



PASSWORDS: SIMPLE WAYS TO INCREASE YOUR SECURITY



When we think of how people's identity is verified, we usually think of documents such as a driver's license, tax file number, or passport. These days, passwords, passcodes, and secret questions are the new set of information used to verify that we are who we say we are. Unfortunately, we often approach passwords too casually and don't realize how important they are to securing our privacy and identity.

Below are some things to consider when creating or using a password:

Use a password that is hard for someone else to guess. Don't use a common word or phrase or something that someone you know could guess, such as the name of your pet.

Use different passwords for different accounts. If you use the same password, once someone discovers it, they'll have access to all your accounts.

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.

The best passwords are longer than 8 characters and contain numbers and symbols. 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 test your password at www.howsecureismypassword.net 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 52 seconds for a program to crack, but "blahblahblahblah" would take 345 THOUSAND years!!! (Now don't just go and use that one; figure one out your own!)

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. You might share food with someone you love, but your password? Think about it first and 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.

Passwords: Simple ways to increase your security

www.techsafety.org.au (or www.wesnet.org.au/safetynet) • ☎1-800-WESNET • ✉ [techsafety\[at\]wesnet.org.au](mailto:techsafety[at]wesnet.org.au)

© 2016 WESNET Adapted with permission from the National Network to End Domestic Violence, Safety Net Project under license

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.