ADVISORY FOR GENERAL PUBLIC ON CYBER CRIME DURING CORONA EMERGENCY

Cyber Crime Wing (CCW) - FIA

Ministry of Interior

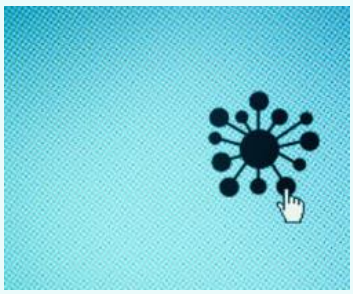
Government of Pakistan

Context

The outbreak of Corona Virus (COVID-19), has led people quarantine themselves at home. In times when eerie silence, everywhere, is echoed by the sounds of social distancing; social media remains omnipresent to mitigate social distancing on its omni present platform. In such scenario, most of the people, especially youth, are found connected to their internet screens most of the time. This increased activity in cyber space is quite attractive for some criminals who see opportunity in exploiting the general public for their nefarious offences.

Cyber Crime Wing, FIA, being the front-line fighter against such cyber criminals, wants you to be aware of the risks of cybercrime and the recourse you can take in case you are victimized by the cyber criminals.

POSSIBLE RISKS



- Children and youngsters, using social media platforms (e.g. Facebook, Twitter, Instagram, Snapchat etc.) may become an easy prey to the criminals who using real or false profiles lure children/youngsters into their trap by sending friendship requests/messages/pictures. They subsequently trap children/ youngsters into doing objectionable activities which may be filmed and used for criminal purposes against their consent. Such criminals may also convince children/youngsters for sharing their extremely private, even inappropriate pictures, with them which they later use to blackmail them with the threat of sharing the same with their family members or the friends.

- Criminals may deceit the general public for plundering their money through online accounts/platform/ websites claiming to sell and deliver medical/ personal safety products including masks, gloves, hand sanitizers, anti-viral medicines, vaccines, COVID-19 test kits, etc. Victims, in such cases, are cheatingly asked to pay via bank transfer/credit card etc.

- Adopting the phishing method, some criminals falsely claim themselves to be the health authorities and send concocted emails and in doing so trick the victims into connecting to a specific webpage and to login with email address and password. These culprits use the credentials, thus obtained, to access the sensitive information and ultimately vacate the accounts.

Preventive Measures

- Never share your personal information with any one on internet.
- Never share private pictures/videos with anyone on social media.
- Never open Email from any unknown source containing a link or any such thing.
- Never accept “friend request” from any stranger.
- Youngsters should be allowed to use internet only under supervision and in a shared space.

What to do in case of being victimized?

- Never stay silent if you have become victim to a cybercrime of any sort including blackmailing, harassment or bullying.

- Identify and report false/misleading scams online

- You may also file an online complaint through email at:
  - **helpdesk@nr3c.gov.pk**

- You can lodge a complaint to CCW-FIA, by calling at Helpline No. **9911** or at any of the following Cyber Crime Reporting Centers:

Cyber Crime Reporting Centers	**Phone Numbers**
Islamabad (ICT)	051-9262106, 051-9262107-08
Rawalpindi	051-9330717, 051-9334919,051-9330720
Lahore	042-99332744
Peshawar	091-9217109
Quetta	081-2870057
Karachi	021-99333950
Multan	061-9330999
Sukkar	071-9310849
Faisalabad	041-9330865
Gujranwala	055-9330015-16
Dera Ismail Khan	0966-852945
Hyderabad	022-9250009
Gawadar	0322-2451500
Gilgit	05811-920409
Abbottabad	099-2384148

****