

Hacking & Digital Arrest Scams – Cyber Crimes Decoded



Context:

- The **United Nations General Assembly** adopted a landmark **cybercrime convention** on **December 24**, paving the way for significant changes to how governments police the internet.
- The **Convention against Cybercrime** was adopted without a vote and by consensus after a five-year negotiation.
- According to cyber cell data, **Indians lost Rs 1,777 crore to cyber fraud** in just the **first four months of 2024**. Of this, **Rs 120 crore was lost to digital arrest scams**.
- **Digital arrest**, among other scams, was highlighted by **Prime Minister Narendra Modi** during his monthly radio address 'Mann Ki Baat' on **October 27, 2024**.

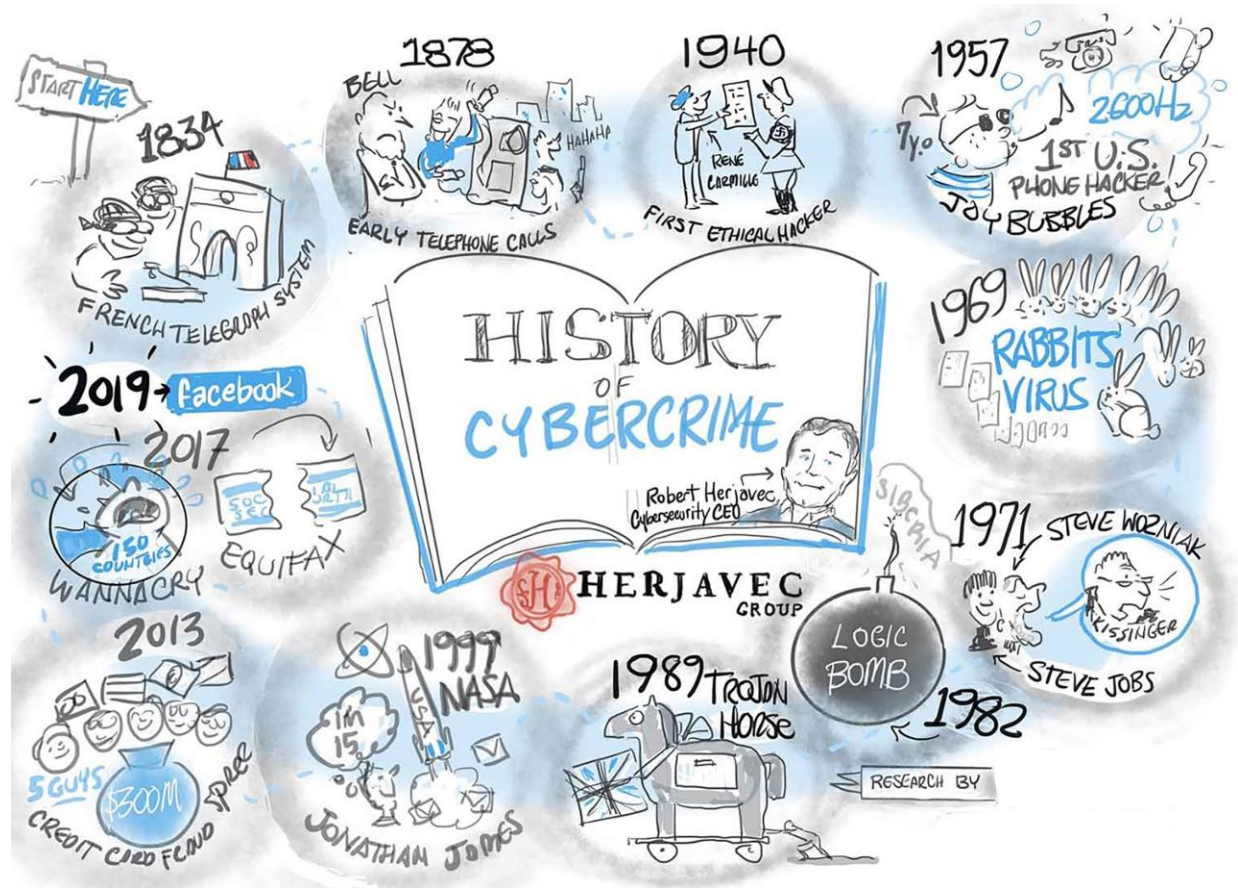


1. What is cybercrime?



- In general cybercrime may be defined as “**Any unlawful act where a computer or communication device or computer network is used to commit or facilitate the commission of crime**”.
- These crimes involve the use of **technology to commit fraud, identity theft, data breaches, computer viruses, scams,** and expanded upon in other malicious acts.
- **Cybercrime** is a serious issue in India, and the **Information Technology Act (IT Act) of 2000** covers many types of cybercrimes.

2. What is the history of cybercrime?



- The history of cybercrime can be traced back centuries, with the **first recorded cyber attack in 1834 in France.**

Incident	Analysis
The telegraph system	<ul style="list-style-type: none"> • In 1834, two thieves infiltrated the French telegraph system, gained access to financial markets, and stole data. • Many experts consider this event the first cybercrime, followed by other cybercrimes, each focusing on newly invented technologies.
The telephone	<ul style="list-style-type: none"> • The 19th and 20th centuries saw attacks focused on the telephone system.

<p>system</p>	<ul style="list-style-type: none"> • In 1876, Alexander Graham Bell patented the phone, which allowed transmitting speech using telegraphy. • Two years after the commercialization of this invention, teenage boys broke into Bell's telephone company and misdirected calls. • In later years (1960s-1980s), phone hacking (phreaking) became popular.
<p>Ethical hacking</p>	<ul style="list-style-type: none"> • In 1940, Rene Carmille, a French computer expert, hacked into the Nazi data registry. • Carmille, a punch card computer expert, used his expertise to reprogram Nazi punch card machines to prevent them from registering information correctly. • His work blocked the Nazis' attempts to register and track Jewish people.
<p>Phishing scams and malware</p>	<ul style="list-style-type: none"> • In the 1980s, emails became a popular communication form, and by the 1990s, web browsers and computer viruses rose in popularity. • In these years, hackers started using email attachments to deliver malware and phishing scams and web browsers to spread computer viruses.
<p>Social media scams</p>	<ul style="list-style-type: none"> • In the 2000s, social media networks gained worldwide popularity, and hackers started utilizing these platforms for data theft and other cybercrimes.

	<ul style="list-style-type: none">• In the following years, cybercriminals improved malware infections and data theft techniques.• Today, these attacks are deployed in the thousands, constantly increasing with no signs of slowing down.
First conviction	<ul style="list-style-type: none">• Lan Murphy, better known as Captain Zap, was the first person to be convicted of cybercrime, which occurred in 1981.• He had managed to hack the American telephone company's internal clock to allow consumers to make free calls during busy hours.

3. What is the UN cybercrime treaty?



- The **UN Convention against Cybercrime** aims to **prevent and combat cybercrime more efficiently and effectively**, including by **strengthening international cooperation** and by providing technical assistance and capacity-building support, **particularly for developing countries**.
- The adoption of this landmark convention is a **major victory for multilateralism**, marking the **first binding international anti-crime treaty in 20 years**.
- The **UN Office on Drugs and Crime (UNODC)** served as **secretariat to the negotiations**.
- The **General Assembly** adopted the **resolution without a vote**.
- The Convention will open for signature at a **formal ceremony to be hosted by VietNam in 2025** and will enter into force **90 days after being ratified by the 40th signatory**.

4. Enlist various types of cybercrimes?

Types of cybercrimes	Analysis
Child Pornography/ Child sexually abusive material (CSAM)	<ul style="list-style-type: none"> • Child sexually abusive material (CSAM) refers to material containing sexual images in any form, of a child who is abused or sexually exploited. • Section 67 (B) of IT Act states that “it is punishable for publishing or transmitting material depicting children in sexually explicit acts, etc. in electronic form.

KEEPING A WATCH

A 14-member panel in the Rajya Sabha led by Congress leader and MP Jairam Ramesh submitted recommendations to check child sex abuse material on social media. Here are some of the suggestions:

- > Broadening of PocsO Act by include written material, visual representation and audio recording advocating sexual activity with a minor
- > Defined "sexually explicit" in the existing definition and included "cyber-grooming" (when a person with sexual intent persuades or coerces and arranges a meeting with a child) as an offence
- > Requested PM to take the lead in creating a global alliance to combat CSAM on social media
- > Called for amendment of the IT Act to enhance scope of the darknet investigators
- > The committee has also recommended a code of conduct for social media platforms, mandatory apps on all devices sold in India that monitor children's access to pornographic content
- > Filters for parental control and age verification

COUNTRY IN FOCUS
Findings from The Out of Shadow Index by the Economist Intelligence Unit examining how 40 countries are dealing with child sexual abuse

India ranks 15th with a score of 57.6
WHERE IT'S SLIPPING

Indicator	Score
National policies	30
Victim support programme	40
Contextual legal framework	42
Law enforcement capacity	43
Complaint mechanism	50
Civil society engagement	50
Child-specific rape laws	50

STORY IN THE DETAILS
Other global findings of The Out of the Shadows Index

- > Nine of 60 countries established mandatory law for reporting, content blocking or deleting and record keeping of child sex abuse material
- > Research in 28 countries, including the USA, China, India, Russia, and Brazil, found 17% children faced cyberbullying (one aspect is online sexual harassment)

Interpol's Child Sexual Exploitation database holds more than 15 million images and videos, recording the abuse of more than 19,400 victims worldwide


30% of internet users are children

Internet Watch Foundation found more than **105,000** websites hosting child sexual abuse material

Cyber Bullying

- **Cyber Bullying is a form of harassment or bullying inflicted through the use of electronic or communication devices such as computers, mobile phones, laptops, etc.**



<p>Cyber stalking</p>	<ul style="list-style-type: none">• Cyber stalking is the use of electronic communication by a person to follow a person, or attempts to contact a person to foster personal interaction repeatedly despite a clear indication of disinterest by such person or monitoring the internet, email or any other form of electronic communication commits the offence of stalking.  <p>The illustration shows a person wearing a grey hoodie and a white hood, looking out from a window. The window has a white frame and a light-colored curtain. Outside the window, a woman with dark hair in two braids, wearing a green top, is looking at her smartphone with a worried expression. The background is a white brick wall.</p>
<p>Online Job Fraud</p>	<ul style="list-style-type: none">• Online Job Fraud is an attempt to defraud people who are in need of employment by giving them a false hope/ promise of better employment with higher wages.

Fraud Alert

How fraudsters operate to gain jobseekers' trust:

- ▶ Clone sites of legitimate consultancies
- ▶ Create similar company logos/letterheads, etc
- ▶ Conduct interviews online or from offices

Endgame:

- ▶ Collect personal info, such as bank account details
- ▶ Scam them by collecting money under heads such as agency fees, visa fees, charges to push their candidature, etc

What legitimate recruitment agencies are doing:

- ▶ Spreading awareness through various channels on tactics employed by scamsters
- ▶ Putting up advice/warnings on websites


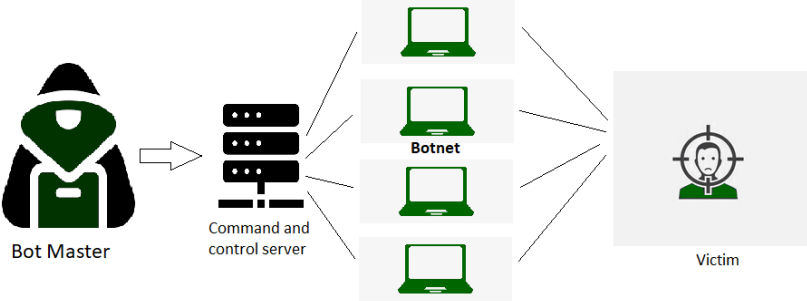
Online Sextortion

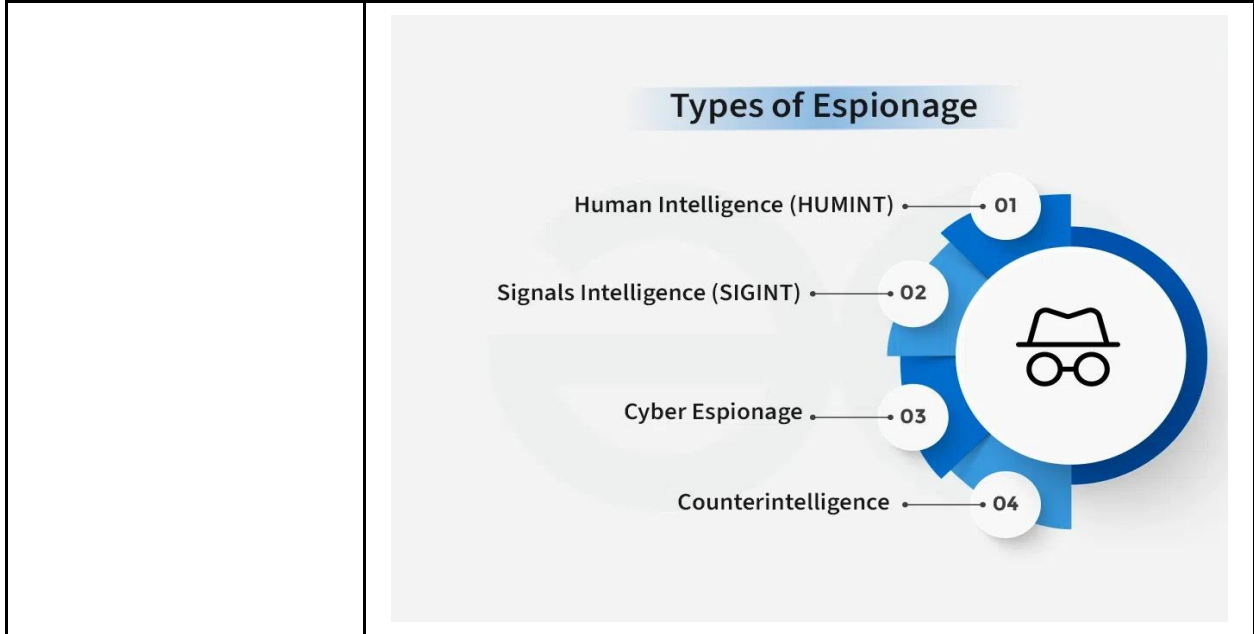
- **Online Sextortion** occurs when someone threatens to distribute **private and sensitive material** using an **electronic medium** if he/she doesn't provide images of a **sexual nature, sexual favours, or money**.

How to deal with Sextortion and Online Blackmailing?

