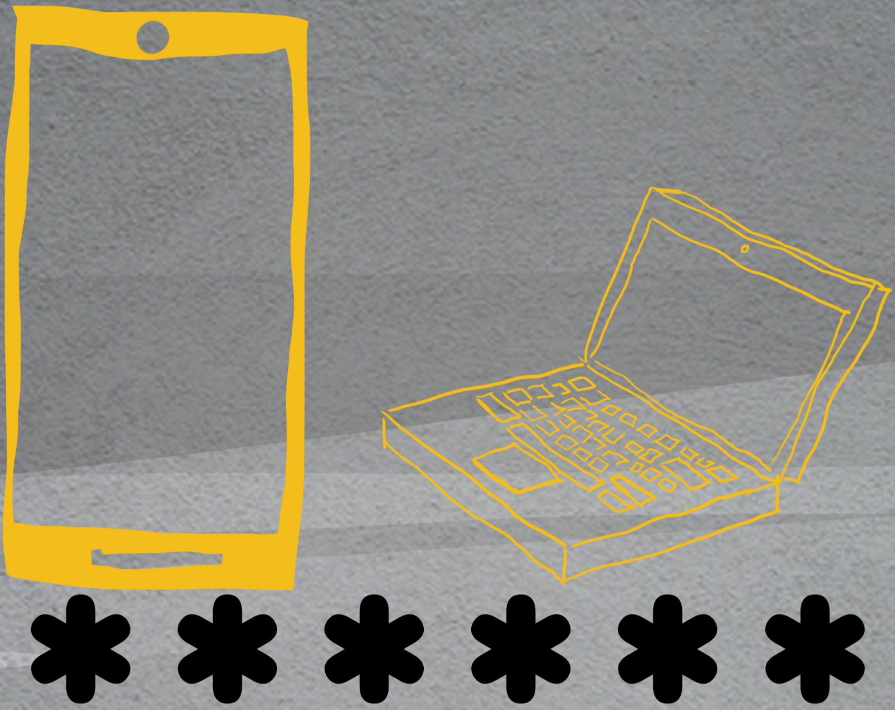
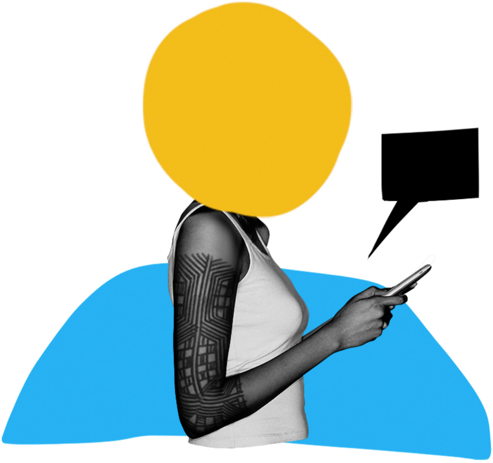


secure passwords

[Passwords are key to our personal security on and off the internet.]

We use passwords to access our bank accounts, make phone calls or send messages on social networks. We use passwords to shop, access content, communicate and even to access physical locations. As digital data continues to expand at rapid rates, consider how many passwords we currently have? Dozens? Hundreds? Maybe thousands of password. In this zine, we present some tips for creating and keeping your passwords and your data safe.



