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 179

ACG-CSB 121219179

Reference Number ACG-CSB 121219179

How Cyber Criminals Steal your Personal Identifiable information (PII) to Steal your Money

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

Identity theft is the deliberate use of someone else's identity, usually as a method to gain a financial advantage or obtain credit and other benefits in the other person's name, and perhaps to the other person's disadvantage or loss. The person whose identity has been assumed may suffer adverse consequences, especially if they are held responsible for the perpetrator's actions. Identity theft occurs when someone uses another's personal identifiable information (PII), like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes.

Online identity theft occurs when users fall for tactics like phishing and confidence scams, or download malware onto their computers or smartphones that steals their information, use wireless networks that are insecure, take out money from an ATM that has been rigged with a skimming device that collections your information, share their passwords with untrustworthy people, or by having their information stolen when data records are breached on companies, government, and educational sites.

When this information is stolen, it could greatly impact a user’s finances. A cybercriminal can use information for simple malicious activities such as paying bills, performing fraudulent online transactions, and transferring money out of victims’ bank accounts.

There are many different types of schemes identity criminals use. This can range from non-technological to technological schemes. The following is a listing of just some of the most common methods identity criminals have been known to use to obtain your personal identifiable information, the ways scammers obtain personal or banking information are:

- fake online quizzes and surveys
- fake job advertisements

- remote access scams in which the scammer has direct access to everything on your computer
- sourcing information about you from social media platforms
- direct requests for scans of your driver's license or passport, often in the course of a dating and romance scam.

Your identity has value, as much as your online partial identities. When your partial identity is with your bank or a brokerage house, for example, it may have clear monetary value. When it is with a social networking site, such as Facebook, Instagram or Twitter account, the value may be less tangible but equally important to you. Simply by being an active Internet user, you may find that you accumulate tens or even hundreds of online partial identities.

If you become the victim of identity theft, chances are it will cause severe damage to your finances and your good name, especially if you don't find out about it immediately

RECOMMENDATION

The public are advised to follow these tips in order to understand the risks and prevent Steal your Personal Identifiable Information to Steal your Money:

- Protect your computer and smartphone with strong, up-to-date security software;
- Learn to spot spam and scams.
- Use strong passwords.
- Be cautious with shortened links
- Always be careful in giving out personal information in a website, email, instant messaging systems, chat rooms and message boards.
- Don't open up e-mails, files or website links from unknown sender.
- Consult with financial institution on any unusual activities on your accounts
- Immediately close compromised credit card accounts.

For additional information, please refer to the following websites:

- https://en.wikipedia.org/wiki/Identity_theft
- https://www.thoughtco.com/ways-identity-thieves-get-your-information-972208
- https://www.utica.edu/academic/institutes/cimip/idcrimes/schemes.cfm
- https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/what-do-hackers-do-with-your-stolen-identity

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.