NO.DG-II/ Cyber.Advisory/4/111/2023
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY
DEPARTMENT
Karachi, Dated: 30th January, 2025

To,

1. The Chairman, Enquires, Anti-Corruption, Establishment of Sindh, Karachi.
2. The Chairman Sindh HEC Karachi.
3. The Senior Member Board of Revenue (BOR)Sindh, Karachi.
4. The Additional Chief Secretary, Govt of Sindh
5. The Principal Secretary to Governor Sindh, Governor Secretariat, Karachi.
6. The Principal Secretary to Chief Minister Sindh, Chief Minister Secretariat, Karachi.
7. The Administrative Secretary, Government of Sindh (All).
8. The Provincial Ombudsman, Sindh.
9. The Inspector General of Police Sindh, Karachi
10. The Divisional Commissioner (All) in Sindh.
11. The Deputy Commissioner, District

Subject: - **CYBER SECURITY ADVISORY- BULK PHISHING EMAILS ORIGINATING FROM IMPEROSANTED / FAKE ISPR EMAIL (Advisory No. 01001).**

Introduction. Reportedly, a new impersonated Email ID portraying as legitimate ISPR Email ID used by hacker groups has been identified. The ID is used for sending bulk phishing/hacking (containing malicious attachments). **Screenshots are enclosed Appex-1.**

2. In this regard, Cyber Security Advisory named Bulk Phishing Emails Originating from Impersonated/Fake ISPR Email is being issued to all concerned Details of fake Email is as follows:

Email ID	Purpose	C&C/IP
official@dgispr.info	Hacking bait via Phishing Email	162.255.119.113 (Atlanta, Georgia, USA)

3. **Mitigation.** Above in view, please avoid opening Emails from abovementioned ID Also, IT administrators are requested to blacklist said Email ID (where applicable).

4. Kindly disseminate the above information to all concerned in your organization, attached/affiliated departments and ensure necessary protective measures.

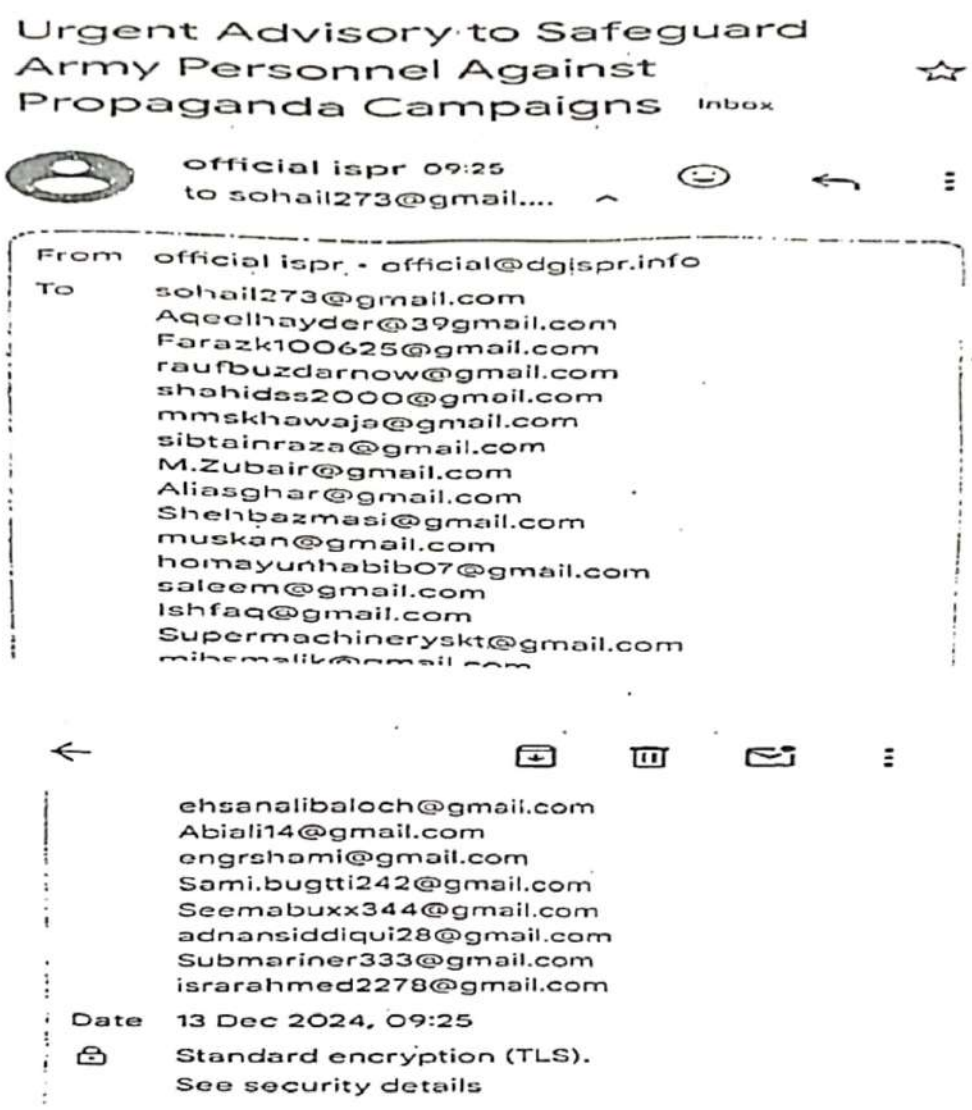
(DR.RANA SHAHZAD QAISER)
DIRECTOR GENERAL-II
0310-2131415

