CYBER SECURITY CHECKLIST

***

1. USE GOOD PASSWORD PRACTICE

- Make strong, unique passwords for all accounts. Good passwords are more than 8 characters, have a combination of letters, numbers, and special characters.
- Store your passwords safely. Don't write passwords down; use password mnemonics or an enterprise password manager to help you remember passwords.
- Update your passwords regularly.

2. BE EMAIL AWARE

Don't open suspicious emails.

The tell-tale signs of a malicious or fraudulent email:

- Mismatched URLs
- Misleading domain name
- Poor grammar and spelling
- Doctored or inferior-looking company logo or email template
- Requests for personal or financial information

3. REPORT THREATS

- If you open a malicious email of file, tell your IT security professional immediately.
- Report any suspicious behaviour, such as the unexpected use of certain computers or accessing of files, to your manager or security professional.

4. KEEP A TIDY DESKTOP

- Don't plug a USB or other device into your pc unless you know it's secure.
- Log out of a terminal before leaving it.
- Install software updates when requested. Updates often include security 'patches' that help to keep your computer safe.
- Avoid storing sensitive information directly on your computer's desktop (or other device), in a Word document, an Excel sheet, or other unencrypted files and folders.
- Don't leave sensitive documents on your desk and do not give information out over the phone.