



Pakistan Telecom Authority, Islamabad

PTA Cyber Security Advisory No: 072

27-March-2020

Name: Cyber Attacks by the name of COVID-19

Summary:

It has been observed that cyber criminals are using the COVID-19 pandemic as an opportunity to carry out online scams and malicious cyber activity. Cyber threat actors may send **emails with subject line COVID-19 and malicious attachments or links to fraudulent websites** to trick victims into revealing sensitive information or donating to fraudulent charities. Such scams or phishing emails may include following:

- Emails with COVID-19 subject line, claiming to be from WHO (World Health Organization)
- Phishing emails claiming to have latest COVID-19 information
- Whatsapp/SMS messages with fake links claiming for COVID-19 testing facilities
- Fake Coronavirus (COVID-19) Maps

The attachments or fake links may allow the attackers to install malicious software on the device resulting in sensitive information breach, such as banking details, passwords etc.

Recommendations:

Communicate to end users and your employees to remain vigilant and take the following precautions:

- Always use trusted sources such as legitimate, government websites for latest information about COVID-19.
- Do not download or open attachment in the email received from untrusted sources.
- Don't click links on untrusted sites and do not reveal or provide personal or financial information.
- Always install latest and updated software when available from device vendors.
- Do not use unknown Wi-Fi networks at public places.
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Regularly perform backups of important data.
- In case of any incident, please report to this office.