ADVISORY FOR SOCIAL MEDIA USERS AGAINST POSSIBLE HACKING OF PERSONAL ACCOUNTS BY CYBER CRIMINALS

Cyber Crime Wing (CCW) – FIA

Ministry of Interior

Government of Pakistan

INTRODUCTION

Hacking is a quite common criminal technique employed by the cyber criminals to steal, corrupt or illegitimately view data. A huge number of complaints are ,nowadays, being reported at Cyber Crime Wing-FIA whereby Hackers are reported to break into victim's social media accounts to steal his/her identity to be later employed for criminal purposes. These social media accounts may include though not limited to Facebook, Twitter, Instagram etc.

Hacking is a crime under section-23 of Prevention of Electronic Crimes Act, 2016 the punishment for which is **imprisonment for a term which may extend to two years or with fine which may extend to one million rupees or with both**.

MOTIVES OF CYBER CRIMINALS

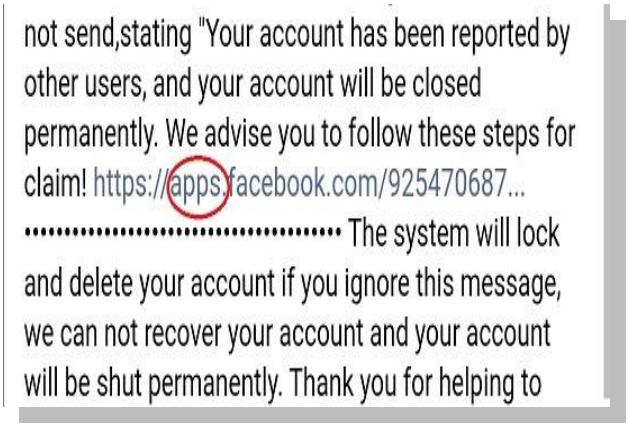
Hackers may do hacking with one of the following criminal intentions:

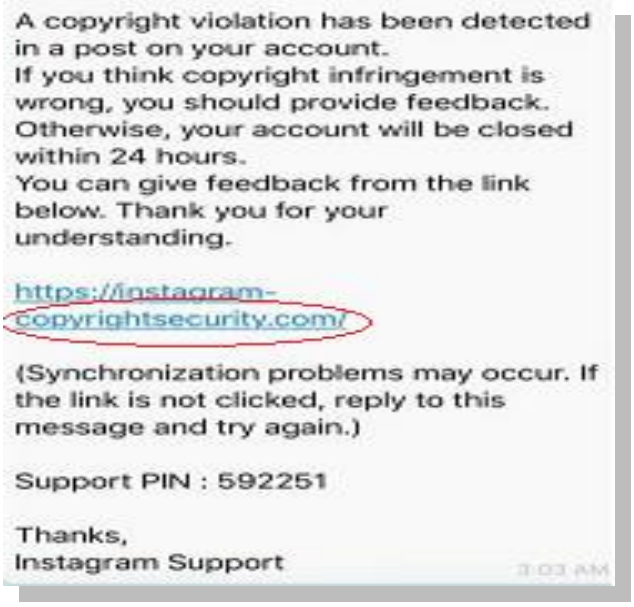
- To send out messages to family members, friends or colleagues for monetary help quoting emergencies and providing with account numbers where money has to be transferred.
- To give vent to some personal grudge or vendetta against the victim.
- To get personal/confidential information from relatives, friends and colleagues of victims or related persons and later misuse the same for illicit purposes.
- To share personal/confidential information of actual account holder to scandalize/defame him/her through actual or forged document, audio video material, pictures or other type of information.
- To blackmail victim for illegal favors, demands or extort money in exchange for (undertaking by the criminal) not using the stolen/hacked data to scandalize or defame the victim.

METHODS USED BY CYBER CRIMINALS

Cyber criminals may use a variety of methods to create interest, excitement, anxiety and fear to compel them to click on the forwarded bogus links/pictures and inadvertently become victim of cyber crimes. Normally the cyber criminal use following type of messages to deceive the unsuspecting users:

- **"**A **Suspicious activity** has been detected on your Facebook account. Please click on the link below to reset your password." Example for such a case is as follows:


not send,stating "Your account has been reported by other users, and your account will be closed permanently. We advise you to follow these steps for claim! https://apps.facebook.com/925470687...
..... The system will lock and delete your account if you ignore this message, we can not recover your account and your account will be shut permanently. Thank you for helping to


A copyright violation has been detected in a post on your account.
If you think copyright infringement is wrong, you should provide feedback. Otherwise, your account will be closed within 24 hours.
You can give feedback from the link below. Thank you for your understanding.

