इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

CYBER HYGIENE
for
GOVERNMENT EMPLOYEES

Protecting National Assets

Supported by

certin Enhancing Cyber Security in India

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Digital India Power To Empower

mygov मेरी सरकार

Indian Cyber Crime Coordination Centre

सी डैक CDAC

Report cyber frauds at

1930

or

https://cybercrime.gov.in/

ISEA Mobile APP

Scan here to **Download the APP**

BE AWARE SECURED

Supported by

HRD Division
Ministry of Electronics & Information Technology,
Government of India

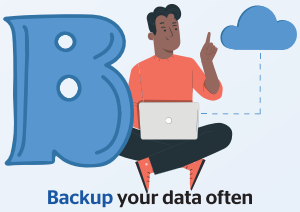
इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

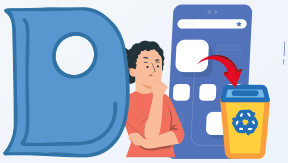
ABCs of Information Security

Antivirus should always be enabled with auto updates



Backup your data often

Clear cookies at the end of the online session



Diagnose for unwanted apps in your mobile device

Encrypt your Data

Firewalls protects your computer from unwanted traffic. Turn it On

Game Addiction is a kind of disorder. Protect your child from such disorders

HTTPS protects your credentials sniffing

Use Bluetooth in **Invisible** mode unless its required to connect with known device

Avoid **Jailbreaking** your mobile OS to protect it from possible threats

Keyloggers are used to steal sensitive information. Be Aware

Logout after you finish accessing your email account

Multi-Factor Authentication will add additional layer of security

Secure **Network Access Point** by enabling firewall and VPN

Optimize security settings of your social media account regularly

Passphrase is the best way to ensure strong password

Quarantine all unused apps

Respect the privacy of others

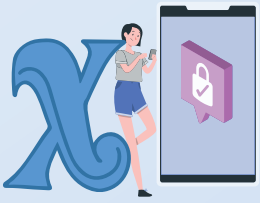
Search engine safety settings should be turned on Kids **Safe browsing**

Keep **Track** of Your Digital Footprint

Unknown sender emails are not to open or click

Prefer **Virtual Private Network** VPN while using public Wi-Fi

Watch out for online scams



eXamine the app permissions in your device regularly

Use **Yubikey** for enabling multi factor authentication

Not all mistakes can be undone with **ctrl Z** . Be Proactive to secure your information

Supported by

certin
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
Digital India
mygov मेरी सरकार
Indian Cyber Crime Coordination Centre
सी डैक CDAC

CYBER HYGIENE FOR GOVERNMENT EMPLOYEES

PROTECTING NATIONAL ASSETS

In the contemporary digital landscape, the government's operational framework is intricately woven with interconnected systems and vast repositories of sensitive data. This data, which spans national security intelligence, citizen records, and critical financial information, has become a prime target for sophisticated cybercriminals. The potential consequences of a successful cyberattack are not merely disruptive; they can be catastrophic, ranging from the compromise of national security and the disruption of essential public services to the erosion of public trust and the undermining of democratic institutions. Therefore, the implementation of robust cyber hygiene practices is not just a recommended precaution but a mandatory requirement for every government employee, regardless of their role or technical expertise.

This handbook is designed to serve as a comprehensive guide, providing actionable insights and practical strategies to understand and mitigate a wide array of cyber threats. It aims to equip government employees with the knowledge and skills necessary to ensure the security and integrity of government operations in an increasingly complex digital environment. By emphasizing the importance of proactive security measures, continuous vigilance, and a culture of cybersecurity awareness, this handbook seeks to empower employees to become active participants in safeguarding national assets.

Furthermore, this document will underscore the critical importance of adhering to national cybersecurity policies, which serve as the foundation for protecting our digital infrastructure and ensuring the resilience of our government systems.

For example, in India, the Indian Computer Emergency Response Team (CERT-In) provides guidelines and advisories that must be followed. (Link: https://www.cert-in.org.in/) Additionally, the National Informatics Centre (NIC) offers secure infrastructure and guidelines for government systems. (Link: https://www.nic.in/) Adherence to these resources and guidelines is essential for maintaining a strong cybersecurity posture.

Why Cyber Hygiene is Important for Government Employees ?

Government employees, in the course of their daily duties, handle an extensive range of sensitive information that demands the highest levels of protection. This information includes:

1. **National Security Data:**
Intelligence reports, defence strategies, classified communications, strategic plans, and critical infrastructure data. The compromise of this information can have severe implications for national security and international relations

2. **Public Records:**
Citizen data such as Aadhaar numbers, PAN details, voter IDs, health records, tax information, and educational records. This data is essential for providing public services and must be protected from identity theft, fraud, and other forms of misuse.

3. **Financial Data:**
Budgets, procurement records, tax information, financial transactions, and grant allocations. The integrity of this data is crucial for ensuring transparency and accountability in government operations.

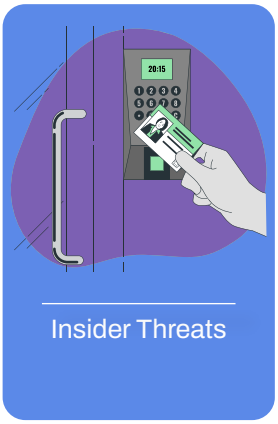
The consequences of poor cyber hygiene practices can be far-reaching and devastating, including:

1. **Data Breaches:**
Unauthorized access and disclosure of classified or personal information, leading to identity theft, financial losses, and damage to national security. Examples of large scale data breaches can be found in resources like the haveibeenpwned website. (Link: https://haveibeenpwned.com/)

2. **Service Disruption:**
Inaccessibility of critical public services due to cyberattacks, resulting in delays in service delivery, economic losses, and public inconvenience.

3. **Reputation Damage:**
Loss of public trust and confidence in government institutions, leading to decreased citizen engagement and erosion of democratic principles.

Different types of Cyber Threats



Insider Threats

Page 8

Phishing and Social Engineering

Page 12

Ransomware

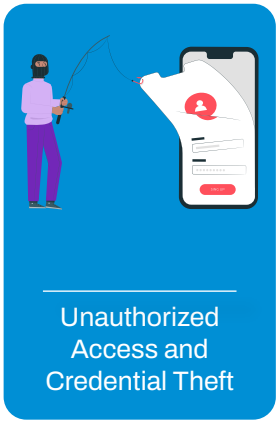
Page 16

Malware and Viruses

Page 22

Distributed Denial-of-Service (DDoS) Attacks

Page 26

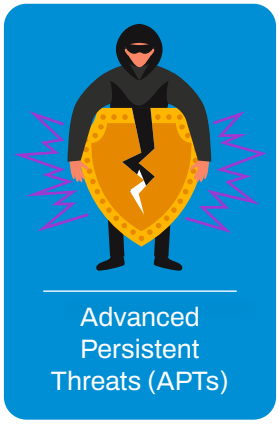


Unauthorized Access and Credential Theft

Page 30

Software and System Vulnerabilities

Page 33

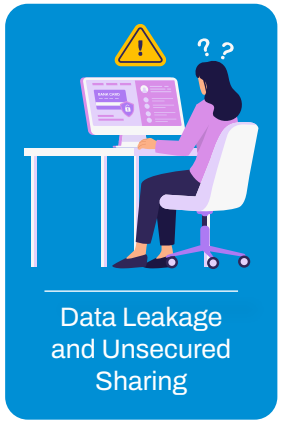


Advanced Persistent Threats (APTs)

Page 36

Insecure Mobile and Remote Work Practices

Page 40

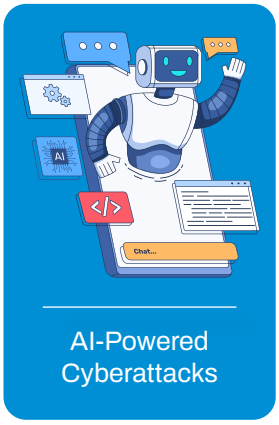


Data Leakage and Unsecured Sharing

Page 44

Supply Chain Attacks

Page 47



AI-Powered Cyberattacks

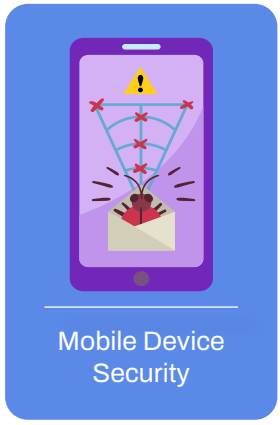
Page 51

Hardware Attacks

Page 57

Data Exfiltration

Page 61



Mobile Device Security

Page 65

Insider Threats

Meaning:
Insider threats originate from individuals within the organization, such as employees, contractors, or partners, who have authorized access to sensitive systems and data. These threats can be intentional (malicious) or unintentional (negligent).

Types:

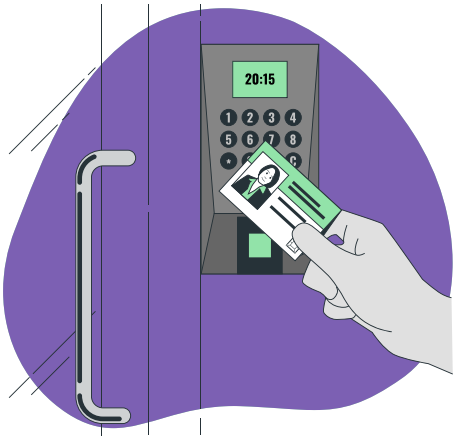
- **Malicious Insiders:**
  Individuals who intentionally steal or damage data for personal gain, revenge, or other malicious purposes.

- **Negligent Employees:**
  Individuals who unintentionally cause security breaches through errors, carelessness, or lack of awareness.

- **Compromised Credentials:**
  Legitimate user accounts that have been compromised by external attackers.

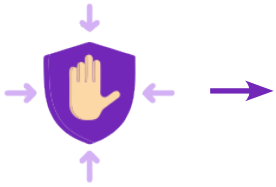
Mitigation:

Strict Access Controls:
Access control is a fundamental security practice that dictates who can access what resources within a system or network. In the context of government environments, where sensitive data and critical systems are handled, implementing strict access controls is paramount. The core principle that should guide access control policies is the "principle of least privilege.



The Principle of Least Privilege:
The principle of least privilege (PoLP) dictates that users should be granted only the minimum level of access necessary to perform their job functions. This means that users should not have access to data or systems that are not required for their work. By adhering to this principle, organizations can significantly reduce the risk of unauthorized access, data breaches, and insider threats.

Why is Least Privilege Important?



Reduces the Attack Surface:
By limiting access to sensitive data and systems, organizations minimize the potential impact of a security breach. If an attacker compromises a user account, the damage is contained to the resources that the user was authorized to access.

Mitigates Insider Threats:
Whether intentional or unintentional, insider threats can cause significant damage. Implementing PoLP ensures that even if a user's account is compromised, the attacker's ability to access sensitive data is limited.

Enhances Accountability:
When access is strictly controlled, it becomes easier to track user activity and identify who accessed what resources. This enhances accountability and facilitates forensic investigations in the event of a security incident.

Improves Compliance:
Many regulatory requirements, such as those related to data privacy and security, mandate the implementation of access controls. Adhering to PoLP helps organizations comply with these requirements

Implementing Strict Access Controls:

1

Reduces the Attack Surface:
By limiting access to sensitive data and systems, organizations minimize the potential impact of a security breach. If an attacker compromises a user account, the damage is contained to the resources that the user was authorized to access.

2

Attribute-Based Access Control (ABAC):
Define access policies based on user attributes, resource attributes, and environmental attributes. This provides more granular control over access permissions.

3

Regular Access Reviews:
Conduct periodic reviews of user access permissions to ensure that they are still appropriate. Remove or modify access permissions as needed.

4

Privileged Access Management (PAM):
Implement PAM solutions to control and monitor access to privileged accounts, such as administrator accounts.

5

Just-in-Time (JIT) Access:
Grant temporary access to resources only when needed, and revoke access immediately after use.

6

Multi-Factor Authentication (MFA):
Implement MFA to add an extra layer of security and prevent unauthorized access, even if user credentials are compromised.

7

Logging and Auditing:
Maintain detailed logs of user activity to track access to sensitive resources and identify any suspicious behaviour.

8

Background Checks:
Conduct thorough background checks and security clearances for employees with access to sensitive systems.

9

Monitoring:
Monitor user activity for anomalies and suspicious behaviour.

10

Training:
Provide regular security awareness training to employees.

Do's & Dont's

- Implement least privilege access.
- Monitor user activity for anomalies.
- Enforce security policies and procedures.

- Grant excessive access to users.
- Ignore suspicious behaviour or security incidents.
- Neglect to implement robust logging and auditing mechanisms.

Warning signs of Tailgating

- Unidentified person moving around in the office premises
- A person found in the office premises, not able to show the relevant ID card upon enquiring
- Physical theft of devices or assets
- Signs of attempts of unauthorized access to systems or networks

Phishing and Social Engineering

Meaning:
Phishing and social engineering are deceptive tactics used to trick users into revealing sensitive information, such as login credentials, financial data, or personal details.

Types:

Phishing Emails:
Emails that impersonate legitimate organizations to trick users into clicking malicious links or providing sensitive information.

Spear-Phishing:
Targeted phishing attacks that are tailored to specific individuals or organizations.

Baiting:
Using false promises to entice victims to give up private information or install malware.

