रक्षा लेखा नियंत्रक का कार्यालय, गुवाहाटी उदयन विहार, नारंगी, गुवाहाटी-781171
OFFICE OF THE CONTROLLER OF DEFENCE ACCOUNTS
UDAYAN VIHAR, NARANGI, GUWAHATI: 781171.
ई-मेल/e-mail:cda-guw@.nic.in फैक्स/FAX:0361-2640204 फोन/Ph: 0361-2640394, 2641142.

No. CDA GUW/IT&SW/1304/CYBER-SECURITY/2025 Date –29/07/2025

Circular No: -94

To
The Officer In-charge
All Sub-Offices
All sections (Local)

Subject: - Advisories on Cyber Security.

****

Advisories on Cyber security on the following subject matters have been received from HQrs. for strict compliance.

Sr.No.	Advisories
1.	Threat Intel Alert on Adversary TTPs targeting Windows/Linux.
2.	Advisory on use of DeepSeek for Defence Personnel.
3.	Advisory on usage of Artificial Intelligence (AI) Models (Online Models and Smart Devices with Inbuilt DeepSeek Features).
4.	Advisory on the usage of 'AI Generated Imagery' for Indian Defence Community.
5.	Advisory on Spurious/Suspicious call.
6.	Advisory on Phishing Attack

In order to avoid Cyber Vulnerabilities and associated frauds, all Officers In-charge are here-by directed to ensure that the guidelines issued by HQrs. Office as mentioned above, are to be strictly followed by all the officials in and outside office.

A compliance and action taken report in this regard may be furnished at the earliest please.

Enclosure: - As Above

(Kavya Tangirala)
Dy. CISO

Advisory - I

THREAT INTEL ALERT ON ADVERSARY TTPs TARGETTING WINDOWS/LINUX

1. **Background**.Cyber threat intelligence has revealed that new tactics are being tested for performing phishing attack which can deliver malicious script on internet facing machines (including Linux and windows).

2. **Aim.** The advisory is to sensitise all IN personnel regarding a new phishing technique being used by threat actors to compromise internet facing machines (Windows and Linux) using new attack vectors.

3. **Modus Operandi.** The modus operandi employed by the threat actor is enumerated below:

   (a) A phishing mail with a malicious URL is delivered to the user.

   (b) The malicious URL hosts a fake website akin MoD website thus luring the user to click on **"Click here"** button.

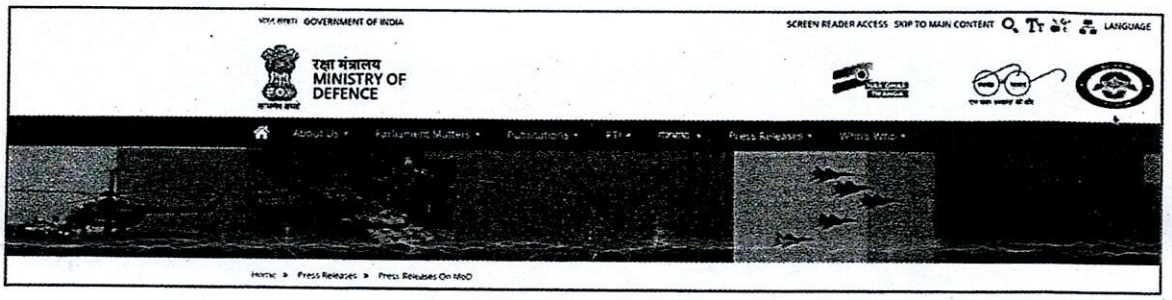


Fig1 Phishing page

(c) Once the user clicks on "Click Here" the website prompts the user for additional interaction, in this case the user is required to click on **"Continue"/"I am not a Robot"**. This action results in a malicious script getting copied on PCs clipboard which will later be used to get the reverse connection to the victim endpoint.

