PHILIPPINE NATIONAL POLICE
INFORMATION TECHNOLOGY MANAGEMENT SERVICE
INFORMATION SYSTEMS SECURITY DIVISION

#BeCyberSmart: IDENTITY THEFT AND INTERNET SCAMS

Today's technology allows us to connect around the world, to bank and shop online, and to control our televisions, homes, and cars from our smartphones. With this added convenience comes an increased risk of identity theft and internet scams. #BeCyberSmart on the internet – at home, at school, at work, on mobile devices, and on the go.

COMMON INTERNET SCAMS

Top three kinds of threats:

- **Identity theft** is the illegal acquisition and use of someone else's personal information to obtain money or credit. Signs of identity theft include bills for products or services you did not purchase, suspicious charges on your credit cards, or new accounts opened in your name that you did not authorize.
- **Impostor scams** occur when you receive an email or call from a person claiming to be a government official, family member, or friend requesting personal or financial information.
- **Debt Collection scams** occur when criminals attempt to collect on a fraudulent debt. Signs the "debt collector" may be a scammer are requests to be paid by wire transfers or credit cards.

SIMPLE TIPS TO SECURE IT.

- **Double your login protection.** Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. Enable MFA by using a trusted mobile device, such as your smartphone, an authenticator app, or a secure token – a small physical device that can hook onto your key ring.
- **Shake up your password protocol.** Use longest password or passphrase permissible. Get creative and customize your standard password for different sites. Use password managers to generate and remember different, complex passwords for each of your accounts.
- **Be up to date.** Keep your software updated to the latest version available. Maintain your security settings to keeping your information safe by turning on automatic updates so you don't have to think about it, and set your security software to run regular scans.

PROTECT YOURSELF FROM ONLINE FRAUD

Stay Protected While Connected: Whenever you're online, you're vulnerable.

- Practice safe web surfing wherever you are by checking for the "green lock" or padlock icon in your browser bar – this signifies a secure connection.
- Avoid free internet access with no encryption.
- If you do use an unsecured public access point, practice good internet hygiene by avoiding sensitive activities that require passwords or credit cards. Your personal hotspot is often a safer alternative to free Wi-Fi.
- Don't reveal personally identifiable information such as your bank account number, SSN, or date of birth to unknown sources.
- Type website URLs directly into the address bar instead of clicking on links or cutting and pasting from the email.