CYBER HYGIENE ESSENTIALS

PROTECT YOUR DIGITAL LIFE

Prepared by UPOU ICT Development Office

Audit your passwords and keep them secure

Secure your devices

Use a Password Manager

Be cyber aware and cyber prepared

Enable MFA (Multi-factor Authentication)

Apply workplace best practices

Action plan

- ☑ **Audit** your passwords and keep them secure
- ☑ Use a **Password Manager** to help generate, store, and manage all your passwords
- ☑ Enable **MFA**(Multi-factor Authentication) on all your essential accounts such as email, social media, and bank apps
- ☑ Secure your devices
- ☑ Be cyber aware and cyber prepared
- ☑ Apply workplace best practices

Audit Your Passwords

Passwords are your first line of defense against unauthorized access to your online accounts and personal information. That's why it's important to regularly audit your passwords to **ensure** they are **strong** and **secure**. With today's powerful computers and technologies, **weak passwords** are **easy** for hackers to **guess** or **crack**. Below is a table of time estimates for cracking a password based on length and complexity:

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

(https://www.hivesystems.io/password-table)

To keep your password **secure**, your password must:

- Be at least 14 characters long(and ideally longer)
- Be a mix of uppercase and lowercase characters plus symbols and letters
- Avoid common and obvious sequences: **dictionary words** (12345, password123, food) and **personal information**(birthdate, pet names)

Weak Passwords

“password123”

- common and default

“qwerty”

- common, simple, and short

“123456”

- common, simple, and short

“p@s$w0rd123!”

- complex but short

“Oct161980”

- contains personal information

Strong Passwords

CZttaiL46Evs@LU2Fu@xnpR$th

- 27 characters **generated** by password manager

Up@0uSeCuRe!FROM99=11hax~

- 25 characters with your **personalized** secret code/pattern
- **not advisable** because it is hard to manage and remember

Chance-ecology-Tableful-startling-Dyslexia-report-Shakable

- 58 characters
- a passphrase

Regularly change passwords. **Never reuse passwords**, even your old ones.

They may already have been compromised in a data breach.

Password management is key.

Use a Password Manager

Passwords can be hard to manage, especially if you have many accounts and use strong passwords.

- We recommend using **iPortal** (iportal.upou.edu.ph) based on Passbolt. There are also good alternatives such such as ***KeePassXC*** and ***BitWarden***.
- **Built-in password managers** inside popular browsers such as **Google Chrome**, **Firefox**, and **Safari** are all **viable** options as well but may have less quality-of-life features. They are also limited to the websites you visit and do not automatically integrate with your mobile apps.
- If you need access to and/or training for *Passbolt*, you may contact us at *techsupport@upou.edu.ph*

Enable MFA(Multi-Factor Authentication)

MFA adds an extra layer of security to your accounts..

The most common application of this is **two-factor authentication** (2FA), which requires two factors of authentication to log in: **something you know** (such as a password or PIN) and **something you have** (such as a smartphone, card, or key). For example, an implementation of 2FA may require you to enter a security code from your phone in addition to your password when you log in.

By enabling this, no one can access your account unless they have **both** of your factors of authentication**.** Attackers cannot do anything even if they have your password, as long as you protect your phone, and vice versa.

Securing your Devices

Attackers don't stop at the office, so security shouldn't either.

Desktop/Laptop Security

It is important to secure all devices, both personal and professional, especially when you are at home. Attackers are constantly looking for new ways to exploit vulnerabilities, and your personal devices and accounts are a prime target.

- **Check if Windows Defender is enabled.** *Windows Defender* is a built-in antivirus program that can help protect your computer from malware.
- **Check if your computer's Windows Operating System (OS) is licensed.** A *licensed OS* is more secure than an unlicensed OS because it receives regular security updates.
- **Enable and always run Windows Update to fix vulnerabilities and ensure maximum security.** *Windows Update* is a service that provides security updates for your Windows OS and other software applications.

- **If already available and installed, enable your antivirus.** If you do not have an antivirus program installed, we recommend downloading a reputable free version, such as *Kaspersky*.

