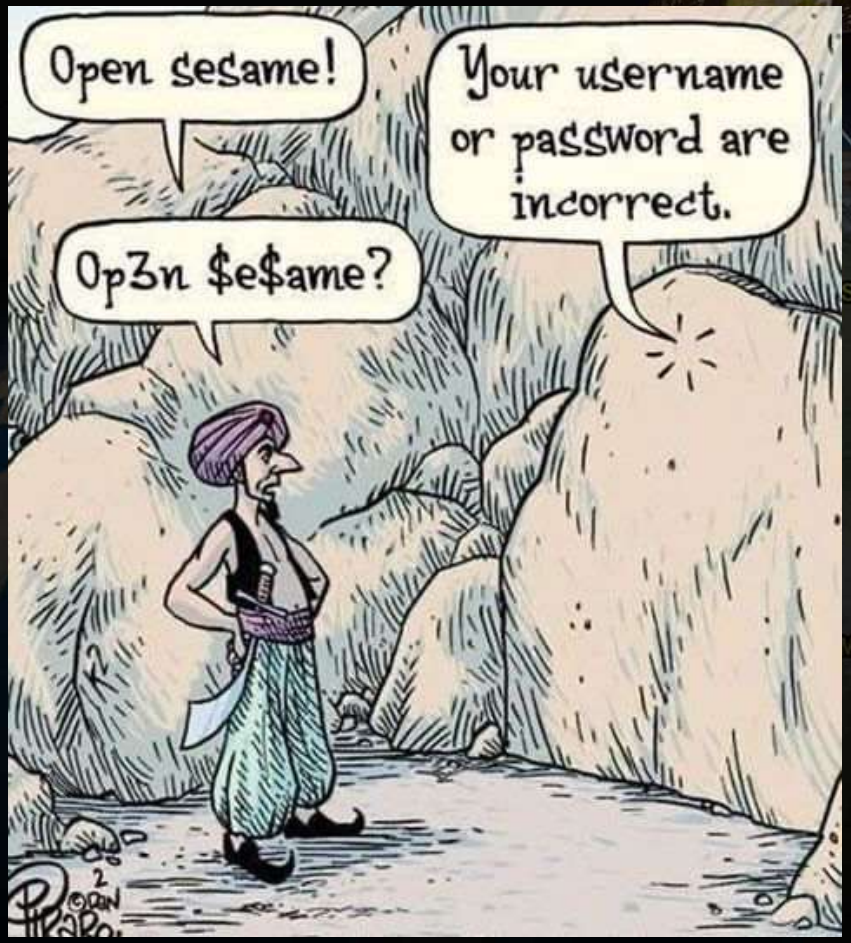
Attack Surface

Network insecurities		Software bugs		Physical security loopholes		Social engineering-prone people	
Open ports	Weak protocols	Insufficiently secured in-house-developed applications	Vulnerable commercial programs (e.g., WordPress, etc.)	Rogue or dissatisfied current and former employees	Openly displayed login credentials (e.g., username-password combinations on sticky notes, etc.	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?



- 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

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.

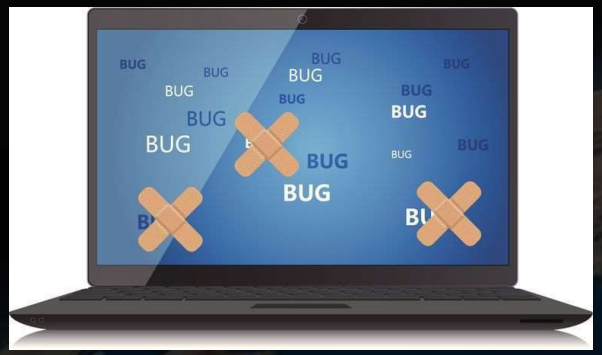
Multi-Factor Authentication (MFA)

