

Silent access to the main door

A STOLEN PASSWORD IS WORTH MORE THAN AN EXPLOIT

And it could be the start of a whole disaster.

BEST PRACTICES FOR STRENGTHENING YOUR PASSWORDS

- An email arrives:
“Your session has expired. Check here.”
- Without thinking too much, you click.
- Enter your password.
- You continue with your day.

But someone else too.



“I NEED VERY SIMPLE PASSWORDS”

“IT'S OKAY IF MY PASSWORDS ARE VERY SHORT”

“SOMETIMES I USE THE SAME ONES FOR DIFFERENT ACCOUNTS”

¿HAS THIS HAPPENED TO YOU?

You don't see anything strange, there are no alerts, everything seems normal.



The access you saw was legitimate, there's nothing to worry about.



You go on with your day, your files remain intact.



¿HOW TO STRENGTHEN YOUR PASSWORDS?

✓ Make them long, not just complicated; at least 18 characters. The longer, the more secure.

✓ Never share your credentials; no legitimate company will ever ask for your password by mail, message or call.

✓ Do not reuse passwords; if you use the same password on multiple sites, if one is leaked, they are all exposed.



* * * *

A strong password isn't an exaggeration, it's prevention, because protecting your password is protecting your digital identity.

#CyberSecurityAwareness