HEADQUARTERS
ARMED FORCES OF THE PHILIPPINES CYBER GROUP
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN: 2022-03

HOW CAN I PROTECT MYSELF FROM IDENTITY THEFT ONLINE?

1. Background:

Identity theft is any kind of deception, scam, or crime that results in the loss or compromise of personal data of an individual, which could include usernames, passwords, banking information, credit card numbers, Social Security Numbers and health ID's, that is then used without his/her permission to commit fraud and other crimes.

For some consumers, identity theft is an annoying inconvenience and they can quickly resolve their problems and restore their identity. For others recovering their identity can cost a lot of money, take months to resolve, cause tremendous damage to their reputation, cause them to lose job opportunities, even influence the rejection of loan applications for school, homes or cars because would-be employers or loan companies see the damage on their credit scores. Some consumers have even been arrested for crimes committed by someone using their identities and have had to prove that they were not guilty.

2. How are identities stolen?

Consumers become victims of identity theft through many types of exploits. These can happen the old-fashioned ways when crooks (including family members!) steal mail from your mailbox, rummage through your trash for bills and bank statements, steal wallets and purses, or make an extra copy of your credit card - perhaps when your waiter or clerk walks off to process your payment.

Online identity theft occurs when people fall for tactics like phishing and confidence scams; download malware onto their computers or smartphones that steals their information; use wireless networks that are insecure; transacts at ATM that have been rigged with a skimming device that collects user information; share their passwords with untrustworthy people, or by having their information stolen when data records are breached on systems owned by private companies, government offices, and educational sites.

3. **Recommendations**

Military personnel and Civilian Human Resource are advised to follow a few key steps below to prevent identity theft online:

a. Protect your computer and smartphone with strong, up-to-date security software. If your computer or phone is infected with malicious software, other safeguards are of little help because you've given the criminals the key to all your online actions. Also, be sure that any operating system updates are installed.

b. Learn to spot spams and scams. Though some phishing scams are easy to identify, other phishing attempts in an email, IM, on social networking sites, or websites can look very legitimate. The only way to never fall for a phishing scam is to never click on a link that has been sent to you. For example, if the email says it is from your bank and has all the right logos and knows your name, it may be from your bank – or it may not be. Instead of using the link provided, find the website yourself using a search engine. This way you will know you landed on the legitimate site and not some mocked-up fake site.

c. Use strong passwords. Weak passwords are an identity thief's dream – especially if you use the same password everywhere. Once the thief knows your password, they can login on your financial accounts and wreak havoc. You need passwords that are long (over 10 characters), strong (use upper and lower case letters, numbers, and symbols), and that have nothing to do with your personal information (like name, age, birthdate, pet). Password managers and two-factor authentication (2FA) are also both best practices for password management.

d. Review your credit score. Look to see if there are new credit cards, loans, or other transactions on your account that you are not aware of. If there are, take immediate steps to have these terminated and investigated.

e. Freeze your credit. Criminals use stolen IDs to open new lines of credit. You can thwart their efforts to use your identity by simply locking (also called freezing) your credit so that no new credit can be given without additional information and controls. Contact your bank or credit card provider for more details on locking or freezing your account.

f. Only use reputable websites when making purchases. If you don't know the reputation of a company that you want to purchase from, do your homework. How are they reviewed by other users? Do they use a secure, encrypted connection for personal and financial information? Hypertext transfer protocol Secure (https), as its name suggests, is a more secure variant of the older Hypertext transfer protocol (http). The new protocol was developed to validate the safety and privacy of a site, so it's important you see "https" in a website's URL whenever it asks for personal or financial information.

g. Stay alert. Watch for common signs of identity theft like:

- False information on your credit reports, including your Social Security number, address(es), name, or employer's name.
- Missing bills or other mail. If your bills don't arrive or come late, contact your creditors. A missing bill may indicate that an ID thief has hijacked your account and changed your billing address to help hide the crime.
- Getting new credit cards sent to you that you didn't apply for.
- Having a credit approval denied or being subjected to high-interest rates for no apparent reason.
- Receiving calls or notices about past due bills for products or services you didn't buy.
- Be wary of public WiFi and think twice before joining an unsecured network. Virtual private networks, or VPNs, are tools that can help you shield yourself from prying eyes on public WiFi networks.

Consistently applying these steps to both defend and monitor your credit score will reduce the risks of having your identity stolen, and alert you instantly if such a problem arises. Internet security solutions with identity theft protection can guard against specialized malware designed to steal personal information by logging your keystrokes or snooping on your browsing sessions. Protect usernames, account numbers, and other personal information against spyware and other online threats targeting valuable personal data.

4. Dissemination

The information provided is intended to increase the security awareness of AFP personnel mobile smartphone users and to help them behave more securely within their work environment. The increased awareness is intended to help improve the organization's overall cybersecurity posture. All units and offices are given permission and are encouraged to redistribute this bulletin that will benefit as a whole for educational, and non-commercial purposes.

Reference:

https://www.webroot.com/us/en/resources/tips-articles/how-can-i-protect-myself-from-identity-theft-online