Double your Login protection / Lock down your login

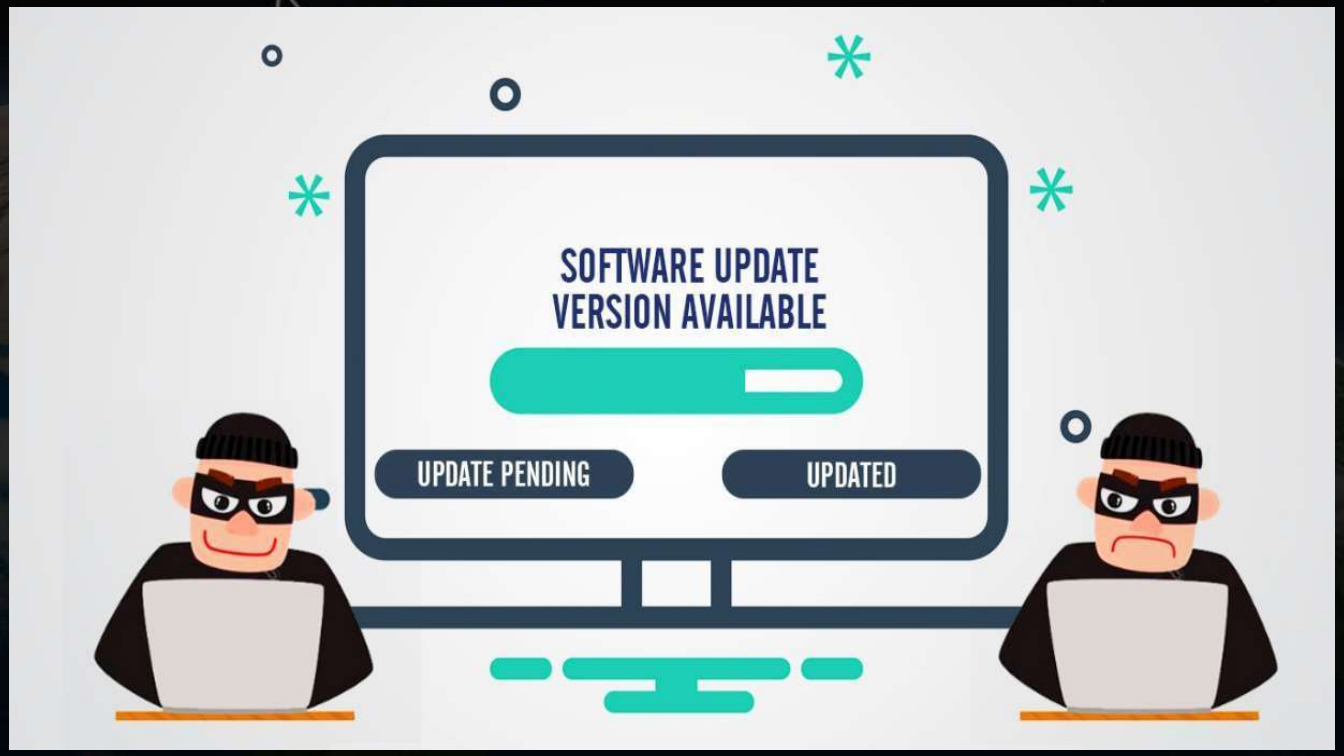
IS ALL ABOUT YOU

Something you know, or "knowledge factor."	Something you have, or "possession factor."	Something you are, or "inherence factor."
who YOU are	what YOU know	what YOU own
• fingerprint scanners • voice verification • facial recognition	• security questions • passwords and passphrases • PINs	• SMS authentication • application-based authenticators • hardware tokens
Something you know, e.g: "Password"	Something you possess, e.g: "Mobile phone"	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**.

