H E A D Q U A R T E R S
ARMED FORCES OF THE PHILIPPINES CYBER GROUP
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN: 2022-16

PROTECT YOUR PC AND YOUR ONLINE ACCOUNTS WITH 5 EASY TASKS

Protecting your personal data isn't just smart these days it's a necessity. As the world grows more and more connected, your private info becomes more and more valuable. Whether it's using leaked info from website breaches to hack into your other accounts or holding your personal computer ransom for money, malicious evildoers won't hesitate to ruin your day if it puts profits in their pockets you still need to be mindful of how you respond to security threats.

1. Use a Password Manager

On of the biggest security risks these days is password reuse. Major Websites and services report massive data breaches on a shockingly regular basis. If you're using the same email and password for multiple accounts, and any of those accounts leak, attackers can hack into your other ones using the information.

Using strong, unique passwords for every account you own protects against that but memorizing a different random password for every website you create an account for is next to impossible. That's where password managers come in. These tools can create strong randomized passwords for you, store the information, and automatically fill in login fields on websites and software alike. Browsers are starting to offer basic password management tools too. Investing in a proper password manager is well worth it

LastPass – Best overall password manager

Dashlane – Best overall runner-up

Keeper – Most security-minded

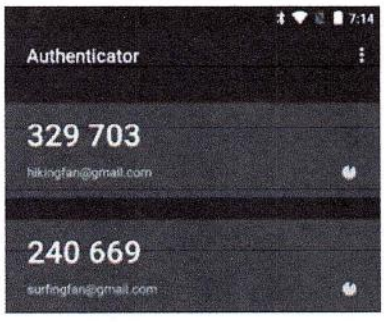
Bitwarden – Best free password manager

2. Enable two-factor authentication

Two-factor authentication requires you to confirm your account two ways before you're able to log in: with something you know, and something you have. The "something you know" is your username and password. The "something you have"

comes courtesy of an authorized tool you have in your possession. Usually, 2FA requires you to input a code that's either sent to you via text message or email when you try to log in on a device for the first time, or to grab a code from a supported 2FA app, or connect a security device devoted to account authentication. The exact method varies by service, and many offer several 2FA options. Without that code, hackers can't break into your account even if they have your login information.

Google Authenticator: Best overall



One of the more common ways of using two-factor authentication is Google Authenticator. This is a free smartphone app from Google available for both Android and iOS.

LastPass Authenticator: Runner up

LastPass's free authentication app uses a feature called one-tap push notifications that lets you log in to select sites on PCs with a click instead of entering codes.

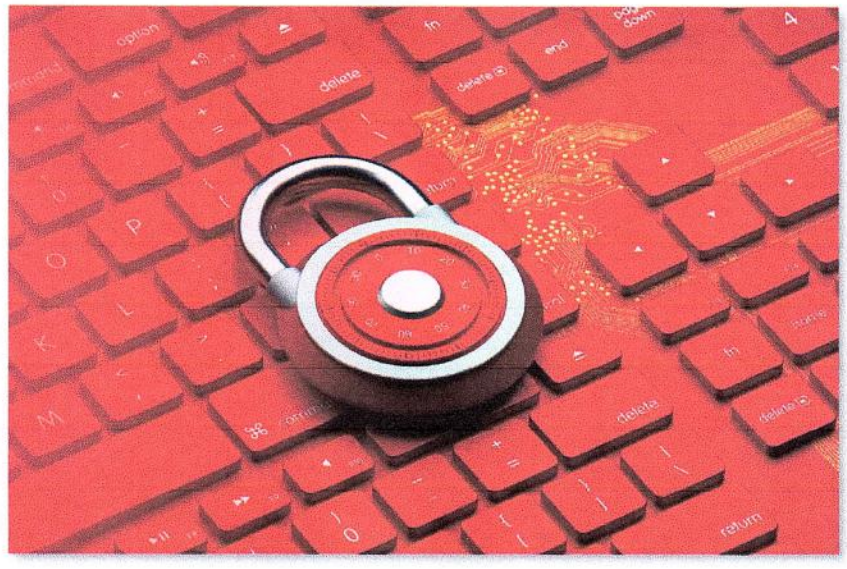
Microsoft Authenticator

Microsoft also has a free authenticator app for Android, iOS, and Windows 10 Mobile.

Authy: Best multi-device solution

Authy's free service aims to solve that problem by storing all your 2FA tokens the behind the scenes data that makes your 2FA codes work in the cloud on its servers. To use this feature you have to enable encrypted backups first, and then your tokens are stored on Authy's servers.

3. Stay safe with security software



Now that your online accounts are locked down, it's time to turn our attention to security for your personal computer. You don't want malware secretly siphoning off your information while you're banking or browsing your medical history, after all, while ransomware can lock you out of your computer completely until you pay a bounty.

That's where security software comes in. Yes, you still want to run antivirus and a firewall even in 2021. Good news, though: The Microsoft firewall that ships with Windows 10 gets the job done just fine these days, while the Windows Security tools that come bundled with the operating system (including antivirus) now offer surprisingly good protection. Better yet, they're enabled by default in Windows 10 if you aren't running a third-party alternative.

You still may want to run paid-for security software, as those suites offer much more than mere antivirus protection these days you'll also receive tools that protect against malicious ads, more advanced firewalls, family protection for several devices, VPN access, and more.