Pretexting:
Creating a false scenario to manipulate victims into providing sensitive information.

Mitigation:

Identifying Phishing Emails:
Phishing emails aim to trick you into revealing sensitive information or clicking malicious links. Here's how to spot them:

- **Suspicious Sender Address:**
  - Look for misspellings or variations in the sender's email address.
  - Verify the domain name. Legitimate organizations use their official domain.
  - Be wary of generic addresses (e.g., "[email address removed]").
- **Generic Greetings:**
  - Phishing emails often use generic greetings like "Dear Customer" or "Valued User" instead of your name.
  - Legitimate organizations usually personalize their emails.
- **Urgent or Threatening Language:**
  - Phishers create a sense of urgency or fear to pressure you into acting quickly.
  - They might threaten account suspension, legal action, or financial loss.
- **Suspicious Links:**
  - Hover your mouse over links (without clicking) to see the actual URL.
  - Look for misspellings or shortened URLs.
  - Be cautious of links that redirect to unfamiliar websites.
- **Attachments:**
  - Avoid opening attachments from unknown senders.
  - Be wary of common file extensions like .exe, .zip, or .scr.
  - Even .pdf or .doc files can contain malicious code.
- **Grammatical Errors and Typos:**
  - Phishing emails often contain grammatical errors, typos, and poor formatting.
  - Legitimate organizations usually have professional communication standards.
- **Requests for Sensitive Information:**
  - Legitimate organizations rarely ask for sensitive information like passwords or credit card details via email.
  - Be suspicious of any email that requests such information.
- **Unusual Requests:**
  - Be cautious of emails that ask you to perform unusual actions, such as changing your password or transferring funds.

Mitigation:

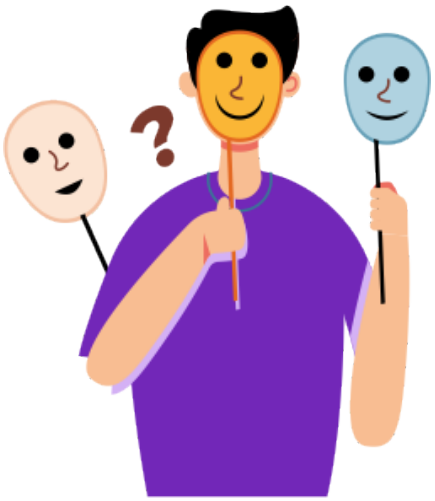
Identifying Social Engineering Tactics:
Social engineering manipulates people into performing actions that compromise security. Here are common tactics:

- **Pretexting:**
  - The attacker creates a false scenario or pretext to gain your trust.
  - They might impersonate a colleague, IT support, or a government official.
  - Be wary of anyone who asks for sensitive information without proper verification.

- **Baiting:**
  - The attacker offers a tempting "bait," such as a free gift or download, to lure you into clicking a malicious link or providing information.
  - Be cautious of offers that seem too good to be true.

- **Quid Pro Quo:**
  - The attacker offers a service or favour in exchange for information or access.
  - Be wary of anyone who offers unsolicited help or assistance.

- **Tailgating:**
  - The attacker physically follows you into a restricted area without authorization.
  - Be aware of who is following you and challenge anyone who seems suspicious.



- **Impersonation:**
  - The attacker pretends to be someone they are not. This can be over the phone, email, or in person.
  - Always verify the identity of the person you are communicating with.

- **Urgency:**
  - Social engineers often create a sense of urgency, pressuring you to act quickly without thinking.
  - Take your time to verify requests and avoid making hasty decisions.

- **Authority:**
  - They might claim to be someone in a position of authority, such as a manager or IT administrator.
  - Always verify the authority of the person making the request.

- **Trust Exploitation:**
  - Social engineers often exploit your trust in familiar people or organizations.
  - Be cautious of requests from people you know, and always verify their identity.

Other Related Threats :

Vishing (Voice Phishing):
Phishing attacks conducted over the phone. Be wary of unsolicited calls requesting sensitive information.

Smishing (SMS Phishing):
Phishing attacks conducted via text messages. Be cautious of links or requests in SMS messages.

Watering Hole Attacks:
Attacks that target websites frequently visited by a specific group of users. Be cautious of visiting unfamiliar websites.

USB Drops:
Attackers leave infected USB drives in public places, hoping someone will plug them into a computer. Be cautious of using unknown USB drives.

Do's & Dont's

- Verify the sender's email address.
- Hover over links to inspect the URL.
- Report suspicious emails to the IT department.

- Click on unknown or suspicious links.
- Share login credentials or sensitive information via email.
- Download attachments from untrusted sources.

Ransomware

Meaning:
Ransomware is a type of malicious software (malware) that encrypts a victim's files or locks their system, rendering them inaccessible. The attackers then demand a ransom, typically in cryptocurrency, in exchange for the decryption key or to restore system access.

Types:

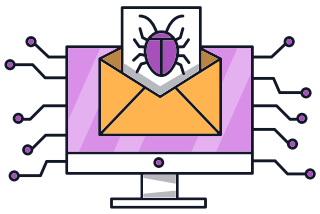
Crypto-ransomware:
Encrypts files and demands a ransom for the decryption key.

Locker Ransomware:
Locks the victim's computer screen and demands a ransom for unlocking it.

Mitigation:

Infection:
Ransomware can enter a system through various means, including:

- Phishing emails with malicious attachments or links.
- Exploiting software vulnerabilities.
- Malicious advertisements (malvertising).
- Compromised websites.
- Infected USB drives.



Encryption/Locking:

- Once inside, the ransomware encrypts files or locks the entire system, making them inaccessible to the user.
- Some ransomware variants may also delete or corrupt backup files.

Ransom Demand:

- The attackers display a ransom note, typically with instructions on how to pay the ransom and obtain the decryption key.
- Ransom demands often include a deadline, threatening to increase the ransom or permanently delete the data if not paid within the specified time.

Defend your Digital Domain

Always
Update
Scan
&
Surf
with care

How to Identify Ransomware ?

Unusual File Extensions:
Encrypted files may have strange or unfamiliar file extensions.

Encrypted Files:
Files that suddenly become inaccessible and display error messages when opened.

System Lockout:
A locked screen or inability to access the operating system.

Ransom Notes:
Pop-up windows or text files demanding payment for file decryption or system access.

Sudden System Slowdown:
Unusually high CPU or disk usage can be a sign of ransomware encryption.

Disabled Security Software:
Ransomware may attempt to disable antivirus or other security software.

Unusual Network Activity:
Increased network traffic can indicate data exfiltration or communication with command-and-control servers.

Protecting Your System from Ransomware:

Regular Backups:

- The most effective defence against ransomware is to regularly back up critical data to offline or offsite locations.
- Ensure backups are isolated from the network to prevent them from being encrypted.

Antivirus and Anti-Malware Software:

- Use reputable antivirus and anti-malware software with real-time scanning capabilities.
- Keep security software updated with the latest virus definitions.

Principle of Least Privilege:

- Grant users only the minimum level of access necessary to perform their job functions.

Email Security:

- Be cautious of suspicious emails, especially those with attachments or links from unknown senders.
- Verify the authenticity of email senders before clicking on links or opening attachments.
- Implement email filtering.

Software Updates:

- Keep operating systems, applications, and security software up to date with the latest security patches.
- Patch vulnerabilities promptly to prevent attackers from exploiting them.

User Education:

- Educate users about the risks of ransomware and how to identify phishing emails and other social engineering tactics.
- Promote a culture of security awareness.

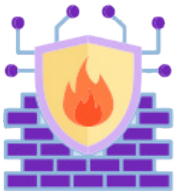
Network Segmentation:

- Segment your network to limit the spread of ransomware in case of an infection.

Strong Passwords and Multi-Factor Authentication (MFA):

- Use strong, unique passwords for all accounts.
- Enable MFA whenever possible to add an extra layer of security.

Protecting Your System from Ransomware:



Firewall Protection:

- Use a firewall to block unauthorized network traffic.

Web Filtering:

- Block access to known malicious websites and domains.

Incident Response Plan:

- Develop and implement an incident response plan for ransomware attacks, including steps for containment, eradication, and recovery.

Disable Macros:

- Disable macros in office documents by default, as they can be used to deliver ransomware.

Do's & Dont's

- Regularly backup critical data.
- Keep systems updated with the latest security patches.
- Use reputable antivirus and anti-malware software.

- Pay the ransom, as it does not guarantee data recovery.
- Open email attachments from unknown senders.
- Disable security features or ignore security warnings.

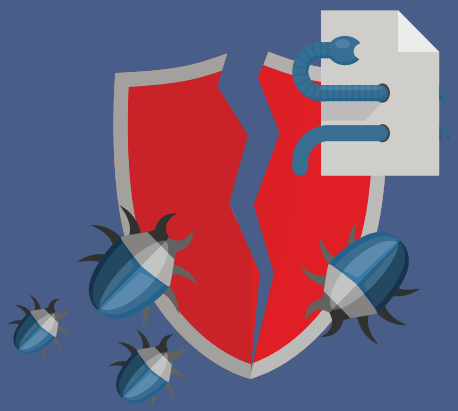
इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

WARNING SIGNS

virus attacks on systems and devices



Computer runs more slowly and stops responding

Computer crashes and restarts every few minutes

Computer applications don't work correctly

Disk drives are inaccessible

Can't print correctly and unusual error messages

Distorted menus and dialog boxes

Supported by

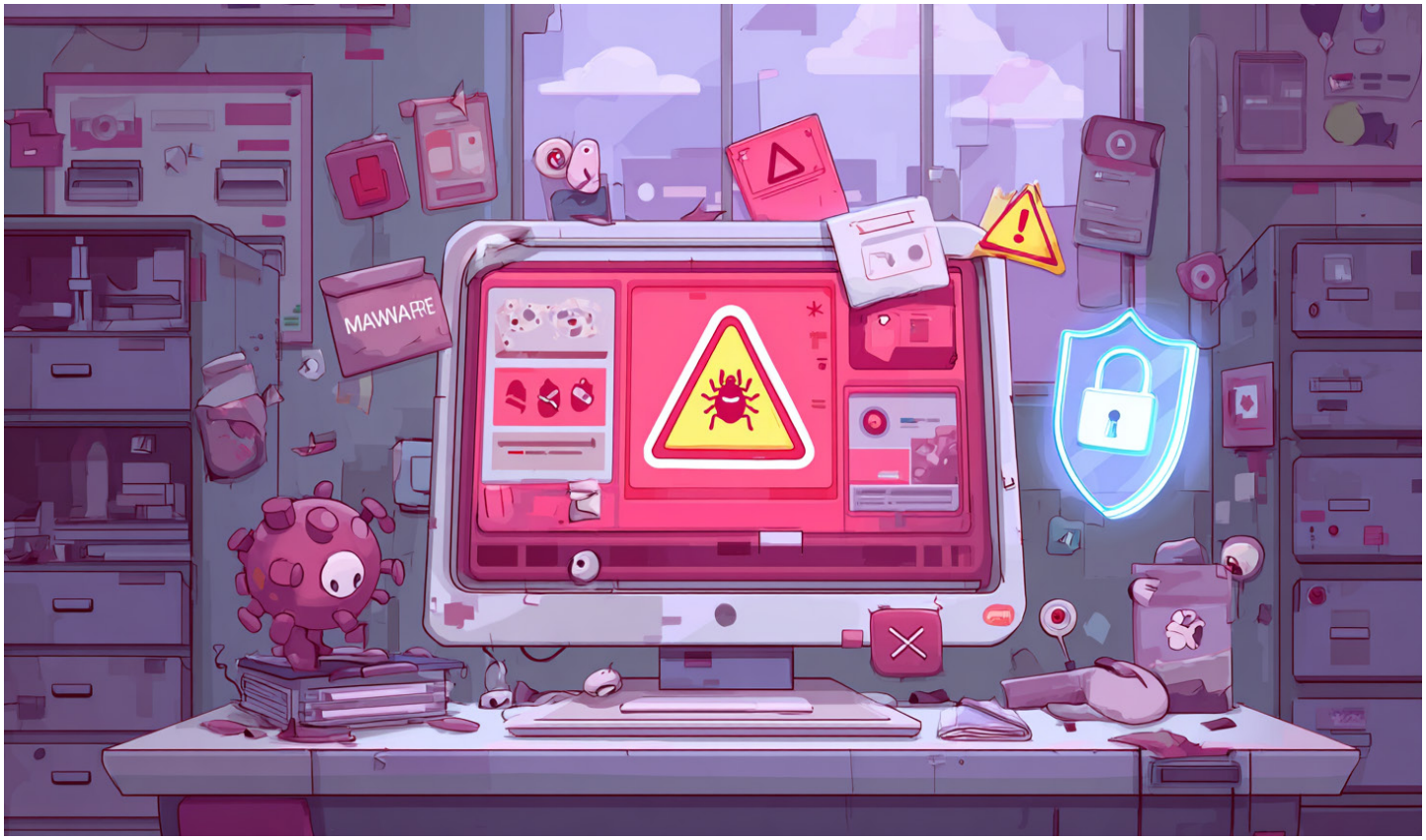
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Digital India
Power To Empower

mygov
मेरी सरकार

Indian Cyber Crime Coordination Centre
Working Together With Vigour

सी-डैक
CDAC



Malware and Viruses

Meaning:
Malware and viruses are broad terms that encompass various types of malicious software designed to harm or exploit computer systems. While “virus” is a specific type of malware, the terms are often used interchangeably in general conversation. Here’s a breakdown of malware and viruses, how to identify them, and how to protect your systems:

Understanding Malware and Viruses:

Malware (Malicious Software):
This is a general term for any software designed to cause harm to a computer system. It includes viruses, worms, Trojans, spyware, adware, ransomware, and more.