A copy is forwarded for information and necessary action to: -

1. AS(Staff) to Chief Minister Sindh, Karachi.
2. The Assistant Secretary (NTISB), Cabinet Secretariat, Cabinet Division (NTISB), GoP.
3. PS to Chief Secretary, Sindh.
4. PS to Secretary I&C, SGA&CD, Govt. of Sindh, Karachi.
5. Staff Officer to S&IT Department, Govt. of Sindh, Karachi.
6. Webmaster, for uploading the advisory on url: *https://www.sindh.gov.pk/*

APPex-I

IMPERSONATED/ FAKE ISPR PHISHING EMAIL – SCREENSHOT



Urgent Advisory to Safeguard Army Personnel Against Propaganda Campaigns Inbox

official ispr 09:25
to sohail273@gmail....

From official ispr - official@dgispr.info
To sohail273@gmail.com
Aqeelhayder@39gmail.com
Farazk100625@gmail.com
raufbuzdarnow@gmail.com
shahidss2000@gmail.com
mmskhawaja@gmail.com
sibtainraza@gmail.com
M.Zubair@gmail.com
Aliasghar@gmail.com
Shehbazmasi@gmail.com
muskan@gmail.com
homayunhabib07@gmail.com
saleem@gmail.com
Ishfaq@gmail.com
Supermachineryskt@gmail.com

ehsanalibaloch@gmail.com
Abiali14@gmail.com
engrshami@gmail.com
Sami.bugtti242@gmail.com
Seemabuxx344@gmail.com
adnansiddiqui28@gmail.com
Submariner333@gmail.com
israrahmed2278@gmail.com
Date 13 Dec 2024, 09:25
Standard encryption (TLS).
See security details

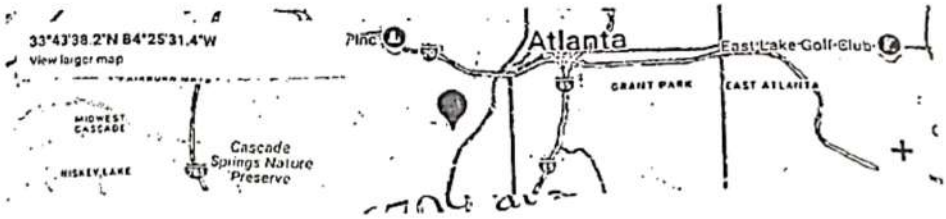
1. The Directorate of Inter-Services Public Relations (ISPR) has issued an Urgent advisory to all Pakistan Army officers in light of an intensifying campaign aimed at maligning the Army's reputation. The advisory outlines precautionary measures to protect officers, their families, and the institution from falling victim to **disinformation and malicious**

1. The Directorate of Inter-Services Public Relations (ISPR) has issued an Urgent advisory to all Pakistan Army officers in light of an intensifying campaign aimed at maligning the Army's reputation. The advisory outlines precautionary measures to protect officers, their families, and the institution from falling victim to **disinformation and malicious activities.**