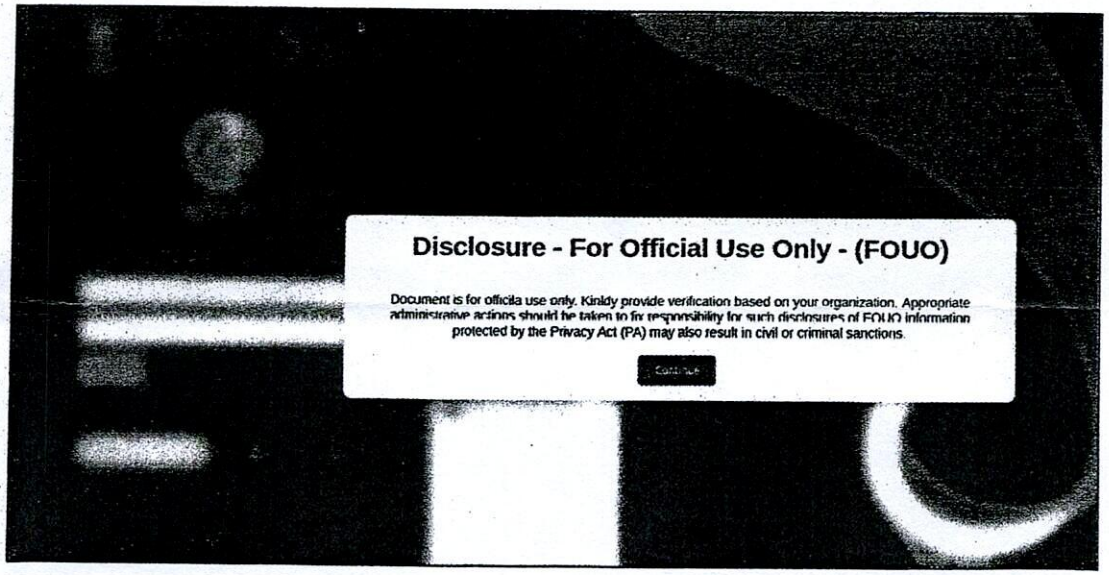


Fig 2: User interaction required to click on continue

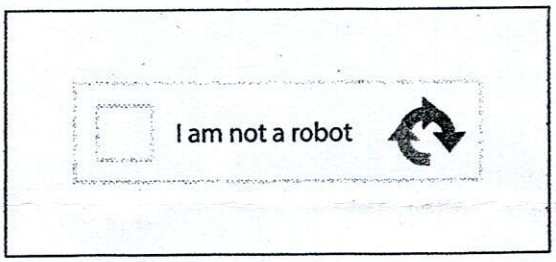


Fig 3: User interaction required to click on I am not a robot

(d) Further, a fake CAPTCHA "**Verify you are human**" and "**Verification Steps**" according to the Operating System of the user is prompted to the user. If the user follows the steps, the malicious script copied will get executed and the final payload is downloaded, which may further lead to compromise of the PC,

