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.

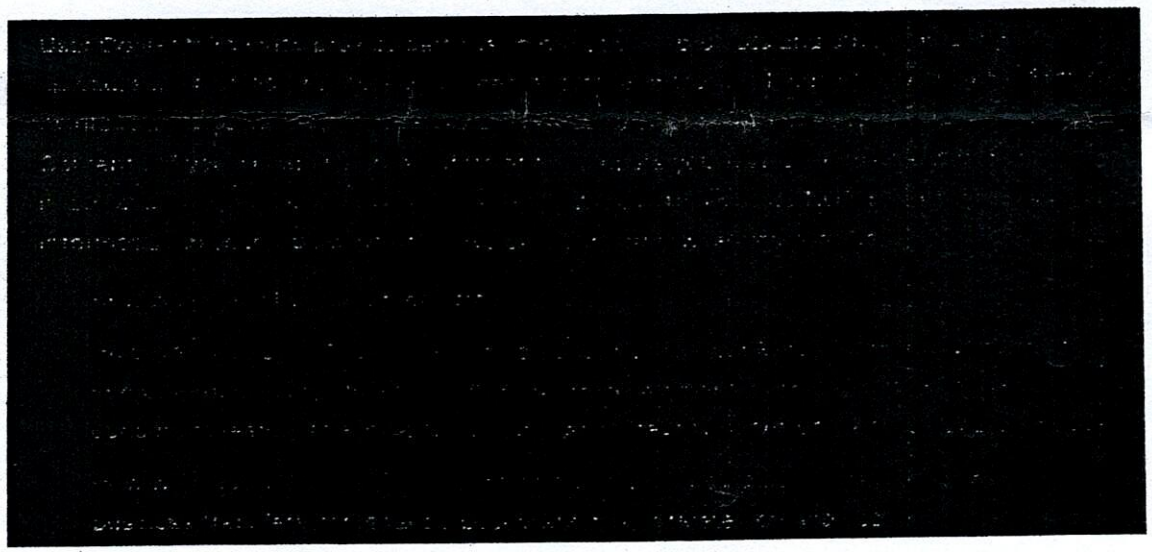
4. **Sharing of Data.** When users upload their images to these platforms, they may unknowingly grant broad based rights to the service provider. Many AI- powered image generators include terms and conditions that allow the platforms to **store, modify, and redistribute** the images without explicit 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:

---

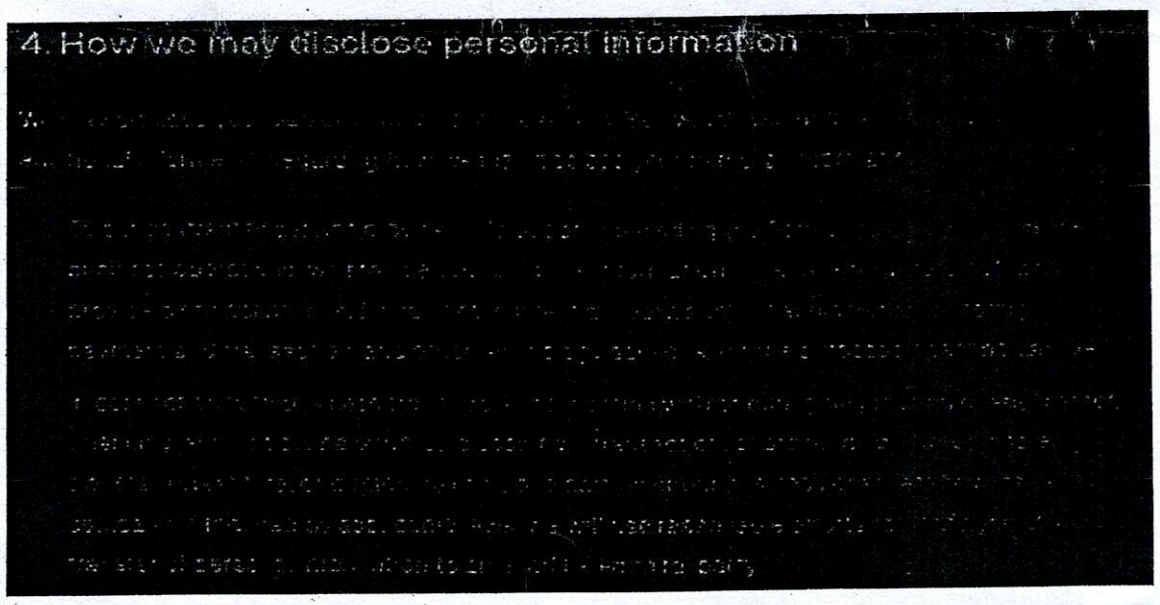
[1] **Generative Adversarial Network** — A Generative Adversarial Network is a type of machine learning model that uses two neural networks, a generator and a discriminator, in a competitive adversarial training process to generate new data samples that resemble the training data.

(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.