Republic of the Philippines
NATIONAL POLICE COMMISSION
**PHILIPPINE NATIONAL POLICE**
**ANTI-CYBERCRIME GROUP**
Camp BGen Rafael T Crame, Quezon City

# ACG-CYBER SECURITY BULLETIN NR 190

## ACG-CSB 060820190

Reference Number ACG-CSB 060820190

### Beware of a Fake Facebook Account

The following information was obtained from different cyber security sources for notification to all parties concerned pursuant to the mandate of the Philippine National Police Anti-Cybercrime Group (PNP ACG) and classified as “Restricted” pursuant to the PNP Regulation 200-012 on Document Security and Impact Rating as high based on PNP Information Communication Technology (ICT) Security Manual s.2010-01 p. 22 and p.129.

### SUMMARY

A fake account is an account where someone is pretending to be something or someone that does not exist. Fake accounts can include accounts for fake or made up people, pets, celebrities or organizations. Because of the very nature of social networking sites where people are encouraged to share personal information users are automatically at risk of becoming victims of identity theft. Facebook users should be aware that identity thieves are constantly coming up with new scams aimed at stealing personal data.

Although these cases involved well-known stores, any of Facebook's users could see their profile copied and stolen. It is also possible that the person whose identity has been stolen does not have a Facebook account. Both adults and children are potential victims, once a cyber thief knows the phone number of a potential victim, the thief can then enter the number into the Facebook search box, and the individual's profile will come up, which can include information such as birthdate, hometown, recent whereabouts and where the individual works, worked in the past, and went to school..

Facebook does not prevent users from having duplicate user names, so pretty much anyone can copy the name and pictures of one of your friends and pretend to be you. Depending on what they want to extract, a fake Facebook friend can either seek to learn valuable information about his target, such as secret data from the company you work at or credit card details. In most cases, however, they will pretend to be the friend in question and ask you for a loan or some other “friendly favor”.

The next thing they do is block the person they are impersonating and send friend requests to everyone on the victim’s friends list. This is done to infiltrate their social network. Once this part of the mission is complete, the scammer has a variety of options at their disposal. Data mine the accounts they have friended under the bogus profile. Even if you have your privacy and sharing options set to “Friends Only,” you are still at risk if you accidentally accept a duplicate friend request.

The scammer contacts people close to the victim and tells them that they are in trouble of some kind, usually stranded on vacation, arrested or in some other legal trouble, etc. This is accompanied by an urgent plea to send money thru different money remittances. Unknown con artists are not the only ones creating duplicate profiles and pages. Bullies often create fake profiles with the intention of humiliating or harassing their intended victim.

Facebook users can take some steps to protect their privacy and make it much harder for identity thieves to compromise their personal information. For starters, users can select which friends can view their personal information, including their birthdate, relationship status, phone number and hometown, in the “About Me” section of their profile. They can limit this to different groups of people, such as friends, work colleagues and so on.

All PNP personnel as well as the public are advised to be aware of fake facebook account to avoid being a victim of cybercrime:

## RECOMMENDATION

The public are advised to follow these tips in order to prevent being victimized of credit card fraud, to wit:

- Check your privacy settings;
- Do not include personal information in your user name or email address;
- Do not confirm “Friend Requests” from people you do not know;
- Think twice when you want to purchase Facebook services that require your credit card information;
- Change your passwords regularly;
- Do not automatically click on any links that you receive on social media, especially when they appear to have been sent to you by someone you know; and
- Let your current friends know about the fake profile.

For additional information, please refer to the following websites:

- https://www.lifelock.com/learn-internet-security-facebook-glitch-can-lead-to-identity-theft.html
- https://www.equifax.co.uk/resources/identity_protection/safeguard-your-identity-on-facebook.html
- https://heimdalsecurity.com/blog/fake-facebook-scams/

## POINT OF CONTACT

Please contact PMAJ ANGELICA STARLIGHT L. RIVERA, Asst. Chief, ARMD thru e-mail address acg@pnp.gov.ph or contact us on telephone number (632) 7230401 local 3562 for any inquiries related to this CYBER SECURITY BULLETIN.