CENTRAL RESERVE POLICE FORCE

SEPTEMBER-2025

CYBER BYTE

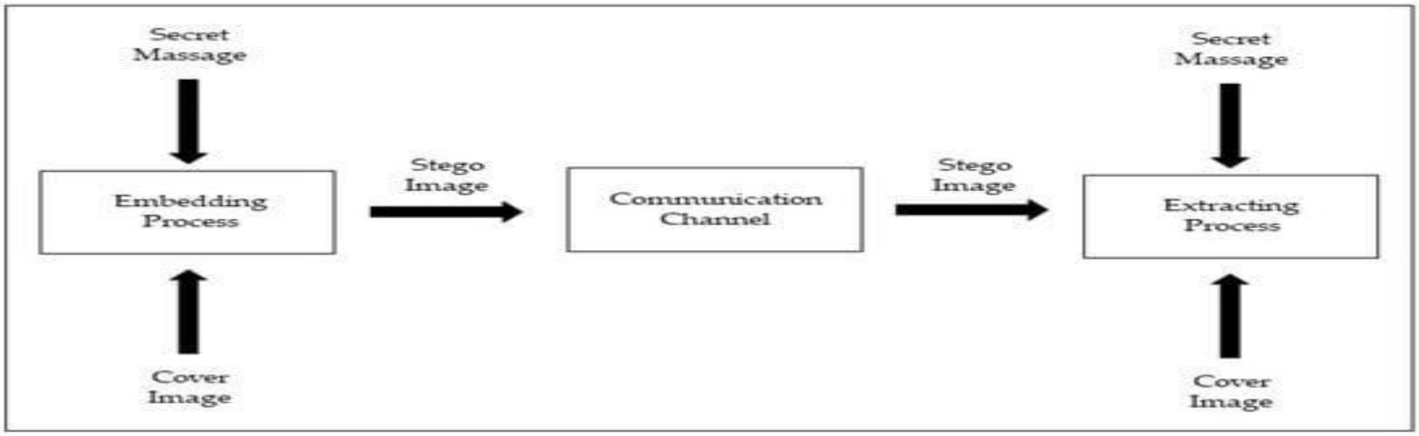
Google issues red alert as new cyber-attack targets Gmail users using AI with ‘indirect prompt injections’

FileFix attack uses steganography to drop StealC malware

1. CYBER GEEKS NEWS

(A) FileFix attack uses steganography to drop StealC malware.

A newly discovered FileFix social engineering attack impersonates Meta account suspension warnings to trick users into unknowingly installing the StealC infostealer malware.



FileFix is a new variant of the ClickFix family of attacks, which uses social engineering attacks to trick users into pasting malicious commands into operating system dialog boxes as supposed "fixes" for problems.

The FileFix technique was created by red team researcher and instead of convincing users into pasting malicious PowerShell commands into the Windows Run dialog or terminal, FileFix abuses the address bar in File Explorer to execute the commands.

This is not the first time FileFix has been used in attacks, with the Interlock ransomware gang previously using FileFix to install its remote access trojan (RAT). **However, these earlier attacks utilized the original FileFix proof-of-concept (PoC), rather than evolving it with new lures.**

The new campaign, discovered by Acronis, **uses a multi-language phishing page that poses as Meta's support team, warning recipients that their account will be disabled in seven days unless they view an "incident report"** allegedly shared by Meta.

(B) Google issues red alert as new cyber-attack targets Gmail users using AI with ‘indirect prompt injections’

Google, which has 1.8 billion Gmail users worldwide, recently issued a serious warning about a **new kind of cybersecurity threat linked to advances in artificial intelligence, reported Men's Journal.**

DynaRisk
Google Issues Red Alert: AI-Driven Cyber Threat Targets Gmail Users

This threat affects not just people but also businesses and governments. Google also explained the danger, **“With the rapid adoption of generative AI, a new wave of threats is emerging across the industry with the aim of manipulating the AI systems themselves. One such emerging attack vector is indirect prompt injections.**”

The difference with this attack is that instead of directly putting harmful commands into the AI prompt, **hackers hide malicious instructions inside things like emails, documents, or calendar invites.** These hidden commands can make the AI leak user data or do other bad things, the post explained.

Google warned that this threat puts everyone at risk. “As more governments, businesses, and individuals adopt generative AI to get more done, this subtle yet potentially potent attack becomes increasingly pertinent across the industry, demanding immediate attention and robust security measures.

Growing trend of the elderly citizens being systematically targeted by cyber criminals and duping large sums of money is raising concerns.

2. CYBER FRAUDS

(A) Elderly citizens emerging as prime targets in cyber frauds.

Recent cases in the city reveal that **scammers are exploiting the trust and limited digital awareness of senior citizens to siphon off lakhs of rupees through investment, loan, and trading scams**.