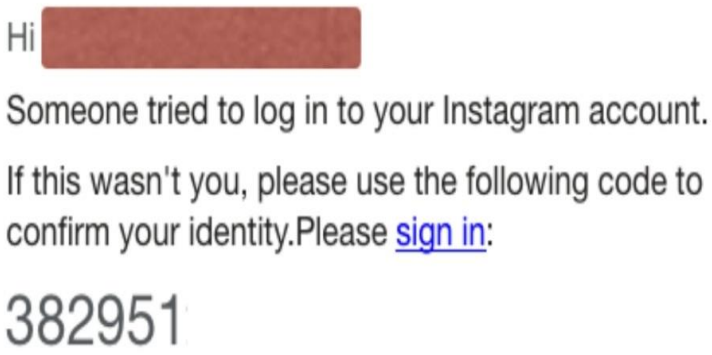
https://instagram-copyrightsecurity.com/

(Synchronization problems may occur. If the link is not clicked, reply to this message and try again.)

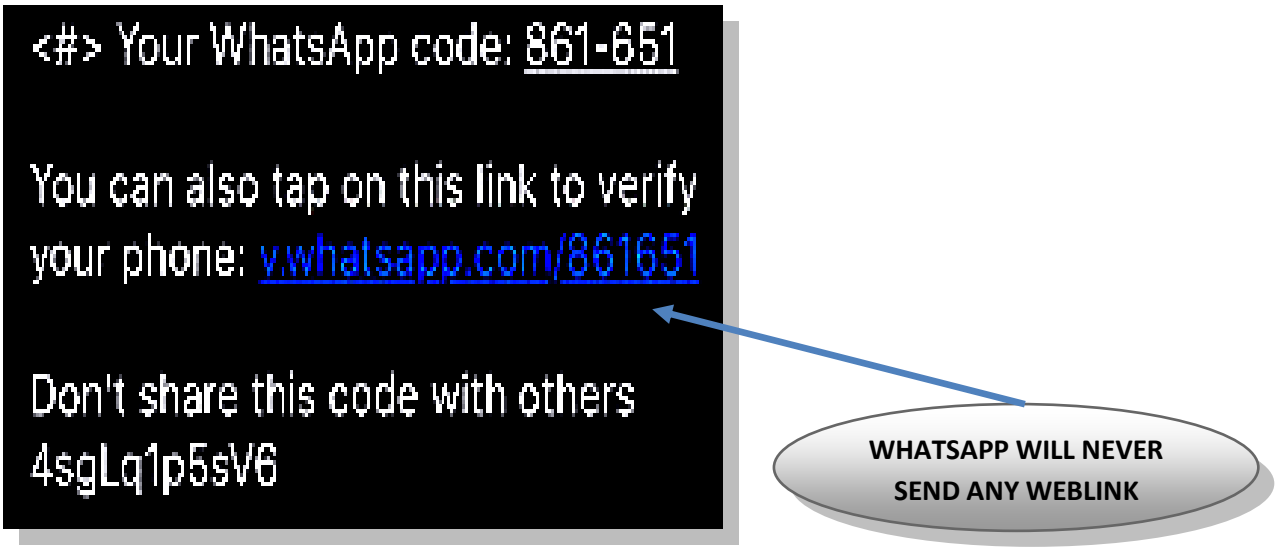
Support PIN : 592251

Thanks,
Instagram Support

- “Someone tried to **login** from your Instagram account. If it is you, kindly confirm through the link below.” Example of such a case is as follows:

