PHILIPPINE AIR FORCE
950TH COMMUNICATION, ELECTRONICS AND
INFORMATION SYSTEM GROUP
954th CYBERSPACE OPERATIONS SQUADRON
Colonel Jesus Villamor Air Base, Pasay City

RNDF

SUBJECT: **Cyber Security Reminder (24 Aug 2020)**

TO: **Group Commander, 950th CEISG**
POST

1. References: Cyber Security Reminder, PAF Official Website: https://www.paf.mil.ph/cyber-security-reminders

2. In view of the above reference, attached herewith is the Cyber Security Reminder for 02 August 2020.

3. For information and reference

CELBERT REY P CA-AS
1LT PAF
Squadron Commander

SIGNATURE AUTHENTICATION
20200811184028 PAF

Incl:
a/s

Smart Reminders to Help You Stay Cyber-Safe

BY: JUDY MCKINNON, THE NEWS DESK

Many of us are spending whole lot more time online as we adopt new ways of tackling everyday tasks – be it working, staying connected with friends and family, shopping or banking. While it's always a good time to revisit our online habits from a safety standpoint, it's now more important than ever as scammers attempt to take advantage of vulnerabilities created by COVID-19.

What can you do to help ensure you're staying cyber-safe? Using resources offered by the Canadian Anti-Fraud Centre, the Canadian Centre for Cyber Security and the RBC Cyber Security Centre, we've compiled a few simple guidelines to help you stay vigilant.

Be Aware of Unsolicited Calls, Emails and Texts

Canada's cyber authorities are seeing an increased number of phishing attempts – in which emails or texts appear to be from a legitimate source but contain infected attachments or malicious links that can harm your device or steal your data. Government tax agencies will never contact taxpayers by email, text message or social media requesting personal or financial information. Banks also won't ask you to divulge your personal information or credentials in an email or text.

Red flags: Urgent or threatening tones to messages, spelling errors in messages or website addresses, unknown senders or callers.

Tip: Keep your computer anti-virus and anti-malware programs up to date to help keep files from being corrupted or lost.

Watch Out for Fake Websites

A number of fake websites are cropping up to spread misinformation or attempt to scam individuals, according to the Canadian Centre for Cyber Security. Authorities have been removing malicious websites spoofing government agencies such as the Public Health Agency of Canada and the Canada Revenue Agency.

Red flags: Spelling errors in web addresses or lack of a security symbol in the address bar.

Tip: In the address bar, look for a lock symbol or an 's' at the end of the "http," which can confirm a site's security. Don't enter login information or credit card details unless you are sure a site is legitimate.

Use Strong, Unique Passwords

If you haven't moved beyond the common “123456" or “password" choices, now's the time. Unique, strong passwords and passphrases can help ensure you're protecting your devices and information.

Red flags: Using the same password for multiple applications or Internet services, or choosing obvious passwords such as family or pet names, birthdays, street names and telephone numbers.

Tip: Use a combination of letters, numbers and special characters with a minimum of eight characters, change passwords regularly and create a new password for every application or Internet service you subscribe to or use. How? One idea is to think of a favourite song, use the first letter in each word of the title and add in a few unique numbers and/or symbols.

Keep Your Software and Browsers Up to Date

Your device's operating system has many built-in security features, but in order to be as effective as possible, it's got to be kept up to date to help avoid breaches of your personal information. The browser you use to search on the Internet also has its own security settings - and requires updating.

Red flags: You've been ignoring those prompts to update your operating system or browser, which means you can be exposing yourself to risk.

Tip: You may be able to enable automatic updates or try setting a reminder to update your device at a time you won't be using it.

Consider Your Work-from-Home Setup

With so many of us working from home, Canadian cyber authorities are warning that attackers are looking to exploit remote, or “telework," connections.

Red flags: loss of control of mouse or keyboard or strange pop-up ads.

Tip: Secure your home wireless router with strong passwords or phrases, turn off Wi-Fi, Bluetooth and GPS when not in use and keep software up to date.

References: https://www6.royalbank.com/en/di/hubs/tech-and-culture/article/smart-reminders-to-helpyou-stay-cyber-safe/k8kupbvr?fbclid=IwAR3iu87JxXdqaKM5P3tLwpKDtljunvczdIbQY78LO2nLuHYmy9TI74b5YYc