Viruses:
- A specific type of malware that replicates itself by inserting its code into other programs or files.
- Viruses typically require user interaction (e.g., opening an infected file) to spread.
- They can corrupt files, damage systems, or steal data.

Worms:
- Self-replicating malware that spreads across networks without user interaction.
- Worms can consume system resources and disrupt network operations

Trojans:
- Malware disguised as legitimate software.
- Trojans can perform various malicious activities, such as stealing data, opening backdoors, or installing other malware.

Spyware:
- Malware that secretly monitors user activity and collects sensitive information.

Adware:
- Software that displays unwanted advertisements.

Ransomware:
- Malware that encrypts files and demands payment for decryption.

Mitigation:

Identifying Malware and Viruses:
- Slow System Performance: Unusual slowdowns, crashes, or freezing.
- Unexpected Pop-ups and Ads: Frequent and intrusive pop-up windows or advertisements.
- Changes to Browser Settings: Unexpected changes to your homepage, search engine, or other browser settings.
- Suspicious Activity: Unusual network activity, such as increased traffic or connections to unknown servers.
- Missing or Corrupted Files: Files that suddenly disappear or become unreadable.
- Disabled Security Software: Malware may attempt to disable your antivirus or firewall.
- Unusual Error Messages: Error messages from programs that normally function correctly.
- Increased Hard drive activity: If the hard drive is constantly working, even when you are not using programs, this could be a sign of malware.

Protecting Your System from Ransomware:

Antivirus and Anti-Malware Software:

- Install and maintain reputable anti-virus and anti-malware software.
- Keep the software updated with the latest virus definitions.
- Perform regular system scans.

Safe Browsing Practices:

- Avoid clicking on suspicious links or downloading files from untrusted sources.
- Be cautious of pop-up windows and advertisements.
- Verify the authenticity of websites before entering sensitive information.

Software Updates:

- Keep your operating system, applications, and browser up to date with the latest security patches.
- Enable automatic updates.

Email Security:

- Be wary of email attachments from unknown senders.
- Avoid clicking on links in suspicious emails.
- Enable email filtering.

Strong Passwords:

- Use strong, unique passwords for all accounts.
- Enable multi factor authentication when possible.
- Regular Backups:
- Regularly back up important data to an external drive or cloud storage.
- This allows you to restore your system in case of a malware infection.

Principle of Least Privilege:

- Limit user access to only the files, and programs that are needed to perform their job

Firewall Protection:

- Use a firewall to block unauthorized network traffic.

Avoid Pirated Software:

- Pirated software often contains malware.

User Education:

- Educate yourself and other users about the risks of malware and safe computing practices.

Scan External Devices:

- Scan all external devices, like usb drives, before using them on your computer.

Do's & Dont's

- Use reputable antivirus and anti-malware software.
- Scan external devices before using them.
- Keep operating systems and software up to date.

- Download software from untrusted sources.
- Ignore security warnings or disable security features.
- Fail to implement firewalls or intrusion detection systems.

It's important to stay vigilant and take up required measures to mitigate the risk of virus infections and protect computer systems from potential threats.

Distributed Denial-of-Service (DDoS) Attacks

Meaning:
A Distributed Denial-of-Service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming it with a flood of internet traffic from multiple compromised computer systems. Essentially, it's like a massive traffic jam on the internet, preventing legitimate users from accessing the targeted resource.

Types of DDoS Attacks:

Volume-Based Attacks:
Flood the target with high volumes of traffic, such as UDP floods, ICMP floods, or SYN floods.

Protocol Attacks:
Exploit weaknesses in network protocols, such as SYN floods, ping of death, or smurf attacks.

Application Attacks:
Target specific applications or services, such as HTTP floods or DNS attacks

Mitigation:

Sudden Increase in Traffic:
A sharp and unexpected surge in network traffic.

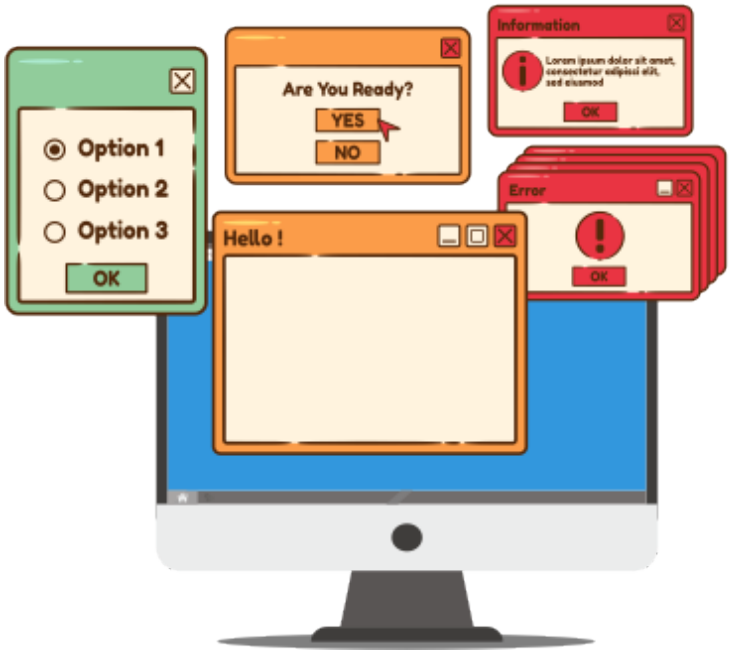
Slow or Unresponsive Services:
Websites or online services that become unusually slow or inaccessible.

High CPU or Memory Usage:
Servers experiencing unusually high resource consumption.

Network Congestion:
Increased network latency or packet loss.

Unusual Network Traffic Patterns:
Traffic originating from numerous different IP addresses.

Error Messages:
Many failed connection attempts, and resulting error messages.



Unwanted pop ups appearing on screen ?

Beware it can be malware attacking your device

Protecting Your System from Ransomware:

DDoS Mitigation Services:

- Use DDoS mitigation services from reputable providers.
- These services can filter and block malicious traffic before it reaches your network.

Firewalls and Intrusion Prevention Systems (IPS):

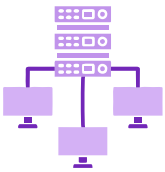
- Implement firewalls and IPS to block malicious traffic and detect anomalies.

Traffic Filtering and Rate Limiting:

- Filter and rate-limit incoming traffic to prevent excessive traffic from overwhelming your systems.

Content Delivery Networks (CDNs):

- Use CDNs to distribute traffic across multiple servers, reducing the impact of DDoS attacks.



Redundant Network Infrastructure:

- Establish redundant network infrastructure to ensure service availability in case of an attack.

Incident Response Plan:

- Develop and implement an incident response plan for DDoS attacks.
- This plan should include steps for detection, mitigation, and recovery.

Regular Security Audits:

- Conduct regular security audits to identify and address vulnerabilities.

DDoS Drills

- Conduct Simulated or Hired DDoS Drills to Assess Infrastructure Resilience

Work with your ISP:

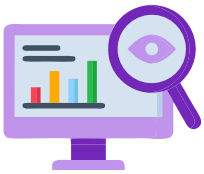
- Contact your internet service provider, as they may have tools to help mitigate the attack.

Implement strong access controls:

- Limit access to important systems, so that even if a bot is on your internal network, it is limited in what it can do

Keep Software Updated:

- Patch all software and firmware to prevent attackers from exploiting known vulnerabilities.



Monitor Network Traffic:

- Implement network monitoring tools to detect anomalies and suspicious activity.

Do's & Dont's

- Use DDoS mitigation services.
- Implement firewalls and intrusion prevention systems.
- Monitor network traffic for anomalies.

- Ignore traffic spikes or unusual network behavior.
- Rely on single-server protection.
- Fail to monitor network traffic and performance.

Unauthorized Access and Credential Theft

Meaning:
Unauthorized access occurs when an individual gains access to computer systems, networks, or data without proper authorization. Credential theft is a common method used to achieve this, where attackers steal or obtain user credentials such as usernames and passwords.

How it Works:

- An attacker uses a phishing email to trick a government employee into revealing their login credentials.
- The attacker then uses these stolen credentials to access the government's network and steal sensitive data.

Mitigation:

Strong Passwords:
Employees should use strong, unique passwords for their accounts. Passwords should be complex, containing a combination of uppercase and lowercase letters, numbers, and symbols.

Multi-Factor Authentication (MFA):
Implement MFA to add an extra layer of security. MFA requires users to provide multiple forms of verification, such as a password and a code sent to their mobile device, before granting access.

Regular Password Changes:
Enforce regular password changes (e.g., every 90 days) to minimize the impact of compromised credentials.

Account Lockout Policies:
Implement account lockout policies to prevent brute-force attacks, where attackers try to guess passwords by repeatedly entering different combinations.

Monitoring for Suspicious Activity:
Monitor login attempts and account activity for any suspicious patterns, such as multiple failed login attempts or logins from unusual locations.

Additional Considerations for Government Employees:

- Government employees often handle highly sensitive information, making their accounts a prime target for attackers.
- The compromise of government employee accounts can lead to severe consequences, including data breaches, disruption of services, and damage to national security.
- It is crucial for government agencies to implement robust access controls and authentication mechanisms to protect employee accounts.

Do's & Dont's

- Use strong, unique passwords for all government accounts.
- Enable MFA whenever possible.
- Change passwords regularly.
- Report any suspicious activity to the IT department.
- Use Only Trusted and Secure Devices
- Stay Alert to Physical Threats like should surfingUse updated antivirus and anti-malware tools to detect and block keyloggers, which can silently record your keystrokes.

- Share passwords with anyone.
- Use the same password for multiple accounts.
- Store passwords in plain text.
- Bypass security measures or policies.

Fortify your device with anti-phishing and anti-malware tools to guard against SIM swapping frauds

Software and System Vulnerabilities

Meaning:
Software and system vulnerabilities are weaknesses or flaws in software or hardware that can be exploited by attackers to gain unauthorized access, cause damage, or steal data.

How it Works:

- Attackers identify a vulnerability in a government agency's software.
- They develop an exploit to take advantage of this vulnerability.
- The exploit is used to gain access to the agency's systems, install malware, or steal data

Types of Vulnerabilities:

1. **Zero-day exploits:**
Vulnerabilities that are unknown to the software vendor and have not been patched.

2. **Unpatched software:**
Vulnerabilities in software that have been publicly disclosed but have not been patched by the system administrator.

3. **Buffer overflows:**
Occur when a program writes more data to a buffer than it can hold, potentially overwriting adjacent memory and causing the program to crash or execute arbitrary code.

4. **SQL injection:**
A code injection technique used to attack data-driven applications, allowing attackers to manipulate database queries.

5. **Hardware Attacks:**
Attacks that exploit vulnerabilities in the physical hardware of a system.

6. **Firmware attacks:**
Targeting the software embedded in hardware devices. Supply chain attacks: Compromising hardware during manufacturing or transit.

Mitigation:

Patch Management:
Implement a robust patch management process to ensure that all software and systems are updated with the latest security patches in a timely manner.

Vulnerability Scanning:
Use vulnerability scanning tools to identify vulnerabilities in systems and applications.

Secure Coding Practices:
Follow secure coding practices to minimize the introduction of vulnerabilities during software development.

Additional Considerations for Government Employees:

- Government systems often run critical infrastructure and store sensitive data, making them attractive targets for attackers.
- Vulnerabilities in government systems can have severe consequences, including disruption of essential services, data breaches, and compromise of national security.
- Regular security assessments and audits are essential to identify and mitigate vulnerabilities in government systems.

Hardware Security Measures:

- Use hardware from trusted vendors.
- Verify the integrity of hardware.
- Implement secure boot processes.

Do's & Dont's

- Keep all software and systems up to date.
- Use vulnerability scanning tools.
- Follow secure coding practices.
- Implement hardware security measures
- Apply System Hardening Techniques

- Ignore software updates or security patches.
- Use unsupported or outdated software.
- Develop software without considering security best practices.
- Fail to secure hardware adequately.

Advanced Persistent Threats (APTs)

Meaning:
Advanced Persistent Threats (APTs) are sophisticated, long-term attacks carried out by highly skilled attackers, often with nation-state backing. These attacks are typically targeted, stealthy, and persistent, aiming to compromise specific organizations or individuals for espionage, sabotage, or other malicious purposes.

How it Works:

- An APT group targets a government agency to steal classified information.
- They use a combination of techniques, including phishing, malware, and zero-day exploits, to gain initial access.
- They move laterally within the network, establish persistence, and exfiltrate data over an extended period.

Typical Stages of an APT Attack:

1 **Reconnaissance:**
Gathering information about the target, including network infrastructure, systems, and personnel.

2 **Initial Access:**
Gaining entry into the target's network through various means, such as phishing, exploiting vulnerabilities, or using stolen credentials.

3 **Lateral Movement:**
Moving within the network to gain access to valuable assets and systems.

4 **Persistence:**
Establishing a long-term presence in the network to ensure continued access.