- Never post personal information online
- Use strict social media privacy settings
- Be cautious on dating apps
- Never accept friend request from unknown people
- Never click on unverified links
- Do not accept video call requests from unknown numbers

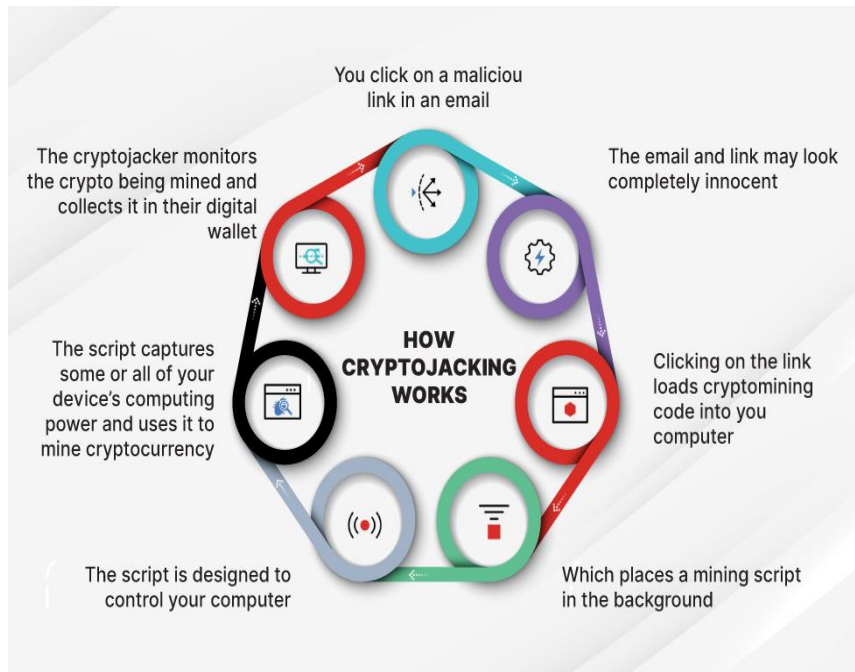
<p>SIM Swap Scam</p>	<ul style="list-style-type: none"> • SIM Swap Scam occurs when fraudsters manage to get a new SIM card issued against a registered mobile number fraudulently through the mobile service provider. • With the help of this new SIM card, they get One Time Password (OTP) and alerts, required for making financial transactions through the victim's bank account. • Getting a new SIM card against a registered mobile number fraudulently is known as SIM Swap. <div data-bbox="565 810 1414 1493" style="text-align: center;"> <h3 style="background-color: #003366; color: white; padding: 10px; margin: 0;">How a SIM Swap Scam Works:</h3> <p>Attacker collects data on victim (through social media, phishing, etc.)</p> <p>Now, thief gets incoming calls and texts meant for the victim — including account access codes.</p> <p>Thief calls phone service provider, impersonates victim.</p> <p>Thief tricks carrier into switching victim's mobile number to SIM card on thief's phone.</p> </div>
<p>Phishing</p>	<ul style="list-style-type: none"> • Phishing is a type of fraud that involves stealing personal information such as Customer ID, IPIN, Credit/Debit Card number, Card expiry date, CVV number, etc. through emails that appear to be from a legitimate source.

	
<p>Denial Of Services /Distributed DoS</p>	<ul style="list-style-type: none"> • Denial of Services (DoS) attack is an attack intended for denying access to computer resources without permission of the owner or any other person who is in-charge of a computer, computer system or computer network. • A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. 
<p>Spamming</p>	<ul style="list-style-type: none"> • Spamming occurs when someone receives unsolicited commercial messages sent via email, SMS, MMS and any other similar electronic messaging media.

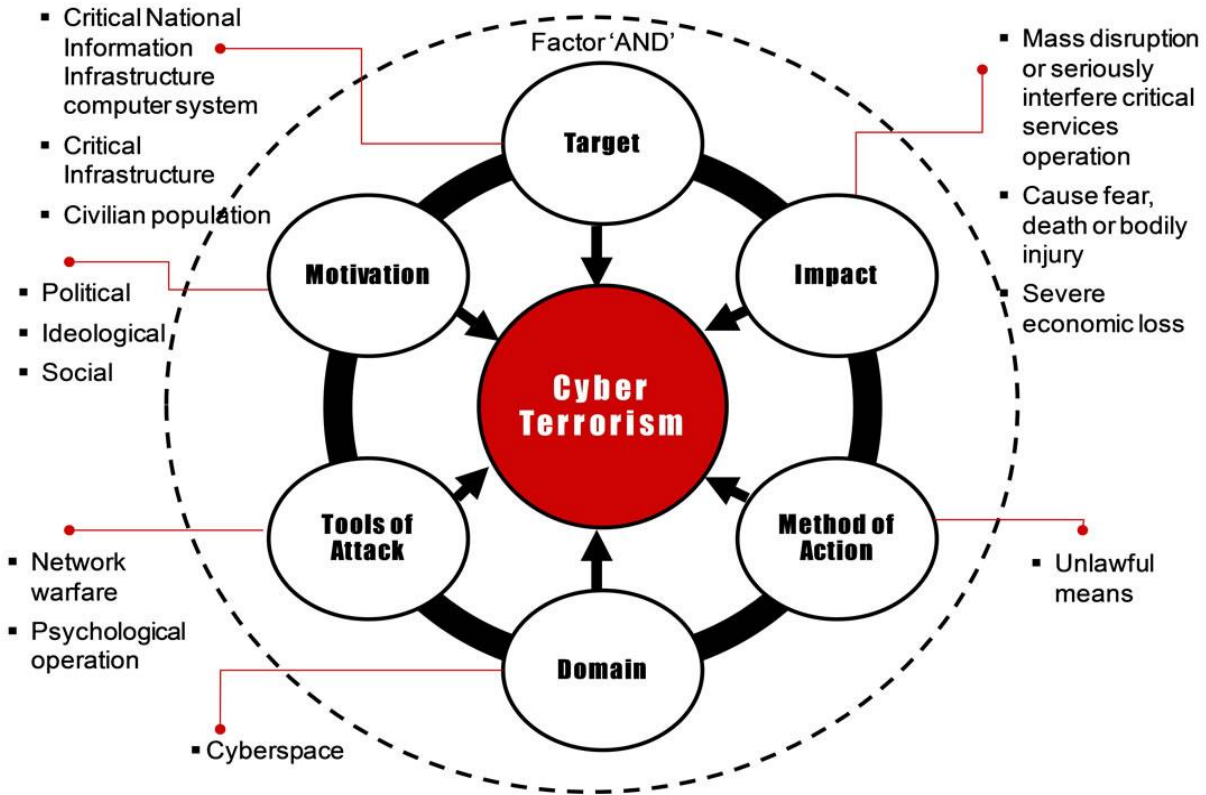


Cryptojacking


- **Cryptojacking is the unauthorized use of computing resources to mine cryptocurrencies.**



5. Enlist a range of cybercrimes against the government?



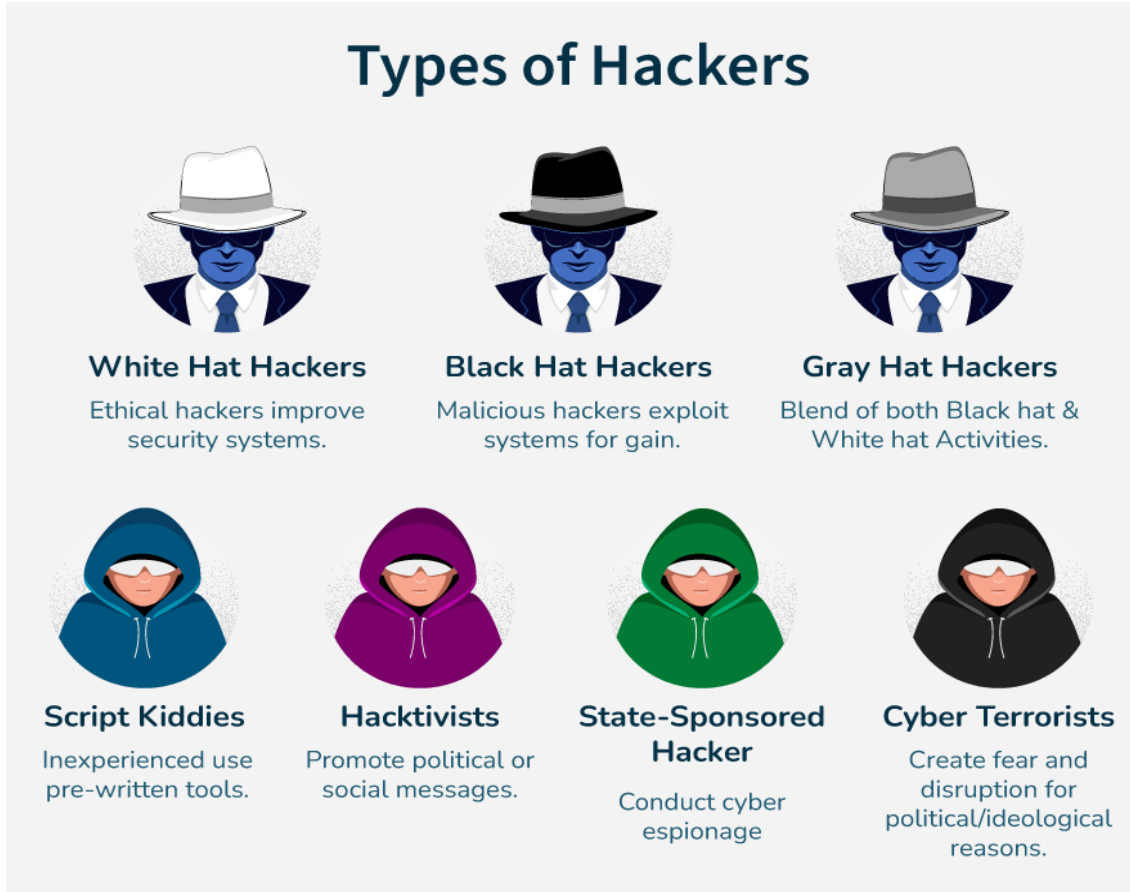
Cybercrime	Analysis
<p>Cyber Terrorism</p>	<ul style="list-style-type: none"> ● Cyber Terrorism is a major burning issue in the domestic as well as global concern. ● The common form of these terrorist attacks on the internet is by distributed denial of service attacks, hate websites and hate emails, attacks on sensitive computer networks etc. ● Cyber terrorism activities endanger the sovereignty and integrity of the nation.
<p>Cyber Warfare</p>	<ul style="list-style-type: none"> ● It refers to politically motivated hacking to conduct sabotage and espionage.

	<ul style="list-style-type: none"> • It is a form of information warfare sometimes seen as analogous to conventional warfare although this analogy is controversial for both its accuracy and its political motivation. <p style="text-align: center;">7 Types of Cyberwarfare Attacks</p> <div style="text-align: center;">  <p style="text-align: center;"> Espionage Sabotage Denial-of-service (DoS) Attacks Electrical Power Grid Propaganda Attacks Economic Disruption Surprise Attacks </p> </div>
<p>Distribution of pirated software</p>	<ul style="list-style-type: none"> • Distribution of pirated software means distributing pirated software from one computer to another intending to destroy the data and official records of the government.
<p>Possession of Unauthorized Information</p>	<ul style="list-style-type: none"> • It is very easy to access any information by the terrorists with the aid of the internet and to possess that information for political, religious, social, ideological objectives.

6. What is Hacking and enlist its types?

- **Hacking in cyber security** refers to the **misuse of devices like computers, smartphones, tablets, and networks to cause damage to or corrupt systems, gather information on users, steal data and documents, or disrupt data-related activity.**

- **Hacking first appeared as a term in the 1970s** but became more popular through the **next decade**.
- **Hacking can be of following types:**



Types of Hacking	Description
Black hat hackers	<ul style="list-style-type: none"> • Black hat hackers are the "bad guys" of the hacking scene. They go out of their way to discover vulnerabilities in computer systems and software to exploit them for financial gain or for more malicious purposes, such as to gain reputation, carry out corporate espionage, or as part of a nation-state hacking campaign.



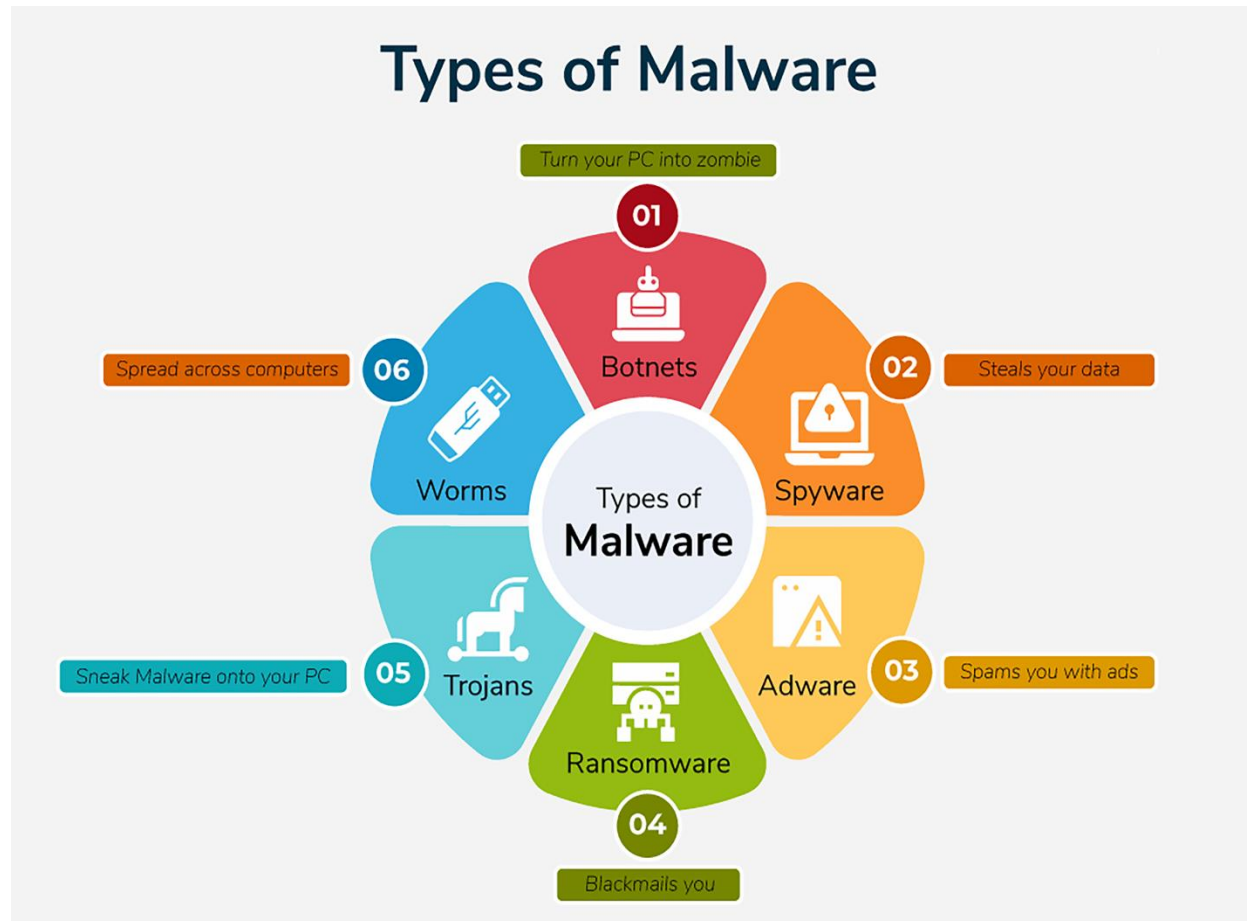
White hat hackers

- **White hat hackers** can be seen as the “good guys” who attempt to **prevent the success of black hat hackers** through **proactive hacking**.
- They use their technical skills to break into systems to **assess and test the level of network security**, also known as **ethical hacking**.
- This helps expose **vulnerabilities in systems before black hat hackers can detect** and exploit them.
- The **techniques white hat hackers use are similar** to or even identical to those of black hat hackers, but these individuals are **hired by organizations to test and discover potential holes in their security defenses**.