For Windows

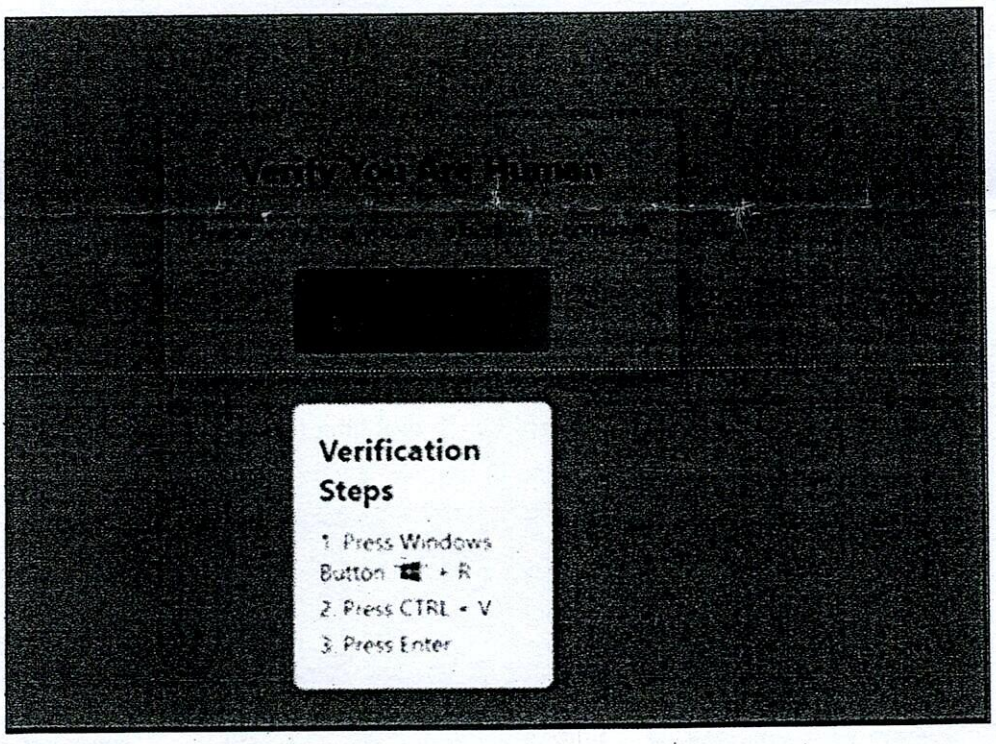


Fig 4: Help Guide for Windows

For Linux

Fig 5: Help guide for Linux

4. **Recommendations.**

The following is recommended to prevent users from falling into modus operandi being used by threat actor to lure victims: -

(a) High Profile/Critical email account holders may explicitly block all emails embedded with links.

(b) Verify website URLs before providing any Personal Identifiable Information (PII).

(c) Scrutinise CAPTCHA verifications on websites.

****

Advisory-II

ADVISORY ON THE USE OF DEEPSEEK FOR DEFENCE PERSONNEL

1. **Aim** The advisory is to sensitise all defence personnel regarding the implications of DeepSeek AI, a large language model (LLM), in terms of cybersecurity and national security.

2. **Background.** DeepSeek is a Large language model trained on massive datasets to understand and generate reply akin to human response, developed by Chinese AI company specialising in natural language processing and artificial intelligence. It aims to provide capabilities similar to models like OpenAI's 'ChatGPT', Google" Gemini

3. DeepSeek is an open-source software created as a part of China's broader efforts to develop independent Al models. It is designed for various natural language processing tasks like text generation, summarisation, and coding assistance. DeepSeek models have been trained on a vast data set including multi-lingual data with focus on Chinese and English.

4. **Information Security Concerns.**

   (a) **Login Concerns**. DeepSeek allows users to login using a new account linked to an email address, Google (Gmail) credentials or a +86-phone number. The Gmail login option, while most convenient, comes with additional risks; as follows: -

      (i) **Potential Exposure of Goole Account Data.** Exposure of user profile details linked contacts or login metadata.

      (ii) **Security Risks.** In case of a data breach, attackers could use stolen access tokens to compromise Gmail-linked accounts.

   (b) **Data Collection and Privacy Issues**. DeepSeek's privacy policy indicates that all user inputs including text, audio, uploaded files, and chat history are collected and stored on servers located in the People's Republic of China. This centralised data storage raises multiple concerns: -

      (i) **Broad Data Collection.** The platform collects extensive user data that can include personal identifiers, keystroke patterns, device information, and potentially sensitive operational data.

      (ii) **Lack of Data Minimisation** Similar to other Al applications, DeepSeek processes user inputs for model improvement

   (c) **Potential Vulnerabilities**. There are credible concerns that DeepSeek may incorporate mechanisms, intentional or otherwise that allow for covert data access. Key factors include: -

      (i) **Mandated Data Sharing under Chinese Law**. Chinese national laws (e.g., the National Intelligence Law of 2017) can compel companies to share user data with state security agencies upon request. This legal framework increases the risk that DeepSeek might be exploited as an entry point for unauthorised data access.

      (ii) **Biased and Self-Censorship Practices**. DeepSeek, like other Chinese AI models, implements self-censorship on topics considered sensitive within China. This raises concerns regarding the objectivity and reliability of the information provided by the platform. The platform's integrated censorship mechanisms can interfere with data integrity and transparency, and they raise additional concerns regarding spreading of Chinese propaganda.

      (iii) **International (Reports of Vulnerabilities.** Recent actions in the US and Europe, including bans on DeepSeek on government-issued devices highlight apprehensions

that the platform's design may allow for unauthorised access to user data by adversarial state actors.

(d) **Comparison of DeepSeek and OpenAI wrt to Security Features.** DeepSeek's open weight models including - DeepSeek R1, DeepSeek-Coder and DeepSeek Chat are some of the most powerful AI models to date. These are open-source models which allows users to download, modify and deploy on their own systems. Unlike the traditional models like OpenAI's GPT-4o, Google's Gemini 1.5 are task specific. A comparative assessment of DeepSeek vs OpcnAI with respect to compliance with security parameters is as mentioned below: -