5 **Exfiltration:**
Stealing sensitive data and transferring it to the attacker's control.

Targets and Motivations of APT Groups:

Government agencies are a prime target for APTs due to the sensitive information they hold, including national security data, diplomatic communications, and citizen records.

Motivations for APT attacks can include:

- **Espionage:**
  - Stealing classified information for political or economic advantage.
- **Sabotage:**
  - Disrupting critical infrastructure or government operations.
- **Financial gain:**
  - Stealing financial data or intellectual property.

Mitigation:

Network Segmentation:
Divide the network into smaller, isolated segments to limit the spread of an attack.

Intrusion Detection and Prevention Systems (IDPS):
Implement IDPS to detect and block malicious activity.
Advanced Threat Protection (ATP) Platforms: Use ATP solutions to identify and mitigate sophisticated threats.

Security Information and Event Management (SIEM):
Employ SIEM systems to collect and analyze security logs and events.

Threat Intelligence Sharing:
Share threat intelligence with other organizations and government agencies to stay ahead of emerging threats.

Additional Considerations for Government Employees:

- Government employees must be aware of the tactics, techniques, and procedures (TTPs) used by APT groups.
- Protecting against APTs requires a multi-layered security approach that combines technical controls, policies, and training.
- Collaboration and information sharing between government agencies are crucial for effective APT defense.

Do's & Dont's

- Implement strong network security controls.
- Monitor network activity for suspicious patterns.
- Keep systems and software up to date.
- Participate in threat intelligence sharing initiatives.

- Underestimate the sophistication of APTs.
- Rely on single-layer security solutions.
- Fail to educate employees about APT threats.
- Neglect to establish incident response plans for APT attacks.

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

www.isea.gov.in

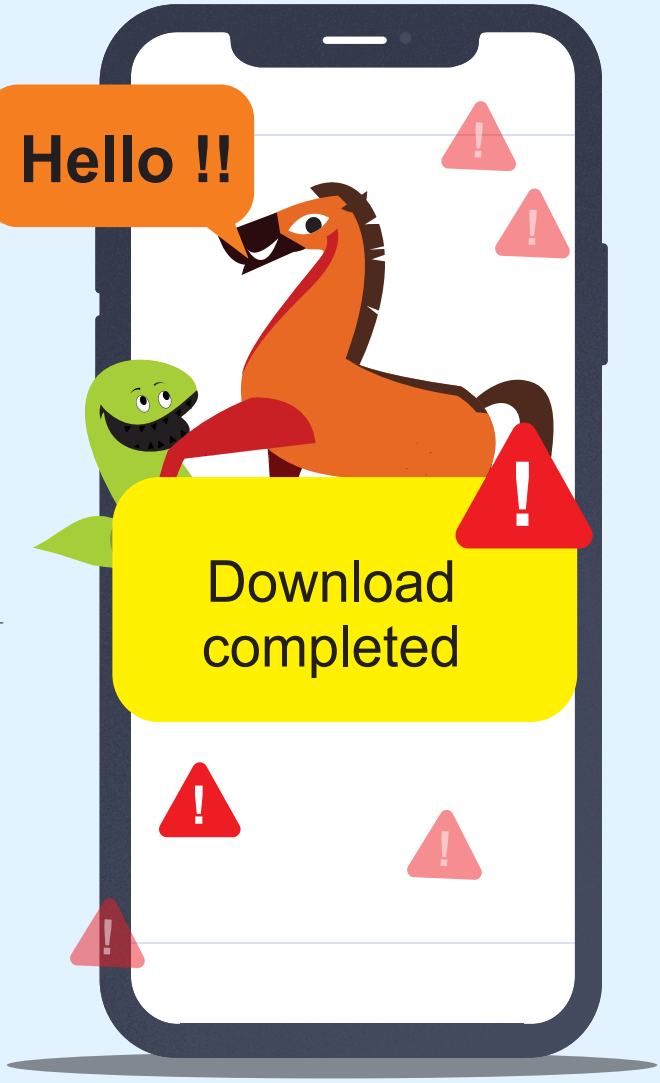
STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

Do not let Malicious Malware say HELLO !

Be smart while downloading apps / attachments

दुर्भावनापूर्ण मैलवेयर को नमस्ते कहने की अनुमति न दें ।

एप्लिकेशन/अटैचमेंट डाउनलोड करते समय स्मार्ट तरीके से व्यवहार करें ।



Supported by

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Digital India
Power To Empower

mygov
मेरी सरकार

Indian Cyber Crime Coordination Centre
सहयोग करना है • Working Together With Vigour

सी-डैक
CDAC

Insecure Mobile and Remote Work Practices

Meaning:
Insecure mobile and remote work practices refer to the vulnerabilities and risks associated with using mobile devices and accessing government resources from remote locations.

How it Works:

- An employee uses an unsecured Wi-Fi network to access government systems.
- An attacker intercepts the communication and steals the employee's login credentials.

Risks Associated with Remote Work:

Unsecured Networks:
Employees working from home may use unsecured home networks, which can be vulnerable to attack.

Compromised Devices:
Personal devices used for remote work may be compromised with malware.

Lack of Physical Security:
Remote work locations may lack the physical security measures of a government office.

Data Leakage:
Sensitive data may be inadvertently exposed when working in a non-office environment.

Risks Associated with Mobile Devices:

Unsecured Wi-Fi:
Connecting to public Wi-Fi networks can expose data to interception.

Mobile Malware:
Mobile devices can be infected with malware that steals data or monitors activity.

Data Leakage:
Sensitive data may be stored on mobile devices, which can be lost or stolen.

Physical Loss or Theft:
Mobile devices are susceptible to loss or theft, which can lead to unauthorized access to sensitive information.

Mitigation:

Mobile Device Management (MDM):
Implement MDM solutions to manage and secure mobile devices used for government work.

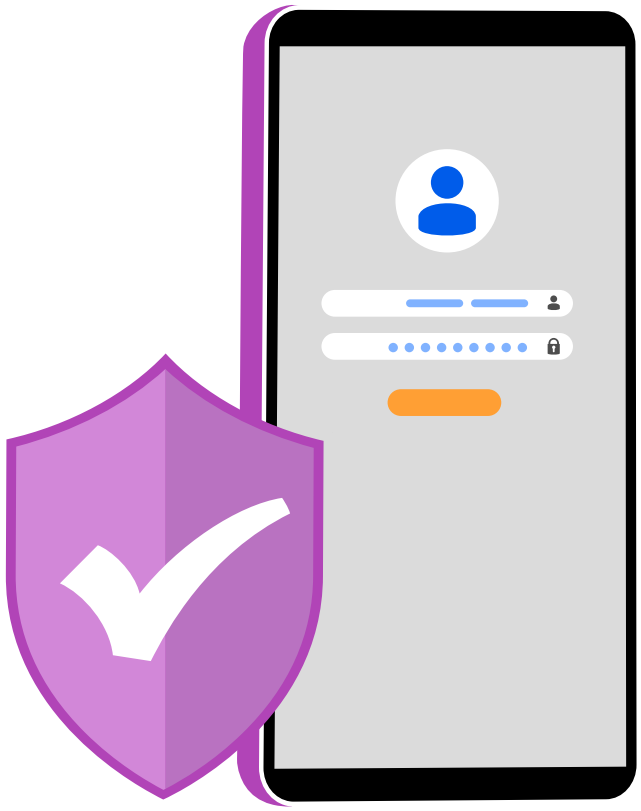
Strong Authentication for Remote Access:
Use strong authentication methods, such as MFA, for all remote access to government systems.

Virtual Private Networks (VPNs):
Require employees to use VPNs to encrypt their network traffic when accessing government resources remotely.

Encryption:
Encrypt sensitive data stored on mobile devices and laptops.

Secure File Sharing:
Use secure file-sharing solutions to prevent data leakage.

Endpoint Security:
Implement endpoint security solutions on all devices used for government work, including laptops, desktops, and mobile devices.



Bring Your Own Device (BYOD) Policies:
If BYOD is allowed, establish clear policies and security requirements for personal devices used for government work.

Security Awareness Training:
Provide regular security awareness training to employees on the risks of insecure mobile and remote work practices.

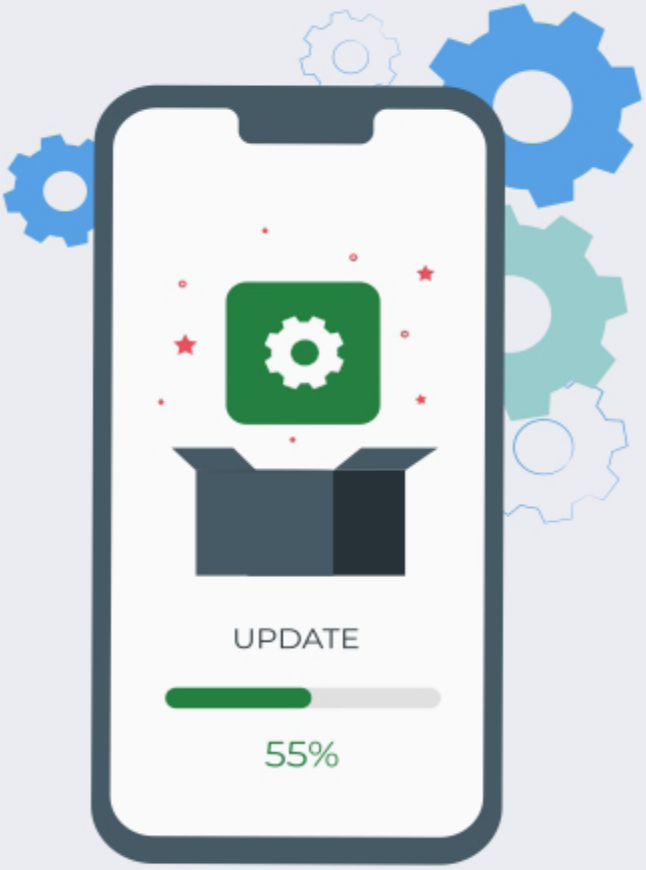
Additional Considerations for Government Employees:

- Government employees increasingly rely on mobile devices and remote work to perform their duties.
- It is essential to balance the flexibility of mobile and remote work with the need to protect sensitive government information.
- Government agencies should establish clear policies and guidelines for secure mobile and remote work practices.

Do's & Dont's

- Use strong passwords and MFA for all devices and accounts.
- Connect to secure networks, such as VPNs, when accessing government resources remotely.
- Keep devices and software up to date.
- Report any lost or stolen devices immediately.

- Use unsecured public Wi-Fi networks for government work.
- Store sensitive data on personal devices.
- Share devices or login credentials with others.
- Bypass security policies or procedures.



App updates often patch security holes

Don't delay, Update today for safer sharing

#UpdateYourApps
#SecurityPatch

Data Leakage and Unsecured Sharing

Meaning:
Data leakage refers to the unauthorized disclosure of sensitive or confidential information to individuals or entities who are not authorized to have it. Unsecured sharing of data, whether intentional or unintentional, is a primary cause of data leakage.

How it Works:

- An employee accidentally sends a classified document to the wrong email address.
- An attacker exploits a vulnerability in a file-sharing application to gain access to sensitive data.

Risks Associated with Unsecured Sharing:

Email:
Sending sensitive information via unencrypted email can expose it to interception.

Cloud Storage:
Storing sensitive data in unsecured cloud storage services can make it vulnerable to unauthorized access.

Physical Media:
Sharing sensitive data on unsecured USB drives or other physical media can lead to data loss or theft.

Collaboration Tools:
Using unsecured collaboration tools can expose sensitive information to unauthorized individuals.

Mitigation:

Data Loss Prevention (DLP):
Implement DLP solutions to detect and prevent sensitive data from leaving the organization's control.

Encryption:
Encrypt sensitive data both in transit and at rest.

Access Controls:
Implement strict access controls to limit access to sensitive data to authorized individuals.

Secure Collaboration Tools:
Use secure collaboration tools that provide encryption, access controls, and audit trails.

Mitigation:

Policies and Procedures for Data Handling:
Establish clear policies and procedures for handling sensitive data, including guidelines for sharing, storage, and disposal.

Regular Audits and Monitoring:
Conduct regular audits and monitoring of data access and sharing activities to detect and prevent data leakage.

Employee Training and Awareness:
Provide regular training and awareness programs to educate employees about the risks of data leakage and the importance of secure data sharing practices.

Additional Considerations for Government Employees:

- Government employees handle a significant amount of sensitive data, including classified information, citizen data, and financial records.
- Data leakage in the government sector can have severe consequences, including harm to national security, violation of citizen privacy, and damage to public trust.
- Government agencies must prioritize the implementation of robust data protection measures and enforce strict adherence to data handling policies.

Do's & Dont's

- Encrypt sensitive data at rest and in transit.
- Use secure file-sharing and collaboration tools.
- Follow established data handling policies and procedures.
- Report any suspected data leakage incidents immediately.

- Share sensitive data via unencrypted email or messaging platforms.
- Store sensitive data in unsecured cloud storage or on personal devices.
- Bypass security controls or data handling policies.
- Neglect to report any potential data breaches.

Supply Chain Attacks

Meaning:
Supply chain attacks target third-party vendors or suppliers to gain access to an organization's systems or data. Attackers compromise a vendor's software or hardware, which is then used to infect the target organization.