<p>Grey hat hackers</p>	<ul style="list-style-type: none"> • Grey hat hackers sit somewhere between the good and the bad guys. • Unlike black hat hackers, they attempt to violate standards and principles but without intending to do harm or gain financially. • Their actions are typically carried out for the common good. For example, they may exploit a vulnerability to raise awareness that it exists, but unlike white hat hackers, they do so publicly. • This alerts malicious actors to the existence of the vulnerability.
--------------------------------	---

7. What is malware and mention its types?



- Malware is **malicious software** that a **cybercriminal/hacker** creates to **disrupt/damage computer/s** or derive financial benefits.
- It is often **spread by way of an unsolicited email attachment** or download link.
- They can be of following types:

Types of Malware	Analysis
Virus	<ul style="list-style-type: none"> • It is a self-replicating program that attaches to a clean file and spreads in a computer system infecting other files.
Trojans	<ul style="list-style-type: none"> • Trojans disguises as legitimate software and users are tricked into uploading Trojans onto their devices where they cause damage or collect data.
Spyware	<ul style="list-style-type: none"> • Spyware is a program that secretly records what a user does, and then this information is misused.
Ransomware	<ul style="list-style-type: none"> • Ransomware locks down a user's files/data, the user can not access them unless a ransom is paid. Example - Wannacry and Petya.
Adware	<ul style="list-style-type: none"> • Adware is advertising software that can be used to spread malware.
Logic Bombs	<ul style="list-style-type: none"> • A logic bomb is a malicious program that uses a trigger to activate the malicious code. • The logic bomb remains non-functioning until that trigger event happens. • Once triggered, a logic bomb implements a malicious code that causes harm to a computer.

- **Cybersecurity specialists recently discovered logic bombs** that attack and destroy the hardware components in a workstation or server including the **cooling fans, hard drives, and power supplies.**
- **The logic bomb overdrives these devices until they overheat or fail.**



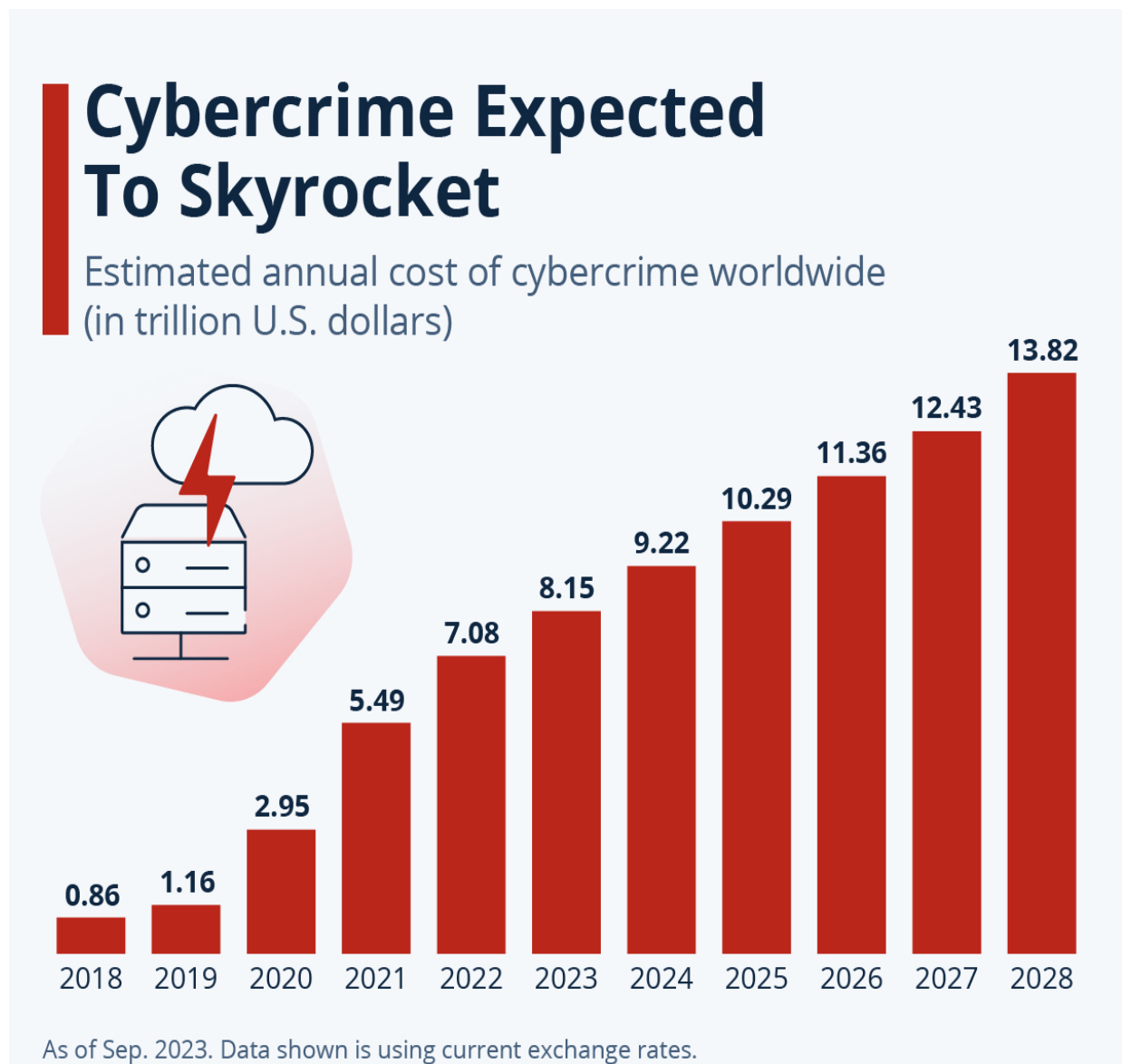
Keyloggers

- **Keylogger** records everything the user types on his/her **computer system to obtain passwords** and other sensitive information and send them to the source of the **keylogging program.**



Backdoors	<ul style="list-style-type: none">• A backdoor bypasses the usual authentication used to access a system.• The purpose of the backdoor is to grant cyber criminals future access to the system even if the organization fixes the original vulnerability used to attack the system.
------------------	---

8. Enlist data on global cyberattacks?



3 Key Cybersecurity Statistics You Must Know

1 The highest number of malware attacks by country

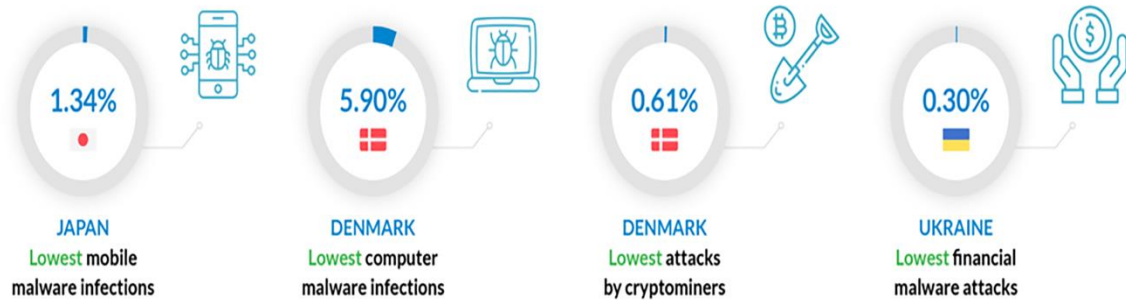


2 Governments & industries worldwide spend more on cybersecurity

Top industries with the fastest security spending growth worldwide:

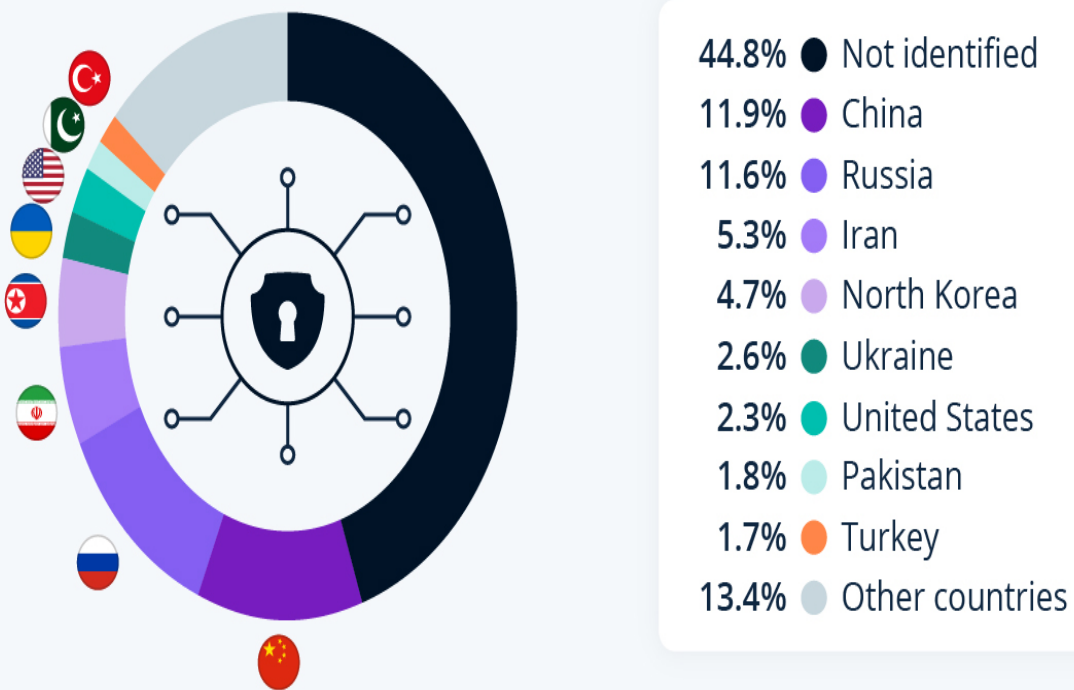


3 The lowest number of malware attacks by country



Who's Behind Cyber Attacks?

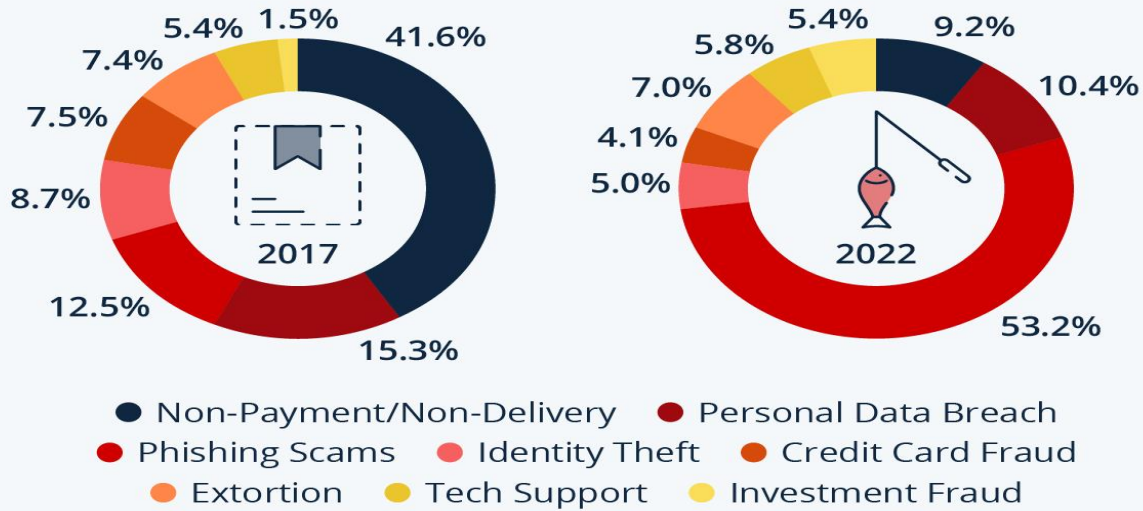
Countries responsible for the largest share of cyber incidents with a political dimension from 2000 to 2023



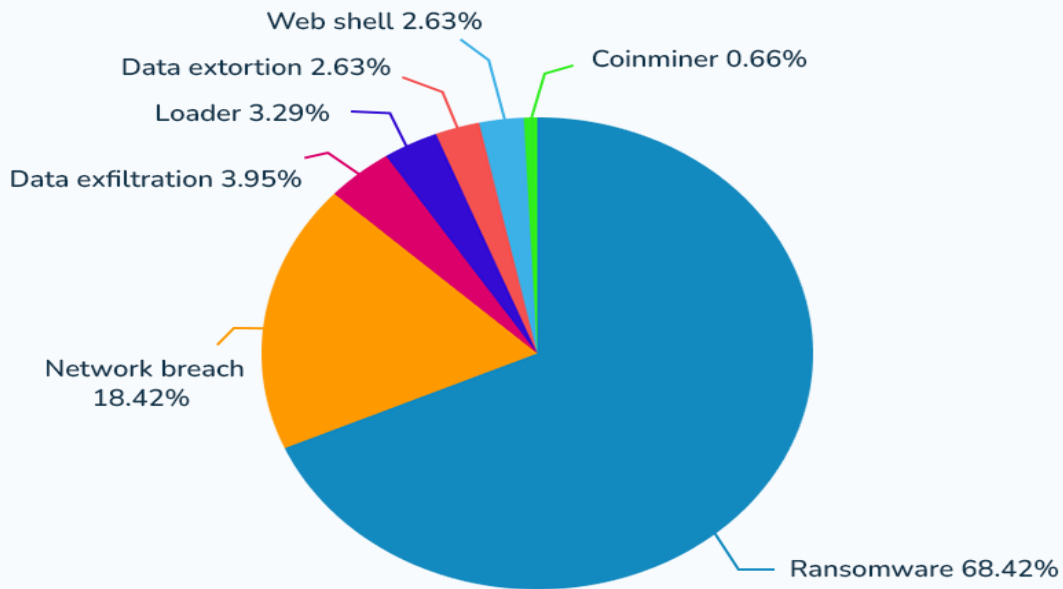
Analysis of 2,506 incidents: politicized/non-politicized attacks on political targets, attacks on critical infrastructure, attacks carried out by states/affiliated groups/non-state actors with political objectives

