Domestic violence can make password safety more complicated

An abusive partner or ex-partner often knows much more about a survivor than others, and this can put our personal information stored in accounts and devices at risk. Sometimes an abusive person may coerce a survivor to share passwords or may even be able to guess them.

It may be important to create a safety plan before changing your passwords in case an abuser is monitoring you in other ways or may become more abusive if they cannot access your information in the same way.

What makes a password less safe?

For someone experiencing violence against women like domestic violence or stalking, often it is an abuser's intimate knowledge about a survivor. These are some common password habits that are NOT safe:

- using common passwords, like 'ABC123' or 'password,'
- using your own, childrens' or pets' names or birthdays in passwords,
- using the same passwords for all accounts,
- answering backup questions with answers that an abuser may know or be able to guess (like your mother's maiden name or your favourite colour).

Good password habits

Use different passwords for different accounts - avoid using 'keychains'

That way, if someone discovers one of your passwords, they won't have access to all your accounts. Resist using keychains via your browser (e.g. Safari or Google Chrome) to store your passwords. These are little messages that you may see at the top of your browser that ask if you would like the browser to store your password. But do consider using a password manager (see below).

Be strategic with your secret questions and answers

Those secret questions aren't really secret. Someone who knows you (or someone who can Google) will be able to guess where you went to high school or your favourite colour. There's no rule that you have to be honest when answering those secret questions so make things up that you will remember but someone else can't guess, or make use of the option to create your own secret question which is sometimes provided.

Keep someone from cracking your password by testing it

It's not just someone who knows you who can guess your password. Computer programs can easily and quickly crack passwords. Words that come out of a dictionary are easier

for these programs to decode. Create a mix of words and symbols or phrases, 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?', then 2) test your password at 'how secure is my password' to see how easy it would be for a password-cracking software to guess. You'll be surprised at what you learn! For example, "blahblah" would only take 5 seconds for a program to crack, but "blahblahblahblah" would take 35 THOUSAND years!!! (Now don't just go and use that one - figure one out for yourself!)

Finally, ensure any recovery email addresses and phone numbers are current and your own before enabling 2-step verification or multi-factor authentication as an additional security step.

Keep accounts separate

Sometimes services like Facebook or Google give you the option to sign into other accounts using the accounts you already have with them. This can be convenient, but if someone gets the password to your Facebook, for example, they may be able to access many other accounts easily.

Keep it simple

I know, this advice contradicts the previous advice. But if you make your password too complex or difficult, chances are you'll forget it and get locked out of your account. Your password should be a phrase or words with numbers mixed in that you can easily memorize. If you must write down your password, be cautious about where you keep it.

Sticking it underneath your keyboard or on your monitor isn't the most secure place. You also don't want to keep it somewhere where someone else could easily find it by going through your belongings. Instead of writing down the password itself, write down a hint so you can remember what it was.

Share your password with no one

Before you share a password, make sure this person is someone you can trust, now and in the future. 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 often

If you think someone knows your password, changing it will keep them from further access to your accounts. It's also good practice to get in the habit of changing your passwords every now and then.

Uncheck the "remember me" or "keep me logged in" feature.

While these features make it super easy to access accounts, it also makes it easy for someone who's using the same computer or device to access those accounts. Be

especially careful to uncheck those features if you're logging into an account on someone else's device or a public computer.

Always remember to log off

Computers and devices are smart—sometimes too smart and your account may remain open for days if you don't log off, allowing others access. Some accounts, such as Facebook and Gmail, allow you to see other places where you've logged in and 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 the app or account. This is an additional hassle but weigh the sensitivity of the information in that account and the risk of someone else accessing that information.

When remembering passwords can be hard

Often women have way more on our minds than remembering a lot of passwords. Sometimes that can be related to things like trauma, sleep deprivation, stress or depression. It is not your fault if you find yourself forgetting passwords. We have some ideas that may help.

Suggestions for making passwords easier to remember

Choose four things

Create a password with four different things that are not related. Try listing them in alphabetical order to help you remember their order. (Example: coconutelephantnetballmicroscope)

Write a sentence

Write a sentence and misspell or use a non-English language for some of the words. (Example: MifavouriteactorisNicoleKiiidman).

Consider using a password manager or vault

These can not only store your passwords in one secure area, they can also generate strong and unique passwords so that you don't have to put the energy into doing that yourself. We recommend researching reputable tech sites to select a password manager that you feel is right for you. Many of these offer free subscriptions at base level - all that is needed is one rock-solid password to 'lock' the vault and all of your other passwords within it.

Additional Resources

Read Documentation Tips for Survivors of Technology Abuse and Stalking.
Learn more about creating a Technology Safety Plan.
Read Dealing with harassing calls, texts, and messages.

Consider using our Stalking and Technology-Facilitated Abuse Log.
Learn about Mobile spyware.
Learn about Securing Your Home Wi-Fi Network/Router.
View our video on how to take a screenshot on a computer and smartphone.
Read about Increasing Privacy and Security when Using Google.