Mitigation:

How Supply Chain Attacks Work:
Vendor Compromise:

- Attackers identify a vulnerable vendor in the target's supply chain.
- They compromise the vendor's systems, software, or hardware.

Malicious Insertion:

- Attackers insert malicious code or hardware into the vendor's products or services.

Distribution:

- The compromised products or services are distributed to the target organization.

Target Compromise:

- The malicious code or hardware allows the attackers to gain access to the target's systems or data.
- This can lead to data breaches, malware infections, or system disruptions

Identifying Potential Supply Chain Attacks:

Identifying supply chain attacks can be challenging, as the initial compromise occurs outside your direct control. However, you can monitor for unusual behavior and implement security measures:

Unusual Software Behavior:
- Unexpected changes in software functionality.
- Unauthorized access to sensitive data.
- Increased system resource usage.

Hardware Anomalies:
- Hardware devices behaving erratically.
- Unauthorized network connections.
- Firmware updates from untrusted sources.

Suspicious Vendor Activity:
- Unusual vendor updates or communication.
- Changes in vendor security practices.
- Vendor data breaches.

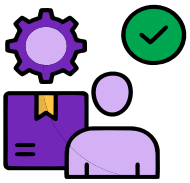
Network Anomalies:
- Unusual network traffic to or from vendor systems.
- Unauthorized connections to external servers.

Software Bill of Materials (SBOM):
- Analyse SBOMs to find known vulnerabilities within the software components used within your organization.

Use strong passwords	Don't share them with anyone
Enable two-factor authentication	Don't rely only on password
Create unique passwords for each account	Don't reuse the same password

Protecting Your System from Ransomware:

A layered defence approach is essential to mitigate the risks of supply chain attacks:



Vendor Due Diligence:
- Conduct thorough security assessments of vendors before engaging their services.
- Evaluate their security practices, certifications, and compliance.

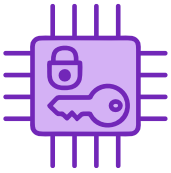
Software Bill of Materials (SBOM):
- Require vendors to provide SBOMs for all supplied software.
- Analyse SBOMs for known vulnerabilities and ensure timely patching.

Strict Access Controls:
- Implement strict access controls for vendor connections and data access.
- Apply the principle of least privilege.

Network Segmentation:
- Segment your network to limit the impact of a compromised vendor.
- Isolate vendor systems and data.

Regular Security Audits:
- Conduct regular security audits of vendor systems and connections.
- Monitor vendor activity for suspicious behavior.

Software Integrity Verification:
- Verify the integrity of software updates and installations.
- Use digital signatures and checksums.



Hardware Security:
- Implement hardware security measures, such as tamper-proof devices and secure supply chains.
- Verify the authenticity of hardware components.

Incident Response Planning:
- Develop and implement an incident response plan for supply chain attacks.
- Include steps for containment, eradication, and recovery.

Continuous Monitoring:

- Implement continuous monitoring of vendor systems and network traffic.
- Use security information and event management (SIEM) systems.

Zero Trust Security:

- Implement a zero trust security model, which assumes no user or device is trusted by default.

Contractual Security Requirements:

- Include security requirements in vendor contracts.
- Define responsibilities and liabilities.

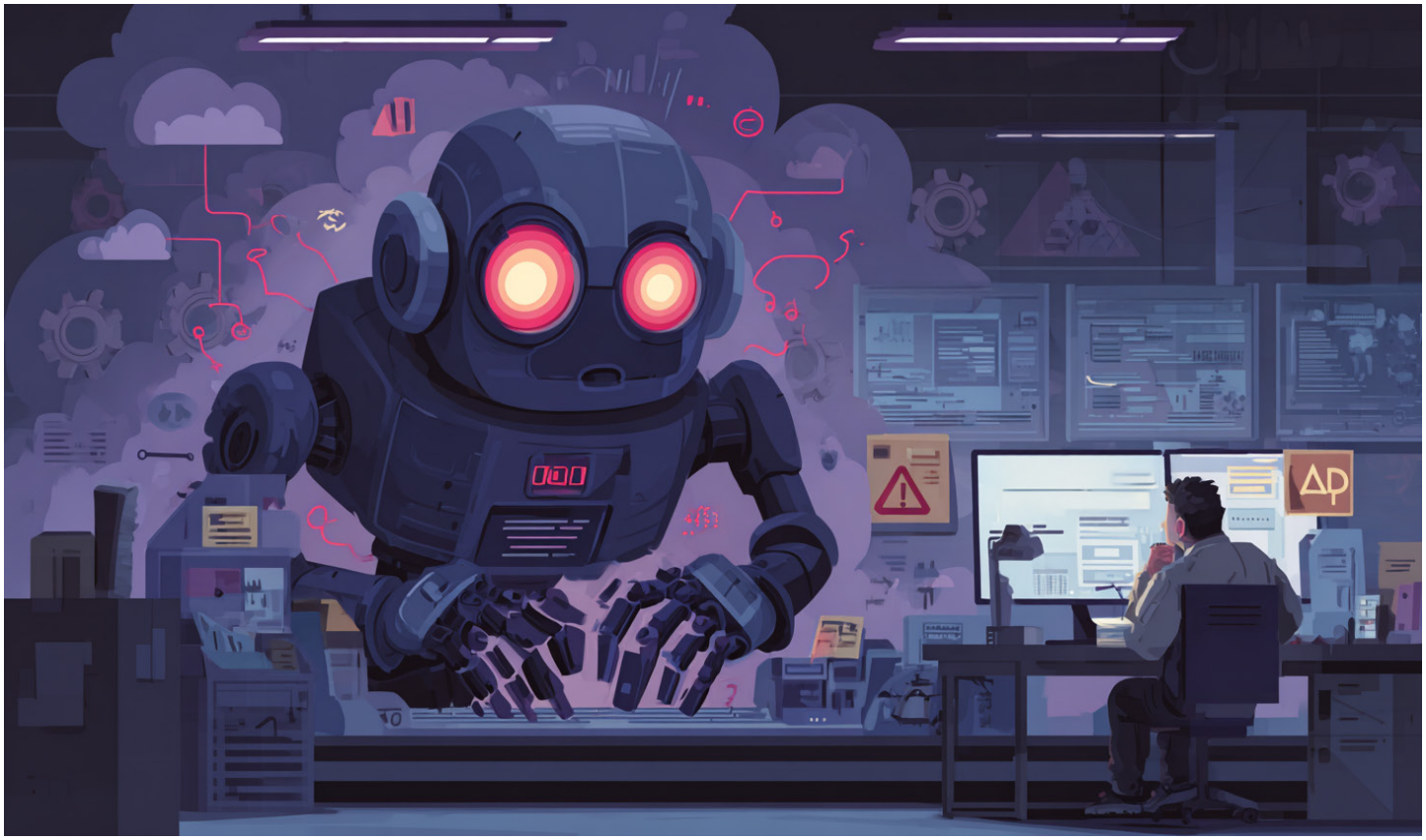
Regularly Review and Update Vendor Relationships:

- Regularly review and update vendor relationships.
- Make sure vendors are still compliant with security standards.

Do's & Dont's

- Conduct vendor due diligence.
- Implement strict access controls.
- Monitor third-party connections.
- Ensure proper agreeements before onboarding

- Trust vendors blindly without proper verification.
- Ignore third-party security practices.
- Fail to monitor third-party connections.



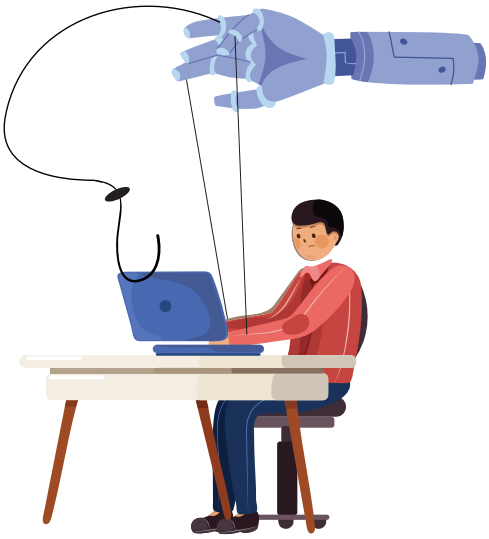
AI-Powered Cyberattacks

Meaning:
AI-powered cyberattacks leverage artificial intelligence (AI) and machine learning (ML) to automate and enhance malicious activities. These attacks are becoming increasingly sophisticated and difficult to detect, as AI enables attackers to adapt and evolve their tactics in real time.

Mitigation:

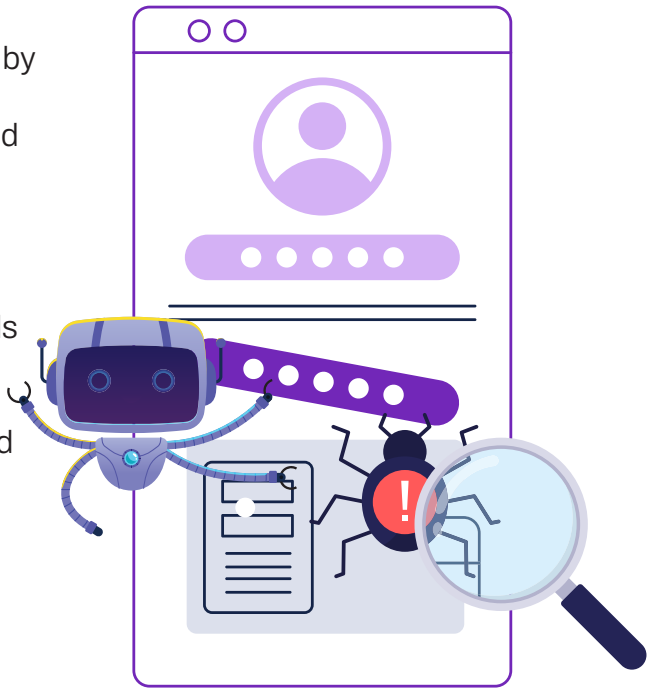
How AI-Powered Cyberattacks Work:
Enhanced Phishing and Social Engineering:

- AI can analyse vast amounts of data from social media, public records, and other sources to create highly personalized and convincing phishing emails or social engineering attacks.
- Natural language processing (NLP) can generate realistic and persuasive messages, making it harder to distinguish between legitimate and malicious communications.



Automated Malware Development and Evasion:

- AI can generate polymorphic malware that constantly changes its code to evade detection by signature-based antivirus software.
- ML algorithms can analyse security systems and adapt malware to bypass defences in real-time.

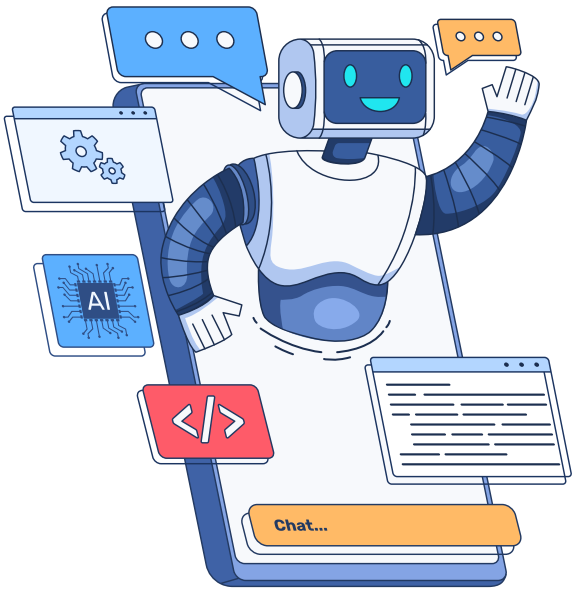


Improved Password Cracking:

- AI-powered tools can use machine learning to analyse password patterns and crack passwords more efficiently than traditional brute-force attacks.
- They can learn from previous data breaches and adapt their techniques to common password patterns.

Automated Vulnerability Scanning and Exploitation:

- AI can automate the process of scanning for vulnerabilities in systems and applications, allowing attackers to quickly identify and exploit weaknesses.
- AI can also automate the exploitation process, making it faster and more efficient.



Deepfake Attacks:

- AI-generated deepfakes can be used to create realistic videos or audio recordings of individuals, which can be used for social engineering, fraud, or disinformation campaigns.

AI-Enhanced DDoS Attacks:

- AI can be used to optimize DDoS attacks, making them more effective and harder to mitigate.
- AI can analyse network traffic patterns and adapt the attack to bypass defences.

Autonomous Attack Systems:

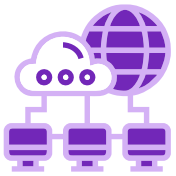
- In the future, AI could be used to create autonomous attack systems that can learn and adapt in real-time, making them extremely difficult to defend against.

Identifying Potential AI-Powered Cyberattacks:

Detecting AI-powered attacks is challenging because they often blend seamlessly with normal activity. However, here are some potential indicators:

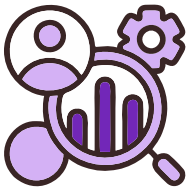
Anomalous Network Traffic:

- Sudden and unexplained spikes in network traffic.
- Unusual patterns of data transfer, especially outbound data.
- Connections to unusual or unknown IP addresses.



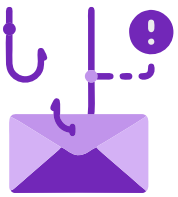
Behavioural Anomalies:

- Users accessing resources or performing actions outside of their normal routines.
- Systems exhibiting unusual resource usage or performance issues.
- Unexplained changes in system configurations.