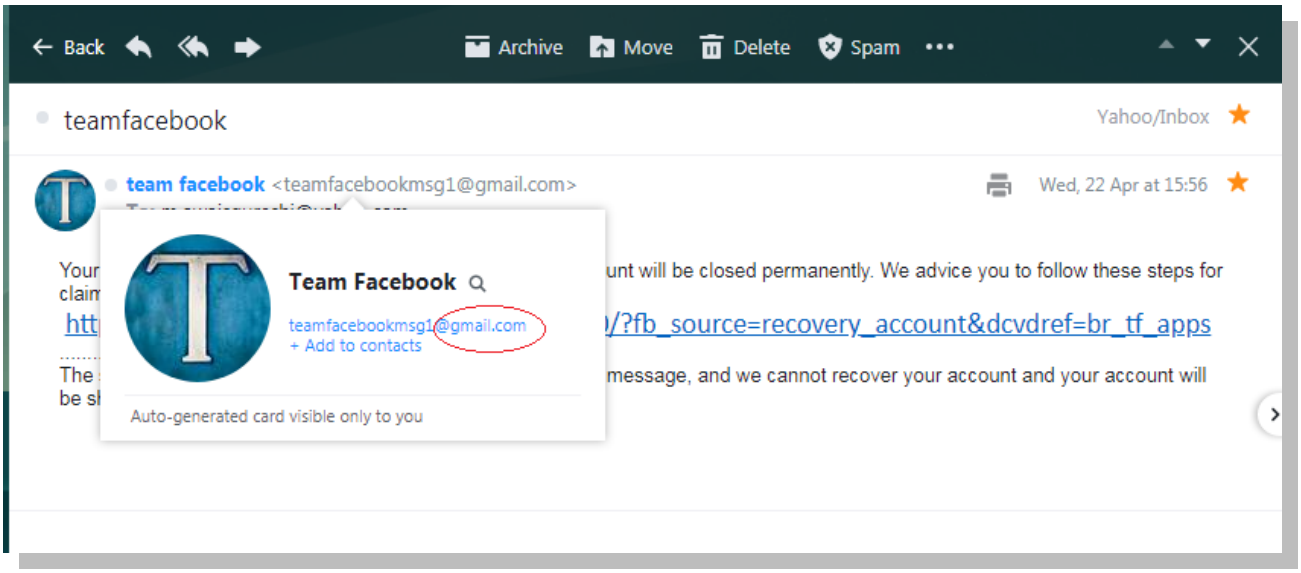


- “Your account is not verified. To **verify your account** please click on this link within 24 hrs. Otherwise your account will be blocked.” Example for such a case is as follows:



MANIPULATED EMAIL ACCOUNTS USED BY CYBER CRIMINALS…

- Cyber criminal may use different **manipulated email IDs** which look like **same** as **original email IDs**, coming from service providers e.g. email with the name "**teamfacebook".**
  - Open an email of team Facebook **(teamfacebookmsg1@gmail.com).**
  - **Place** a **Cursor** on the sender's email address, it will come to know that sent Facebook message is not from the Facebook's actual domain **(@facebookmail.com)**, but it is from the Gmail's domain **(@gmail.com)**.

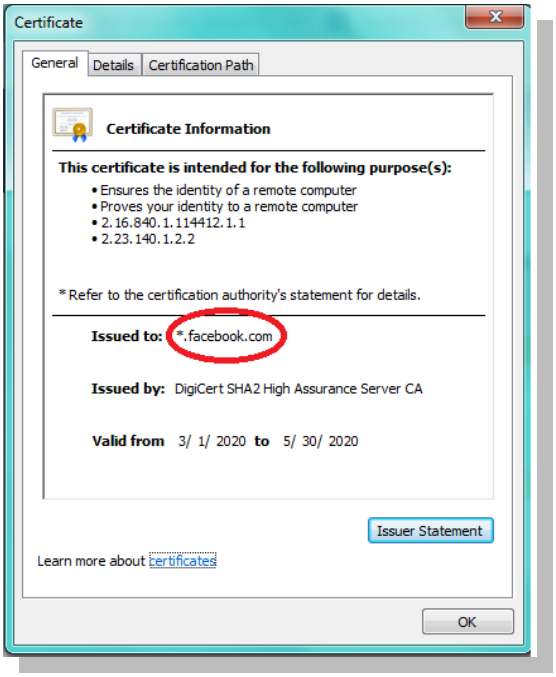


HOW TO KNOW IF CYBER CRIMINALS ARE TRYING TO HACK YOUR ACCOUNT?

Below are some examples to recognize between original and fake links:

Original URL's	Fake URL's
https://web.facebook.com	https://weeb.faaceboook.com/
https://facebook.com	https://usa.faaceboook.com/

When you click on the lock sign then the details are showed to you on a dialogue box.