Ser	Feature	DeepSeek	ChatGPT
(a)	Data Storage Location	China	Unspecified, but adheres to global data protection
(b)	Government Access Risks	Subject to China's strict data laws	No explicit government accesses requirements.
(c)	Data Scope Collection	Extensive user input, device data, behavioural tracking	User input technical information but with more transparency
(d)	User Control over Data	Limited; no clear opt-out mechanism.	Offers deletion, opt outs for mode! training.
(e)	Compliance with Privacy laws	Unclear; no explicit GDPR/CCPA mention	Explicit compliance with GDPR and CCPA

5. **Recommendations.** DeepSeek AI's data collection practices which include transmitting user data to China, raise serious privacy concerns. The use of this application by Defence personnel could lead to the compromise of personally identifiable information (PII) and other sensitive data. There, based on the above findings the following is recommended: -

   (a) **Prohibition on Use:** Use of DeepSeek platform on any official, operational or sensitive devices by IN personnel is strictly prohibited.

   (b) **Do Not Input Sensitive Data:** Under no circumstances should any classified, strategic, or sensitive operational data be ingested on DeepSeek platform.

   (c) **Awareness pnd Training:** All personnel should be briefed on the potentiat security risks associated with using platforms subject to foreign legal regimes that mandate extensive data sharing.

   (d) **Use of Alternetive AI Platforms.** Consider using AI platforms which comply with data protection regulations.

6. **Conclusion.** The combination of extensive data collection practices, potential backdoor vulnerabilities, and the legal obligations imposed on Chinese Companies to share data with the state make DeepSeek a significant security risk. As a matter of operational security, the use of DeepSeek is prohibited. Personnel must ensure that no sensitive or classified information is exposed Via this platform.

******

Advisory-III

ADVISORY 0N USAGE OF ARTIFICIAL INTELLIGENCE (AI) MODELS (ONLINE MODELS AND SMART DEVICES WITH INBUILT DEEPSEEK FEATURE)

1. **Background.** Artificial Intelligence (AI) denotes the simulation of human cognitive functions in machines enabling them to think, learnt and make decisions. This domain encompasses a diverse range of technologies, including machine learning, natural language processing, computer vision, and robotics. However, AI technologies necessitates careful consideration of data privacy and ethical implications.

2. **Aim**. The advisory is to sensitise all IN personnel regarding implications of Artificial Intelligence (AI) models and smartphones/ smart devices with prebuilt AI models in terms of cybersecurity and national security.

3. Commonly used AI models include conversational models, contextual search, image generation, speech recognition, video generation, gaming, simulation, semi-autonomous, content generation, data analysis and forecasting models. However, they are subject to inherent risks of exposing personal data, propagation of biased perspectives, lack of transparency; surveillance, technical risks associated with system integrity and data storage within extraterritorial jurisdiction. Some common AI models are mentioned below:

Ser	Model	Application Area
a)	OpenAI GPT-4	Chatbot used for content generation, contextual search and creative writing
b)	OpenAI DALLE	image generation, creative design
c)	Google BERT	Contextual search, Natural Language Processing (NLP)
d)	DeepSeek R1	Chatbot, content generation and reasoning

4. **Online/ Cloud Hosted AI Models.** A query is initiated by the user which functions as a prompt by the model. This query is sent to the AI server where it is processed, biased as per its own filters and response is sent to the user. The underlying data processing conducted without explicit knowledge of the user, involves the following: -

   (a) The AI model may keep a repository of previous queries, anticipated response formats, user preferences and other customisations. This information is utilised to refine and modulate future responses. While this feature was designed to enhance user experience, this data, if subjected to unauthorised access by malicious actors or mandated disclosure to government authorities, presents a potential vulnerability for individual profiling, intelligence gathering and predictive analysis of future actions.

   (b) The AI servers of the popular models are situated outside India thereby having limited or no data sovereignty.

   (c) Responses generated by AI models are subject to modulation and potential bias, reflecting the national policies and strategic objectives of the jurisdictions in which they originate.

   (d)With the growing integration of AI powered features in the smartphones, smart devices and home appliances and devices equipped with inbuilt AI models present potential security, privacy, and operational risks, particularly for individuals handling sensitive and classified information.

5. **Risks.** Common AI platforms have inherent risks of data collection, user input storage, keystroke pattern recording, undefined data retention periods, data sharing with third-party entities, potential access by respective governmental authorities, international and jurisdictional issues, lack of granular consent mechanism, potential data breaches, unilateral policy modifications, automated data collection like IP address, device ID, keystroke patterns, etc. Devices with integrated AI models may possess the capability to remotely access devices for updates or diagnostics, which could create security vulnerabilities if exploited by malicious actor. This access might enable unauthorised users to control devices or monitor use activities without consent.