Sophisticated Phishing Attacks:

- Highly personalized emails or messages that contain accurate information about the target.
- Emails with perfect grammar and spelling, and realistic-looking attachments.
- Deepfake videos or audio recordings used in social engineering attacks.

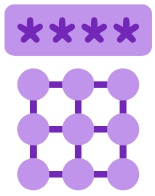


Malware Evasion:

- Malware that evades traditional antivirus detection.
- Files or processes that change their behavior or appearance frequently.

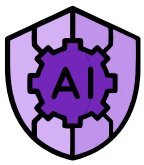
Unusual Login Patterns:

- Logins from unusual locations or devices.
- Rapid and repeated login attempts.
- Logins during unusual hours.



Protecting Your Systems from AI-Powered Cyberattacks:

A multi-layered approach is essential for protecting against AI-powered cyberattacks:



AI-Powered Security Tools:

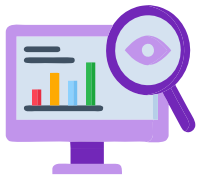
- Implement AI-driven security tools that can detect and respond to AI-powered attacks.
- These tools can analyze behavior patterns and identify anomalies that traditional security systems might miss.

Behavioural Analytics:

- Use security solutions that analyze user and system behavior to detect anomalies.
- These tools can identify deviations from normal patterns and flag suspicious activity.

Adaptive Authentication:

- Implement adaptive authentication methods that consider user behavior and context to verify identity.
- This can include factors such as location, device, and time of day.



Continuous Monitoring:

- Implement continuous monitoring of network traffic, system logs, and user activity.
- Use security information and event management (SIEM) systems to correlate data from multiple sources.

Security Awareness Training:

- Train users to be aware of the risks of AI-powered attacks, such as deepfakes and sophisticated phishing.
- Emphasize the importance of verifying information and being cautious of suspicious communications.

Strong Passwords and Multi-Factor Authentication (MFA):

- Use strong, unique passwords for all accounts.
- Enable MFA whenever possible to add an extra layer of security.

Regular Security Audits:

- Conduct regular security audits to identify and address vulnerabilities.
- Penetration testing is also very valuable.

Software Updates:

- Keep all software and systems up to date with the latest security patches.

Network Segmentation:

- Segment your network to limit the spread of an attack.

Zero Trust Security:

- Implement a zero trust security model, which assumes no user or device is trusted by default.

Deepfake Detection Tools:

- Use deepfake detection tools to identify manipulated videos or audio recordings.

Threat Intelligence Sharing:

- Share threat intelligence with other organizations to stay informed about the latest AI-powered attack techniques.

AI in Security Operations:

- Employ AI in your security operations center (SOC). This will allow for faster detection, and response times.

Ethical AI Use:

- As AI is used in security, it is also important to consider the ethical use of AI, and to make sure that the tools are used responsibly.

Do's & Dont's

- Use AI security tools but Cautiously. .
- Implement adaptive authentication.
- Update security protocols.

- Rely on static security defences.
- Ignore the advancements in AI-powered cyberattacks.
- Fail to update security systems.

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

बिना मांगी वित्तीय सलाह देने वाले एआई चैटबॉट से सावधान रहें; स्रोतों की दोबारा जाँच करें।

#एआईफ़िशिंग

Always double-check AI-generated content before sharing to avoid being influenced by fake media

#AIPhishing

Supported by

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Digital India
Power To Empower

myGov
मेरी सरकार

Indian Cyber Crime Coordination Centre
सहयोग कवचाहे • Working Together With Vigour

सी-डैक
CDAC

Hardware Attacks

Meaning:
Hardware attacks target physical hardware, such as servers, routers, or storage devices, to compromise systems. These attacks can involve tampering, counterfeiting, or exploiting vulnerabilities in hardware components.

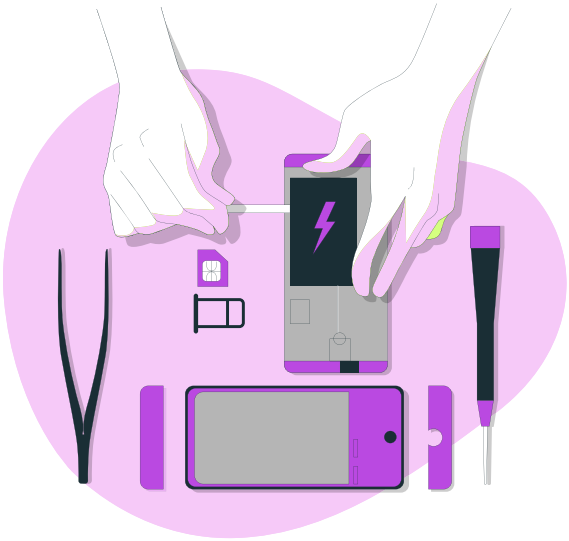
Do's & Dont's

- Use secure hardware.
- Secure physical access.
- Conduct regular audits.

- Ignore physical security measures.
- Use unverified or counterfeit hardware.
- Fail to conduct regular Hardware audits.

Mitigation:

How Hardware Attacks Work:



Tampering:

- Physical modification of hardware components to introduce malicious functionality.
- This can involve inserting malicious chips, modifying firmware, or altering circuitry.

Counterfeiting:

- Replacing genuine hardware components with counterfeit versions that contain malicious code or vulnerabilities.
- These counterfeit components can be difficult to distinguish from genuine ones.

Side-Channel Attacks:

- Exploiting information leaked from hardware during normal operation, such as power consumption, electromagnetic emissions, or timing variations.
- This information can be used to extract encryption keys or other sensitive data.

Fault Injection Attacks:

- Intentionally inducing errors in hardware to bypass security mechanisms.

- This can involve manipulating voltage, temperature, or clock signals.

Hardware Trojans:

- Malicious circuits embedded within hardware components during manufacturing or supply chain distribution.
- These Trojans can perform various malicious activities, such as data theft or system sabotage.

Firmware Attacks:

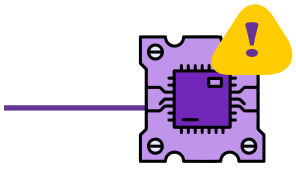
- Malicious modification of firmware, which is software that is embedded into hardware. This can provide very deep access to systems.

Identifying Potential Hardware Attacks::

Identifying hardware attacks can be challenging, as they often leave few software-based traces. However, here are some potential indicators:

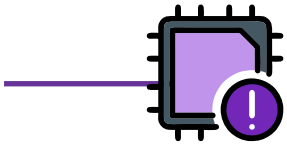
Unexpected Hardware Behavior:

- Hardware devices behaving erratically or malfunctioning.
- Unauthorized network connections from hardware devices.
- Unexplained changes in hardware configurations.



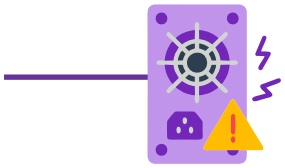
Firmware Anomalies:

- Firmware updates from untrusted sources.
- Unexpected changes in firmware settings.
- Firmware versions that don't match official releases.



Physical Anomalies:

- Signs of physical tampering, such as damaged seals or modified components.
- Counterfeit hardware components.
- Unexpected electromagnetic emissions.



Side-Channel Leakage:

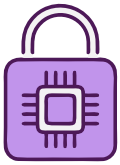
- Unusual power consumption patterns.
- Unexplained electromagnetic emissions.
- Timing variations in hardware operations.

Protecting Your Systems from Hardware Attacks:

A layered defence approach is crucial to mitigate the risks of hardware attacks:

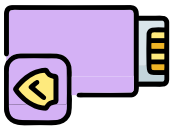
Secure Supply Chain:

- Source hardware from trusted vendors and authorized distributors.
- Implement supply chain security measures to prevent counterfeit components.



Hardware Security Modules (HSMs):

- Use HSMs to protect cryptographic keys and sensitive data.
- HSMs provide tamper-resistant hardware for secure key storage and processing.

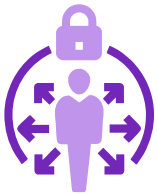


Tamper-Proof Hardware:

- Use hardware devices with tamper-proof features, such as physical security seals and intrusion detection mechanisms.

Firmware Security:

- Verify the integrity of firmware updates.
- Implement secure boot mechanisms to prevent unauthorized firmware modifications.



Physical Security:

- Implement strong physical security measures to protect hardware devices from unauthorized access.
- This includes access controls, surveillance systems, and environmental monitoring.

Side-Channel Attack Mitigation:

- Implement countermeasures to mitigate side-channel attacks, such as power consumption monitoring and electromagnetic shielding.

Hardware Security Audits:

- Conduct regular hardware security audits to identify and address vulnerabilities.
- This includes testing for hardware trojans.

Secure boot:

- Ensure that the systems use secure boot, to ensure that only trusted operating systems and drivers are loaded.

Encryption:

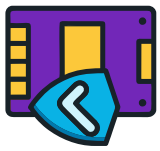
- Encrypt sensitive data at rest and in transit. This will minimize the impact of data loss, even if hardware is compromised.

Zero Trust Security:

- Implement a zero trust security model, which assumes no user or device is trusted by default.

Regular Monitoring:

- Monitor hardware and systems for unusual activity.



Hardware Integrity Verification:

- Verify the integrity of hardware components during installation and maintenance.

Data Exfiltration

Meaning:
Data exfiltration is the unauthorized transfer of data from a computer system or network to an external location. It's a critical threat because it can lead to the loss of sensitive information, intellectual property, and financial data. Attackers may use various techniques to exfiltrate data, making it essential to implement robust security measures.

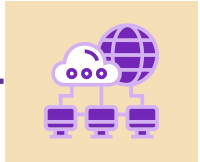
Mitigation:

How Data Exfiltration Works:

Malware:
- Malware, such as Trojans or spyware, can be used to steal data and transmit it to the attacker's server.

Insider Threats:
- Employees or contractors with authorized access may intentionally or unintentionally exfiltrate data.

Network Tunnelling:
- Attackers can create hidden communication channels to bypass security controls and exfiltrate data.



Physical Access:
- Attackers with physical access to systems can use USB drives or other devices to steal data.

Cloud Exfiltration:
- Attackers can take over cloud accounts, and exfiltrate data that is stored in cloud services.

API Abuse:
- Attackers can use legitimate API's to pull data out of a system.

Data in transit interception:
- Attackers can intercept data while it is moving over a network.

Identifying Data Exfiltration:

Unusual Network Traffic:
- Sudden spikes in outbound network traffic.
- Data transfers to unusual or unknown IP addresses.
- Unusual protocols being used for data transfer.

Large File Transfers:
- Transfer of large files or data sets that are not typical for normal operations.

Access to Sensitive Data:
- Users accessing sensitive data that they don't normally need.
- Unauthorized access to sensitive files or databases.

Log Anomalies:
- Unusual entries in system or application logs.
- Attempts to disable logging or auditing.

Cloud Activity Anomalies:
- Unusual download activity from cloud storage.
- Login activity from unusual locations.

Data Loss Prevention (DLP) Alerts:
- DLP systems triggering alerts for suspicious data transfers.

Increased Database Reads:
- Unexpected increases in database read operations.

Protecting Your System from Data Exfiltration:

A layered defence approach is crucial to prevent data exfiltration:tacks:

Data Loss Prevention (DLP) Systems:

- Implement DLP systems to monitor and control data movement.
- DLP can detect and block sensitive data from leaving the network.

Encryption:

- Encrypt sensitive data at rest and in transit.
- This protects data even if it is exfiltrated.

Access Controls:

- Implement strict access controls to limit user access to sensitive data.
- Apply the principle of least privilege.

Network Segmentation:

- Segment your network to limit the spread of an attack and prevent lateral movement.

Intrusion Detection/Prevention Systems (IDS/IPS):

- Implement IDS/IPS to detect and block malicious network traffic.

User Behaviour Analytics (UBA):

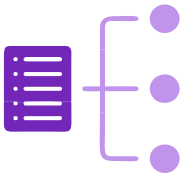
- Use UBA to monitor user activity and detect anomalous behavior.

Security Information and Event Management (SIEM):

- Implement SIEM systems to collect and analyse security logs from various sources.

Regular Security Audits:

- Conduct regular security audits to identify and address vulnerabilities.



Data Classification:

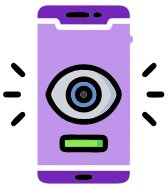
- Classify data based on sensitivity to prioritize protection efforts.
- Regular Backups:
- Regularly back up data, so that if data is stolen, it can be recovered

Endpoint Protection:

- Use endpoint protection software that detects and blocks malicious activity on individual computers.

Zero Trust Security:

- Implement a zero-trust security model, which assumes no user or device is trusted by default.



Monitoring API usage:

- Monitor the usage of API's, and ensure that they are used in a normal way.

Training and Awareness:

- Educate employees about the risks of data exfiltration and how to identify suspicious activity.

Do's & Dont's

- Implement DLP tools.
- Encrypt sensitive data.
- Monitor network traffic.

- Leave sensitive data unencrypted.
- Ignore network anomalies.
- Fail to restrict access to sensitive data.

