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

CYBERSECURITY BULLETIN: 2022-06

PASSWORD MANAGEMENT TIPS FOR WORK AND LIFE

1. Background:

In today's digital age, focusing on password management is crucial to safeguarding personal and professional data against identity theft or hacks against your business. In addition to password management solutions, many businesses are turning to additional security measures such as biometric scanning to protect their corporate devices.

2. Six Password Management Tips for Work and Life

a. Keep Your Passwords Unique

For stronger security practices, you must keep all your passwords unique. Repeating passwords between applications and websites means if one application is compromised, other accounts where that password is used are vulnerable as well.

b. Change Your Passwords on a Regular Basis

Having unique passwords doesn't mean you get out of changing them on a regular basis, because it's security mitigation that any user can perform for themselves. Most enterprise IT departments have policies for employees to change passwords, and enterprise and SaaS applications often have a similar requirement for users. Changing user passwords regularly is part of many corporate compliance programs. It's also a best practice to change passwords after a known security breach.

c. Skip Paper for Your Passwords

It's easy enough to write down your passwords and keep them in a paper notebook, or worse, on a sticky note on your cubicle wall. But keeping passwords in plain sight is an invitation for the wrong people to learn them. You should also skip using your battered college dictionary for coming up with passwords; there's password cracking software available that can run through dictionary lists in little time.

Implementing a software management solution limits the number of people who have access to your passwords, decreasing the risk of discovery.

d. Replace Your Passwords with Biometrics

Modern cybersecurity is focused on reducing the risks for this powerful security solution: traditional passwords have long been a point of weakness for security systems. Biometrics aims to answer this issue by linking proof-of-identity to our bodies and behavior patterns.

Biometrics are rising as an advanced layer to many personal and enterprise security systems. With the unique identifiers of your biology and behaviors, this may seem foolproof. However, biometric identity has made many cautious about its use as standalone authentication.

e. Use Two-Factor Authentication for Added Security

Two-factor authentication (2FA) requires not only one password, but another authentication factor to verify the identity of a user. A standard 2FA method is to text a passcode to the user's smartphone. Some programs allow you to use biometric authentication as part of your 2FA.

Further, another emphasis on biometric scanning is that it serves as ultimate unique identifier for securing your personal or corporate mobile device. Further, since it is quick and easy, it also enhances the user experience while strengthening security, offering a more seamless solution to 2FA mobile security.

f. Educate Yourself on the Organization's BYOD Program

Password policies are also part of many BYOD programs. An organization could use an enterprise mobility management (EMM) solution to set the following policies:

- Lock screen password to protect the physical security of the device
- Password protection over any corporate-mandated secure containers on the device
- Encryption to protect corporate data residing on the device
- Encryption over any corporate online communications from the device

An organization can look for ways to participate in the BYOD initiative. Attend any training your company offers so you know and understand the password policies. Each personnel can also consider offering constructive feedback through proper channels about how password policies are affecting their work and personal device use for better and worse.

g. Password Management and You

Password security is an individual responsibility — both at work and at home. If you are proactive and use a password management solution with biometric authentication, you'll be better prepared against potential attacks against your personal and corporate data.

3. Recommendations

Passwords are the key to almost everything you do online, and you probably have multiple passwords that you use throughout the day. Choosing hard-to-hack passwords and managing them securely can sometimes seem inconvenient. Password management applies in work and personal environment and is a crucial part of the organization's cybersecurity posture. This Group highly recommends that every personnel follows the best practices in managing their passwords as stated above.

4. Dissemination

The information provided is intended to increase the security awareness of AFP personnel 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 the AFP organization as a whole for educational, and non-commercial purposes.

References:

- *https://insights.samsung.com/2017/04/13/six-password-management-tips-for-work-and-life/*
- *https://www.kaspersky.com/resource-center/definitions/biometrics*
- *https://www.it.ucsb.edu/secure-compute-research-environment-user-guide/password-best-practices*