COMMUNITY CYBER SAFE · TAKE-HOME GUIDE

Lock It Down

Strong passwords, a password manager, and multi-factor authentication

Do this first: Secure your email account with multi-factor authentication. Whoever controls your email can reset every other account you own — so it's the most important one to protect.

1. Use passphrases, not passwords

- **Length beats complexity.** "purple-tractor-coffee-window" is stronger and easier to remember than "P@ss1!".
- **Never reuse a password.** One breached site shouldn't unlock the rest of your life.

2. Let a password manager do the remembering

- You memorize one strong master passphrase; it stores and fills in all the rest.
- Reputable managers keep everything encrypted — even the company can't read it.

3. Turn on multi-factor authentication (MFA)

- **What it is:** a second step after your password — a code or a tap in an app.
- **Why it matters:** a stolen password alone is no longer enough to get in.
- **Best option:** an authenticator app where offered, but any MFA beats none.

Your priority checklist

☐ Email — strong passphrase + MFA (do this today)

☐ Bank and financial accounts — MFA on

☐ Set up a password manager

☐ Replace any reused passwords on important accounts

☐ Social media accounts — MFA on

Community Cyber Safe — a complimentary program from Bullium Consulting · bullium.com/community-cyber-safe