1 Search Result Shows Brand

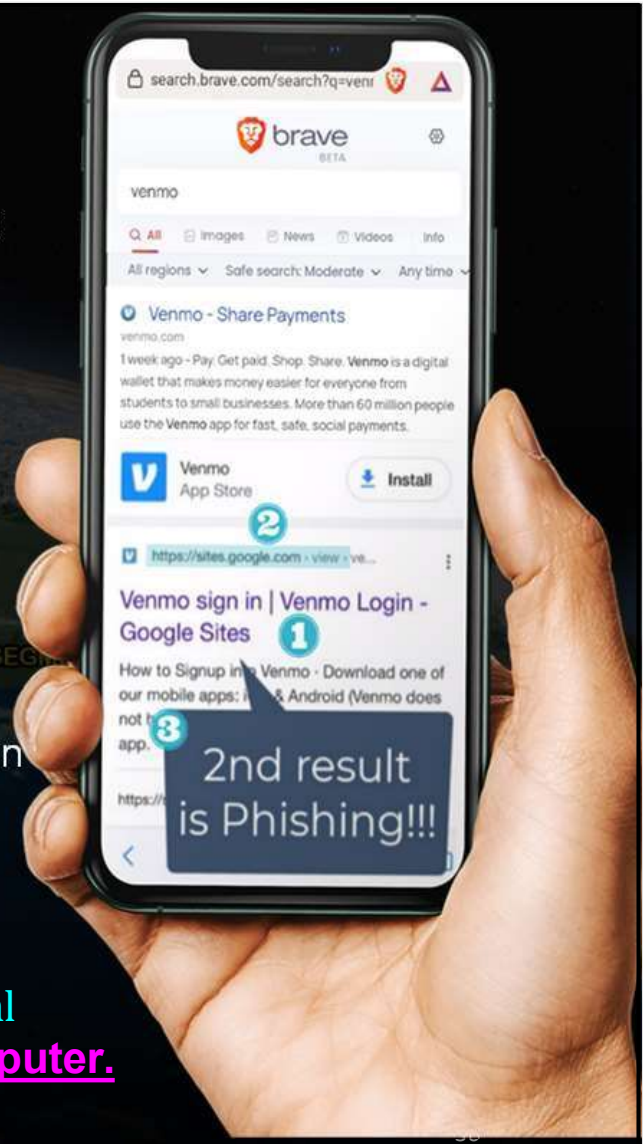
Title displays correct brand name

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



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

QR Code Scam

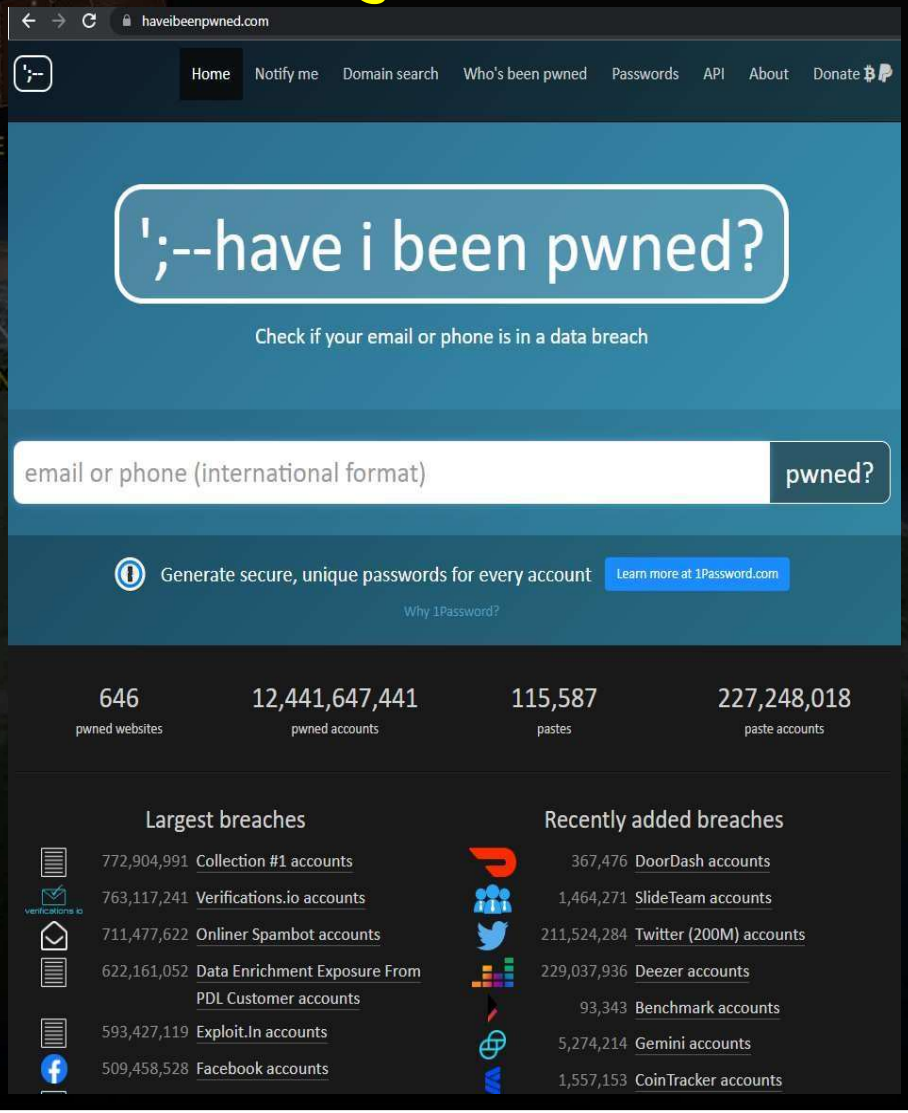
Who thought a QR code could be dangerous?