The Most Prevalent Forms of Cyber Crime

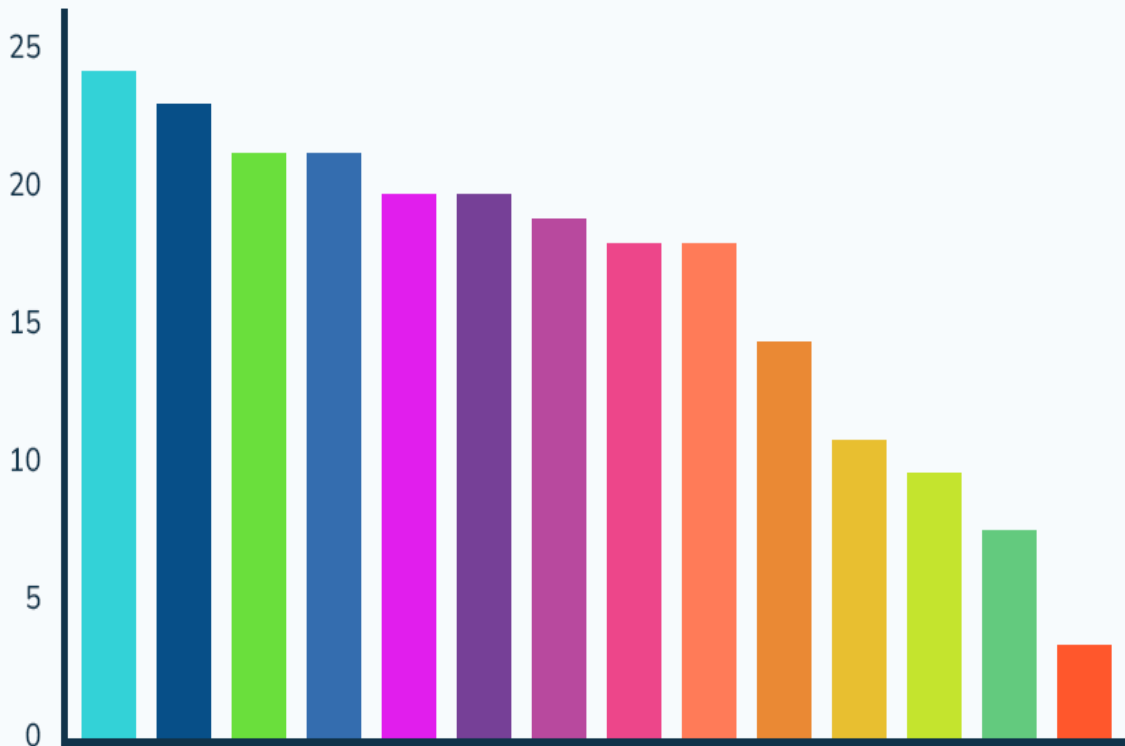
Share of worldwide cyber attacks by type



Distribution of Detected Cyberattacks Worldwide in 2022, by Type

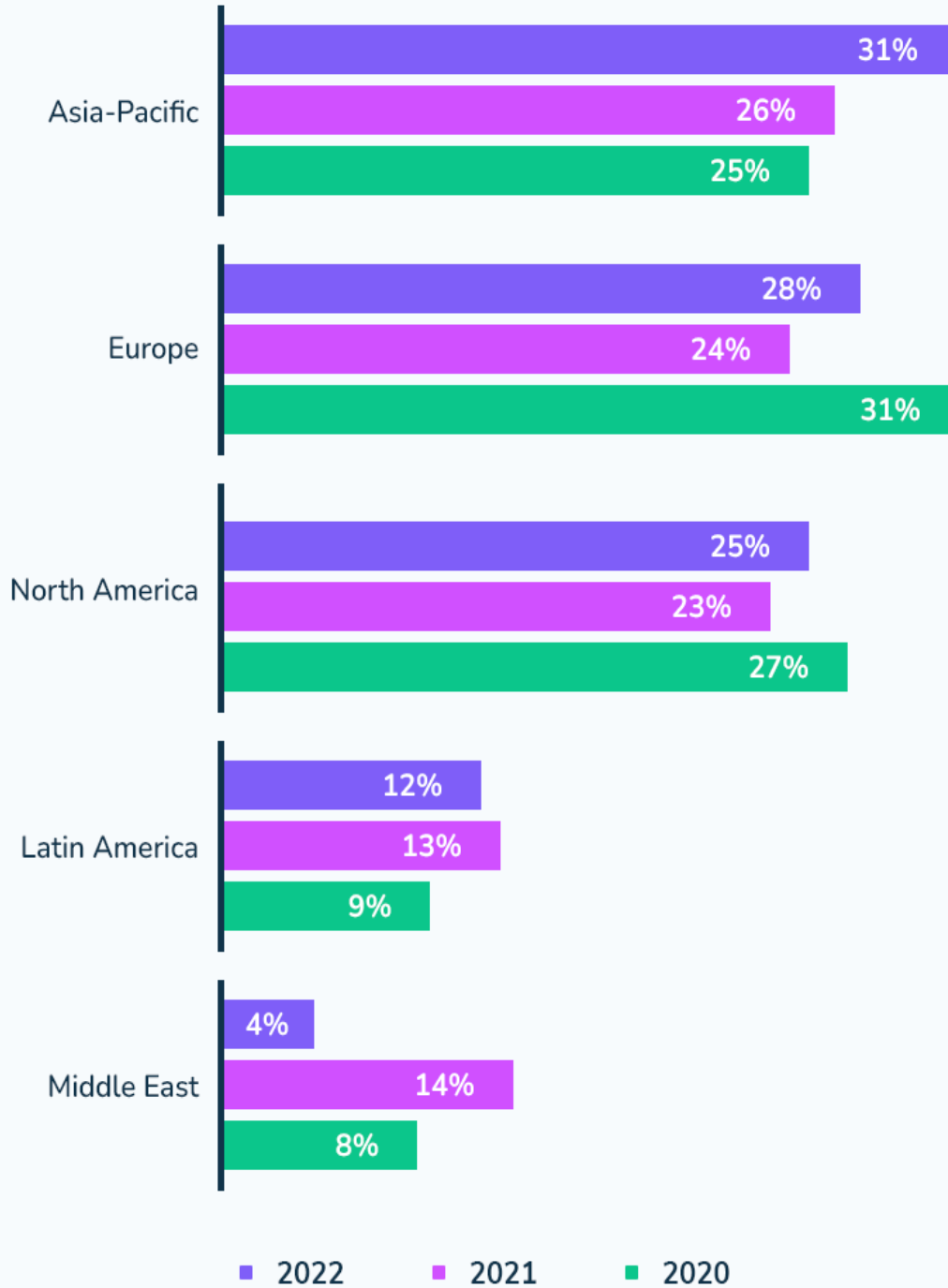


Biggest Cyber Security Threats Identified by Security Leaders in APAC-based Organizations

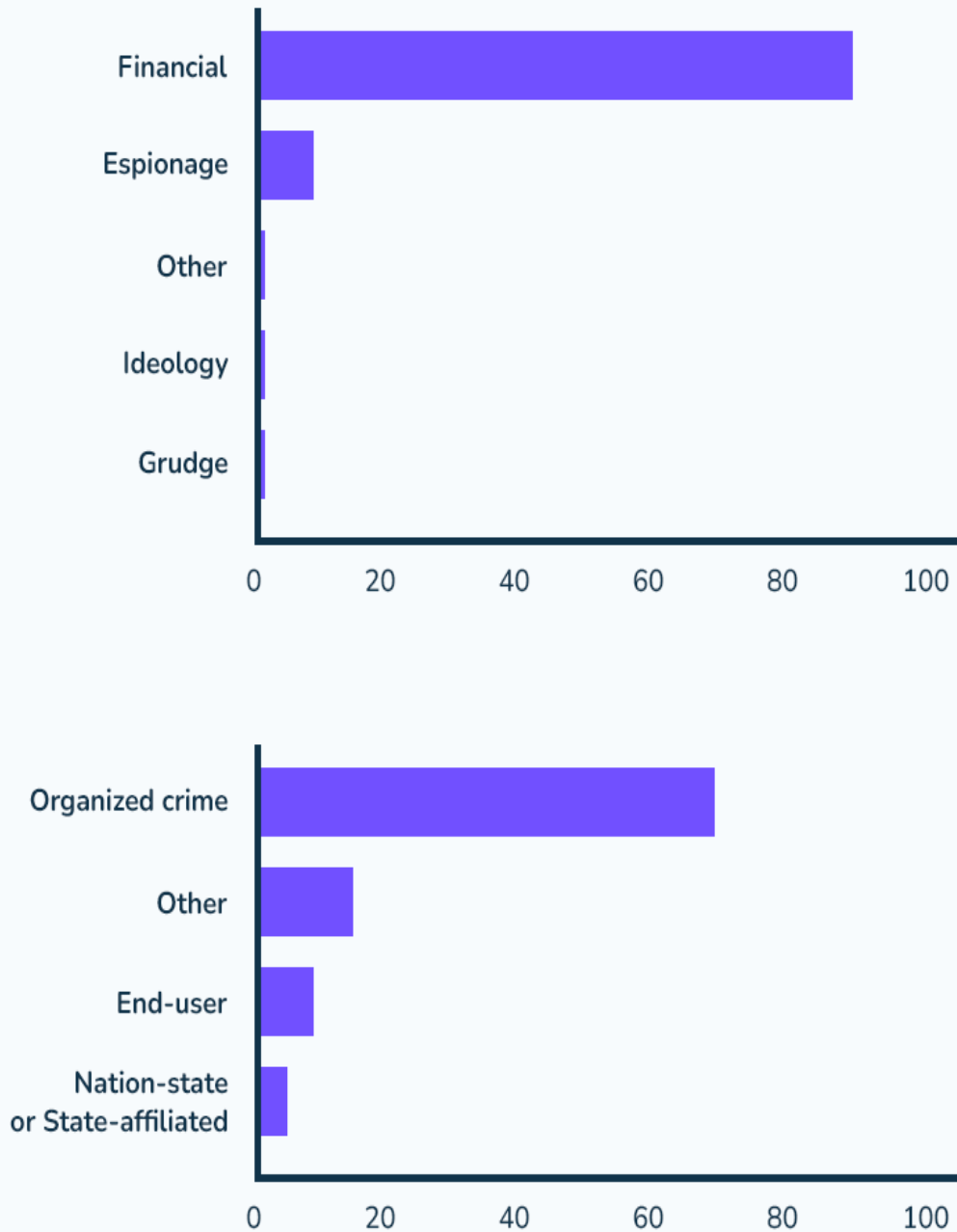


- DDoS attacks
- Malicious code commits
- Key employee/role targeting or unsafe cloud apps
- Malware
- Account takeover/BEC/
- Third-party breach
- Man-in-the-middle attack
- Malicious cloud apps
- Ransomware
- Malicious mobile apps
- Phishing
- Social engineering
- Wire transfer fraud
- All threats are equally impactful

Cyber Security Incidents by Region, 2022



Cyber Security Threat Actor Motives and Identity Categories



9. What is Digital Arrest?

- **Digital Arrest** is a new and **innovative tactic** employed by cybercriminals to defraud gullible victims and extort money.

WEB OF CRIME



Feb 2024: The founder-CEO of a private firm lost Rs 2.3 crore to FedEx fraudsters. The resident of CV Raman Nagar filed a complaint with East CEN Crime police on Feb 16

Feb 2024: A retired IAS officer lost Rs 11.5 lakh to tricksters. The resident of CBD area filed a complaint with High Grounds police

Jan 2024: A 70-year-old journalist lost Rs 1.2 crore. The resident of CBD area was under 'digital

arrest' from Dec 15 to Dec 23. She filed a complaint with East CEN crime police

Dec 2023: Criminals duped an IISc professor of Rs 82 lakh. The 60-year-old professor was under 'digital arrest'. She lodged a complaint with Sadashivanagar police

Nov 2023: A 58-year-old retired man was conned of Rs 1.8 crore. As he filed a complaint in the golden hour, North CEN Crime police were able to freeze most of his money and arrest eight fraudsters

In 2024, India faced significant losses from digital arrest scams, with ₹1,777 crore lost in the first four months alone.

‘DIGITAL ARREST’

What exactly is ‘Digital arrest’?

- New **cyber fraud**
- Accused video call and **pose as law enforcement agency officials**, like CBI or customs officials
- They **give threats of arrest** in the name of fake international parcels of banned drugs
- **Organised economic crime** operated by cross-border crime syndicates



‘DIGITAL ARREST’

How Fraudsters Trick Victims and Evade Police (1/2)

➤ They use **studios** modelled on police stations and government offices while video-calling victims



➤ They wear **uniforms** to appear genuine

➤ They play **police sirens** in the background and send **fake IDs** to make the 'digital arrest' seem real

‘DIGITAL ARREST’

How Fraudsters Trick Victims and Evade Police (2/2)

- They use **third-party** bank accounts
- They tell victims that the investigation is **confidential**, deterring them from discussing it with anyone
- They transfer money received from victims into **fraudulent accounts**, cash it out and split it among themselves



‘DIGITAL ARREST’

What to do if someone contacts you and threatens you with arrest?

- ▶ Stop all further communication and disconnect from the internet immediately
- ▶ Report the incident to local police or cyber crime authorities by calling **1930** (24/7 helpline number)
- ▶ Contact your bank and freeze accounts or change passwords if necessary
- ▶ Keep evidence like call recordings, messages, and screenshots



‘DIGITAL ARREST’

How do you avoid getting trapped?

