CENTRAL RESERVE POLICE FORCE

CYBER BYTE

JANUARY 2025

11 TIPS TO PROTECT YOURSELF FROM DIGITAL ARREST

Tips for using CHROME EXTENSIONS securely and efficiently

ANGEL ONE

PERSONAL DATA LEAK

The hacker also claimed to have accessed customers' stock holdings and profit and loss statements.

INDIANS LOST NEARLY RS 12,000 CRORE TO CYBER SCAMS IN 2024

1.CYBER GEEKS NEWS

A) India is topping the list for global mobile malware attacks as per a cybersecurity firm Zscaler-

India now accounts for 28% of total mobile malware attacks worldwide, surpassing the United States (27.3%) and Canada (15.9%), the Zscaler ThreatLabz 2024 Mobile, IoT, and OT Threat Report revealed.

The report analysed a dataset from June 2023 to May 2024 that included more than 20 billion threat-related mobile transactions and associated cyber threats. A blog by Zscaler said their research team tracked a rise in financially motivated mobile attacks that showed a 111% growth in spyware and 29% growth in banking malware.

One of the most recent cases in India was that of fake wedding cards. In their latest trick, scammers send pdf documents of wedding cards on WhatsApp, which when opened downloads malware on the recipient's device.

Earlier this year, in the month of August, nearly 300 small Indian banks were forced to go offline due to a ransomware attack. One-fifth of the nearly 1,500 cooperative and rural regional banks in the country were affected.

In 2022, AIIMS Delhi was under attack for more than 15 days, which the then minister of state for electronics and information technology, Rajeev Chandrasekhar, called "a conspiracy and planned by external forces."

The cyber-attacks also have become more sophisticated, Zscaler said in its blog post, adding that enterprises should adopt a zero-trust approach that mitigates cyber threats and improves their security posture.

B) 2024: cyberattacks in India BSNL data breaches.

Bharat Sanchar Nigam Ltd (BSNL) suffered a data breach in June this year, with threat actor "kiberphant0m" claiming to have accessed over 278 GB of sensitive data, including international mobile subscriber identity (IMSI) numbers, SIM card details, home location register data and security keys. The breach involved server snapshots that could be used for SIM cloning and extortion.

Angel One personal data leak

A data breach at Mumbai-based stock broking firm Angel One last year led to the personal information of 7.9 million customers being published on a hacker forum. The hacker also claimed to have accessed customers' stock holdings and profit and loss statements.

WazirX cyberattack

Cryptocurrency platform WazirX experienced one of the largest cyberattacks on an Indian exchange in July, with hackers stealing $235 million worth of investor holdings, nearly half of the platform's estimated reserves, affecting about 15 million users.

Ransomware attack on small Indian banks

Another significant cyber scam involved a ransomware attack that forced nearly 300 small Indian banks to go offline. Around one-fifth of the country's 1,500 cooperative and rural regional banks were affected, with C-Edge Technologies, a service provider to these banks, being the target of the attack.

Fake wedding card scam

A new scam tactic this year involved fake wedding cards. Scammers send PDF wedding invitations via WhatsApp, which, when opened, download malware onto the recipient's device.

By the numbers

Indians lost nearly Rs 12,000 crore to cyber scams this year, with scams increasing by 300%. A report from the non-profit Prahar predicts that India could face nearly 1 trillion cyberattacks annually by 2033, growing to 17 trillion by 2047.

This increase underscores the need for stronger cybersecurity across industries, especially in sectors targeted by cybercriminals.

2.CYBER FRAUDS

(A)Dozens of Chrome Extensions Hacked, Exposing Millions of Users to Data Theft

A new attack campaign has targeted known Chrome browser extensions, leading to at least 35 extensions being compromised and exposing over 2.6 million users to data exposure and credential theft.

"The attacker gained requisite permissions via the malicious application ('Privacy Policy Extension') and uploaded a malicious Chrome extension to the Chrome Web Store," Cyberhaven said in a separate technical write-up. "After the customary Chrome Web Store Security review process, the malicious extension was approved for publication."

"Browser extensions are the soft underbelly of web security," says Or Eshed, CEO of LayerX Security, which specializes in browser extension security. "Although we tend to think of browser extensions as harmless, in practice, they are frequently granted extensive permissions to sensitive user information such as cookies, access tokens, identity information, and more.

Further investigation has uncovered more extensions [Google Sheets] that are suspected of having been compromised, according to browser extension security platforms Secure Annex and Extension total:

- AI Assistant - ChatGPT and Gemini for Chrome
- Bard AI Chat Extension
- GPT 4 Summary with OpenAI
- Search Copilot AI Assistant for Chrome
- TinaMInd AI Assistant
- Wayin AI
- VPNCity
- Internxt VPN
- VidHelper Video Downloader
- Bookmark Favicon Changer
- Castorus
- Uvoice
- Reader Mode
- Parrot Talks
- Primus
- Tackker - online keylogger tool
- AI Shop Buddy

These additional compromised extensions indicate that Cyberheaven was not a one-off target but part of a wide-scale attack campaign targeting legitimate browser extensions.

(B) Cyber scamsters targeting PM- KUSUM applicants

There is not a sector that has been left untouched by cybercrime in today's world. The latest addition to this list is the PM – KUSUM scheme's Component B under which solar pump sets are provided to farmers. In recent times, many farmers have lost money after people posing to be associated with Karnataka Renewable Energy and Development Limited (KREDL) allegedly took money from them.

According to KREDL officials, in the last year, farmers have been reporting that they are receiving calls and WhatsApp messages from people claiming that they are KREDL officials and are forcing them to pay money. KREDL has also found that many others have taken to social media sites like Facebook and YouTube and were spreading misinformation about the PM Kusum scheme. In some cases, they also got the farmers to transfer money to them.

