LESSON 4

Passwords and Protecting Your Accounts

Quick reference — print this page and keep it nearby.

THREE THINGS TO SET UP ONCE

1. **Set up a password manager**
   It creates and stores a unique, long password for every account. You remember one main password; it handles the rest.
2. **Turn on two-factor authentication**
   2FA blocks more than 99% of automated account takeovers, and it’s free. Start with email, main social, and your bank or payment app.
3. **Pick the right 2FA method**
   Worst to best: text-message codes (can be intercepted), an authenticator app (the right default), a hardware key (strongest).
4. **Tighten your privacy settings**
   On the platforms you actually use: set accounts to private, turn off activity status, and pre-approve photo tags.
5. **Delete old accounts yearly**
   Every unused account is one more place your password can leak. Once a year, clear out the ones you don’t use.

IF YOU TAKE ONE THING FROM THIS LESSON

Turn on two-factor authentication on your email account tonight. If a scammer gets your email, they can reset everything else — lock that one down first.

TRY THIS TODAY Pick the platform you use most, open its privacy settings, and spend five minutes there. You’ll be safer than 90% of its users.