In one of the latest incidents, a 63-year-old retired person was cheated of over Rs 43 lakh after receiving **WhatsApp messages from fraudsters posing as executives of a reputed financial institution.**

The gang lured him with promises of discounted IPO shares and fake trading dashboards, eventually forcing him to make repeated transfers under the pretext of additional investments and loan repayments.

Cybercrime officials say such frauds are becoming increasingly common, with criminals **using sophisticated tactics such as fake websites, cloned customer support numbers and polished financial jargon to appear credible.** “Many victims only realize the deception after exhausting their savings or when they are unable to withdraw their so-called profits.

(B) Govt warns SMEs of festive season cyber fraud

CYFIRMA
How Festive Events Have Become Prime Targets for Digital Exploitation and Fraud

As the festive season brings a surge in sales for small businesses, cyber experts have cautioned that it also **creates fertile ground for fraudsters.** According to the Indian Computer Emergency Response Team (CERT-In) and the Data Security Council of India (DSCI), nearly 74 per cent of small and medium enterprises (SMEs) faced at least one cyber incident in the past year.

With teams stretched and order volumes rising, scammers are known to exploit the festive rush through tactics **such as fake payment receipts, phishing links, forged delivery messages and urgent order scams**.

Fraudsters often impersonate buyers, suppliers or even large companies to trick businesses into shipping goods without payment, updating bank details to fraudulent accounts, or granting access to sensitive systems.

Officials have urged businesses to remain vigilant and adopt basic cyber hygiene. Setting up a simple system for staff to log and report suspicious activity is also recommended. Even a brief oversight, such as clicking on a malicious link or rushing through a payment, can cause significant financial and reputational damage.

3. TIPS OF THE MONTH

(A) Safety Tips for Using ChatGPT

1. Don't Share Personal or Sensitive Information

Avoid entering:

- Full name
- Address
- Phone number
- Government ID numbers (like force id , Aadhaar)
- Financial information (credit card, bank details)
- Login credentials or passwords

Tip: Treat ChatGPT like a public space. If you wouldn't say it to a stranger, don't type it here.

2. Be Careful with Medical, Legal, or Financial Advice

ChatGPT can help **explain concepts**, but it's **not a substitute** for professionals.

Always consult a qualified doctor, lawyer, or financial advisor for critical decisions.

3. Verify Important Information

ChatGPT may provide outdated or incorrect answers.

- **Check facts** against official or trusted sources.
- Use it to **summarize**, **draft**, or **brainstorm**, but **don't rely solely** on it for accuracy.

4. Don’t Use ChatGPT to Cheat or Plagiarize

Using AI to:

- Write school essays without understanding
- Answer exam/test questions dishonestly
- Copy others’ work can lead to academic or professional consequences.

Tip: Use ChatGPT to **learn**, not replace your thinking.

5. Avoid Prompting for Harmful Content

Do **not** use ChatGPT to share or seek harmful medical advice (e.g., how to misuse drugs)

6. Understand Privacy Limits

ChatGPT does **not remember** previous conversations unless you’ve enabled memory.

Conversations are **not visible to others**, but **OpenAI may use them** to improve the model.

For extra privacy, turn off **chat history** in settings.

7. Be Aware of AI Limitations

ChatGPT can:

- **Hallucinate facts**
- Sound confident but be wrong
- Make up sources or citations

So, ask follow-up questions and **use critical thinking**.

8. Don’t Assume It's Human

ChatGPT is not a person:

- It doesn’t have feelings, beliefs, or intentions
- It doesn’t understand like humans do—it generates text based on pattern

(B) Do's for Google Gemini

1. **Do** ask clear and specific questions to get better answers.

2. **Do** verify important information from trusted sources.

3. **Do** use Gemini to brainstorm ideas, draft text, summarize info, or learn new topics.

4. **Do** protect your privacy by checking and adjusting your settings regularly.

5. **Do** review and edit any AI-generated content before sharing or publishing.

6. **Do** keep your software and apps updated to access the latest features securely.

7. **Do** ask for citations or sources when dealing with facts or data.

Don'ts for Google Gemini

1. **Don't** share personal, financial, or sensitive information in your queries.**For example:** - location based photo, **uniform photos....**

2. **Don't** rely solely on Gemini for critical medical, legal, or financial advice.

3. **Don't** use it to create or spread misinformation, harmful, or inappropriate content.

4. **Don't** plagiarize or cheat using AI-generated content—use it as a learning aid.

5. **Don't** assume all responses are 100% accurate or up to date.

6. **Don't** use Gemini to generate spam, malware, or any malicious software.

7. **Don't** ignore Google's privacy and data policies—review them regularly.

8. **Don't** input confidential work or client data without approval, especially in shared environments.

Launch of high-Altitude Bike expedition from **LAL CHOWK** Srinagarwith#yashasviniCRPF

Constable Toman Kumar won Gold in the Individual event at World Para Archery Championship 2025 in South Korea.

DG CRPF & CWA PRESIDENT at Vishwa Karma Pooja at directorate CRPF.