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

Your trash is someone's hack

Dumpster Diving is a security knack

Shred before dumping

SHREDIT

Supported by

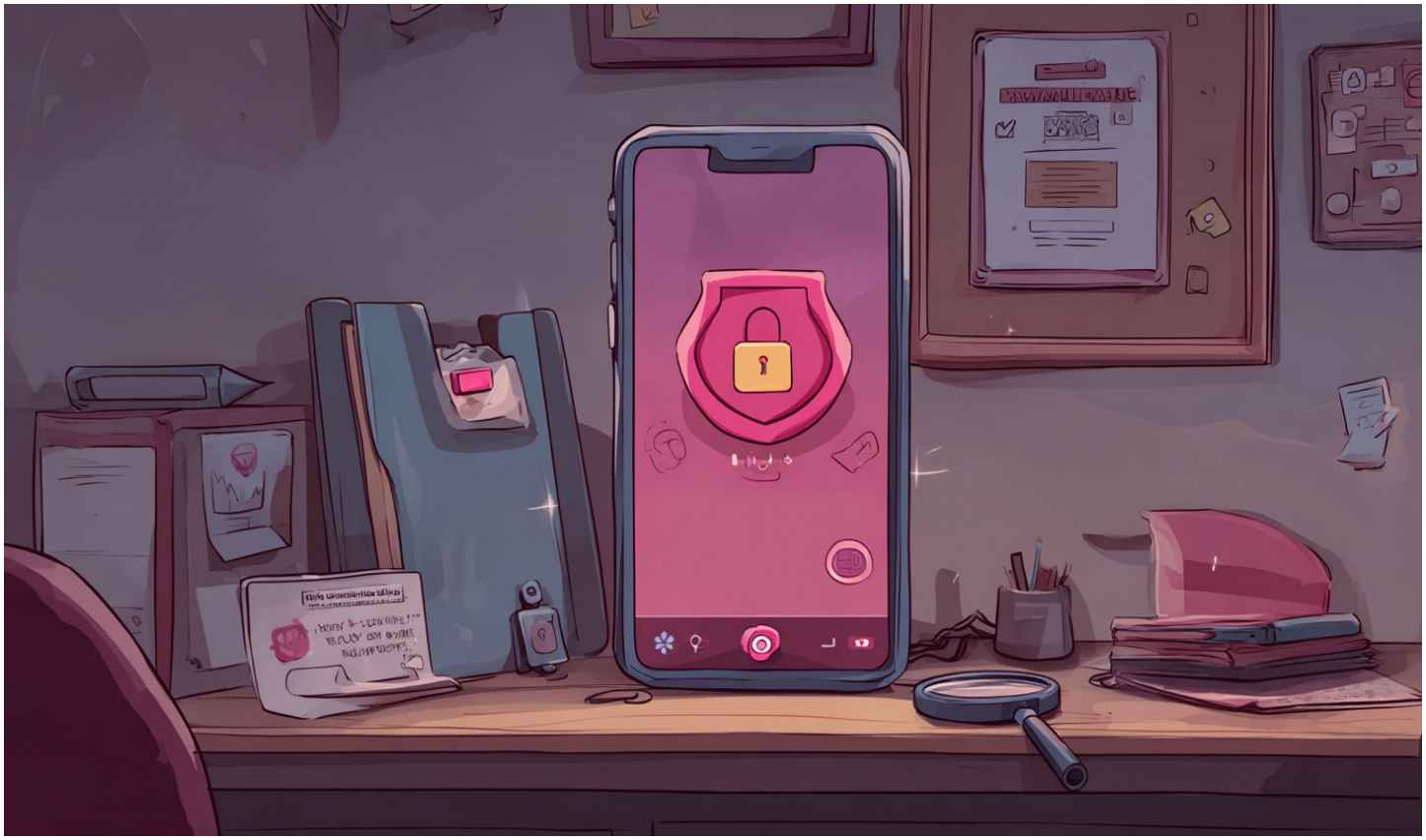
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Digital India
Power To Empower

myGov
मेरी सरकार

Indian Cyber Crime Coordination Centre
सहयोग कवचाहे • Working Together With Vigour

सी-डैक
CDAC



Mobile Device Security

Meaning:
Mobile devices have become essential tools for both personal and professional use, but they also introduce significant security risks. With the increasing amount of sensitive data stored and accessed on these devices, it's crucial to implement robust security measures.

Do's & Dont's

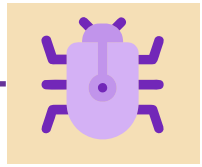
- Encrypt devices.
- Install secure apps.
- Use VPNs.

- Install untrusted apps.
- Use public Wi-Fi without VPN.
- Leave devices unattended.

Mitigation:

Mobile Device Security Threats:

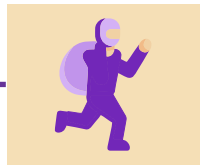
Malware:
- Malicious apps can steal data, track your location, or damage your device.
- Malware can be distributed through app stores, websites, or phishing attacks.



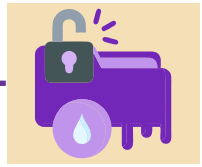
Phishing and Smishing:
- Phishing emails or SMS messages (smishing) can trick you into revealing sensitive information.
- These attacks often mimic legitimate communications.

Unsecured Wi-Fi:
- Public Wi-Fi networks can be vulnerable to eavesdropping and data interception.
- Attackers can steal your login credentials or other sensitive information.

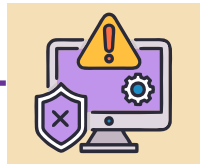
Physical Theft or Loss:
- Lost or stolen devices can provide attackers with access to your data.
- Lack of strong authentication can exacerbate the risk.



Data Leakage:
- Apps or services may unintentionally leak sensitive data.
- Cloud storage or backup services can also be vulnerable.



Operating System Vulnerabilities:
- Outdated operating systems may contain security vulnerabilities.
- Attackers can exploit these vulnerabilities to gain access to your device.



Rooting/Jailbreaking:
- Modifying the operating system to gain root or administrative privileges can introduce security risks.
- It may disable security features.

Side-loading apps:
- Installing applications from untrusted sources, outside of official app stores.

Identifying Mobile Device Security Threats:

Detecting AI-powered attacks is challenging because they often blend seamlessly with normal activity. However, here are some potential indicators:

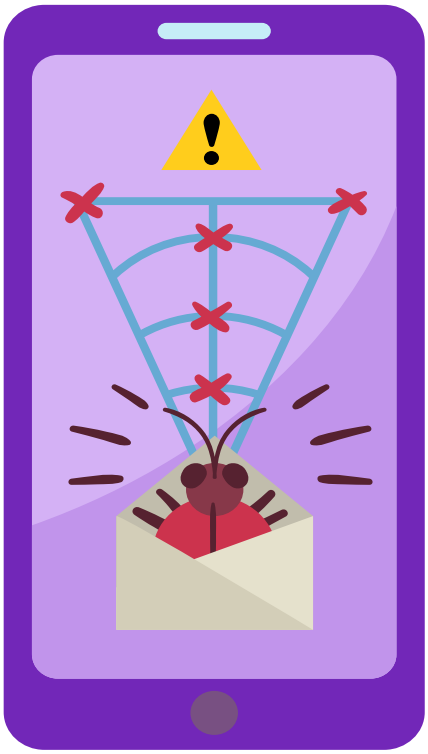
Unusual App Behaviour:
- Apps requesting excessive permissions.
- Apps consuming excessive battery or data.
- Apps crashing or malfunctioning frequently.

Suspicious Messages:
- SMS or email messages with suspicious links or attachments.
- Messages that request sensitive information.
- Messages that create a sense of urgency.

Unfamiliar Wi-Fi Networks:
- Public Wi-Fi networks with generic or unfamiliar names.
- Wi-Fi networks without password protection.

Device Performance Issues:
- Slow performance or overheating.
- Unexpected pop-up ads or browser redirects.

Unauthorized Access:
- Unusual login activity on your accounts.
- Changes to device settings without your knowledge.

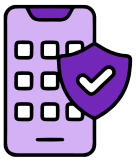


Protecting Your System from Data Exfiltration:

A layered defence approach is crucial to prevent data exfiltration:tacks:

Strong Passwords and Biometrics:
- Use strong, unique passwords or passcodes.
- Enable biometric authentication, such as fingerprint or facial recognition.

Software Updates:
- Keep your operating system and apps up to date with the latest security patches.
- Enable automatic updates.



App Security:

- Download apps only from trusted sources, such as official app stores.
- Review app permissions before installation.
- Delete unused apps.

VPN Usage:

- Use a VPN (Virtual Private Network) when connecting to public Wi-Fi.
- VPNs encrypt your internet traffic and protect your data.

Remote Wipe and Locate:

- Enable remote wipe and locate features to erase data or locate a lost device.

Encryption:

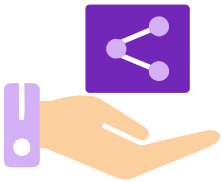
- Enable device encryption to protect your data at rest.

Antivirus and Anti-Malware:

- Install reputable mobile security software.
- Keep the software updated.

Secure Browsing:

- Avoid clicking on suspicious links or visiting untrusted websites.
- Use a secure browser.

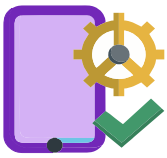


Limit Data Sharing:

- Be cautious about sharing personal information with apps or websites.
- Review privacy settings.

Disable Unnecessary Features:

- Disable Bluetooth and Wi-Fi when not in use.
- Disable location services when not needed.



MDM (Mobile Device Management):

- For work devices, use MDM solutions to enforce security policies.

Monitor App activity:

- Periodically check the permissions, and background activity of installed applications.

Avoid Rooting/Jailbreaking:

- Refrain from modifying the OS, unless you fully understand the risks.

Backups:

- Regularly back up your device data.

User Training:

- Educate users about mobile security best practices.

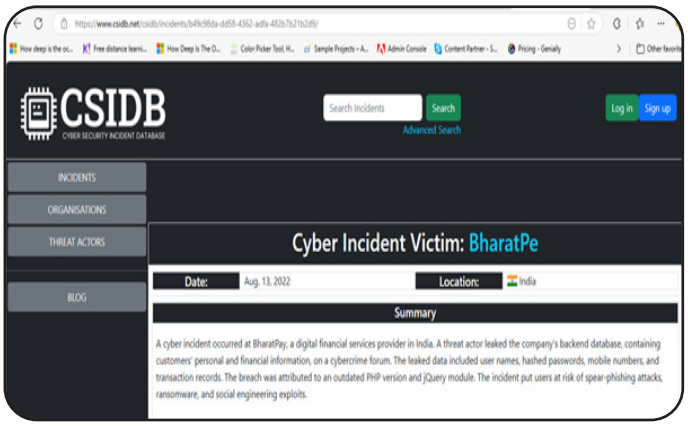
"Don't download without a thought, Fake apps can steal your data leaving you shocked

- Review app permissions regularly
- Disable unnecessary tracking
- Maintain updated privacy settings

25 Biggest Cyber attacks in India

Let us see the 25 of the most significant cyberattacks in India, analysing their consequences and the insights they provide. By reviewing these incidents, you can understand the evolving cybersecurity landscape and the necessity of protecting sensitive data.

1. BharatPay Hacked (August 2022)

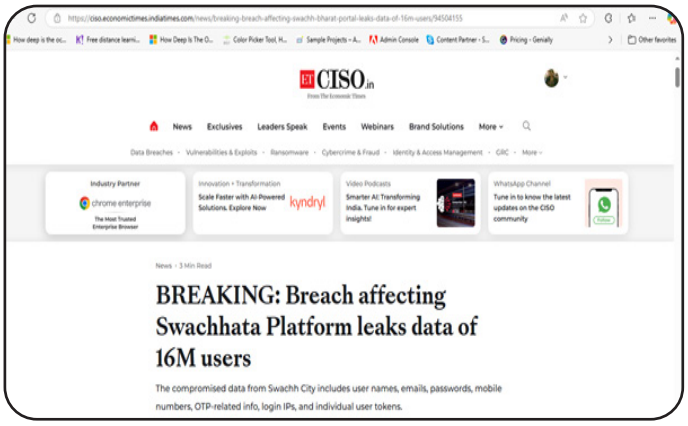


What happened?
BharatPay, a fintech service provider, suffered a major data breach, exposing personal information of about 37,000 users. Sensitive details such as usernames, hashed passwords, and transaction data were leaked.

Impact:
The breach raised concerns about the security of financial data in digital payment platforms.

Lesson:
Fintech companies must implement advanced encryption and multi-layered security mechanisms to safeguard user data.

2. Swachhta Platform Hacked (September 2022)



What happened?
Attackers known as LeakBase breached the Swachh City platform, leaking data of 16 million users, including email addresses, password hashes, and phone numbers.

Impact:
The data was put up for sale on the dark web, increasing the risk of phishing attacks and identity theft.

Lesson:
Government platforms handling citizen data need stronger security policies, including multi-factor authentication (MFA) and encryption.

3. Cyberattack on AIIMS (December 2022)

What happened?
AIIMS faced a ransomware attack that encrypted 1.3 TB of data across five servers, disrupting hospital operations.

Impact:
The breach exposed vulnerabilities in healthcare infrastructure. The hospital had to restore data from backups.

Lesson:
Healthcare institutions must improve cybersecurity defenses and have reliable backup recovery plans.

4. RailYatri Data Breach (December 2022)

What happened?
RailYatri, an Indian Railways e-booking service, suffered a breach that leaked records of over 30 million users on a cybercrime forum.