- ▶ **Never trust unsolicited calls** claiming to be from law enforcement agencies
- ▶ **Verify caller’s identity** by contacting the agency directly through official numbers



- ▶ **Do not share personal details** like ID, bank, or passport information over video calls
- ▶ **Install a reliable cybersecurity app** to alert you of potential scams

‘DIGITAL ARREST’

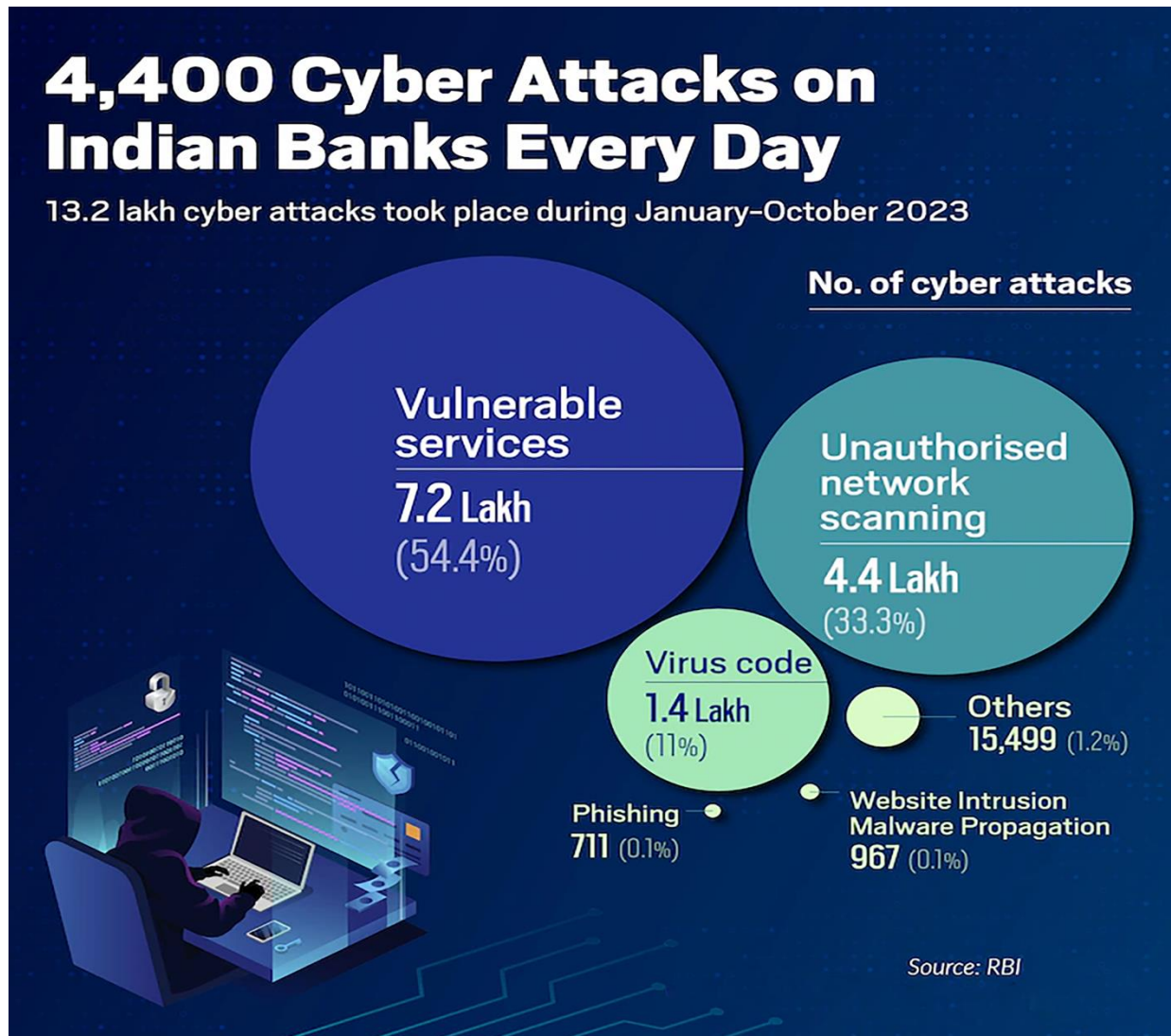
Steps to take if you’re already a victim and have lost money



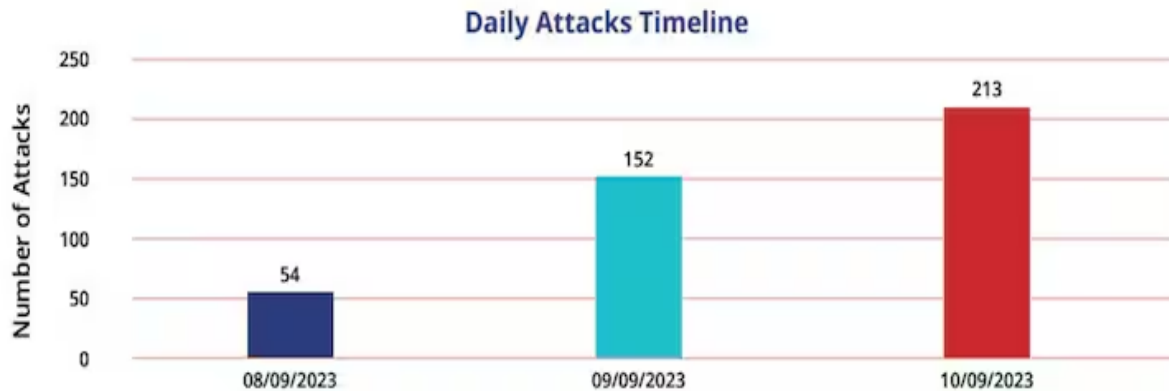
- Immediately report the transaction to your bank and request a reversal or freeze
- File a formal complaint with the National Cyber Crime Reporting Portal (cybercrime.gov.in)
- Seek help from a lawyer to assist in legal matters and protect your identity
- Gather all evidence for the authorities, including call logs, messages, and transaction details

10. What is the status of cybercrime in India?

- **India was placed on the 80th position** in a report focusing on local threats in the year **2023**.
- The position is based on the **malicious programmes found directly on users' computers or removable media connected to them** (flash drives, camera memory cards, phones, external hard drives) or that initially made their way onto the computer in non-open form, including programmes in **complex installers or encrypted files**.
- Additionally, nearly **34% of users in India were targeted by local threats, amounting to some 74,385,324 local incidents being blocked by Kasperksy products**.



Several hacktivist groups target India during the G20 Summit



₹276

CRORE

AMOUNT INVOLVED
IN DEBIT AND
CREDIT CARD FRAUD
IN 2022-23, PER AN
RBI REPORT

5.2

MILLION

MOBILE
CONNECTIONS
USING FAKE
DOCUMENTS CULLED
BETWEEN APRIL AND
AUGUST 2023

700

THOUSAND

COMPLAINTS OF
ONLINE FRAUD ON
1930 HELPLINE IN
APRIL 2023 ALONE

71.8

THOUSAND

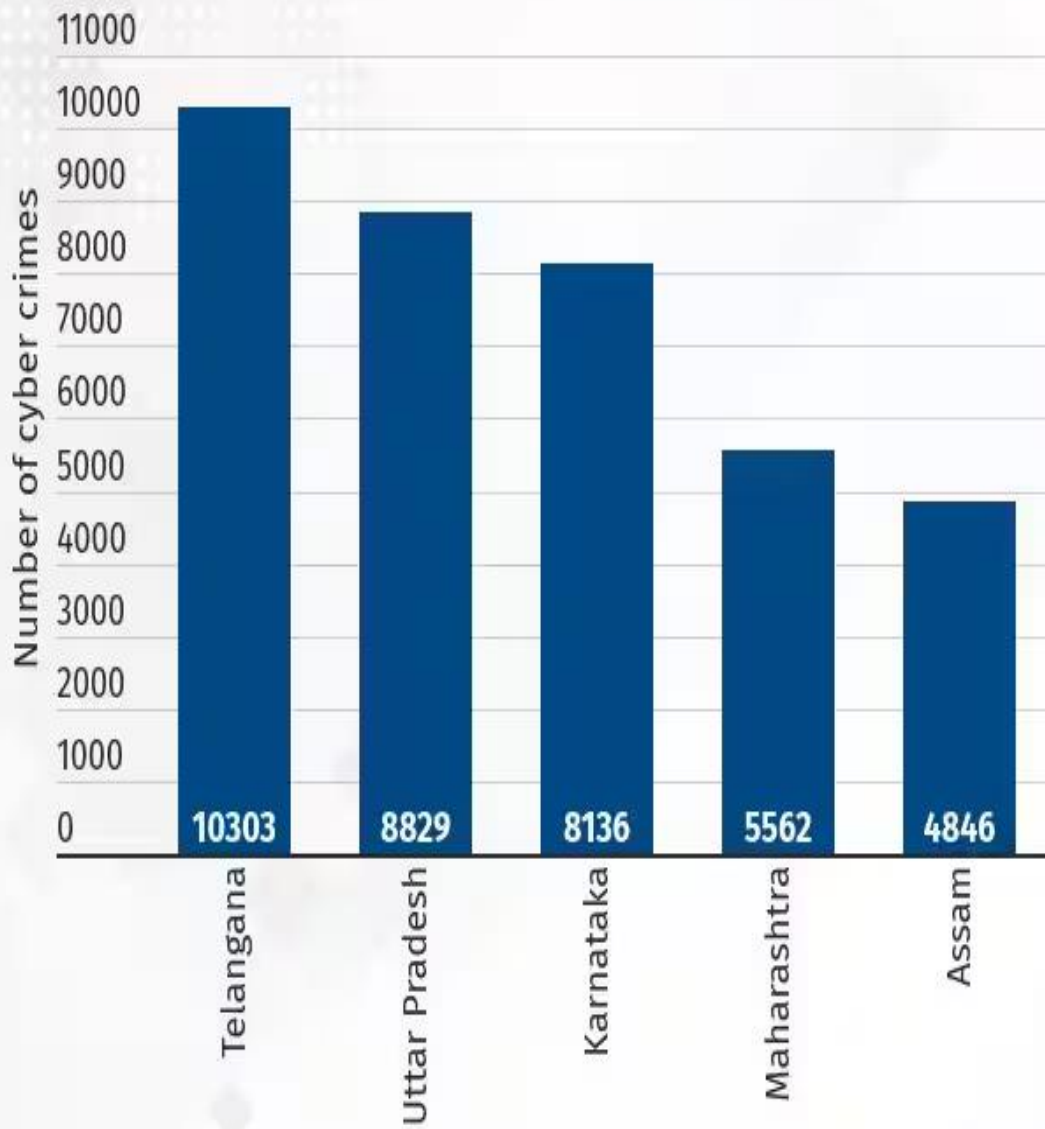
CYBERCRIME
CASES PENDING
INVESTIGATION AT
THE END OF 2021,
PER NCRB DATA

40

PER CENT

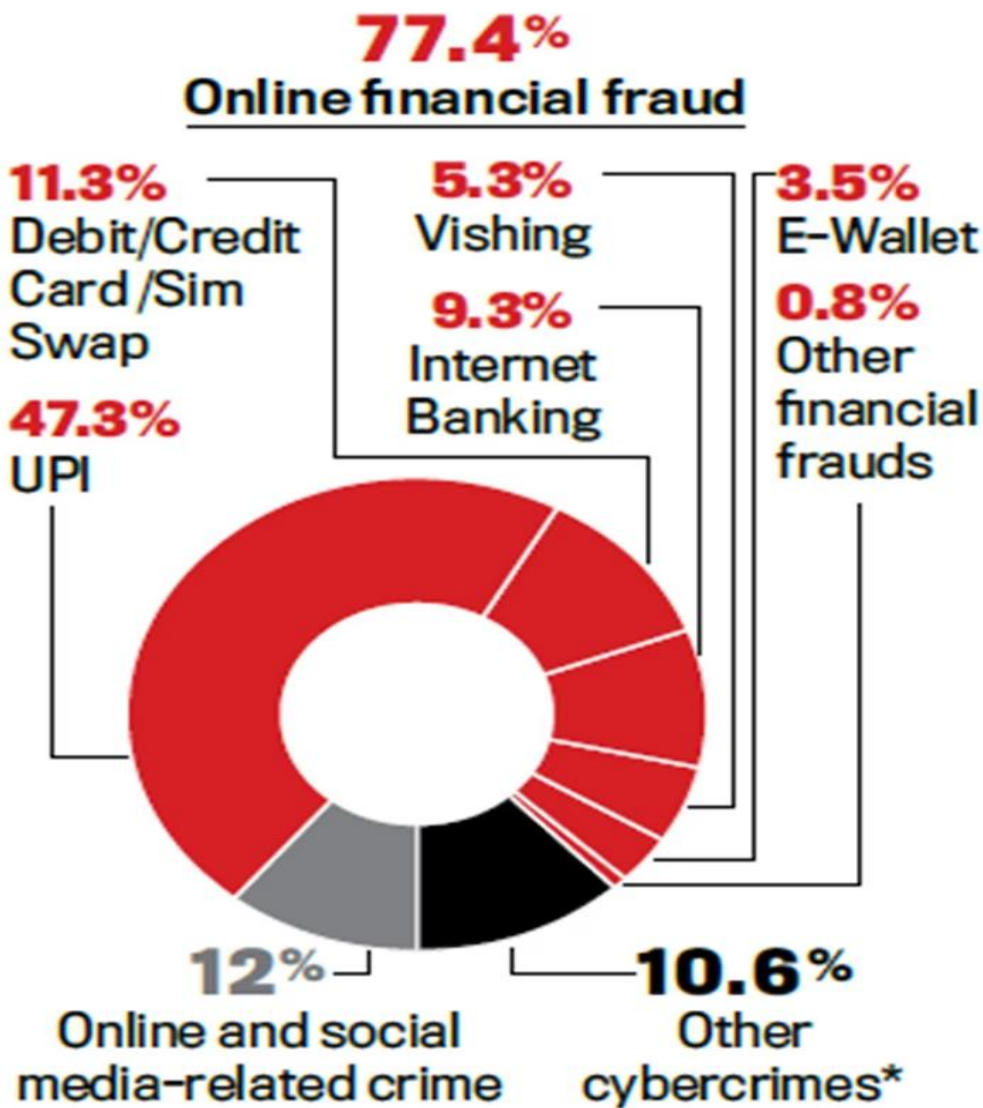
INDIA'S SHARE IN
GLOBAL DIGITAL
PAYMENT USAGE,
ACCORDING TO THE
GOVERNMENT

STATES WHICH RECORDED THE HIGHEST NUMBER OF CYBER CRIMES IN 2021

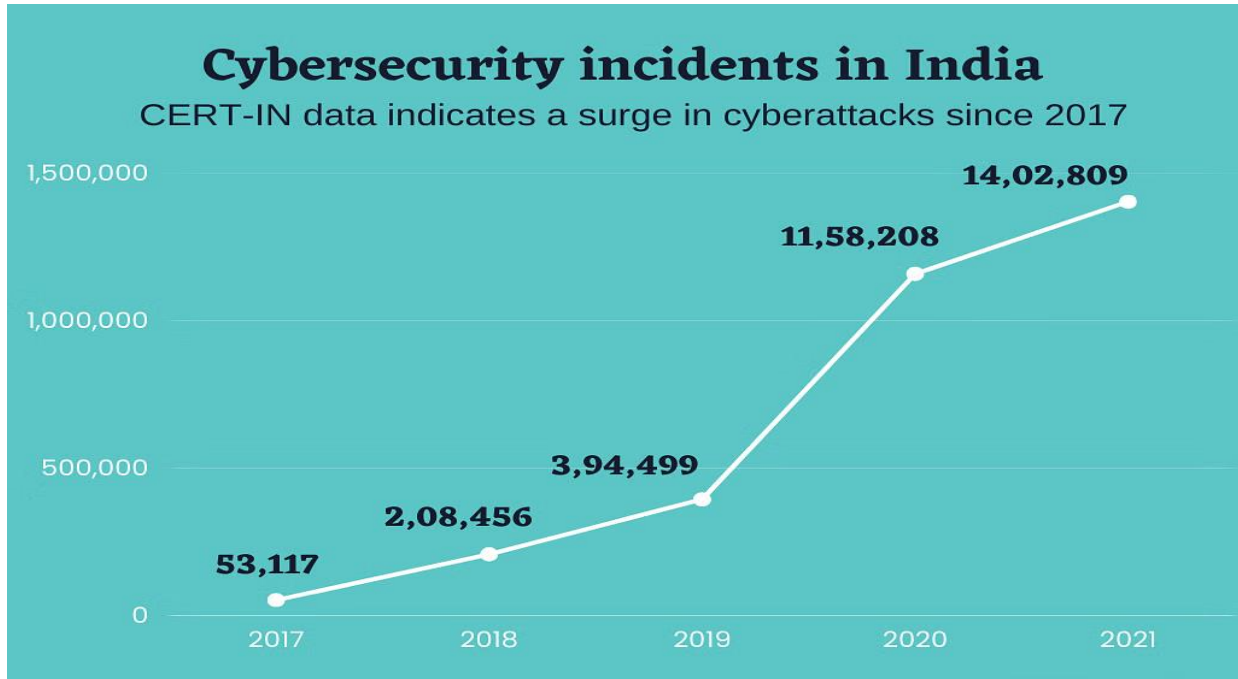


CYBERCRIME TRENDS

Break-up of internet offences between Jan. 2020 and Jul. 2023



**Hacking, cyber trafficking, ransomware, cryptocurrency frauds, cyber terrorism and deepfake crimes; Source: Future Crime Research Foundation*



11. Enlist the findings of the India Cyber Threat Report 2023?

- The India cyber threat report 2023 is released by the Data Security Council of India (DSCI) and Quick heal.

