PAKISTAN REVENUE AUTOMATION (PVT.) LTD.

File No. CM-NWI/251120c

Wednesday, November 25, 2020

Important Advisory

Work from Home – Cyber Security

Switching to remote working because of the ongoing Coronavirus pandemic can create cybersecurity problems for an organization like FBR and its employees. Attackers are exploiting the situation, so look out for phishing emails, scams and other hacking attempts.

A new type of phishing attack is rising which is focusing on Coronavirus (COVID-19). Adversaries' sends phishing & spam emails to users to open the infected word document claiming an update report from World Health Organization (WHO) or Pakistani Health Authorities.

Therefore, all FBR resources who are authorized by the competent authority to Work from Home (WFH) are directed to adhere to the strategy points given below:

1. Avoid public Wi-Fi networks and use PRAL recommended VPN for secure communications.
2. Use of remote desktop software such as TeamViewer, Anydesk, etc. are strictly prohibited.
3. Make sure you are using a secure connection for your WFH environment.
4. Keep passwords strong and change it regularly. Always memorize the passwords, never write it.
5. Enable Two-Factor (2FA) or Multi-Factor Authentication, wherever possible.
6. Encrypt your home PC hard drives and USB sticks to safe data in case of theft.
7. Keep your home PC operating system patched. Install & update your home PC with top-rated Antivirus, Anti- Malware & Firewalls. You may also get latest freeware antivirus and other security software from PRAL technical support team.
8. Check all security software is up to date in your home PC. Privacy tools, add-ons for browsers and other patches need to be checked regularly.
9. All WFH resources are advised to communicate using official FBR email only.

10. All FBR remote workers are advised to be suspicious of any emails asking them to check or renew their passwords and login credentials, even if they seem to come from a trusted source.
11. Please try to verify the authenticity of the request through other means, do not click on suspicious links or open any suspicious attachments.
12. Always scan suspicious file using antivirus software recommended by PRAL Technical Support team.
13. All sensitive information be handled with care and dissemination to all concerned be done through secure means.
14. Be aware of pop-ups in internet browsers or desktop screen and never enter confidential information in a pop-up screen.
15. Establish & sign a departmental-wise cybersecurity policy/undertaking from your team members working remotely from home.
16. Have a back-up strategy. All-important data should be backed up regularly.
17. All officers are requested to provide their team with basic security knowledge. Please contact PRAL for assistance in this regard.
18. All functional heads are advised to develop contingency plan in coordination with PRAL.
19. Contact PRAL Technical Support team for any assistance.
20. In case of infection/compromise in your home computer system, immediately disconnect the computer from internet and contact PRAL Technical Support team for advice.

Further information about cyber security threats and support, please contact PRAL at:

Information & Support During Office Hours	
Landline	(051) 9208681
FBR House Intercom	466
PRAL IT Support	itsupportfbr@pral.com.pk

Information & Extended Support 24x7	
Landline	(051) 9212374 (051) 8431155
IP Phones	1492 & 1155
Email	datacenter@pral.com.pk