Impact:
The breach highlighted risks in transportation sector security.

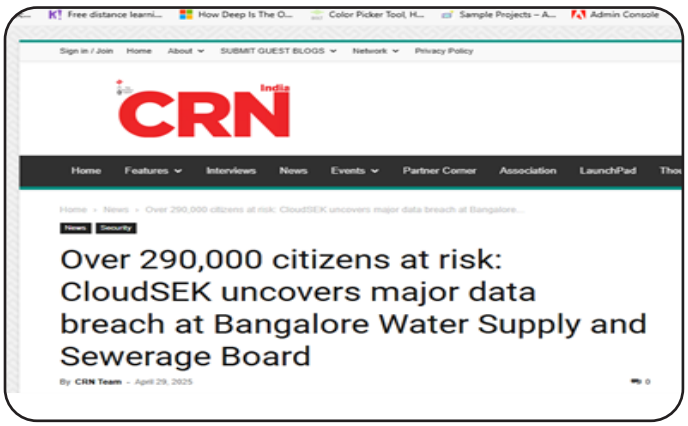
Lesson:
Such platforms should implement strong data protection measures and conduct frequent security audits.

5. CloudSEK Data Breach (December 2022)

What happened?
Cybersecurity firm CloudSEK faced a targeted attack in an attempt to damage its reputation. The attackers claimed to have stolen sensitive data, though the company denied it.

Impact:
The incident stressed the risks even cybersecurity firms face.

Lesson:
Security firms must enhance their internal security and threat monitoring to prevent breaches.

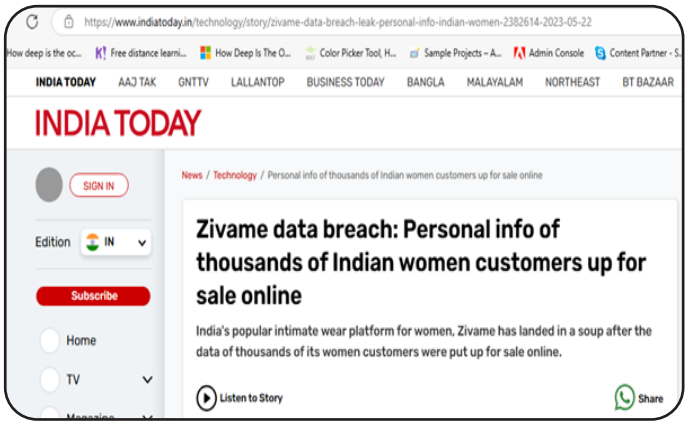


6. Zivame Data Breach (2022)

What happened?
Zivame, an online lingerie retailer, suffered a breach affecting 1.5 million customers, with personal data being sold online for $500 in cryptocurrency.

Impact:
The breach raised concerns about e-commerce security.

Lesson:
E-commerce platforms need robust encryption and better monitoring of unauthorized access.



7. Motilal Oswal Cyber Incident (2023)

What happened?
The LockBit group attempted to extort Motilal Oswal Financial Services through a cyberattack.

Impact:
No major disruption occurred, thanks to quick action by the company.

Lesson:
Financial institutions must strengthen employee cybersecurity training and incident response.

8. Polycab Ransomware Attack (2023)

What happened?
Polycab India, a wires and cables manufacturer, faced a ransomware attack on its IT systems.

Impact:
While core systems remained unaffected, the attack revealed risks in industrial cybersecurity.

Lesson:
Manufacturing companies should enforce strong cyber defense measures, including network segmentation.

9. Sun Pharma Cyber Attack (2023)

What happened?
Sun Pharmaceutical Industries experienced a cyberattack that disrupted its operations.

Impact:
The breach increased concerns about cybersecurity in the pharmaceutical sector.

Lesson:
Healthcare and pharma companies should secure their intellectual property and sensitive patient data.

10. MoChhatua Data Breach (May 2023)

What happened?
Hackers leaked user data from Odisha's MoChhatua app, used for ration distribution.

Impact:
Sensitive information of citizens was compromised.

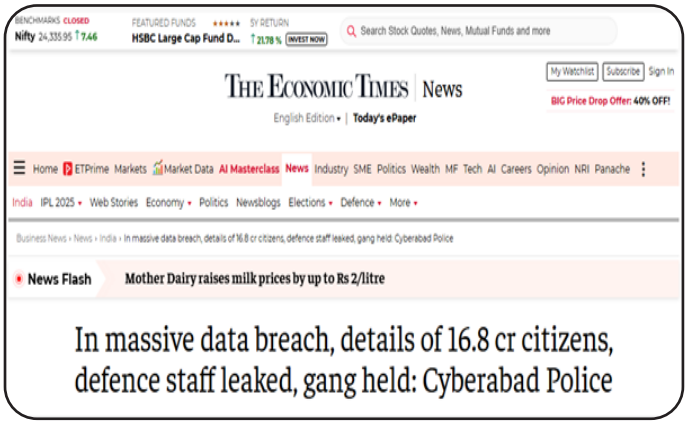
Lesson:
Government applications need robust cybersecurity frameworks and frequent security audits.

11. Cyberabad Police Data Leak (April 2023)

What happened?
A breach affected 66.9 crore individuals and organizations.

Impact:
The data theft highlighted weak security in law enforcement databases.

Lesson:
Stronger data protection and monitoring mechanisms are required for police databases.



12. Rentomojo Cyber Attack (April 2023)

What happened?
The rental platform Rentomojo was breached due to cloud misconfiguration.

Impact:
Users' personal data was exposed, risking identity theft.

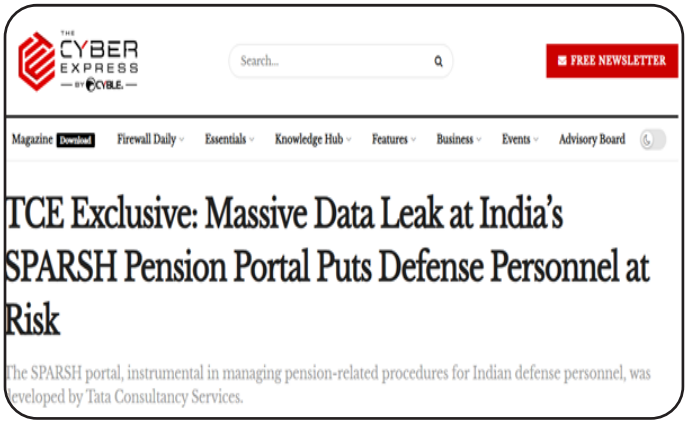
Lesson:
Cloud security must be prioritized with proper access control and encryption.

13. SPARSH Data Breach (2023)

What happened?
A breach in the pension management system for defense personnel led to data being sold on the dark web.

Impact:
Pension details were compromised.

Lesson:
Government portals must implement stricter access controls.



14. Hathway ISP Data Breach (2023)

What happened?
A hacker leaked 200GB of sensitive data from Hathway's systems.

Impact:
Personal data of over 41.5 million customers was compromised.

Lesson:
ISPs must enhance security measures to prevent unauthorized access.

15. Telangana Police's Hawk Eye App Data Breach (2023)

What happened?
Hackers leaked personal data of 200,000 citizens from the app.

Impact:
The breach exposed flaws in law enforcement's digital security.

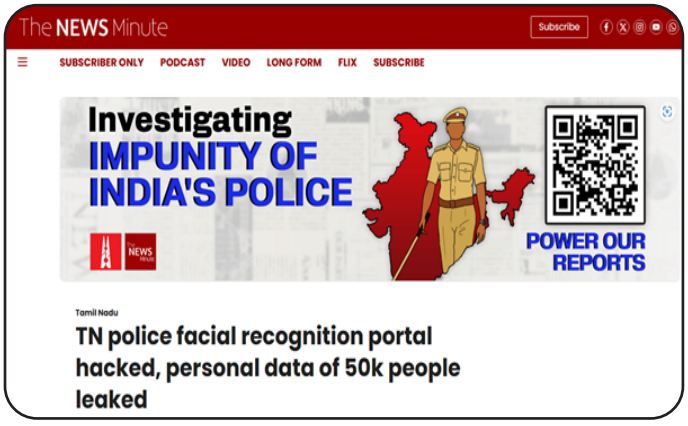
Lesson:
Police apps should enforce advanced authentication and encryption.

16. Tamil Nadu's Facial Recognition Portal Data Breach (2023)

What happened?
Hackers gained unauthorized access using compromised credentials

Impact:
Raised concerns over biometric data security.

Lesson:
Government agencies must adopt zero-trust security models.



17. NDMA Data Breach (2023)

What happened?
Hackers leaked personal data of 93,000 volunteers.

Impact:
The breach highlighted vulnerabilities in disaster management infrastructure.

Lesson:
Security best practices must be enforced in critical government agencies.

18. boAt India Data Breach (2023)

What happened?
Personal details of 7.5 million boAt users were leaked online.

Impact:
The breach raised consumer privacy concerns.

Lesson:
Stronger data protection laws are needed in the e-commerce sector.

19. Hyundai Motor India Data Leak (2023)

What happened?
Customer data was exposed through a vulnerability in shared web links.

Impact:
Exposed personal and vehicle details.

Lesson:
Automakers must improve security in customer service portals.

20. BSNL Data Breach (May 2024)

What happened?
A hacker stole 278GB of BSNL customer data.

Impact:
Millions of users' telecom details were compromised.

Lesson:
Telecom firms must conduct frequent security assessments.

21. UP Marriage Assistance Scheme Fraud (2024)

What happened?
Hackers manipulated the website, fraudulently transferring Rs. 1 crore.

Impact:
The breach led to financial fraud in a government welfare scheme.

Lesson:
Stronger transaction monitoring and two-factor authentication are required.

Key Takeaways from These Attacks

The rise in cyber incidents across India underscores critical cybersecurity lessons for businesses and individuals:

- **Stronger Security Infrastructure:** Companies must implement advanced security frameworks, regular system updates, and encryption techniques to prevent breaches.
- **Employee Awareness & Training:** Educating employees on phishing threats and cyber hygiene can significantly reduce risks.
- **Robust Data Backup & Recovery:** Maintaining secure and accessible backups ensures minimal downtime in case of an attack.
- **Incident Response Planning:** Organizations should establish and regularly test response strategies to mitigate the impact of cyberattacks.
- **Frequent Security Audits:** Regular assessments can identify vulnerabilities before they are exploited.
- **Public Awareness & Transparency:** Clear communication about breaches fosters trust and encourages users to take necessary precautions.

Case Study

The "Golden Data" Breach at the National Treasury Department (NTD)

Background:

The National Treasury Department (NTD) manages vast amounts of highly sensitive financial data, including budget allocations, tax records, and government expenditure details. They recently implemented a new cloud-based financial management system to streamline operations and enhance accessibility. However, due to budgetary constraints and pressure to meet deadlines, several critical security measures were overlooked.

Scenario:

In the spring of 2024, NTD experienced a severe data breach. The initial point of entry was a phishing email targeted at a junior accountant, who inadvertently clicked a malicious link. This led to the installation of keylogger malware on their workstation. The attackers then used the captured credentials to gain access to the cloud-based system.

Exploiting unpatched vulnerabilities in the system's API, the attackers were able to escalate their privileges and gain administrative access. They disabled the system's intrusion detection system (IDS) and began exfiltrating large volumes of financial data over several weeks.

The breach went undetected for an extended period due to:

- **Insufficient Logging and Monitoring:** The system lacked robust logging and real-time monitoring capabilities.
- **Lack of Multi-Factor Authentication (MFA):** User accounts were protected only by passwords, making them vulnerable to credential theft.
- **Delayed Patch Management:** Critical security patches were not applied promptly, leaving known vulnerabilities exposed.
- **Inadequate Network Segmentation:** The cloud environment was not properly segmented, allowing the attackers to move laterally within the network.

The consequences were devastating:

- **Massive Data Exfiltration:** Sensitive financial data, including taxpayer information and government budget details, was stolen. 1
- **Financial Losses:** The department incurred significant costs for incident response, forensic investigation, and system remediation.
- **Reputational Damage**: Public trust in the government's ability to protect financial data was severely eroded.
- **Regulatory Fines:** The department faced potential fines for non-compliance with data protection regulations.

Post-Incident Analysis:

The forensic investigation revealed a systemic failure in the department's cybersecurity posture, highlighting the importance of comprehensive security measures.

इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY
सत्यमेव जयते

www.isea.gov.in

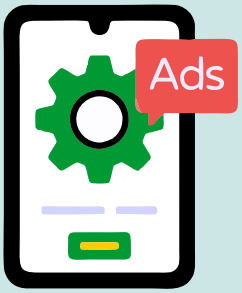
STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

3 Steps to

Prevent Data Leakage

#Be Safe
Stay Safe
www.staysafeonline.in

Adjust- ad settings



Off - location tracking

Delete- Location history

Supported by

certin Enhancing Cyber Security in India

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Digital India Power To Empower

mygov मेरी सरकार

Indian Cyber Crime Coordination Centre
सहयोग करवाहे • Working Together With Vigour

सी डैक CDAC

इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY
सत्यमेव जयते

www.isea.gov.in

सी डैक
CDAC

https://isea.gov.in/

https://staysafeonline.in/

Social Media Presence

Contact us

pmu-isea@cdac.in & isea@cdac.in