PASSWORD SAFETY

techsafety.org.au

Please note that the contents of this document should not be regarded as legal advice. The information contained within is relevant as of March 2025.

Passwords serve as a first line of defence to protect our sensitive data and information, the vast majority of hacking-related leaks such as data breaches and identity theft are due to weak or stolen passwords. Below we've listed some key tips to increasing your password security.

An abusive partner or ex-partner often knows intimate details about a survivor, and this can make their passwords less secure which puts their digital data at risk. An abuser may easily guess a survivor's passwords, or they may actively seek them out or obtain them by coercion. Additionally, when the details of data breaches and word lists are published online it makes it even easier for abusers to track down survivors' passwords.

An abuser's behaviour may escalate when they discover they can no longer access your devices or data, therefore if you suspect your online activities are being monitored, create a Safety Plan before changing your passwords.

Before We Start: Prioritise Safety

It is important to acknowledge that for many survivors, using strong passwords isn't enough, and updating passwords can even be dangerous. If an abusive person regularly monitors devices and accounts, they may know that a password has been changed, and may be able to change the password themselves. In addition, abusive people can coerce or force survivors to share their passwords.

There isn't one "right" way to respond to an incident, only ways that do or don't fit your situation. What works for someone else may not work or be safe for you. Always prioritize safety and trust your instincts. Making changes will often alert the other person. They might force you to unlock your phone or share your passwords. They might become more abusive. In some situations, making changes could also erase evidence. You may find these safety steps useful:

- Use a safer device. If you think that someone is monitoring your phone or accounts, use a different device (such as a library computer or a friend's phone) and an

account that the person cannot access (and that they have not had access to in the past).
- Get more information. Navigating violence, abuse, and stalking can be difficult and dangerous. Advocates can help you figure out options and local resources and help you create a plan for your safety. You can contact a national helpline to be connected with local resources.

What makes a password less safe?

The intimate knowledge an abuser has about a survivor of domestic violence or stalking can put them in real danger. This is one reason why security is so important when online. These are some common password habits that are NOT considered to be safe or secure:

- Using common passwords, like '123456', 'admin' or 'password'
- Using names, birthdays, cities, countries or swear words in passwords
- Using the same password and email combination across numerous accounts
- Choosing answers to account security questions that an abuser may already know, or may be able to guess easily (e.g., mother's maiden name)

Good password habits

Use passphrases over using passwords

Since the beginning of password security we have been guided to creating strong passwords, incorporating numbers, capitalisation and symbols. This has led to over complicated passwords that are difficult to remember. Instead, best practice is to create a strong passphrase, these are longer and stronger than a standard password. Aim to make your passphrase with four or more random words totally to at least 14 characters. For example, a password 'Tr0ub4dor&3' would take 3 days to guess, whereas a passphrase 'correcthorsebatterystaple' would take 550 years!

Use different passwords for different accounts and avoid using cloud based password managers

That way, if someone discovers one of your passwords, they won't have access to *all* your accounts. Resist storing passwords in a cloud based password manager (e.g. Apple Passwords or Google Password manager), although it may be tempting as you do not have to manually log into each account, if someone has access to your cloud account that is linked to the password manager, then they will have access to all accounts associated.

Be strategic with your account security questions and answers

Those security questions that we use to recover locked accounts, such as "Where did you go to high school?" or "What's your mothers maiden name?", aren't private or secure if someone knows you intimately or can 'Google' the answers. There's no rule

that you have to be honest, so make up untruthful answers that you will remember but someone else won't be able to guess. Alternatively, create your own unique question, which is sometimes also an option.

Keep someone from cracking your password by testing it

It's not just someone who knows you intimately who can determine your passwords. Computer programs, or 'bots', offer a quick and easy way to crack passwords, and they find dictionary words much easier to decode. Try creating a mix of words and symbols or phrases instead, and make it long so it's more difficult to crack.

You can:

1) Check to see if your email address has been breached at 'have i been pwned?'

2) Test the strength of your password at 'how secure is my password':

3) Review and update recovery email addresses and phone numbers before enabling additional security steps such as 2-step verification or multi-factor authentication (MFA).

Keep accounts separate and resist using other accounts to log in

Online accounts may allow you to sign in using your login details for other main accounts, such as Facebook, Google or iCloud. Although convenient, if the password to one of those accounts is compromised, your other accounts could be accessed easily.

KISS - Keep It Simple, Sunshine!

This may sound like a contradiction, but if you make your password too complex, you'll likely forget it and get locked out of your account.

If you must write down your passwords, be cautious about where you keep them. Instead of writing them in full, use a hint to remind you. Sticking them on a Post-It note on your monitor or taking a photo on your smartphone are not recommended practices. You also want to refrain from keeping them somewhere they could easily be found.

Take extra care if you choose to share

If you opt to share a password with someone voluntarily, ensure this person is trustworthy. Most of our online accounts hold a significant amount of personal information about us, and you might not want it shared with others.

Change your password when required

If you think someone knows your password, changing it will keep them from further accessing your accounts. Some accounts may even prompt you to update your password after a certain period of time. If, however, you change your passwords often yet an abuser still seems to be able to access your accounts, then we recommend you refer to the handouts referenced in this resource to assist you in securing your tech.

Uncheck the “Remember me” or “Keep me logged in” feature.

While these features save time and effort when accessing your accounts, it makes it easy for someone who’s using the same computer or device to also gain access. Be especially careful to uncheck those features if you’re logging into an account on someone else’s device or on a public computer.

Always remember to log off

Computers and devices are smart and are designed to make life easier. Therefore, your account may remain open for days if you don’t log off, potentially allowing others access to your data. Some accounts, such as Facebook and Gmail, allow you to see other places where you’re logged in, and you can then opt to deactivate those log-ins.

Delete the account or app

If you’re using an app on a smart device that doesn’t allow you to log off, you might want to consider deleting it. This is an additional hassle so consider the sensitivity of the information in that account versus the risk of someone else accessing that information.

When remembering passwords can be hard

Often women have a lot going on in their heads that can make remembering passwords difficult. That may be related to things like trauma, sleep deprivation, stress or depression. This is understandable and we have some ideas below that may help.

Suggestions for making passphrases easier to remember but harder to crack

Choose four things

Create a passphrase with four different things that are not related. Try listing them in alphabetical order to help you remember their order e.g., ‘coconutElephantNetballMicroscope’.

Write a sentence

Write a sentence and misspell words or use a non-English language for some words in the phrase, e,g., ‘MifavouriteactorisNicoleKiiidman’.

Consider using an external password Manager or Password Vault

These tools can store your passwords in one secure place and can also generate strong and unique passwords for you. If safe to do so, external password managers (those that are not linked to cloud accounts) can be a very useful tool for survivors. We recommend researching reputable tech sites to select one that you feel is right for you. Many offer free subscriptions at the base level - all that is needed is one rock-solid password to ‘lock’ the vault and all of your other passwords within it! Ensure this is linked to a secure email address and the recovery details are accurate. If you are using an external

password manager, it is best practice to keep this to yourself and not share with anyone.

Acknowledgement

This handout has been created by Wesnet under licence from the National Network to End Domestic Violence.