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

RNDF

August 06, 2020

SUBJECT: **Cyber Security Reminder (02 October 2020)**

TO: **Group Commander, 950th CEISG**
Colonel Jesus Villamor Air Base
Pasay City

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 October 2020.

3. For information and reference

PHILIPPINE AIR FORCE
20200806178564

CELBERT REY P CA-AS
1LT PAF
Squadron Commander

Incl:
a/s

How to Protect Yourself from Hackers

Hackers might be glorified and glamorized on television, showing off their hacking skills, breaking into extremely secured systems of companies, and saving the world. However, in reality, hackers break into systems with malicious intentions stealing confidential data and harming the entire system or the entity all in all.

To save yourself from cybercrimes, data theft, etc. make sure to remain extra secure and keep your software updated to avoid breaching. Here are a few tips on how you can keep your system from hackers:

1**. Public WIFI**

Social media is something that you can run from, but you can't hide from it. A lot of people have a habit of snap-chatting events, posting pictures of Instagram, or checking in on Facebook. It requires an internet connection, which makes people sign in to public WIFI and other systems. Public WIFI is the least safe way to access the internet

for personal usage. God knows how many people access their bank accounts and additional personal information using public internet providers.

Passive Risk

Public WIFI can passively affect your system as well as the data stored on it. If the connection provider is reliable, the traffic on that connection might have a hacker in it. You never know when you become one of the victims. There can be other parties (near that connection) that can also penetrate your system once you have signed into a public WIFI as it becomes more vulnerable.

HTTPS

If you need internet urgently and public WIFI is your only choice, make sure you are connecting to one that is HTTPS, which is more secure than a regular HTTP. Even though your personal information and data would still be at stake, there is less risk in HTTPS.

2. Location and Tracking

Leaving GPS and other trackable connections can put your system as well as data at quite a risk. Let me put it in simpler words. This makes your location quite accessible to the hacker. Wireless connections are vulnerable as well as more prone to hacker attacks, so it is better to turn off your GPS, geotag, and other wireless links that connect your devices to keep them from breaching. You can remain safe from contradiction as well as getting tracked.

Apps Require Access to The Location

Applications (mostly social media) require access to your current location for more accurate friend suggestions and check-ins. People often allow it and then leave it on. This exposes your device, making it easy for a hacker to locate and track you.

Reputable Apps

I do not recommend turning on the location for any application, but in case you need to do so to access desired information on the internet, make sure the app you are using is reliable. The app made a decent programmer or company and has a firm privacy policy, so your data remains safe.

3. Encryption

Passcodes and pins will always help you keep your gadgets, data, and other information safe. It can be on the internet or stored offline on your device. The purpose of encryption is to convert your data into cipher text, which is hard to read. This does not precisely provide protection but delays the process of breaching and attacking.

Convenience and safety are ensured by encryption while transporting data. This provides more confidentiality. Moreover, it will keep the data and system subjected to regulations.

3 Types of Encryption

Various types of encryptions are used based on the type of usage (personal or organizational).

DES (Data Encryption Standard)

It provides low-level security for personal gadgets and is unsuitable for sensitive data.

Triple DES

Although people use it for sensitive data, I would not recommend it. There have been cases of hackers being able to crack into it.

RSA

Based on a secure algorithm, this type of encryption is reliable for all sensitive data. It is a popular choice for data transfer.

AES (Advanced Encryption Standard)

AES is a worldwide used form of encryption that has quite an advanced setting providing high security and easy for transferring all kinds of data.

4. Two-Factor Authentication

Usually, when you sign in into an email or any account on the website. This is a great way to provide more security to the data stored, primarily online. The most recommended method for two-factor authentication is SMS. This way, you can connect your online account to your mobile number (personal), which will make sure that every time you log in to your account, you require verification from your mobile number for confirming it is you.

Keep The Mobile Number Unpublicized

Keeping the verification mobile number personal is essential as it mitigates the risk and ensures that the verification is always legitimate and done by you.

5. Firewall & V-Checker

Setting up a firewall is undoubtedly a lengthy and challenging process, but it is worth it you have done it right. It will not only keep hackers from penetrating your system and accessing your information but also deliver long-term security.

- macOS comes with a pre-installed firewall. You just have to enable it from the settings.
- Windows firewall is also a part of the system and is quite reliable.
- You can always take it up a notch and use a third-party firewall to enhance security.

Virus checkers are quite useful, especially if your device (the one with sensitive data on it) is usually connected to the internet most of the time. You can regularly scan your system for viruses using a mild scan or an intelligent scan based on the load of online data you have received.

Always opt for a smart virus checker so you can remove malware, viruses, threats, cookies, etc. This will guarantee maximum security by lifting in the minutest risks of your system getting breached.

Another essential point to remember is never to agree or accept options like ‘allow access’ or ‘do not ask for permission.’ Doing so will allow any website to easily penetrate your system WITH your permission despite having a firewall and antivirus, which fails the purpose of a firewall and a security system all in all.

6. Updated Software

Keeping all your applications all with the operating system up to date is essential as it fixes bugs and provides improved security. An updated version of the software makes it quite hard for a hacker to breach in as it changes the codes and encryptions, and high-strength system security is set up with each update.

Updates hold significance for operating systems, but when it comes to a browser like Bing Google or Opera, you must keep them updated to protect your online privacy. Browsers tend to track your search and movements to provide accurate suggestions. It is part of digital marketing for studying consumer buying behavior. When you keep it up to date, the tracking and privacy invasions you make are the minimum keeping your hacker attacks.

7. Back Up Sensitive and Essential Data

Backing up should be prioritized regardless of security issues. It has quite the utility as keeping a copy of essential data ensures that you can access it whenever you like despite losing a copy. If a hacker attacks your system, the external backup drive, or built one, both would keep your critical data safe and sound from the hacker’s reach.

Built-in Backup

Many operating systems provide internal backup utility, including Mac’s Time Machine and Windows’ File History. Keep your data safe and duplicated here to

avoid permanent data loss. This option is also available in mobile technology for the safekeeping of personal data.

External Backup

You can create internal backups, but in case of breaching of the complete system, the external backup will help you retrieve data.

8. Understand What You Are Clicking On

Spam emails and messages are no big deal. The problem begins when you click on them without knowing what harm they cause to your system. Such emails claim to be sponsored by Amazon, PayPal, or banks to seem legitimate, but they are nothing but spam with a hacker at the back ready to get into your system as you click on them.

Such emails, texts always claim that you have a problem in your bank account or some information, maybe an entire account of yours has been compromised which requires your consideration for your safety and privacy. They would ask for a passcode reset. Doing so, you grant them access to your account (or whatever they are attacking). Make sure to report such emails and NOT reply to them.

- Avoid clicking on URLs present in such emails.
- Beware of zip exe and another compressed file. There can be viruses like a trojan horse in there.
- Keep auto pay disabled in your system to avoid the files in the email to auto-play leading to an invasive attack.
- Do not download any file present in the email or message to avoid adding it to your system. Report immediately.

References: https://nancy-rubin.com/2020/07/02/how-to-protect-yourself-from-hackers/