6. **Risk Scenarios w.r.t Military Personnel.** In recent years, a proliferation of AI platforms has emerged within the public domain. AI platforms such as DeepSeek which have a direct affiliation with China, engage in collection of substantial personal and network information pertaining to users. Sample scenarios and risks associated with their usage are highlighted below. These factors necessitate careful consideration when evaluating the utilisation of such applications and models for personal or organisational purposes.

Ser	Scenario	Impact
a)	**Location and Deployment Tracking.** AI models such as DeepSeek logs IP addresses, device identifiers and behavioural patterns. Adversaries monitoring such data could potentially identify login recurring activity originating from specific geographic coordinates.	(i) If adversarial intelligence services could successfully correlate these access points as military locations, they may deduce patterns of troop deployments. (ii) Strategic locations could be mapped and targeted for cyber-attacks, surveillance, or even kinetic attacks (iii) The microphone, and AI-driven sensors activated remotely to classified discussions. camera, may be capture
b)	**Data Breach Leading to Social Engineering Attacks.** Anti-national elements may compromise servers of such AI models and exfiltrate chat histories, device-specific data, and record user interactions. Thereby analyse stored of military conversations personnel discussing operational matters.	(i)Adversaries use extracted data to craft highly convincing phishing emails spear phishing attacks on military personnel. (ii)They impersonate trusted contacts using leaked chat histories to gain access to classified networks or extract further intelligence. (iii) Psychological profiling of individuals could be used for blackmail, coercion, or insider by recruitment adversarial intelligence agencies.
c)	**Compromised AI Outputs Leading to Disinformation.** Anti-national elements may infiltrate such AI models and manipulate its responses. Military personnel relying on these models for open source intelligence, translations, or quick research may receive altered misleading information	(i)Manipulated outputs from AI models may be leveraged to execute disinformation campaigns, resulting in operations disruptions. (ii)Adversaries may disseminate fabricated narratives designed to influence strategic decision-making.

7. **Recommendations.** Threats, risks and vulnerabilities in use of AI models, raise serious security and privacy concerns. Therefore, following is recommended: -

   a) Ensure AI model comply with Data Privacy laws - DPDP Act, GDPR etc.
   b) Use only for non-sensitive tasks.

c) Apply data masking and sanitisation before submitting to AI model
d) Monitor for Data Exfiltration Risks.
e) Beware of Al-Generated Phishing & Deepfakes.
f) Verify Al Output for Bias & Misinformation.
g) Restrict API Access to Al models.
h) Modify Firewall blocklist to block / grant selective access using IAM.
i) Prepare a local policy for use of Al models based on ICSP Guidelines.
j) Educate users on Al risks, cybersecurity, and misinformation.
k) Anonymise prompts/data inputs.
l) Use disposable accounts to hide identity.
m) Clear Al chat histories and cache.
n) Disable browser autofill for Al sites.
o) Understand that AI responses can be biased based on their country of origin or intent.
p) Enforce Zero Trust Architecture before deploying AI models.
q) Disable all optional features.
r) Minimise data sharing.
s) Disable GPS when not in use, turn off location services for excessive apps, and use VPN to mask IP location.
t) Use end-to-end encrypted messaging apps.
u) Regularly review and adjust app permissions to ensure that applications only have access to necessary data only.
v) Users should consider turning off features like facial recognition and predictive text to minimise data collection and potential exploitation.
w) Activate full-device encryption to protect stored data from unauthorised access in case of loss or theft.

9. **Conclusion**. End users should be sensitised that Al Models have very limited security features to protect data privacy and AI models in smart devices possess inherent potential security and privacy risks. Hence, Al models are **NOT to be used for official work** and great caution be exercised when used for personal requirements. Cybersecurity is not an individual task; it's a shared responsibility', every member of the Defence community must be cautious of the potential vulnerabilities associated with such AI models.

Advisory-IV

ADVISORY ON THE USE OF 'AI GENERATED IMAGERY' FOR INDIAN DEFENCE COMMUNITY

1. **Background.** Artificial Intelligence (AI) generated image enhancement and generation have gained immense popularity recently. Many online platforms now offer the ability to transform photos into artistic avatars, anime-style portraits, or even hyper-realistic edits. Whilst these tools provide visually appealing results, they also come with significant security and privacy risks. Therefore, the defence community must be made aware of the potential consequences before sharing images or personal data with these platforms.