2. This campaign, which has notably escalated since 26 November 2024, relies heavily on the misuse of social media and other platforms. To counter these threats effectively, the ISPR calls for heightened vigilance and disciplined conduct across all levels. Key measures are included in the file as attachment. It is mandatory that the Advisory is strictly followed in spirit. **Password of the attachment - ispr321 ,** recommended to be **open in any Browser with WinRAR installed.**

EMAIL ORIGN IP/ HOSTING DETAIL

IP:	162.255.119.113	Usage type:	DCH
Country:	US	Region:	Georgia
Latitude:	33.72729	City:	Atlanta
Longitude:	-84.42538	ISP:	Namecheap Inc.
Mobile:	-	Domain:	namecheap.com



NO.DG-II/ Cyber.Advisory/4/111/2023
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY
DEPARTMENT
Karachi, Dated: 30th January, 2025

To,

1. The Chairman, Enquires, Anti-Corruption, Establishment of Sindh, Karachi.
2. The Chairman Sindh HEC Karachi.
3. The Senior Member Board of Revenue (BOR)Sindh, Karachi.
4. The Additional Chief Secretary, Govt of Sindh_____
5. The Principal Secretary to Governor Sindh, Governor Secretariat, Karachi.
6. The Principal Secretary to Chief Minister Sindh, Chief Minister Secretariat, Karachi.
7. The Administrative Secretary, Government of Sindh (All). _____
8. The Provincial Ombudsman, Sindh.
9. The Inspector General of Police Sindh, Karachi
10. The Divisional Commissioner (All) in Sindh_____.
11. The Deputy Commissioner, District _____

Subject: - **CYBER SECURITY ADVISORY- USE OF INDIAN ORIGIN PRODUCTS & SERVICES (ADVISORY NO.02001).**

Context: India has emerged as a significant hub for Apple device manufacturing, producing iPhone and other components for global markets. This shift aligns with Apple's strategy to diversify its supply chain beyond China and leverage India's growing capabilities. However, for Pakistan, this development could pose cybersecurity risks due to geopolitical tensions between the two nations.

2. GoP's Stance. GoP is already cognizant of the risks associated with Indian ICT products and services over a period of time. 3 x exclusive advisories were issued in 15th November, 2019 (Advisory No. 23), 14 December, 2022 (Advisory No. 52) and 23 June, 2023 (Advisory No. 33), reflecting the associated risks, like:

a Possibility of presence of backdoor or malware for collection of logs/data, traffic analysis and Pil.
b. Direct Indian ingress in Pakistan's CII through technical means/access control with passive monitoring capability.
c. Imposition/ban of Software/Firmware update to gain political/strategic motives.

3. Potential Risks - Apple iPhones. Few critical risks associated with Indian manufactured iPhones are as follows:

a. **Supply Chain Vulnerabilities** Manufacturing components in India could introduce security concerns for devices exported to Pakistan through legal and illegal channels such as:

(1) Potential tampering with hardware or software during assembly.
(2) Risks of embedded malware in devices.

b. **Geopolitical Exploitation.** Could lead to targeted cyber activities using compromised devices or data interception.

c. **Phishing Scams**
(1) Attackers could pose as Apple support agents or service centers based in India to target Pakistani Users.
(2) Phishing emails or SMS could direct users to malicious websites mimicking official Apple portals to steal credentials, payment information or sensitive data.

d. Espionage Risks:
(1) Devices or components could potentially be compromised during manufacturing, enabling surveillance or data collection targeting Pakistani users.
(2) Risk of pre-installed spyware that remains undetected by typical security measures.

4. Recommendations for Pakistani Users:

a. Verify Device Authenticity:
(1) Purchase Apple products only from authorized resellers in Pakistan.

(2) Check device seals and packaging for tampering.

b **Update Regularly.** Keep your Apple devices updated with the latest iOS updates and security patches to protect against vulnerabilities.

c **Avoid Rooting or Jailbreaking.** Modifying devices can expose them to security risks and compromise built-in protections.

d. **Monitor for Suspicious Activity.** Watch for unusual behavior in devices, such as overheating, unexplained network traffic or apps behaving unusually.

e. **Use End-to-End Encryption.** Ensure your communications (iMessages, FaceTime) are secure by using encrypted services and strong passwords.

f. **Install Anti-Spyware Tools.** Use reputable anti-spyware applications to detect and block malicious software.

g. **Stay Informed.** Follow updates from Apple's official channels and local cybersecurity advisories for any emerging risks or patches.

