WORLD PASSWORD DAY

neoRhino
IT SOLUTIONS

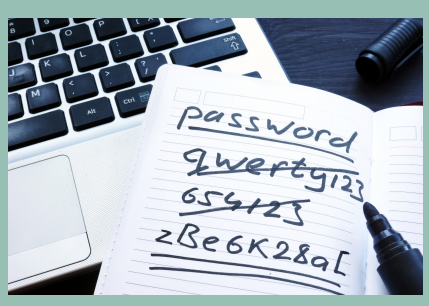
To protect your online accounts from being hackable, it's about making unique, strong passwords for EVERY login. Keeping up with multiple passwords can be frustrating, especially with login requirements becoming more complex in today's landscape.

It's World Password Day! Question for you: **How Strong are YOUR Passwords?**

HERE ARE 5 THINGS TO NOT DO WHEN MAKING STRONG PASSWORDS.

DO NOT USE A SIMPLE CHARACTER SEQUENCE.

Some of the most used passwords are simple keyboard sequences such as "123456" or "qwerty." Even numerical sequences on your 10-key pad should be avoided as well, such as "7410" or "789456." Consider using passphrases instead.



DO NOT USE EASY, COMMON PHRASES.

We mentioned using passphrases but make sure they are not simple ones such as:
"iloveyou"
"darthmaul"
"mother"
"football"
Or even "houstontexans"

DO NOT USE ACTUAL NAMES, PLACES, OR RECOGNIZABLE THINGS.

You may think these are confidential pieces of information that only you know about, but you can never be too careful. Do not use recognizable things like pet names, high schools, birth dates, anniversaries, or even previous online handles.

DO NOT USE THE DEFAULT SIGN-UP PASSWORD

Some logins will provide a password for you but do not automatically require you to change it upon login. Always change these default passwords, such as a default Wi-Fi password when you get a new modem or router.

DO NOT USE THE SAME PASSWORDS FOR MULTIPLE LOGINS

You need unique passwords for **EVERY** login. Using the same passwords for multiple sites makes you vulnerable. If you are, once one website with your login is compromised, they are all compromised. Consider a Password Manager if you need help retaining multiple complex passwords.

(And PLEASE do not use sticky notes for your passwords!)

VISIT US AT WWW.NEORHINO.COM
281.779.4850

Our Security Awareness Team is here to keep you alert and protected.