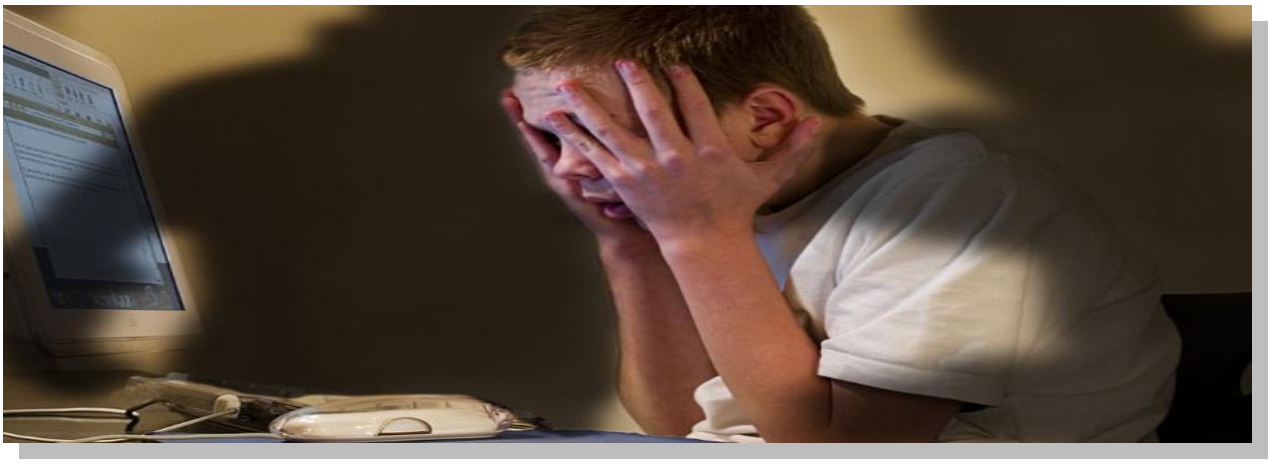
Original URL's	Fake URL's
https://outlook.live.com/	http://hhhhhhhhhhooooottttttttt.bugs3.com/windowslive.hotmail.update/login.html
https://www.instagram.com/	http://Instagram-copyrightsecurity.com/

WHAT TO DO IF YOU NOTICE ANY SUSPICIOUS ACTIVITY?

If you receive such type of links in your email or messages:

- Don't Panic: it might be a fake message or link, so you need to be careful in choosing your next steps. Rather than clicking on link directly, **open your account again and change the password.**
- Don't give any personal information, data, account login details on third party services and apps (such as on Fake Facebook page)
- Don't use same password for your email and social media accounts.
- Do change your passwords regularly and securely, note down them in your diary.
- Do carefully check the address bar of the URL of the webpage as cyber criminal by slightly changing the address may make it look like the original and deceive an innocent user. For instance, **instagram.com,** they would use 1stgram.com which in first glance is hardly noticeable by an ordinary user.

WHAT TO DO IF YOU STILL BECOME A VICTIM OF CYBER CRIMINALS…



If despite observing the necessary precautions, as listed above, you still unfortunately become victim of activities of cybercriminals, please do not hesitate to report Cyber Crime Wing (CCW) of FIA. You may opt to lodge a complaint with CCW through following modes:

Helpline:	**9911**
Phone:	**051-9106384**
Email:	**Helpdesk@NR3C.GOV.PK**

In addition, you can also directly approach one of our 15 regional offices listed below:

CCRC ISLAMABAD	**Land line no: 051-9106412, 051-9262107-08**
CCRC RAWALPINDI	Land line no: **051-9334919, 051-9330720**
CCRC LAHORE	Land line no: **042-99332744**
CCRC PESHAWAR	Land line no: **09-19219565**
CCRC KARACHI	Land line no: **021-99333950**
CCRC QUETTA	Land line no: **081-2870057**
CCRC GUJRANAWALA	Land line no: **055-9330015-16**
CCRC MULTAN	Land line no: **061-9330999**
CCRC FAISALABAD	Land line no: **041-9330865**
CCRC HYDERABAD	Land line no: **022-9250009**
CCRC SUKKUR	Land line no: **071-9310849**
CCRC ABBOTTABAD	Land line no: **099-2384148**
CCRC DERA ISMAIL KHAN	Land line no: **0966-852945**
CCRC GILGIT	Land line no: **05811-920409**
CCRC GWADAR	Mobile no : **0332-2400190**

****