PHISHX

HOW TO KEEP YOUR ACCESSS SECURE

Good passwords are the beginning

Much of our security begins when we create and keep passwords that are safe and secure:

• A strong password should be closer to a phrase than to a word, and its length should be as long as possible.

• A strong password must be a combination of characters, uppercase letters, lowercase letters, and numbers.

• First, write a random password and then, letter by letter, keep changing the type of each character.

• Passwords are individual, temporary, and unique, do not repeat passwords or share with anyone.

• To keep your online identity safe and secure, you need to continue changing your passwords at regular intervals.

Don't have that in your password

To have a secure password, avoid passwords with:

• Simple words: any word or combination that can be found in a dictionary.

• Small variations: be careful when using very slight variations of simple words or names.

• Context: Don't use passwords that reflect something about you, such as the names of people or places you know.

• Keyboard sequence: forget about using a sequence based on letters next to the keyboard.

• Similar or the same password: do not keep the same password for all your accounts.

Update your profile

Always check that your contact information is up to date, so that all service providers can contact you, through notifications or reactivation processes, with you quickly, safely, and efficiently.

It is essential that you check your contact information periodically and keep it updated if you make changes to your address, phone, or email.

When you receive a notification of new access that you have not done, go to your provider's portal to understand what happened and, if necessary, update your password and other settings.

phishx.io

PHISHX

HOW TO KEEP YOUR ACCESSS SECURE

Manage your passwords

As we depend on our calendar to remember birthdays and contacts, use a password manager on your devices to keep your complex passwords even more secure.

In addition to storing your passwords, these apps can help you create strong random passwords according to security tips and standards, as well as remind you to update them often.

Another point is to have subscription to find if any personal account or password has been discovered, or if there were problems with any service you use, telling that you must change your passwords and accesses.

Multiple Factors

Authentication must be multifactorial, for example when we use two factors (2FA) or more (MFA) to increase the security of our accesses).

You must enable multi-factor authentication for all applications, services, and systems that you use in your work and personal life.

Factors can include the following:

- Information that only you know: your unique and secure password.
- Something you own: a code generator app on your phone.
- Something you are: your face or fingerprint.
- Where you are: your location via a GPS or your network access point.

Don't stay logged in

As important as securely accessing, it is also ending your access when you are no longer using it, exiting the application or system.

When using a shared device, remember to sign out of your accounts and avoid checking the "Keep me connected" box when logging in.

If you are away from your device, but will return, lock the screen so that no one can access the data without performing secure authentication.

phishx.io