3. TIP OF THE MONTH

(A) How to protect yourself from digital arrest

Digital arrest refers to a deceptive tactic used by cybercriminals, who falsely claim to have the authority to arrest an individual through digital means, often over the phone or via online communication.

1. **Secure Your Router with a Strong Password**

Change the default administrator login credentials for your broadband router. Most routers come with a default username and password (like "admin" or "password"), which is easily guessable.Use a strong, complex password combining uppercase letters, lowercase letters, numbers, and symbols.

2. Use WPA3 or WPA2 Encryption

Enable the latest WPA3 encryption standard on your Wi-Fi network for enhanced security. If WPA3 isn't available, use WPA2 encryption.Avoid using WEP encryption, as it is outdated and can easily be breached by hackers.

3. Keep Your Router Firmware Updated

Manufacturers frequently release **firmware updates** to patch vulnerabilities and improve router security. Check your router's settings regularly and apply any updates.

- Some routers allow **automatic updates**—enable this if your router supports it.

4. Disable Remote Management

- Turn off **remote access** to your broadband router unless necessary. Remote management allows users to access router settings from the internet, which could be exploited by attackers.
- If remote access is required, consider using a **Virtual Private Network (VPN)** for secure remote management.

5. Use a Firewall

- Enable your router's built-in **firewall** to block unauthorized access. Most routers come with a firewall that adds an extra layer of protection against incoming threats.
- Consider using an additional **software firewall** on your devices for even greater security.

6. Change Your Network Name (SSID)

- Change the default **SSID** (Service Set Identifier) or network name of your broadband connection. Default names often reveal the router's brand, which could help attackers target specific vulnerabilities.
- Avoid using personal information (like your name or address) in the SSID.

7. Disable Wi-Fi When Not in Use

- Turn off your Wi-Fi or broadband connection when not in use (e.g., at night or when you're away). This reduces the chances of an attacker trying to access your network.
- You can set up a **schedule** in the router settings to automatically disable Wi-Fi during specific hours.

8. Enable MAC Address Filtering

- **MAC (Media Access Control) address filtering** allows you to limit which devices can connect to your broadband network. Each device has a unique MAC address, and you can specify which ones are allowed on your network.
- Although MAC addresses can be spoofed, this adds an additional layer of security.

9. Disable SSID Broadcasting

- **Disable SSID broadcasting** to make your Wi-Fi network less visible. This won't make your network entirely hidden but will make it harder for casual attackers to find and target your connection.
- You'll need to manually enter your SSID when connecting new devices to your network..

10. Disable Automatic Connection to Networks

- Turn off the **automatic connection** feature on your devices for joining open or public networks. This prevents your devices from accidentally connecting to potentially insecure or malicious networks.
- Manually choose and verify the network before connecting.

11. Regularly Reboot Your Router

- Rebooting your router can help **clear memory**, improve performance, and mitigate certain types of malware infections that rely on continuous uptime.
- A regular restart schedule can also help prevent long-term vulnerabilities from being exploited.

. By following these **broadband security practices**, you can better protect your internet connection

and the devices connected to it from a wide range of threats. Securing your router, monitoring devices, and enabling encryption are some of the most important steps to safeguard your home or business broadband.

(B) Tips for using Chrome extensions securely and efficiently

1. Only Install Extensions from Trusted Sources

- Always install extensions from the **official Chrome Web Store** or trusted developers. Avoid downloading extensions from third-party websites, as they may contain malware or malicious code.
- Look for extensions with **high ratings and positive reviews** from a significant number of users.

2. Review Permissions Carefully

- Before installing an extension, check the **permissions** it requests. Be wary of extensions that ask for more access than they need (e.g., access to all websites, reading and modifying data).
- If an extension requests sensitive permissions like access to your browsing history or clipboard, make sure it is necessary for the extension's functionality.

3. Keep Extensions to a Minimum

- Only install extensions that you **actively use**. Having too many extensions can slow down your browser, clutter the interface, and increase security risks.
- Periodically review and **remove unused extensions**.

4. Be Wary of Permissions Changes

- If an extension updates and requests **new permissions**, carefully review them. Some malicious developers may update previously safe extensions to gain unauthorized access after an update.
- Chrome will notify you when permissions change after an update—be cautious and decide whether to keep or remove the extension.

5. Disable Extensions You Don't Need

- If you don't want to completely remove an extension but don't use it regularly, **disable it temporarily**. This will help keep your browser fast and reduce potential security risks.
- You can disable an extension by going to **chrome://extensions/** and toggling off the switch for specific extensions.

6. Monitor Extension Behavior

- Watch for unusual browser behavior after installing or updating an extension, such as:
  - **Slow performance**
  - **Unexpected pop-ups or ads**
  - **Changes to your default search engine or homepage**.
- If you notice anything suspicious, **disable or remove the extension immediately**.

7. Be Cautious of Fake Extensions

- Some extensions may imitate legitimate ones. Before installing, check:
  - The **developer's name**.
  - The **extension's rating**.
  - **Number of installs** and the **reviews** to ensure you're getting the legitimate extension.

8. Watch for Phishing or Adware

- Some malicious extensions may inject ads, redirect you to unwanted sites, or engage in phishing attempts. Be cautious when encountering unexpected pop-ups or links.
- Use **ad blockers** or **anti-phishing extensions** to protect yourself from malicious ads and links..

By following these tips, you can keep your Chrome extensions secure, protect your privacy, and enhance your overall browsing experience.


केन्द्रीय रिजर्व पुलिस बल
153 वाहिनी गुण्डम, बीजापुर (छ.ग.)