Mobile Phone Security

- Following our secure password standards, **use a strong password or PIN** to lock your phone. This is your first line of defense against unauthorized access.
- **Biometrics** are a **complex** security topic. They can be very strong, but they are also very weak if compromised. Note that once compromised, biometrics *cannot be replaced*. Some biometric detection systems can also be set **too low**, resulting in **false positives**. *Use biometrics at your own risk.*
- **Keep your phone and its operating systems up to date.** Software updates often include security patches that can help protect your device from known vulnerabilities.
- **Only download apps from trusted sources and keep them up to date.** The **official app stores** for your phone's operating system(such as **Google Play Store** or the **Apple App Store**) are the safest places to download apps.
- **Uninstall** apps you are not using.
- **Regularly search the official app stores for the apps you have installed.** If an app has been removed from the app store, immediately uninstall them. Google and Apple check for malicious apps and ban them if found to be dangerous.
- **Be careful about what permissions you grant to apps.** Though not always malicious, always be wary if the app requests access to your files, camera, photos, and contacts. An example of a red flag is when a notepad app requests permission to access your camera and location.
- **Review** your current permissions.
- **Use a mobile security app**. There are many free and reliable apps such as Bitdefender, Kaspersky, and Avast.
- **To protect against shoulder surfing and account resets, block the message contents of your lock screen notifications and only allow the app name to be displayed.** This will also prevent hackers from accessing your OTP without unlocking your phone, even if they steal it.
- **Backup your phone data**. In case your phone is lost, stolen, or damaged, it's important to have a backup of your data. It is advisable to back up your data to a reputable cloud storage service.

Note:

We will be procuring security solutions and providing licenses to everyone soon. In the meantime, please follow these steps to secure your devices and data.

We're here to help if you have any questions or need assistance with these technical steps.

Cybersecurity Awareness and Preparedness

Threat actors can use compromised accounts, even personal ones, to attack our systems.

- **Be critical and skeptical.** Even if the sender's address looks legitimate, be critical and skeptical of any email or message that seems off.
- **Verify the sender's identity by calling them or messaging** them through a different channel, especially if you are dealing with sensitive transactions.
- **Stay informed and educated about how threat actors operate today. Beware social engineering attacks** such as **phishing**. They are a common way for attackers to steal personal information and account credentials.
- **Your account credentials are meant only for you.** Never share them with anyone, under any circumstances, not even family, friends, or trusted and seemingly legitimate companies or organizations.
- **When using public/free WIFI, never shop online or do any other sensitive transaction** that uses your Personally Identifiable Information***(PII)*** and credentials. Attackers usually deploy "**rogue**" WIFI access points that mimic the actual access points. For example, assume that the NAIA airport terminal has WIFI access points called *"NAIA Wifi 1"* and *"NAIA Wifi 2"* attackers may deploy an access point with the name *"NAIA Wifi 3"*. Once a user connects to their fake access point, the attackers will be able to listen in on any and every network activity you do, similar to wiretapping on phone lines, putting your sensitive information at risk. (see "*Man-in-the-middle attacks*")

Beware Social Engineering Attacks

- **Verify all emails and links, even from trusted sources.** Scammers often impersonate well-known companies and organizations, so be careful about clicking on links or opening attachments without verifying the sender. You may verify by calling, messaging, or asking through a different channel.
- **Beware of fake accounts.** You may receive these attacks via email, social media, or text message. Scammers may create fake accounts to pose as tech support representatives, customer service agents, or even your friends and family. If you receive a message from someone you don't know or trust, be wary of clicking on any links or providing any personal information.
- **Avoid downloading attachments from unexpected senders.** Scammers may send emails or text messages with malicious attachments that can infect your devices with malware. If you receive an attachment from someone you don't know or trust, do not download it.
- **Be wary of ads that promise free stuff or too-good-to-be-true deals.** Scammers often use ads to lure people into giving them money or personal information. If you see an ad that seems too good to be true, it probably is. **They can also be used to make people download malicious files or software.**
- **If an ad or message elicits strong emotions like fear, urgency, pity, panic, or excitement, STOP.** Scammers often try to manipulate people into acting quickly without thinking. If you feel pressured to act right away, it's a red flag.

Workplace Best Practices

- **Avoid connecting personal USBs/drives to office workstations.** USB drives can be infected with malware, which can spread to the office network if you connect them to your workstation.
- **Do not run any installation files or executables downloaded from file sharing sites** such as Google Drive, social media, or email attachments. These files may be infected with malware.
- **Instead, install only approved applications and work productivity tools downloaded from trusted sources**. If you are unsure whether an application is approved, *ask us at ICTDO* .
- **Apply the principle of "Need To Know"**. Be careful about what information you share with your colleagues**.** Only share sensitive information with colleagues who have a need to know.
- **Report any suspicious activity to ICTDO immediately.** If you see anything suspicious, such as an unusual email or a strange file on your computer, report it to ICTDO*(techsupport@upou.edu.ph)* right away.