UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

OHCHR digital security tips series for human rights defenders in South-East Asia

3 Protecting your information "at rest" or in storage (login access)

Information "at rest" is information that resides in a device such as your hard disk, phone, laptop, memory stick, cloud storage (servers). All our information is stored in one or more such devices and places. Ensuring you protect your devices when you login helps to protect your data. To protect your login access, remember the following:

DO

It is recommended to enable 2Factor/ multi-Factor authentication (2FA/MFA) for your online accounts. 2FA/MFA means that you need to first enter the password – your first verification – followed by a code sent via SMS or a prompt through an authentication app, which is your second verification. This means a hacker would need to overcome two authentication steps to break into your account. Your 2FA (2 Factor Authentication) should be something that ONLY YOU have. This can be by either authentication apps or a hardware device.

It is recommended to protect your password
Create a strong password with mixed alphanumeric characters (more than 16 characters). You may use a sentence to decrease the risk of forgetting the password you have created. A strong password protects your account with attempts of guessing attacks and dictionary attacks.

It is recommended to use passphrases
Use a randomly generated phrase and combine it with special characters to create a strong passphrase. Passphrases may add more characters to your password, and it is easier to remember too. If you combine it with special characters, the password is made stronger e.g., &*?$#@!

It is recommended to use password managers (e.g., KeePassXC,[1] StrongBox,[2] and Password Safe.[3]) To create non-dictionary-based passwords and in keeping your passwords. Strong passwords are those that are not based on a dictionary word. Password generators allow you to create randomly mixed characters and special characters to generate a strong and tough to crack password.

2FA/MFA can be enabled using authentication apps (e.g., Aegis[4] and Ravio OTP[5]) or physical keys. Avoid enabling your 2FA/FMA via SMS as SIM cards can be spoofed. Download and keep safe your backup codes. Depending on your service's account recovery feature, backup codes can be the last resort for accessing your account.

It is recommended to use privacy screen protectors when using your computer in public places. Privacy screen protectors is a thin film that darkens areas of your computer screen, only allowing one area of visibility – which is your visibility. This can prevent people from prying eyes or simply people sitting beside you looking at your screen! Using cloth to cover your "keystrokes" in public can prevent anyone from knowing its letters and characters. These shoulder surfers can record your keystrokes with a smartphone and then slowly replay to "decipher" your password.

Consider using non-work email in signing up for online services or social media platforms. Using non-work email for subscription to online services or social media protects you and your organization from profiling and information leaks.

It is recommended to secure your organization's/ team's password-sharing practice, for example, credentials for your organization's Facebook page or website administration. If you do share passwords, do so by sharing a password protected encrypted database created by a password manager (e.g., KeePassXC).

IMPORTANT NOTE: Your password manager "keys" or master password, and your authenticator apps must be protected and backed up (ideally in an encrypted container using VeraCrypt) and, as there are no password recovery options for your authenticator applications. The loss of your 2FA/MFA solution leads to your inability to access your email accounts and other subscriptions. As a last resort, download your backup codes and keep them secure in your password manager.

DON'T

It is not recommended to use weak or common PASSWORDS e.g., your pet's name, relatives, cities, workplace, birthdate, or any names or words relevant to you as these can be gleaned off your social media. Cybercriminals may gather such information about you on social media and access your accounts using automated login tools.

It is not recommended keeping passwords on a notepad, word document or excel spreadsheet. These documents are NOT encrypted and lack security protection.

It is not recommended to re-use old passwords or use the same password for multiple accounts. In hacking practice, the first password that a cyber-criminal discovers will be used to login to all accounts of the target - https://haveibeenpwned.com.

It is not recommended to use sticky notes to store your passwords. These are easy to find and have no encryption nor security.

It is not recommended to use your organization/work email to personal subscriptions to online services due to the risk of information leaking or data breaches. Using your organization's email to subscribe for personal use may expose your organization to attacks. If you use the same password to log in to the organization's email as the password for your subscription, this will increase the risk of exposure since some historical data breaches include both the usernames and passwords of the accounts compromised.

It is not recommended to share passwords. Passwords for **personal accounts** should never be shared with others.

It is not recommended to include an obvious hint to your passwords. Hints are quite easy to identify, such as if you put your dog's name on your password, or your spouse, your kids or anything that is common to you.

TIPS!

Secret questions are there for recovery purposes, however, these questions are straightforward, and are often related to you. Attackers may attempt to ask you these questions unsuspectingly, or it could already be available online on your social media. If you are using password manager and there is no way for you to bypass the security questions then a good approach is to record the selected questions in the password manager and then generate a very long (30+ characters) password in the password manager as the answer to that question. That way nobody can deduct the answers to those questions from public information and you have the answers stored in the password manager, in case you'll need them someday.

How would I know if my security has been breached?

Sign-in to breach notification services exist e.g., HaveIbeenPwned[6] or Dehashed[7] to get a notification if your account has been part of a data breach. Breach notification services alert you of any news or data leak that includes your account.
Make sure you subscribe to one, so in the future, you will know if your account has been part of any known data breach.

[1] https://keepassxc.org
[2] https://strongboxsafe.com
[3] https://pwsafe.org
[4] https://getaegis.app/
[5] https://raivo-otp.com/
[6] https://haveibeenpwned.com
[7] https://www.dehashed.com