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

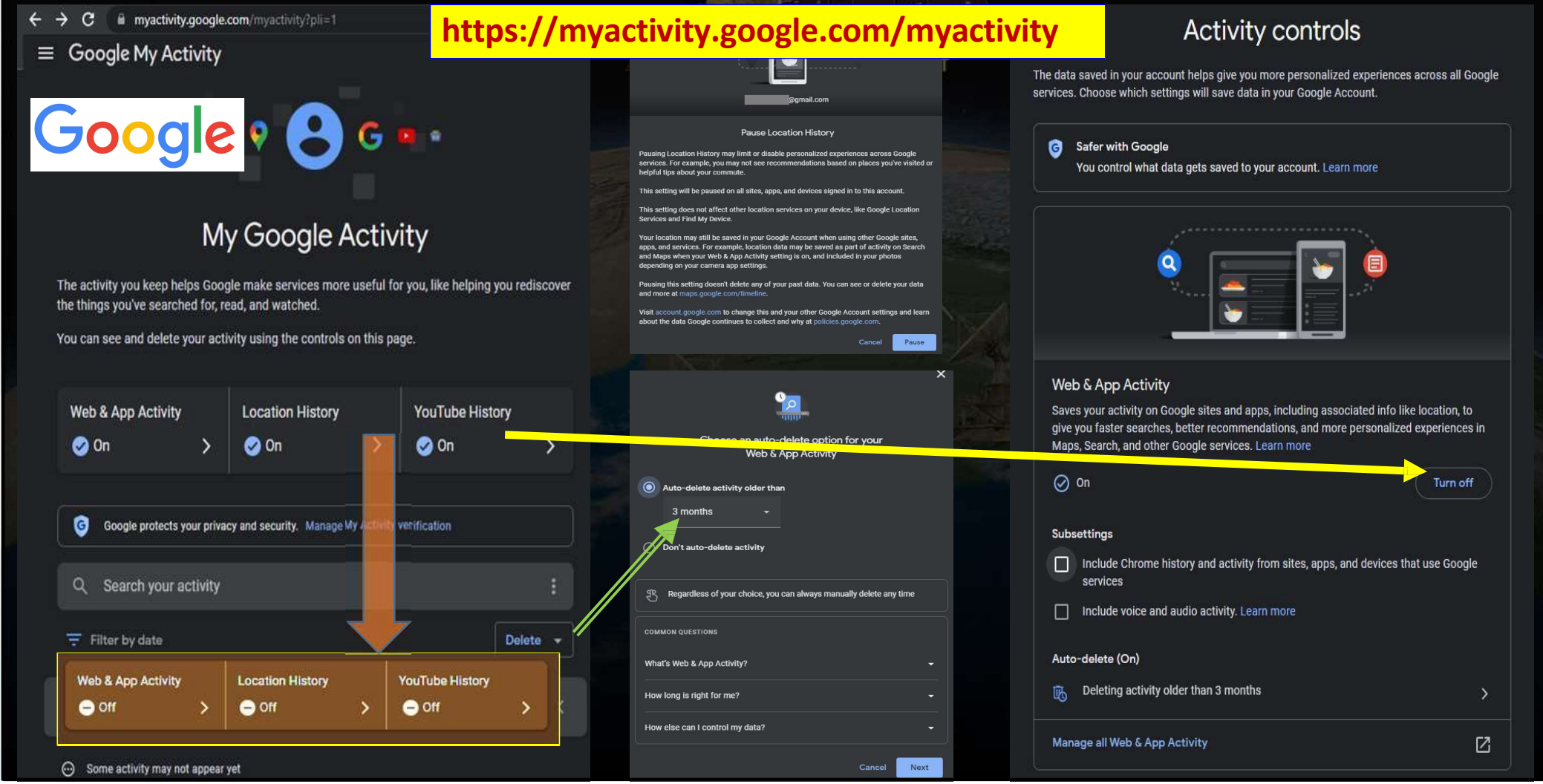


आप पासवड कितना Secure है? Check it out at

