

**WORLD  
PASSWORD  
DAY!**

# THE PROBLEM *with* PASSWORD REUSE

Passwords have long been considered a simple but effective way to protect equipment, data, and networks. As we continue to use more devices, applications, and systems, it can be next to impossible to keep track of our logins and passwords.

The loss of one password for one account can potentially cascade into the loss of multiple accounts. Hackers can quickly tie passwords to users and users to email addresses; potentially selling the obtained information on the dark web. Once that happens, your accounts can be reset by the hackers and fall under their control.

If a compromised password could result in significant damage in terms of identity theft, stolen money, or loss of sensitive or confidential information, then a strong unique password with a combination of mixed letters, numbers, and symbols is needed for that account.

## Follow these best practices:

- Avoid passwords that are easy to guess (e.g., your first name, birth year and children names)
- Create a random word or phrase with a mix of letters, numbers, and symbols
- Vary your passwords from application to application
- Do NOT write your passwords down, instead use a password manager that can be downloaded on your computer and/or mobile device
- Never share your passwords- not even with friends or family
- Change your passwords regularly every 60- 90 days

Every password reuse is another account compromised!

