



PAKISTAN REVENUE AUTOMATION (PVT.) LTD.

*Sunday, May 01, 2022*

## **ADVISORY NOTICE**

### **Prevention against Fake FBR Emails**

National Telecom and Information Technology Security Board (NTISB) has warned the Federal Board of Revenue (FBR) that government job advertisement-related emails are being sent to unrestricted users by hackers with the purpose to acquire confidential information and a potential cyber-attack on government institutions.

A phishing email with the subject "Govt Jobs/ Recruitment" which contains a malicious Word document as an attachment is being spread by Hackers. On downloading the attachment: a malware runs in the background. It is a spear-phishing attack conducted by Confucius APT Group to gather information at a large scale through a Biodata form.

On downloading the malicious email attachment, an individual's computer/device is compromised and the hacker gains access to all the stored data/files. End users are urged to withhold from downloading attachments or clicking links sent via such enticing emails in order to protect their personal information.

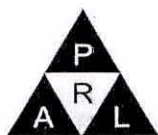
#### **Recommendations:**

1. FBR approved IT Security Policy must be strictly followed. A copy can be obtained from FBR IT Wing.
  2. Do not open attachments in suspicious or strange emails especially Word, Excel, PowerPoint, or PDF attachments.
  3. Verify the sender by checking their email address. Call the sender if you have high suspicion.
  4. Check the link, before you click, make sure the links start with HTTPS:// and not HTTP://.
-



**PAKISTAN REVENUE AUTOMATION (PVT.) LTD.**

5. Be careful when providing personal information, never provide your credentials to third parties.
6. Do not rush or panic reacts, scammers use this in order to pressure you into clicking links or opening attachments.
7. If you gave sensitive information, do not panic. Reset your credentials on sites you have used them. Change your passwords and contact your bank, etc. immediately.
8. Preferably delete the suspicious email without opening it and manually block the sender.
9. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of any intrusion. It is highly recommended that the computer system must be registered with LAN's Active Directory server. Please contact your local technical support for further details.
10. Use of official email is highly recommended.
11. Use of third-party Antivirus is strictly prohibited. Only approved licensed Antivirus software must be installed on computer systems.
12. Always avoid using a suspicious USB flash stick. In case you still want to use the USB flash stick, then always scan the USB using approved Antivirus software.
13. Regular update Operating System, Antivirus software, Internet browsers, and MS Office, and disable macros.
14. Keep Windows firewall enabled on your desktop computer systems.
15. All sensitive information be handled with care and dissemination to all concerned be done through secure means.
16. Change the passwords of your respective accounts regularly.
17. Always memorize the passwords, never write them.
18. Maintain regular offline backups or centralized offline backups of your critical data.
19. Be aware of pop-ups in internet browsers or desktop screens and never enter confidential information on a pop-up screen.
20. Contact your local PRAL technical support team for any assistance.



## PAKISTAN REVENUE AUTOMATION (PVT.) LTD.

21. In case of infection/compromise in your computer system, please disconnect the computer from the internet and immediately contact PRAL Technical Support Team.

For further information about online security threats and support, please contact PRAL Networks & Infrastructure Wing at:


Information & Support During Office Hours		Information & Extended Support 24x7	
Landline	(051) 9259358	Landline	(051) 9212374 (051) 8431155
IP Phones	1234 1400	IP Phones	1492 1155
Email: <a href="mailto:datacenter@pral.com.pk">datacenter@pral.com.pk</a>			

### Distribution to:

- FBR House, Islamabad
- All FBR IR Offices
- All FBR Custom Offices
- PRAL Head Office, Islamabad

20 26 APR 2027

- e. In mobile settings, do not enable installation of apps from "Untrusted Sources".
  - f. Install Android updates and patches as and when available from Android device vendors.
  - g. Do not download or open attachment in emails received from untrusted sources or unexpectedly received from trusted users and forward them to emails mentioned in para 4.
  - h. Avoid using insecure and unknown Wi-Fi network as hostile elements use Wi-Fi access points at public places for distributing malicious applications.
  - i. Use two-factor authentication on all Internet Banking Apps, WhatsApp, social Media and Gmail Accounts.
  - j. All officers/ staff must be guided to adhere recommended cyber security measures at personal smart appliances.
4. For any query or reporting malware, please forward the same on following email address: -
- a. eagle1978@mail.com
  - b. falcon098@writeme.com
  - c. asntisb2@cabinet.gov.pk
5. Disseminate the same message in your organizations, all attached/ affiliated departments and ensure necessary protective measures.

  
Major  
(Muhammad Usman Tariq)  
Assistant Secretary-II (NTISB)  
Ph# 051-9204560

**All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments.**

Copy to: -

1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwana-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

**LIST OF IDENTIFIED MALICIOUS APPLICATIONS**

Ser	Name of Appls
1.	Fruit Chat
2.	Just You
3.	CuCu / CUCKOO+
4.	Rapid Chat
5.	Islamic Chat
6.	Vmate
7.	Lite Chat
8.	Chat On
9.	Chat It
10.	Philions Chat
11.	Phub
12.	Zoiper
13.	Seta/ SA News
14.	Safe Chat
15.	Tweety
16.	Rocket Chat
17.	Pornhub
18.	FMWhatsAPP
19.	Chat PT
20.	LinkUP
21.	Lite Lt
22.	Graphic Version
23.	VIBES
24.	Cherio/ Cherrio
25.	Buzz Version 3
26.	Filos
27.	Quran.Apk
28.	Secure[t/ Spitfire
29.	Buzz
30.	Guftagu
31.	Xpress
32.	U & Me
33.	TeleChatty
34.	Babble/ Babble Ver 3
35.	Chirrup
36.	Converse
37.	Free VPN V3
38.	Face Call
39.	Chat It
40.	Twin Me
41.	Hex Chat
42.	FaceChat
43.	Omegle
44.	Zaning V4
45.	Pvt Chat
46.	Privantechat1
47.	Secure Chat
48.	Safe Dialer
49.	Crypto Chat

50.	SecureIt
51.	Wire
52.	Google Security Framework
53.	Cable-1
54.	Privee Chat
55.	FireChat
56.	Stumped
57.	Zong Chat (Beta)
58.	Buddy Chat
59.	Media Services
60.	CrazyChat
61.	ZangiV2
62.	Zapme
63.	CuCU Chat
64.	Chat 24/7
65.	ZongBoost
66.	Audio & Video Recorder
67.	Kakao Talk
68.	Love Bae
69.	Easy Chat
70.	ISPRNews
71.	<b>PaighamChat</b>
72.	<b>Skymate</b>
73.	<b>Boss</b>
74.	<b>ChitChat Box</b>
75.	<b>Triover</b>
76.	<b>Hideme</b>
77.	<b>LionVPN</b>
78.	<b>Zepp</b>