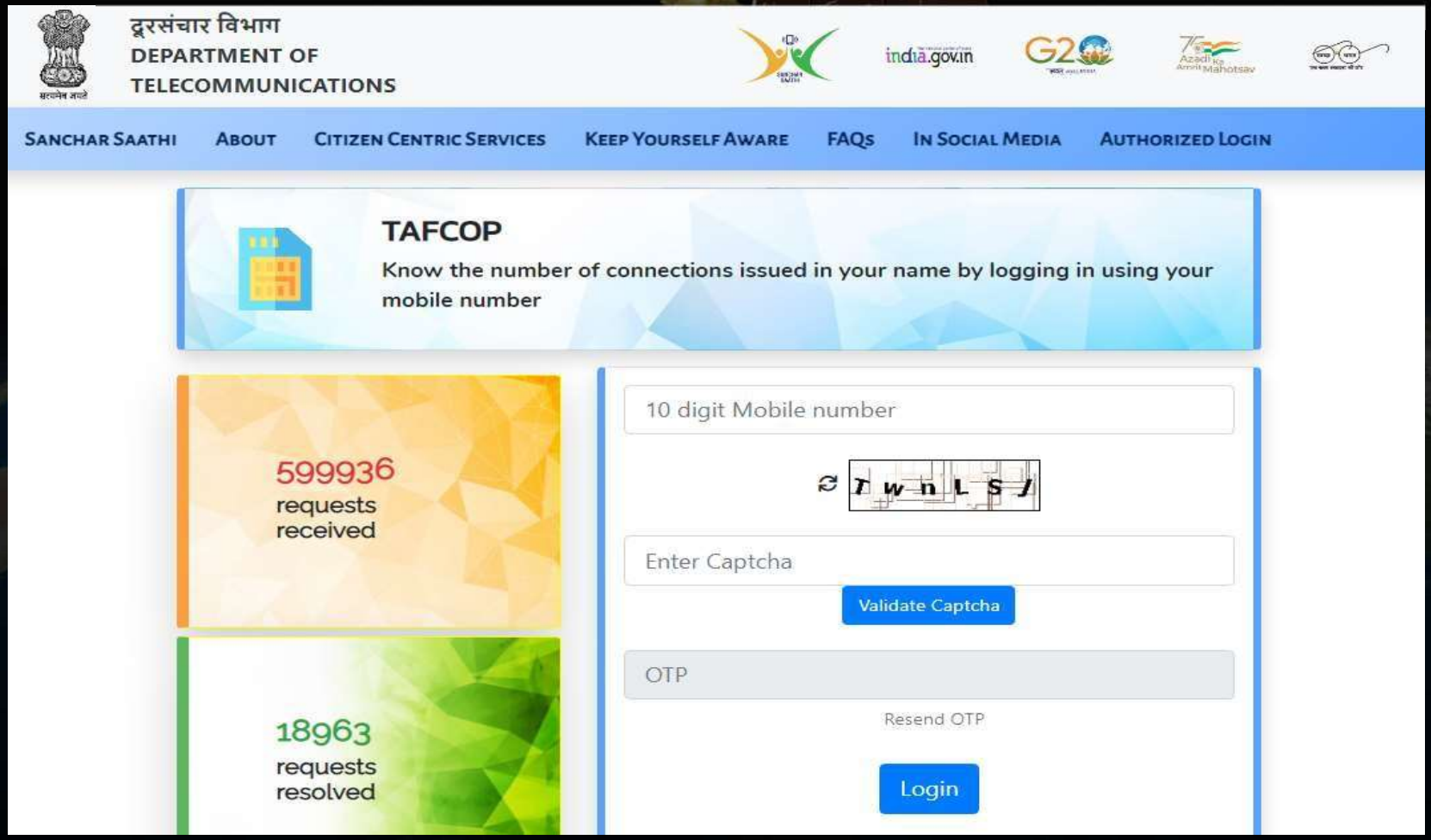
Almost Everything Google know about you…Seriously – Everything !! (since 2 decades)