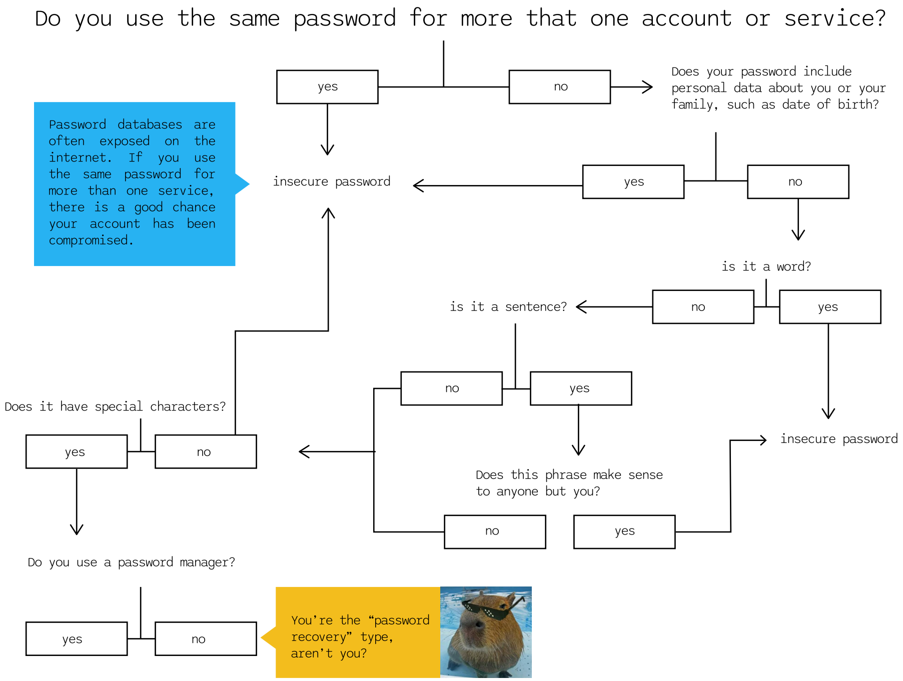
SECURE**PASSWORDS**

S3CuR3-p4s5w0Rds

Password databases are frequently exposed on the internet. If you use the same password for more than one service, it is very likely that your accounts could be compromised. Because of the increasing exposure of our personal data, your personal information is not difficult to find online.

To create a more secure password, it is important to **not to use personal data** (such as names or birthdates, even if they belong to your family/friends).

Increasingly, brute-force attacks are used to capture your passwords. These internet attacks test every possible combination of characters until they manage to find your password combination. The automated attack uses all available dictionaries of possible passwords, starting with the simplest combinations. So, if your password is made up only of numbers or just one word, the possibility of it being discovered by a brute force attack is very high.



Do you use the same password for more that one account or service?

yes → insecure password

no → Does your password include personal data about you or your family, such as date of birth?

yes → insecure password

no → is it a word?

yes → insecure password

no → is it a sentence?

yes → Does this phrase make sense to anyone but you?

yes → insecure password

no → Does it have special characters?

Does it have special characters?

no → insecure password

yes → Do you use a password manager?

yes

no

Password databases are often exposed on the internet. If you use the same password for more than one service, there is a good chance your account has been compromised.

You're the "password recovery" type, aren't you?

Combining multiple words and numbers in a sentence makes your password more secure because it is more complex. Because of the increased complexity level, it is more difficult for hacking programs to deal with. You can increase the complexity and make your password more secure when you **add special characters** such as a comma or a period to your password.

Sharing passwords adds a layer of vulnerability to your security. However, if you must share a password with one person or a group of people, make sure this password is not used for any other service or account.

{ Secure password tips }

Use long passwords, preferably a phrase (pass-phrase) that has no personal data. A tip on how to create a random password is to observe your environment, for example: **2windowsOnthestreet,1manWearsOrange.**
Adding special characters and using upper and lower case letters also increases the security of your password.

If you have many accounts on the internet, and think it will be too hard to remember your passwords, you can use a password manager! The password manager software protects and encrypts your passwords - all you need to remember is one password to use it! Also, the password manager can create complex passwords for you. We recommend using KeepassXC and Bitwarden (remember that for a program to be secure it must always be up-to-date).

Frequently changing your passwords is an important security step: we don't always know if our data has been exposed in a database leak. That's why it's important to add this habit to your routine!

- Check your password strength:
  https://howsecureismypassword.net

- Check to see if your password was hacked (and if so, be sure to update it):
  https://haveibeenpwned.com

- References:
  A Guia de Segurança da Informação: escoladeativismo.org.br

- PT Text Review:
  Bruno R Mundim

- English translation:
  Brenna Wolf-Monteiro

- Technical Review:
  Gustavo Gus

- Made by:
  acaravana.tech