Key Highlights

<p>> 400 million detections across ~8.5 million endpoints</p>	<p>Averaging 761 detections per minute</p>	<p>~49 million detections stem from behaviour-based analysis, constituting 12.5% of all</p>
--	---	--

Ransomware & Malware
Ransoms authors continually evolve their methodologies and employ sophisticated techniques to evade traditional signature-based detection.

<p>Ransomware incident ratio ~1 per 650 detections</p>	<p>Malware incident ratio ~1 per 38,000 detections</p>	<p>Cryptojacking Emerging as a significant threat with over 5 million detections in a year</p>
---	---	---

Malware Attack Spectrum

<p>Dominant Threats 41% Trojans & 33% Infectors</p>	<p>Geographical Hotspots 15% Telangana & 14% Tamil Nadu</p>	<p>City-wise Analysis 15% Surat & 14% Bengaluru</p>
--	--	--

Top Three Industries

 Automobile	 Government	 Education
----------------	----------------	---------------

Attack Vectors

>50% of detections are associated with removable media and network drives.

~25% of attacks result from clicking on malicious links in emails and websites.

Mobile Threat Landscape

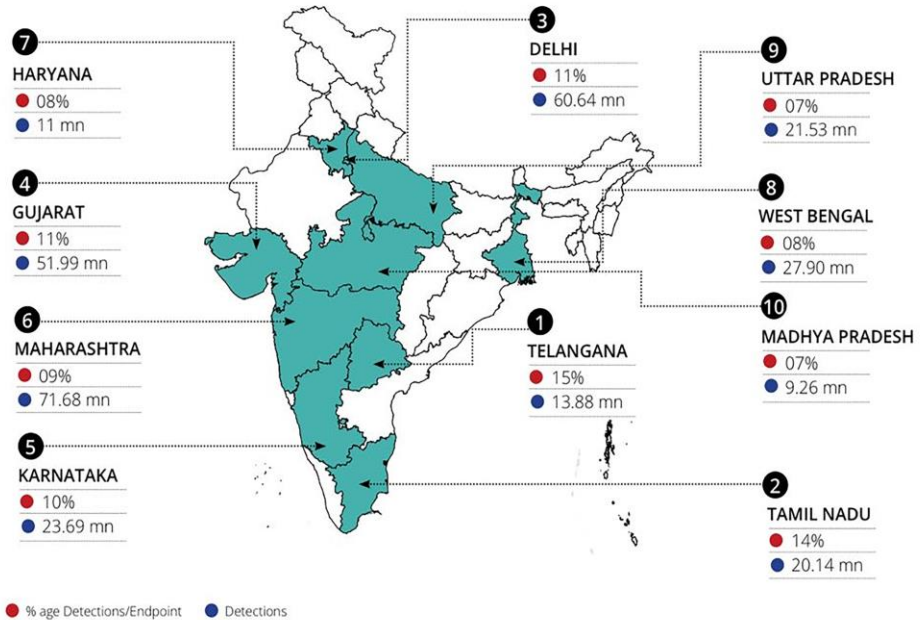
An average of ~3 attacks in a month per Android device

Top 10 States with Highest Malware Detections

~ 70% of the total detections originate from these states.

290 mn Detections

- ▶ The number of detections varies across different states of India, depending on the installation base, the availability of computing devices, and the presence of IT/ITeS industries.
- ▶ Telangana and Tamil Nadu have the highest ratio of detections per installation, while Maharashtra, Gujrat and Delhi have the highest absolute number of detections.
- ▶ Gujarat and Madhya Pradesh show an increase in detections, reflecting the emergence of new IT/ITeS hubs in these states.

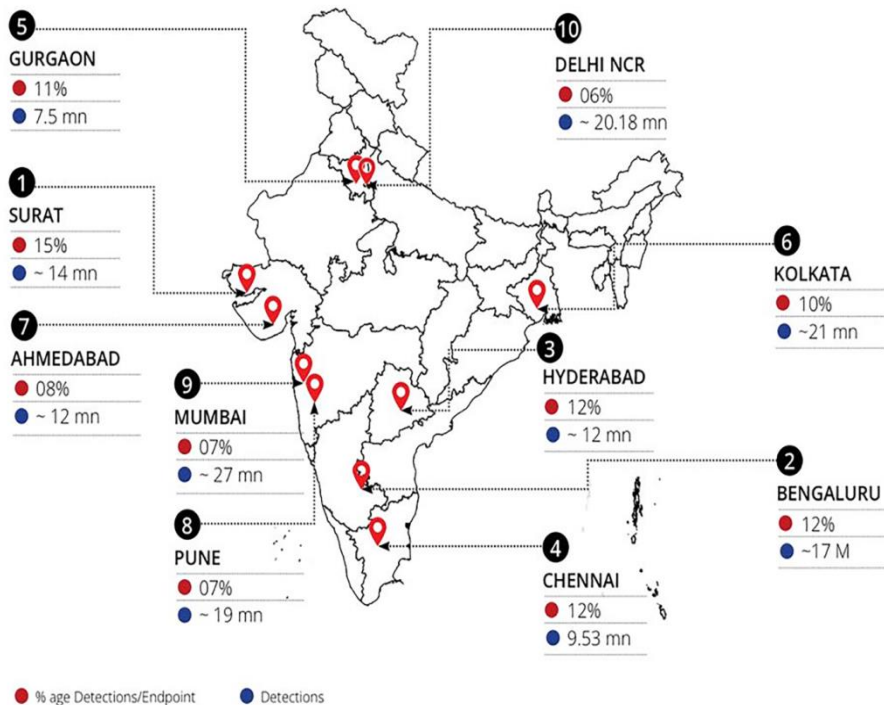


Top 10 Cities with Highest Malware Detections

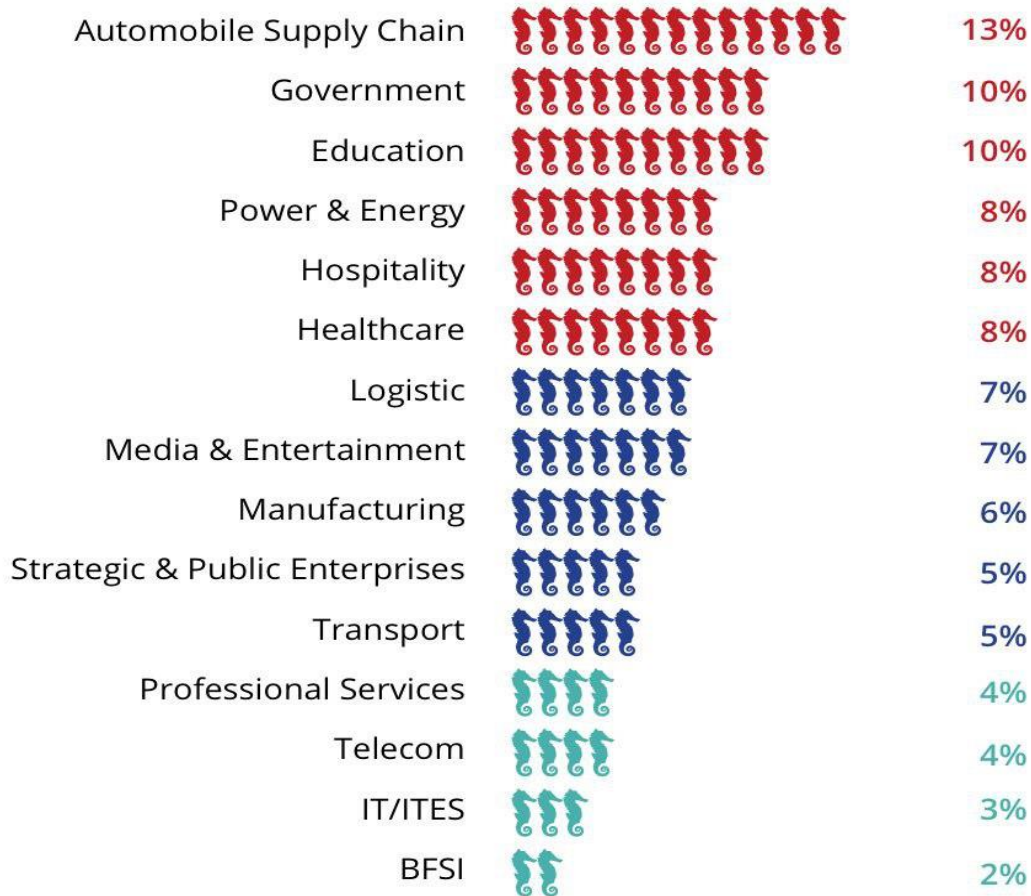
~40% of the total detections originate from these cities.

160 mn Detections

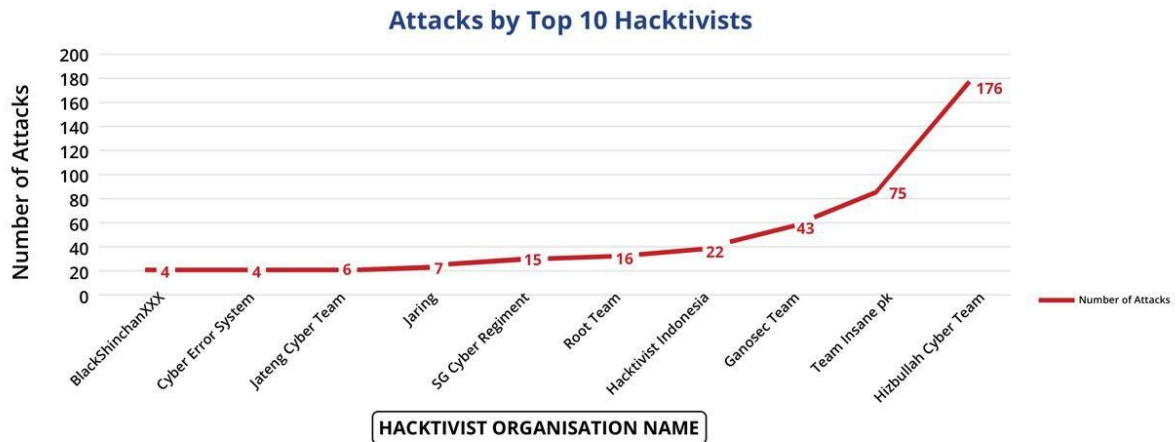
- ▶ A city-wise analysis reveals that Mumbai, Pune, Chennai and Bangalore have the highest number of detections in absolute terms. Surat and Ahmedabad, which have emerged as new IT/ITeS hubs, have high detections relative to their installation base.
- ▶ The top 10 cities account for more than 50% of the detections, while the remaining detections are spread across tier II and III cities and towns in India. This may be due to the rise of work-from-hometown culture amid the pandemic.



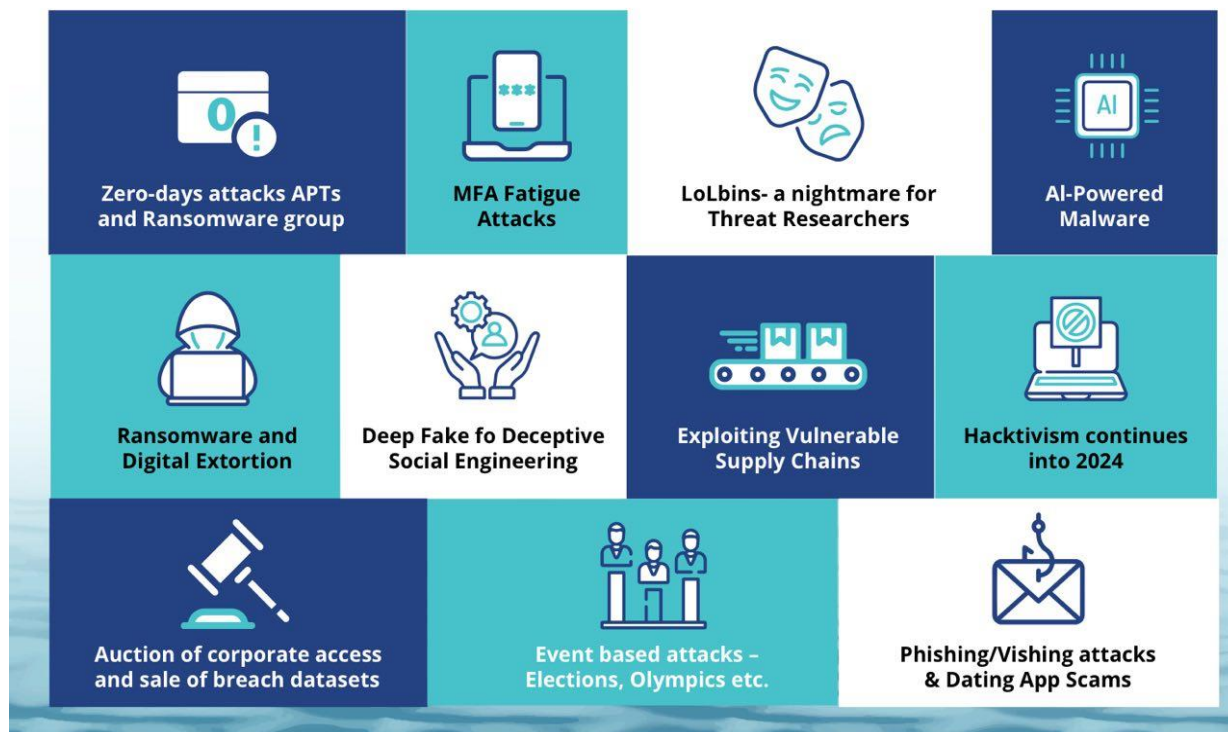
India Malware Landscape: Sectoral Analysis



INDUSTRY-WISE PERCENTAGE DETECTIONS PER INSTALLATION BASE



Cyber Threat Predictions for 2024



12. What are the reasons for rising cyber crimes in India?

India's poor cyber awareness
due to lack of board buy-in
and low digital literacy levels

According to a report by the FBI, India ranked third in the world among the top 20 countries being victimised by cyber crimes!