Norton 360 Deluxe

Norton™

Avast One

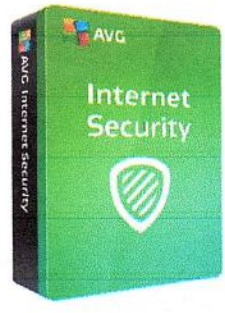
Avast

McAfee Total Protection

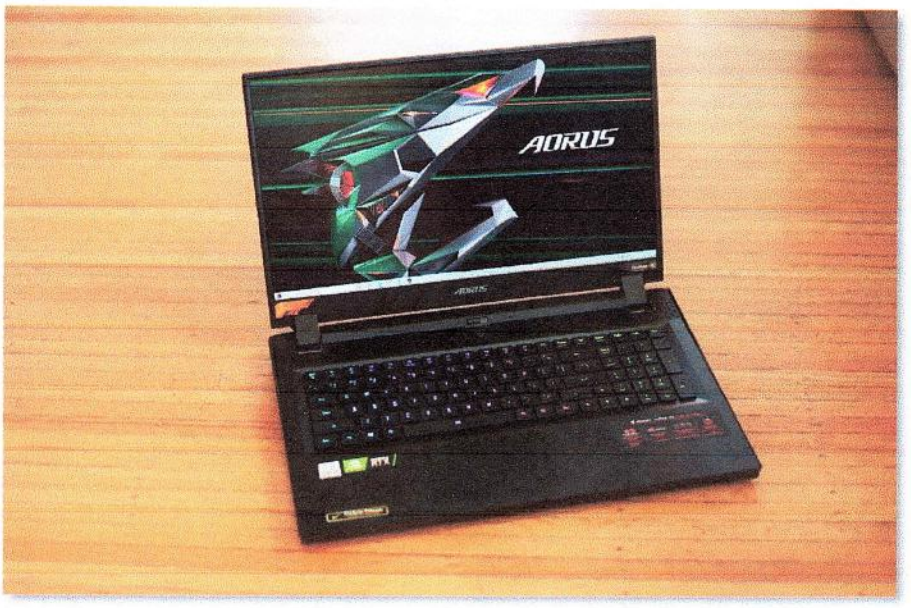
McAfee

Trend Micro Maximum Security

AVG Internet Security



4. Don't use a Windows admin account

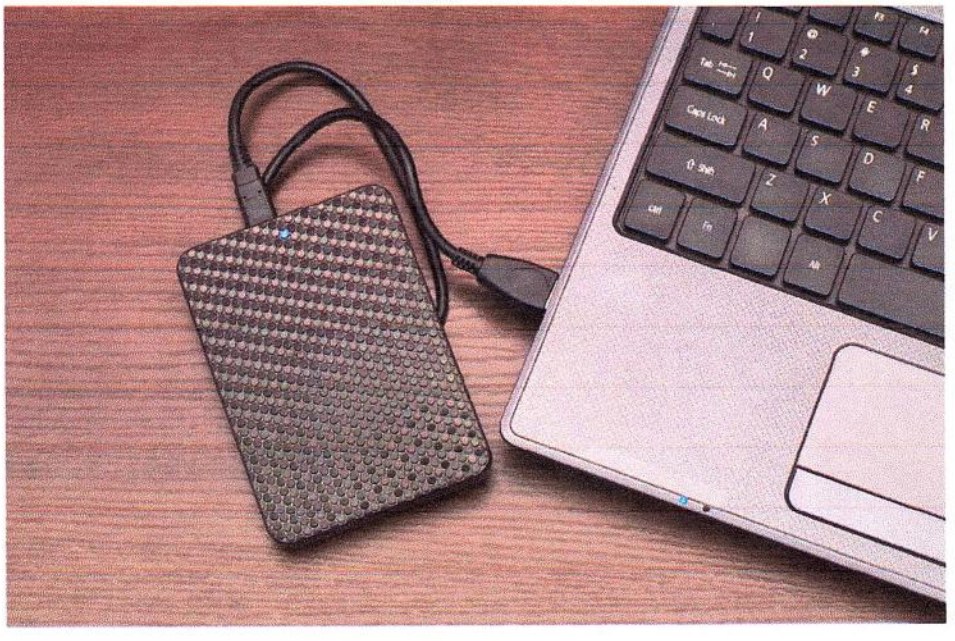


Here's one of the biggest under-the-radar security pro tips around: Don't use a Windows administrator account day-to-day. Instead, use a secondary standard account.

A lot of malware tries to sneak itself on your system. Only administrator accounts can install software in Windows. If you're using a standard account, you won't be able to allow a rogue program onto you PC accidentally (at least not easily). For the best security, set up your computer with all the software you need using an admin account, but then use a secondary standard account to go about your business in general life. It's very easy to switch over to your administrator account quickly when you need to install something new.

And *definitely* set your friends and family up with standard accounts if you're sharing your computer with others.

5. Back up your data



Finally, backing up your data is an underappreciated but vital aspect of your security toolkit. If a virus *does* manage to breach your computer's defenses, having a comprehensive backup can help you restore any lost data, and potentially help you sidestep ransomware bounties.

There's no single way to back up your data. Some people take "images" of the entire operating system, others rely on online backup services, and some folks simply drag key files over to external hard drives on the reg. Any method works as long as you're doing something!

6. 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://www.pcworld.com/article/394001/5-easy-tasks-supercharge-your-security.html*