2. **Aim.** The aim of this advisory is to sensitise all IN personnel and families regarding online tools facilitating 'AI based image enhancements' and to provide guidance on its security and privacy risks. This advisory is to be read in conjunction with Cyber Advisory **on usage of Artificial Intelligence (AI) models (online models and smart devices with inbuilt DeepSeek feature)** dated 17 Mar 2025.

3. **AI Based Image Enhancers.** AI based image enhancers use machine learning models to process, modify and generate images based on user inputs. These tools often require users to upload their photos, which are then analysed using neural networks to apply filters, artistic effects or enhancements. The technology behind these enhancers involves deep learning techniques such as Generative Adversarial Networks (GANs) [1]or transformer-based models, enabling high quality transformations and artistic creations.

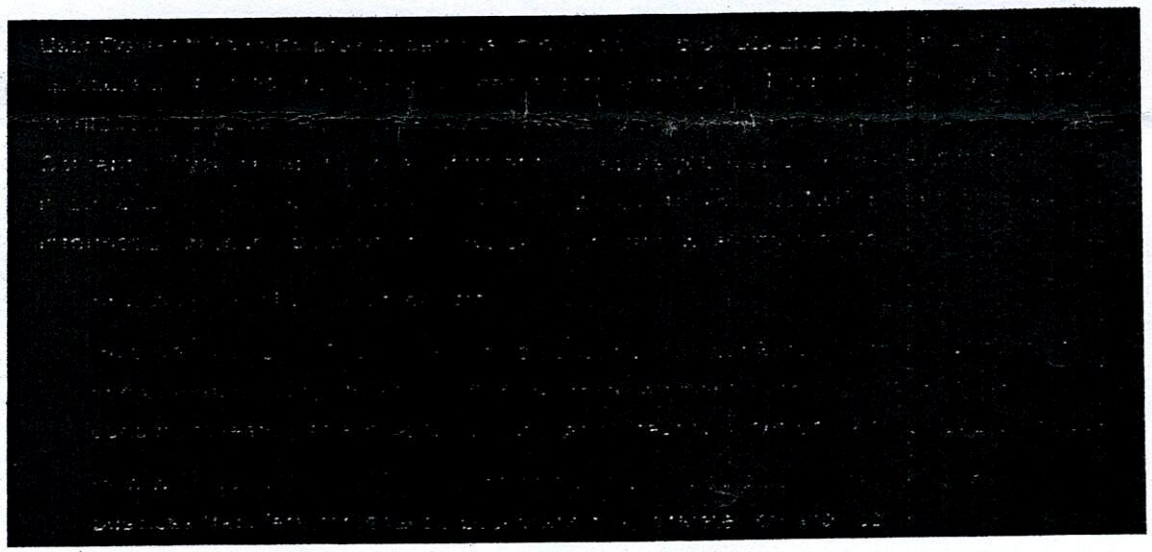
4. **Sharing of Data.** When users upload their images to these platforms, they may unknowingly grant broad based rights to the service provider. Many AI- powered image generators include terms and conditions that allow the platforms to **store, modify, and redistribute** the images without explicit consent. Further, **metadata embedded in the uploaded images, such as geolocation data, timestamps and device information may also be extracted and stored.** Such data if misused could pose security threats, **especially in Defence environment** where identities and locations must be safeguarded.

5. **Privacy and Security Concerns**. The collection and retention of images by AI platforms present serious privacy and security' risks. AI tools store uploaded images on their servers, which has the ever-present risk of data breach, leading to unauthorised access or misuse of personal images. Facial recognition data extracted from these images could be used for unauthorised purposes, including deepfake creation, identity theft, and targeted phishing attacks. Moreover, some AI platforms may sell or share this data with third parties, thereby increasing exposure to privacy breaches. It is pertinent to highlight that even if the user deletes their images from the platform, many services retain the right to use them indefinitely, making it nearly impossible to retract the shared data. Further, under mentioned are the key points covered in the privacy policy of an AI platform which the Defence community should peruse and make a cautious decision prior utilising the said services:

---

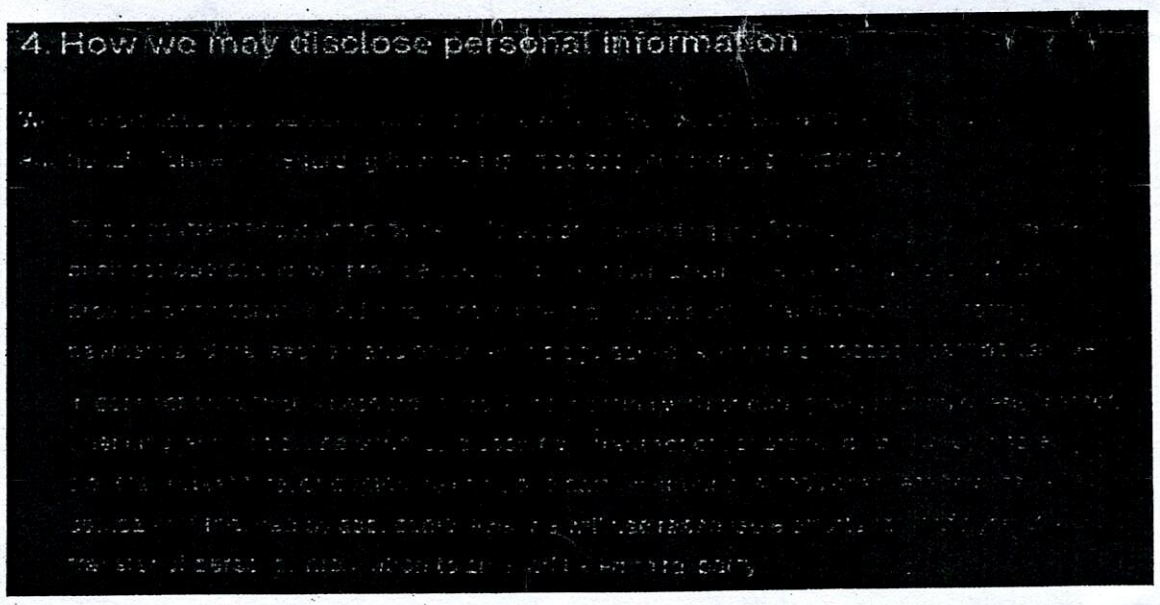
[1] **Generative Adversarial Network** — A Generative Adversarial Network is a type of machine learning model that uses two neural networks, a generator and a discriminator, in a competitive adversarial training process to generate new data samples that resemble the training data.

(a) Personal information collected by the platform viz, account data, communication data, user content, location data, social media data, etc.



Excerpt from Privacy Policy — Grok 3

(b) How personal information is disclosed by the service provider.



Excerpt from Privacy Policy - GETIMG.AI

6. **Recommendations.** AI based image generators/ enhancers pose serious privacy and security risks, therefore following is recommended: -

(a) Avoid sharing personal or work-related images containing sensitive information with AI-based image generators.

(b) Before using any AI tool, review the privacy policy to understand how user data would be handled, stored and shared.

(c) If considered essential, use tools to strip metadata from the photos being uploaded to prevent unintentional sharing of location or device information and use anonymised or generic images instead of personal and sensitive content.

(d) Do not assume that deleting an uploaded images or clearing a chat would remove all associated data from the servers. Prefer, offline or self-hosted tools instead of online cloud-based services.

(e) Prefer, offline or self-hosted tools instead of online cloud-based services.

(f) Users be sensitised to peruse the privacy policy of respective AI applications prior exploiting the application.

7. **Conclusion.** AI-based image enhancers offer creative and engaging features; however, it has a significant privacy risk. AI trends are fun, but they are also a source of data collection tools. Accordingly, Defence community must exercise caution and consider the potential consequences before sharing images or personal data with such platforms.

***

SAO(IT&SW) for u-a please 18/7

कार्यालय रक्षा लेखा महानियन्त्रक
Office of the Controller General of Defence Accounts
(सू.प्रो.एवं प्र. विंग)/ **IT&S Wing**
Ulan Batar Road, Palam, Delhi Cantt – 110010
उलान बाटर रोड, पालम, दिल्ली कैंट – 110010
Ph- 011-25665588, 25665591
e-mail: cybercell.cgda@gov.in

विकसित भारत अभियान 1947 2047

SECRET

No. Mech/ IT&S/810/Cyber Security/Advisory-A Dated: 10.07.2025

To,

The Dy. CISOs,
All PCsDA/CsDA

Subject: Advisory regarding spurious/ suspicious calls and phishing attacks.

