## Week 1 Theme: Work, Teach and Learn from Anywhere

# Good Password Practices

## Password Tips to Remember

- ✓ Use a different password for each website, account or device
- ✓ Change defaults of factory passwords
- ✓ Avoid obvious choices, a reference someone else could guess, personal details or common words or expressions
- ✓ Use a strong password (8 characters or longer (is better), made up of lowercase letters, uppercase letters, numbers and special characters) or passphrase (at least 4 words and 15 characters in length)
- ✓ Check the strength of your password or passphrase using the "How Secure is my Password" online tool
- ✓ Protect your password and do not share it with anyone
- ✓ Check if the password you are using has been compromised using the "Have I been Pwned" online tool
- ✓ Enable multi-factor authentication whenever possible
- ✓ If you suspect an account or password may have been compromised, change it immediately
- ✓ Consider using a password manager to keep track of your passwords. Make sure to do your homework when selecting a password manager
- ✓ Only login from trusted sources

## What you need to know

There is a reason for the above tips. Don't be a victim to the following types of cyber attacks:

- When using weak passwords - **Brute Force**: Most common form of attack, where a hacker tries possible password combinations starting with the easiest-to-guess passwords.
- When using common words - **Dictionnary Attack**: Where a hacker cycles through common words.
- When using the same password on multiple accounts - **Credential Stuffing**: Where a hacker uses a list of stolen usernames and passwords in combination on various accounts, automatically trying over and over until a match is found.

*Created in collaboration with ECNO, participating members from OASBO ICT and the Ministry of Education for the K-12 Cyber Awareness Month 2020.*