- The rise of **cybercrime in India** is a complex issue, with **several key factors contributing to its growth and impact.**
- Here are the **few important reasons for the rise of cybercrime in India.**

Reasons	Analysis
<p>Increasing Internet Penetration</p>	<ul style="list-style-type: none"> • India has witnessed a remarkable surge in Internet penetration, driven by the availability of affordable smartphones and low-cost data plans. • While this digital revolution has brought numerous benefits, it has expanded the potential target pool for cybercriminals. <div style="text-align: center; border-top: 1px solid black; padding-top: 10px;"> <p>INDIA 2ND LARGEST AFTER CHINA</p> </div>
<p>Rapid Digital Transformation</p>	<ul style="list-style-type: none"> • Various sectors in India, including banking, e-commerce, healthcare, and government services, have undergone rapid digital transformation.

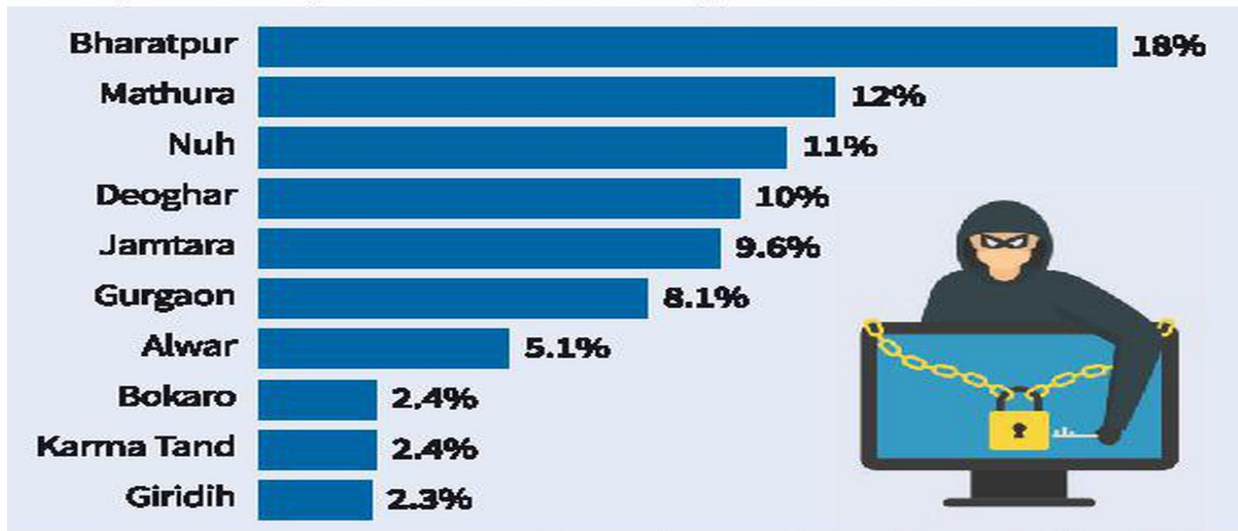
<p>Data Privacy Concerns</p>	<ul style="list-style-type: none"> • With organizations’ increasing collection and storage of personal data, data privacy concerns have risen. • The unauthorized access, theft, or misuse of personal information can lead to identity theft, financial fraud, and other forms of cybercrime.
<p>Lack of cyber hygiene</p>	<ul style="list-style-type: none"> • Cyber hygiene refers to the set of practices and behaviors individuals and organizations adopt to maintain a secure and safe digital environment. • It encompasses a range of actions and precautions aimed at protecting digital assets, systems, and data from cyber threats and vulnerabilities. <div data-bbox="662 1073 1284 1150" style="text-align: center; background-color: #00e0c0; border-radius: 15px; padding: 5px; margin: 10px 0;"> <p>What happens if you have poor cyber hygiene?</p> </div>

CYBER CRIMES AND THEIR MOTIVES		Assam	National
▶ Personal revenge		802	1,724
▶ Anger		144	883
▶ Fraud		704	32,230
▶ Extortion		496	2,883
▶ Causing disrepute		175	1,715
▶ Prank		34	240
▶ Sexual exploitation		1,147	4,555
▶ Political motives		12	311
▶ Terrorist activities		3	11
▶ Inciting hate against country		12	31
▶ Disrupt public service		5	40
▶ Sale/purchase illegal drugs		10	14
▶ Developing own business		15	177

13. Mention about the epicenter of cybercrimes in India?

- According to a 2023 report, ‘A Deep Dive into Cybercrime Trends Impacting India’ by the Future Crime Research Foundation, an IIT Kanpur incubated start-up, among the top 10 cybercrime epicentres are **Bharatpur – Rajasthan (18%), Mathura – Uttar Pradesh (12%), Nuh – Haryana (11%), Deoghar – Jharkhand (10%) and Jamtara – Jharkhand (9.6%)**.
- The report said several common factors contribute to their vulnerability, including **geographical proximity to major urban centers, limited cybersecurity infrastructure, socioeconomic challenges, and low digital literacy**.

Top 10 cybercrime epicentres



INDIA'S CYBERCRIME HOTSPOTS

While Jharkhand's Jamtara district was once the hub of cybercrime in India, the menace has now spread to many parts of the country

DELHI

Ashok Nagar, Uttam Nagar, Shakarpur, Harkesh Nagar, Okhla, Azadpur

HARYANA

Mewat, Bhiwani, Palwal, Nuh, Manota, Hasanpur, Hathn Gaon

GUJARAT

Banaskantha, Surat, Ahmedabad

ANDHRA PRADESH

Chittoor

UTTAR PRADESH

Azamgarh

BIHAR

Banka, Begusarai, Jamui, Nawada, Nalanda, Gaya

ASSAM

Barpeta, Dhubri, Goalpara, Morigaon, Nagaon

WEST BENGAL

Asansol, Durgapur

JHARKHAND

Jamtara, Deogarh



15 NABBED IN DECEMBER



➤ Jamtara, the hub of cyber frauds, accounted for **30% of all cyber crime cases reported in 2022**

➤ Cops arrested **31 cyber criminals** from Jamtara, Giridih and Dhanbad

➤ **Every one of the six criminals**, who were nabbed for **cyber frauds** in the **past one year**, had a **Jamtara connection**

➤ In December alone, a **crackdown** on Jamtara-



➤ Most of these **fraudsters** targeted **senior citizens**, using **fake electricity bills**



A file photo of Jamtara. The area frequently visited by the cops last year during investigations into cyber fraud cases

based cyber fraud gangs led to **15 arrests**

PHISHING CAPITAL OF INDIA

➤ Jamtara resident **Badri Mondal** (25)

would call up people for details to update KYC

➤ He would tell the victims to download an app, ask for the OTP and take control of the bank account

➤ He would buy gift vouchers and send them to other gang members in Mumbai, who would buy costly items like mobile phones



➤ Jamtara is known as the phishing capital of India and a crime thriller is based on true incidents that happened there in 2015-16

ADVISORY

➤ Cyber police have often warned people not to share OTPs with anyone posing as a bank official

➤ They said people must use strong passwords, with a mix of numbers and characters, and separate passwords should be used for e-wallet app




➤ People should also log out after every transaction and should check mobile wallet statements carefully and regularly

14. What are the impacts of cybercrime in India?

Critical Infrastructure in India: Recent Cyberattacks & Security Incidents




Impacts	Analysis
<p>Financial Losses</p>	<ul style="list-style-type: none"> • Cybercrime has resulted in substantial financial losses for individuals, businesses, and the Indian economy as a whole. • Financial frauds, online scams, and identity thefts have become rampant, causing individuals to lose their hard-earned money and businesses to suffer significant financial setbacks. • According to the report of the Norton LifeLock survey, Rs. 1.24 trillion was lost in India in the past 12 months due to cybercrime. • In 2024, India faced significant losses from digital arrest scams, with ₹1,777 crore lost in the first four months alone.

	<ul style="list-style-type: none"> • Karnataka reported the highest number of cases, totalling 641 and ₹109 crore lost.
<p>Data Breaches and Privacy Concerns</p>	<ul style="list-style-type: none"> • Data breaches have become a recurring nightmare for Indian organizations, leading to the compromise of sensitive personal and financial information of millions of individuals. • Such breaches erode public trust and raise concerns about privacy and data protection. <p style="text-align: center;">OVERVIEW OF DATA BREACHES</p> <div style="text-align: center;">  <p>\$4.35 million was the average cost of a data breach in 2022.</p> </div> <hr/> <div style="text-align: center;"> <p>Data breaches impacted nearly 294 million people</p>  </div> <hr/> <div style="text-align: center;">  <p>Cloud-based data breaches made up 45% of all breaches.</p> </div>
<p>Disruption of Critical Infrastructure</p>	<ul style="list-style-type: none"> • Cyberattacks targeting critical infrastructure, such as power grids, transportation systems, and government networks, pose a severe threat to national security. • These attacks can disrupt essential services, cause economic instability, and even compromise public safety.

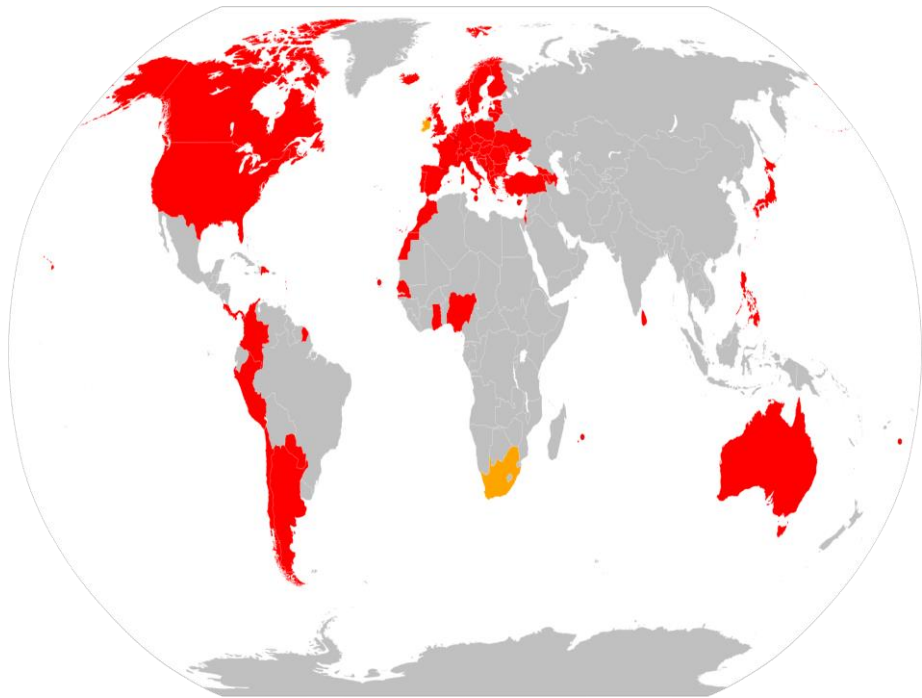
<p>Social and Psychological Impact</p>	<ul style="list-style-type: none"> • Cybercrime not only affects individuals and organizations financially but also has a profound social and psychological impact. • Victims of cyberbullying, online harassment, and cyberstalking often suffer from emotional distress, anxiety, and depression. • The psychological toll of cybercrime can be long-lasting and devastating.
---	---

15. Enlist global measures to tackle cybercrime?

Measure	Analysis
<p>Interpol Cybercrime Global Strategy 2022-2025:</p>	 <p>The diagram illustrates the Interpol Strategic Framework 2022-2025. At the center is a globe. Surrounding it are four main pillars: VISION (Connecting police for a safer world), MISSION (Preventing and fighting crime through enhanced cooperation and innovation on police and security matters), VALUES (Respect, Integrity, Excellence, Teamwork, Innovation), and STRATEGIC OBJECTIVES (Trusted Information for Action, Enrich Policing through Partnerships, Advance and Innovate Policing, Enhance Organizational Performance and Delivery).</p>
<p>Potential UN Cybercrime Treaty</p>	<ul style="list-style-type: none"> • UN member states have been negotiating an international treaty on countering cybercrime. • If adopted by the UN General Assembly, it would be the first binding UN instrument on a cyber issue.

Budapest Convention

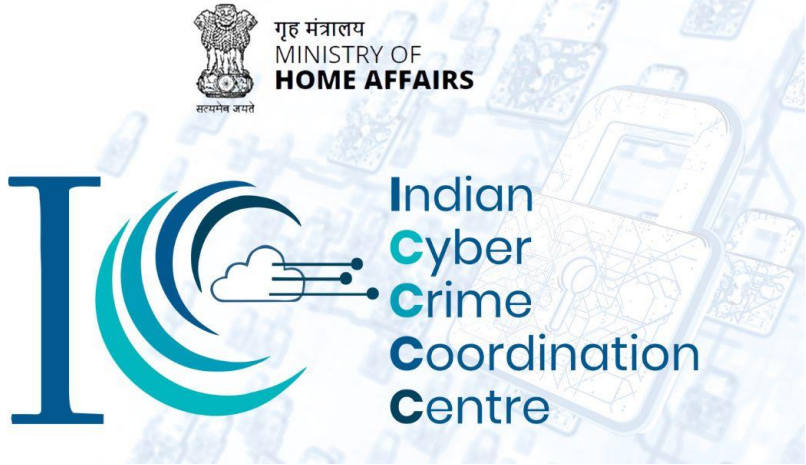

- **The Budapest Convention, also known as the Council of Europe Convention on Cybercrime, is an international treaty that aims to combat cybercrime.**
- **The treaty focused on harmonizing laws and increasing cooperation across borders so that a range of cybercrime could be prosecuted in the multiple countries affected.**
- **India decided not to participate in this convention.**




16. Enlist measures taken by the Government of India to combat cybercrime in India?





Measures	Analysis
<p>Indian Cyber Crime Coordination Centre (I4C)</p>	<ul style="list-style-type: none"> • The Indian Cyber Crime Coordination Centre (I4C) is a government initiative to deal with cybercrime in India, in a coordinated and effective manner. • It is affiliated to the Ministry of Home Affairs, Government of India. • The scheme was approved in October 2018 with a proposed amount of ₹415.86 crore.