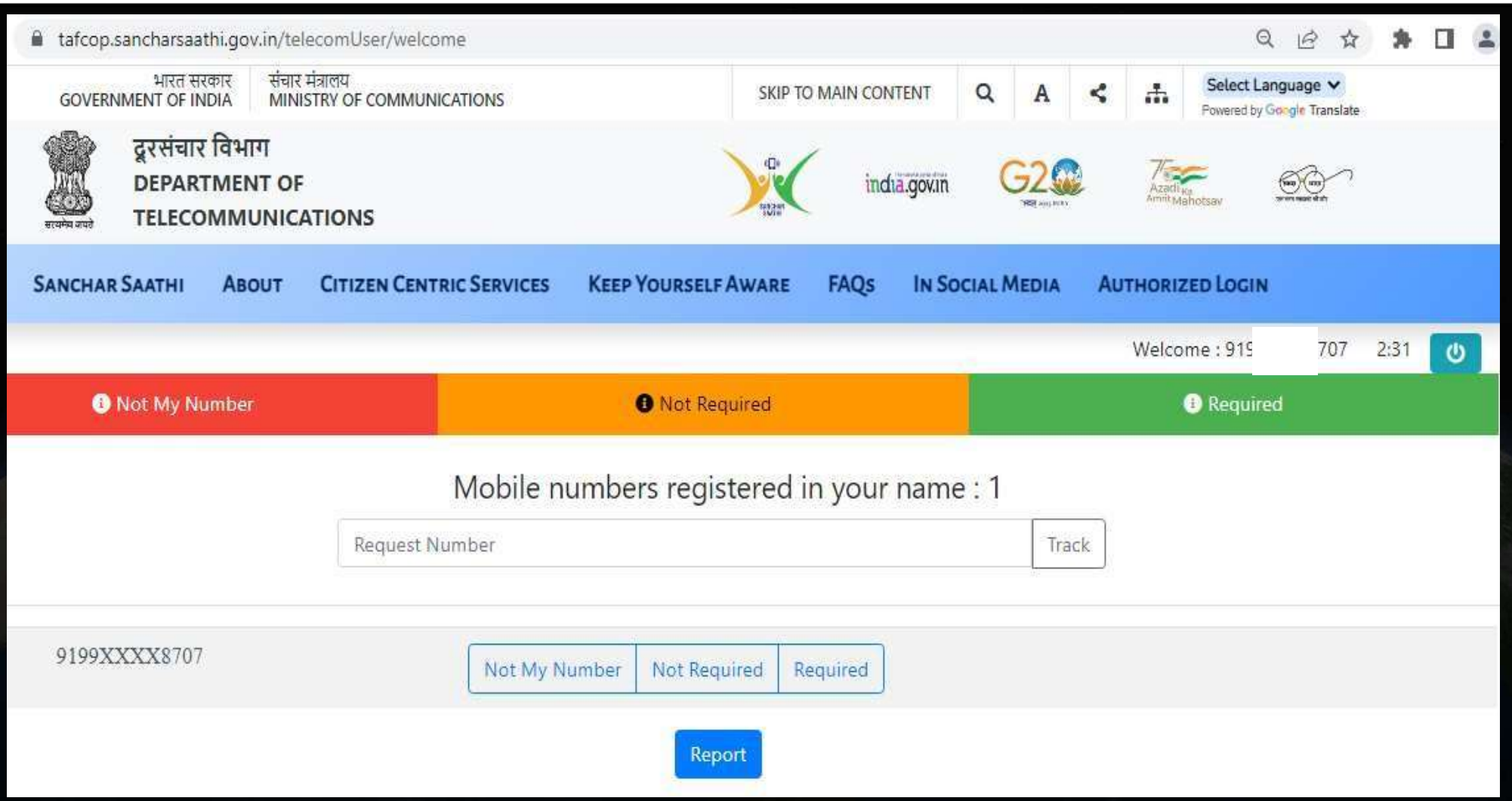
Especially if you use Google's products like: Android, Gmail, Goggle Drive, Google Maps, YouTube, Google Search