4. Kindly disseminate the above information to all concerned in your organization, attached/affiliated departments and ensure necessary protective measures.

(DR.RANA SHAHZAD QAISER)
DIRECTOR GENERAL-II
0310-2131415

A copy is forwarded for information and necessary action to: -

1. AS(Staff) to Chief Minister Sindh, Karachi.
2. The Assistant Secretary (NTISB), Cabinet Secretariat, Cabinet Division (NTISB), GoP.
3. PS to Chief Secretary, Sindh.
4. PS to Secretary I&C, SGA&CD, Govt. of Sindh, Karachi.
5. Staff Officer to S&IT Department, Govt. of Sindh, Karachi.
6. Webmaster, for uploading the advisory on url: *https://www.sindh.gov.pk/*

NO.DG-II/ Cyber.Advisory/4/111/2023
GOVERNMENT OF SINDH
SCIENCE & INFORMATION TECHNOLOGY
DEPARTMENT
Karachi, Dated: 30th January, 2025

To,

1. The Chairman, Enquires, Anti-Corruption, Establishment of Sindh, Karachi.
2. The Chairman Sindh HEC Karachi.
3. The Senior Member Board of Revenue (BOR)Sindh, Karachi.
4. The Additional Chief Secretary, Govt of Sindh_____
5. The Principal Secretary to Governor Sindh, Governor Secretariat, Karachi.
6. The Principal Secretary to Chief Minister Sindh, Chief Minister Secretariat, Karachi.
7. The Administrative Secretary, Government of Sindh (All). _____
8. The Provincial Ombudsman, Sindh.
9. The Inspector General of Police Sindh, Karachi
10. The Divisional Commissioner (All) in Sindh_____.
11. The Deputy Commissioner, District _____

Subject: - **Cyber Security Advisory - Multiple Commonly Used Web Browser Extensions Hacked (Advisory No. 03001).**

Context: Reportedly, a new attack campaign has been unearthed targeting commonly used browser extensions to steal personal information and credentials of applications used via browser e.g facebook, banking websites etc.

Technical Details: Malicious code is sent through phishing techniques in order to compromise targeted publishers of legitimate extensions, further stealing user's PII using said extensions. At least 16 common extensions (including VPN and AI ChatBots) are suspected to be compromised:

a. AI Assistant-ChatGPT and Gemini for Chrome
b. Bard AI Chat Extension
c. GPT 4 Summary with OpenAI
d. Search CoPilot AL Assistant for Chrome
e. Wayin AI
f. VPNCity
g. Internxt VPN
h. Vidniz Flex Video Recorder
i. VidHelper Video Downloader
j. Bookmark Favicon Changer
k. U Voice
l. Reader Mode
m. Parrot Talks
n. Primus
o. Trackker - Online Keylogger Tool
p. AI Shop Buddy
q. Rewards Search Automation etc.

Recommendation: Above in view, following safe usage guidelines are suggested for all browser extension users:

a. Avoid above mentioned extensions for time being and use alternate well reputed options.
b. Only install trusted extensions.
c. Read and review permissions and ratings.
d. Limit permissions where possible.
e. Regularly update extensions.
f. Remove unused extensions.
g. Use well reputed and licensed Antivirus software
h. Be wary of free extensions.
i. Actively monitor system utilities and data usage for abnormal activity.

Kindly disseminate the above information to all concerned in your organization, attached/affiliated departments and ensure necessary protective measures.

(DR.RANA SHAHZAD QAISER)
DIRECTOR GENERAL-II
0310-2131415

A copy is forwarded for information and necessary action to:

1. AS(Staff) to Chief Minister Sindh, Karachi.
2. The Assistant Secretary (NTISB), Cabinet Secretariat, Cabinet Division (NTISB), GoP.
3. PS to Chief Secretary, Sindh.
4. PS to Secretary I&C, SGA&CD, Govt. of Sindh, Karachi.
5. Staff Officer to S&IT Department, Govt. of Sindh, Karachi.
6. Webmaster, for uploading the advisory on url: *https://www.sindh.gov.pk/*