Input from reliable government agency indicate that they have received an alert in which it has come to notice that repeated instances in the recent past of spoofed/ spurious calls being received by various departments/ functionaries of the government seeking confidential information with some cases/ incidents of impersonation of high level officers in various offices of MoD through telephone calls attempting to extract Defence related information have also come to light. Hence, security recommendations for proper utilization of mobile phones are enclosed as Annexure- I.

2. Further, it has also come into notice that incidents related to phishing domains to trick users into divulging sensitive information is surging. In this regard, advisory to be followed for phishing attacks issued by NIC-CERT is enclosed as Annexure-II.

3. For your kind consideration and necessary action please.

This is issued with the approval of Jt. CGDA (IT&S).

Encl.: As above.

Sr. ACGDA (IT&S)
10/7/25

AAO/Aud
Pl. circulate to Sections/ Sub-offices alongwith Annexure II for compliance.
18/7/25 SAO(IT)

Annexure-I

Security Recommendations

1. Don't download apps from third-party sites. Only use **official apps from Google Play or the App Store.**

2. Use a **different password for every account** you own and don't save them in your browser. Use a password manager to help you record and manage unique passwords for every app and test your password strength before using it.

3. Try to **avoid opening links**, even if the sender is familiar. Smartphones are just as susceptible to viruses as computers. Phishing is the most common delivery method for ransomware infections, delivering malware to your phone and your network.

4. Install **antivirus software on mobile devices**. As a best practice for any mobile device – phones, tablets or other – consider adding antivirus software for the additional security it provides against malware or other viruses.

5. Invest in mobile threat defence. This software scans your phone and will alert you to suspicious activity, like rogue applications and fake Wi-Fi networks. It also includes fully managed restoration if data exposure were to lead to an identity theft incident.

6. **Do not "Root" your Android or "Jailbreak" your iPhone**. This is a process that gives you complete access of your device, but in doing so, removes many of the safeguards that manufacturers have put in place.

7. Always **update your phone's Operating System (OS)** when prompted. These updates are meant to protect your device and information.

8. Use caution when connecting to **public Wi-Fi networks**. Cyber criminals can access and monitor your activity if you connect to one of their seemingly trustworthy, "spoof" networks.

9. **Enable two-factor authentication(2FA)** for your key accounts like mobile banking apps and peer-to-peer payment apps. This added layer of security may help prevent a thief from being able to wipe out your financial accounts.

10. **Revoke app permissions** to use camera, microphone etc.

11. Be cautions of whom you are communicating **in social media platforms**.

12. Be cautious to avail **Cloud Storage** for all of your data.

13. Always check you are protected when using **Bluetooth.**

****

Annexure – II

ADVISORY: PHISHING ATTACK

Phishing domains are malicious websites designed to trick users into divulging sensitive information, such as login credentials, financial information, or personal data.

Identifying Phishing Domains

To avoid falling victim to phishing domains:

1. **Be cautious of unsolicited emails or messages:** Legitimate organizations rarely ask for sensitive information via email or message.
2. **Verify the domain name:** Check the URL carefully, looking for misspellings, extra characters, or variations in the domain name.
3. **Watch for poor grammar and spelling**: Legitimate websites usually have professional content.
4. **Be wary of urgent or threatening messages**: Phishing domains often try to create a sense of urgency to prompt users into taking action.
5. **Check for HTTPS and a valid SSL certificate:** Legitimate websites usually have a valid SSL Certificate and use HTTPS.

To protect from phishing domains:

1. **Use strong, unique passwords**: Avoid using the same password across multiple sites.
2. **Enable two-factor authentication (2FA):** 2FA adds an extra layer of security to prevent unauthorized access.
3. **Keep your software and operating system up to date:** Ensure you have the latest security patches and updates.
4. **Use anti-virus software and a firewall:** Protect your device from malware and unauthorized access.
5. **Use a reputable password manager:** Consider using a password manager to securely store and generate strong passwords.

Reporting Phishing Domains

If suspected phishing domain:

1. **Do not interact with the website:** Avoid clicking on any suspicious links or providing any sensitive information.
2. **Report the website to the relevant authorities:** Inform your organization's IT department or report the phishing email to Cyber and Information Security Management Division (NIC).
3. **Delete any suspicious emails or messages:** Remove any emails or messages related to the phishing domain.