https://myactivity.google.com/myactivity

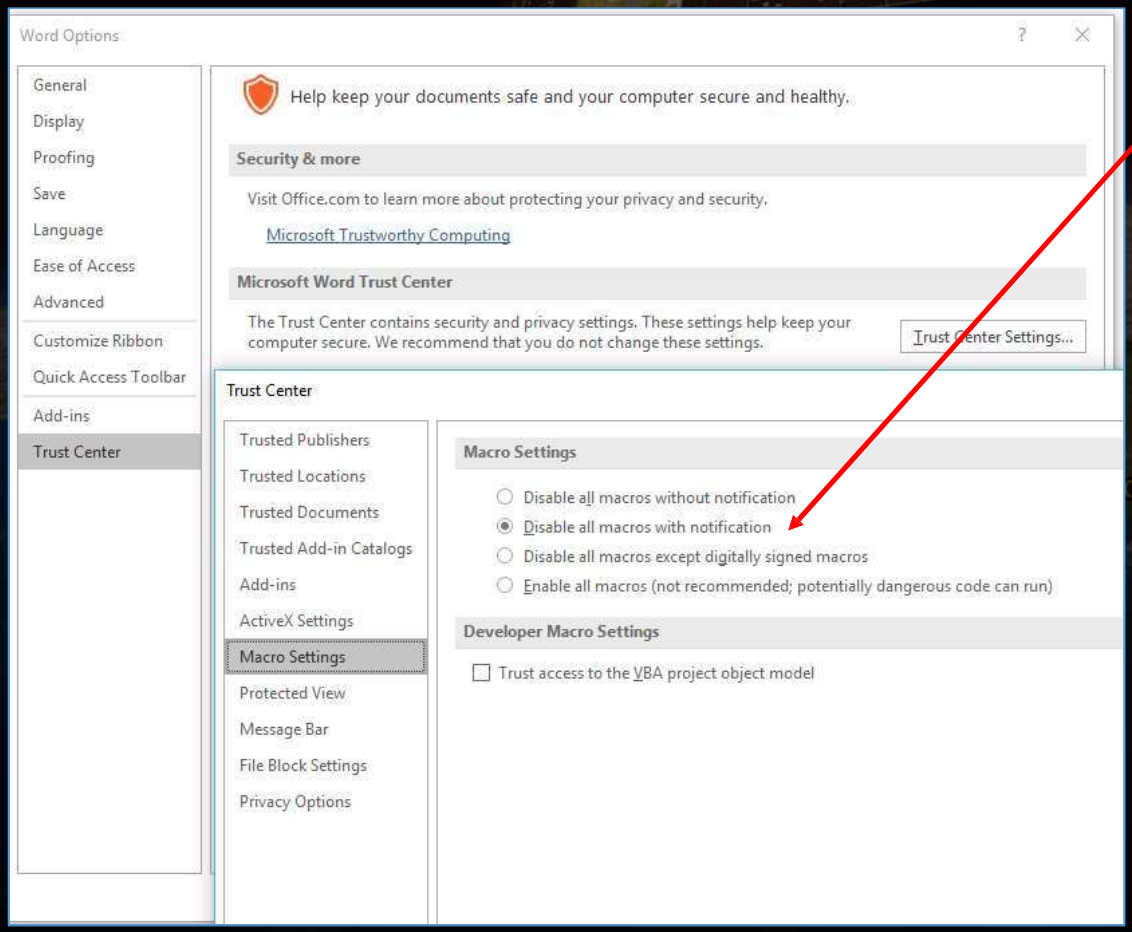


आप के नाम/आधार पर कितने मोबाइल नबर और िसम चलता है?




tafcop.sancharsaathi.gov.in/telecomUser/welcome
भारत सरकार
GOVERNMENT OF INDIA
संचार मंत्रालय
MINISTRY OF COMMUNICATIONS
SKIP TO MAIN CONTENT
Select Language
Powered by Google Translate
दूरसंचार विभाग
DEPARTMENT OF
TELECOMMUNICATIONS
india.gov.in
G20
Azadi Ka Amrit Mahotsav
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

01 **Perimeter protection** (Firewall, AV, DPI, IPS/IDS)

02 **End point Security, System Hardening, Application & NAC**

03 **Network Segmentation**

04 **Application Security (WAF, Email Security)**

05 **Analytics** [SIEM, Network Security Monitoring, Logging]

Security Controls

01 Principle of Least privilege

02 Air-Gapped Networks

03 Secure Code Practices

04 Patch Management

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

06 Cyber Awareness Activities & Incident Reporting

Thank You