	
<p>National Cyber Forensic Laboratory</p>	<ul style="list-style-type: none">• A National Cyber Forensic Laboratory (NCFL) has been set up at the Central Forensic Science Laboratory, Hyderabad to investigate important cases of digital fraud / cyber forensics.• This laboratory acts as a Model Laboratory for other Central and State Forensic Science Laboratories in the country. 


<p>CyTrain Portal</p>	<ul style="list-style-type: none"> • A Massive Open Online Courses (MOOC) platform for capacity building of police officers, judicial officers, and prosecutors through online courses on critical aspects of cyber-crime investigation, forensics, and prosecution. <div style="text-align: center;">  <p>CyTrain Mobile App</p> <p>CyTrain Download the Mobile app</p> </div>
<p>National Cyber Crime Reporting Portal</p>	<div style="text-align: center;">  <p>TIPS TO STAY CYBER SAFE</p> <p>LOST? MONEY ONLINE</p>  <p>REPORT IT TO THE NATIONAL CYBER CRIME HELPLINE NUMBER</p>  <p>Or www.cybercrime.gov.in</p> </div> <div style="margin-top: 20px;"> <p>Don't worry. "The Citizen Financial Cyber Fraud Reporting and Management System" is there to help !</p> <p>Just Follow the Below Steps:</p> <ol style="list-style-type: none"> 1 For immediate support call on Helpline no. 1930, which is manned and operated by the respective State Police officers. 2 Cyber Police notes down the fraud transaction details and other basic personal information of the caller and submits a Ticket on the portal. 3 Ticket gets escalated to the concerned Banks, Wallets, Merchants, etc. According to the Victims' details. 4 An SMS with an acknowledgment number of the complaint is sent, the victim has to submit complete fraud details on the portal within 24 hours. 5 If money is still available with fraudster, this Bank puts it on hold, else the ticket gets escalated repeatedly to the next person with money. 6 Finally, the money held by the bank is returned back to the victim through court. </div>

<p>Information Technology (IT) Act, 2000</p>	<ul style="list-style-type: none"> It is a comprehensive legislation that addresses various aspects of electronic governance, digital signatures, data protection, and penalties for cybercrimes. 
<p>Citizen Financial Cyber Fraud Reporting and Management System</p>	<ul style="list-style-type: none"> It is a system for immediate reporting of financial frauds and assistance in lodging online cyber complaints through a toll-free helpline.
<p>Cybercrime Prevention against Women and Children (CCPWC) Scheme</p>	<ul style="list-style-type: none"> The Government implements a scheme of Cyber Crime Prevention against Women and Children (CCPWC) under Nirbhaya Fund. A National Cybercrime Reporting Portal (NCRP) www.cybercrime.gov.in has been launched under CCPWC to report all types of cybercrimes with special focus on cyber-crimes against women & children. A toll-free Helpline No. 1930 is also operational in all States/ UTs.

- NCRP has had more than **16.18 Crore** visitors.
- **Around 1.94 lakh Child Pornography/ Rape or Gang Rape (CP/RGR)** complaints have been reported as on **30.04.2024**.

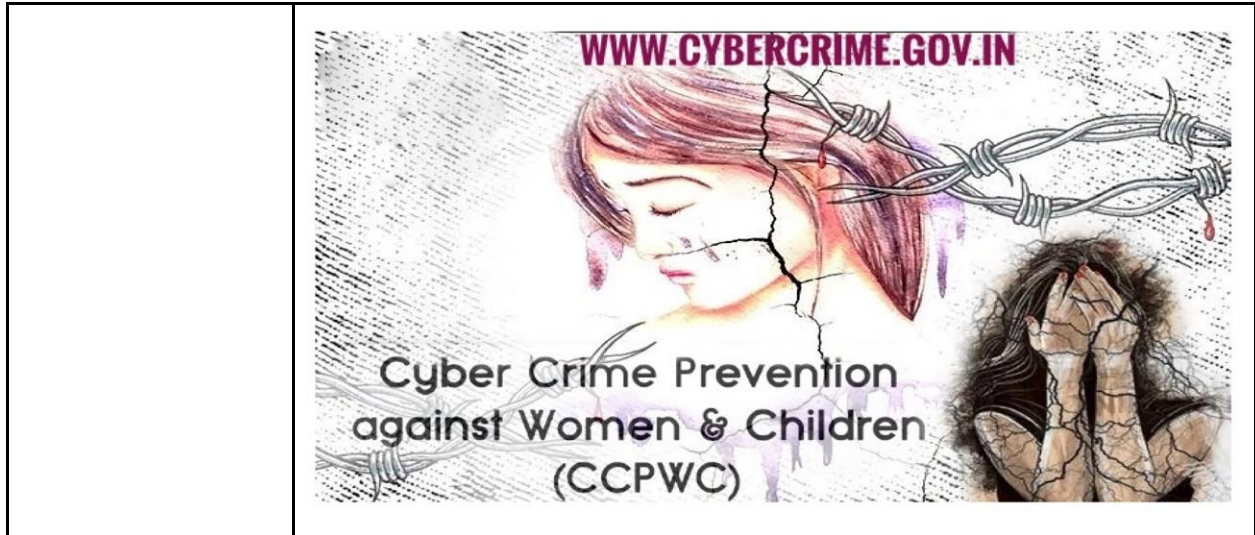
**Citizen
Financial Cyber Fraud Reporting
& Management System**
(Helpline number 155260)
 has helped in saving more than
₹27 Crore



The Helpline number and its reporting platform is now available in all States/UTs

Central Assistance for Modernization of Police

- Providing financial support to **States/UTs for acquiring modern weaponry, advanced communication/forensic equipment**, and cyber policing equipment.
- An overall outlay of **Rs. 4846 crore** under the scheme of **“Assistance to States & UTs for Modernization of Police (ASUMP)”** has been approved for **five years** during the period from **2021-22 to 2025-26**.



17. How to protect oneself from cybercrimes?

BEWARE OF SWINDLERS

HOW TO **PROTECT YOURSELF** FROM ONLINE FRAUDS

DOs



Always visit the official website of bank/merchant for correct customer care number



Keep your contact details updated with the bank to get transaction alerts



Secure your debit/credit cards and set daily limit for transactions



Use strong passwords; should be different for banking & e-commerce



Report any unauthorised transaction to your bank to prevent further losses

DON'Ts



Enter UPI PIN or scan QR code to receive payments; you'll end up losing money



Save your banking username/password in the web browser or your device



Click any link shared in SMSes/ mails typically threatening to block your bank account



Download third-party apps on assurance that it will help resolve your complaints



Share your ID/login password, OTP, CVV, etc. with anyone claiming to be a bank representative

WHAT TO DO IN CASE YOU HAVE BEEN DUPED



Call bank customer care and ask them to freeze account, credit/debit cards, net banking mandate, within the first 48 hours of the fraud occurring



Call 1930, the cyber helpline. Alternatively, file a complaint on cybercrime.gov.in, or visit your nearest cybercrime police branch





















Change PINs and passwords to all online accounts

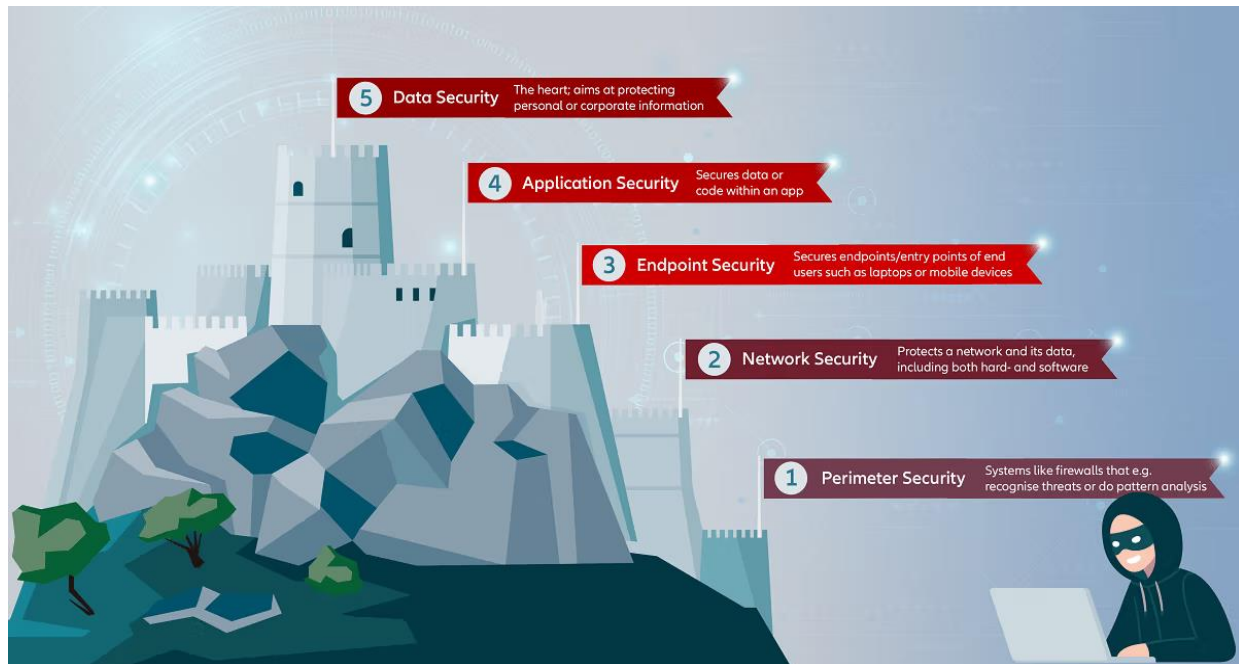


Run phone diagnostics to delete suspect apps or malware

15 Ways to Protect Your Business from a Cyberattack!



<p></p> <p>Security Assessment</p> <p>It's important to establish a baseline and close existing vulnerabilities. When was your last assessment?</p>	<p></p> <p>Spam Email</p> <p>Most attacks originate in your email. Be sure to choose a service designed to reduce spam and your exposure to attacks.</p>	<p> </p> <p>Passwords</p> <p>Apply security policies on your network. Deny or limit USB file storage, enhance password policies, and set user screen timeouts.</p>
<p></p> <p>Security Awareness</p> <p>Train your users—often! Teach them about data security, email attacks, and your policies and procedures.</p>	<p></p> <p>Computer Updates</p> <p>Keep Microsoft, Adobe, and Java products updated for better security. Automate updates to protect your computers from the latest known attacks.</p>	<p></p> <p>Advanced Endpoint Detection & Response</p> <p>Protect your computer's data from malware, viruses, and cyberattacks with advanced endpoint security. Today's latest technology protects against file-less and script based threats.</p>
<p></p> <p>Multi-Factor Authentication</p> <p>Utilize Multi-Factor Authentication whenever you can. It adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.</p>	<p> Nearly half of all cyberattacks are committed against small businesses</p> <p> The frequency of ransomware attacks will continue to rise over the next 5 years and is expected to rise to every two seconds by 2031</p> <p> Cyberattacks will cost businesses more than 10.5 trillion each year by 2025</p>	<p></p> <p>Dark Web Research</p> <p>Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach.</p>
<p></p> <p>SIEM/Log Management (Security Incident & Event Management)</p> <p>Review all event and security logs from all covered devices to protect against advanced threats and to meet compliance requirements.</p>	<p></p> <p>Web Gateway Security</p> <p>Internet security is a race against time. Cloud based security detects web and email threats as they emerge, and blocks them within seconds—before they reach the user.</p>	<p></p> <p>Mobile Device Security</p> <p>Cyber criminals attempt to steal data or access your network by way of your employees' devices. They're counting on you to neglect this piece of the puzzle.</p>
<p></p> <p>Firewall</p> <p>Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM.</p>	<p></p> <p>Encryption</p> <p>Whenever possible, the goal is to encrypt files at rest, in motion (think email) and especially on mobile devices.</p>	<p></p> <p>Backup</p> <p>Backup local. Backup to the cloud. Have an offline backup for each month of the year. Test your backups often.</p>



18. What is the relevance of the topic for UPSC CSE?

- **For Prelims:** Cyber Crime, Seventh Schedule of the Constitution, Internet of Things, Crypto-Currency, Massive Open Online Courses.
- **For Mains:** Internal security, Cyber Crime, Related Challenges and Measures to Deal with it.

Some previous years prelims questions.

Q1. In India, under cyber insurance for individuals, which of the following benefits are generally, in addition to payment for the loss of funds and other benefits?(2020)

1. Cost of restoration of the computer system in case of malware disrupting access to a computer.
2. The cost of a new computer if some miscreant wilfully damages it, if proved so.
3. Cost of hiring a specialized consultant to minimize the loss in case of cyber extortion.
4. Cost of defense in the court of law if any third party files a suit.

Select the correct answer using the code given below:

- (a) 1, 2, and 4 only
- (b) 1, 3 and 4 only
- (c) 2 and 3 only
- (d) 1, 2, 3 and 4

Ans: (b)

Some previous years mains questions.

- Q1. Social media and encrypting messaging services pose a serious security challenge. What measures have been adopted at various levels to address the security implications of social media? Also suggest any other remedies to address the problem. **(2024)**
- Q2. What is the status of digitalization in the Indian economy? Examine the problems faced in this regard and suggest improvements. **(2023)**
- Q3. What are the different elements of cyber security? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. **(2022)**
- Q4. Keeping in view India's internal security, analyse the impact of cross-border cyber attacks. Also, discuss defensive measures against these sophisticated attacks. **(2021)**

Some questions from this year and previous years interview transcripts.

Board B B Swain Sir:

- Does centralisation of web servers have risks?
- What type of cyber risks does it possess?

Board R N Choubey Sir:

- Cyber crimes are transnational, how to deal with them?
- How to prevent them?

Board Satyawati mam:

- Tell me something about cyber crimes.
- Tell me something about social crimes and cyber crimes linkages
- How to prevent cyber crimes in India?

Board Preeti Sudan mam:

- What are cyber crimes?
- Mention a few examples of some cyber crimes?
- What steps need to be taken to tackle those crimes?

Some questions for QUIZ.

Q1. The term “zero-day exploit” closely relates to which of the following.

- (a) Cyber attack
- (b) Vehicular pollution
- (c) Invasive Alien Species
- (d) Cancer Drug Delivery

Ans: (a)

Some questions for POLL.

Q1. Do you think that rising cybercrime can hamper the Digital India mission?

- (a) YES
- (b) NO
- (c) Can't say.

Q2. Should India be part of the UN cybercrime treaty?

- (a) YES
- (b) NO
- (c) Can't say.

