

Follow these top tips to  
stay safe online!

## USE STRONG PASSWORDS...

**Make your passwords:**

**Long:** At least 16 characters

**Complex:** Use upper and lowercase letters, numbers and symbols

**Unique:** Use a different password for each account



## ...AND A PASSWORD MANAGER

**Password managers can**

- Store all your passwords
- Tell you when you have weak or re-used passwords
- Generate strong passwords for you
- Automatically fill logins into sites and apps

## TURN ON MULTIFACTOR AUTHENTICATION



It provides **extra security** by confirming your identity when logging into accounts, like entering a code texted to a phone or generated by an authenticator app.

## RECOGNIZE AND REPORT PHISHING

**Common signs of a phish include:**

- Urgent/alarming language
- Requests for personal or financial info
- Poor writing or misspellings
- Incorrect email addresses or links

**Spot a phish?** Report it, then delete it



## UPDATE YOUR SOFTWARE

Software updates ensure your devices are protected against the latest threats. Turn on the **automatic updates** in your device's or app's security settings!

