

MODULE 3 · WEEK 3 · LESSON 7

AI Safety Habits: Accounts, Devices and the Human Backup

Operational security for everyday AI users

WHAT YOU WILL BE ABLE TO DO

- Implement account and device hygiene for AI tools
- Maintain human-original backups of critical work
- Recognise AI-adjacent scams and phishing

LESSON CONTENT

Account and device hygiene

Unique password per AI account via a free password manager; two-factor authentication on your email first (it resets everything else); dedicated email for AI services; log out on shared devices; keep apps updated; beware 'AI' apps that are data-harvesters in disguise.

The human backup rule

Never let AI-held content be your only copy. Keep originals of documents, photos and prompts in your own storage. Services vanish and change terms; your portfolio must outlive any vendor.

AI-adjacent scams

Voice-clone kidnapping calls, AI-written phishing with perfect grammar, fake 'AI investment' schemes, and paid 'certificates' that certify nothing. Rules: verify unexpected urgent calls via a known number; no AI tool needs your ID or bank login; real courses show curriculum and assessment, like this one does.

KEY TERMS

2FA	Two-factor authentication: a second proof at login.
Password manager	Tool generating/storing unique passwords.
Vendor lock-in risk	Dependence on one service holding your only copies.
Voice-clone scam	Fraud using synthesised familiar voices.

HANDS-ON TASK

Hygiene sprint · Tools: Free password manager + your email settings

1. Enable 2FA on your primary email today.
2. Move AI accounts to a dedicated email; unique passwords.
3. Back up your PoE folder to your own storage (not just the AI tool).

KEY TAKEAWAYS

- ✓ Before you go, three takeaways from this lesson.
- ✓ One: Implement account and device hygiene for AI tools.
- ✓ Two: Maintain human-original backups of critical work.

- ✓ Three: Recognise AI-adjacent scams and phishing.
- ✓ And your hands-on task: hygiene sprint.
- ✓ Enable 2FA on your primary email today.
- ✓ When it is done, mark the lesson complete on your dashboard, keep the artifact for your portfolio, and step into the next lesson.
- ✓ I will see you there.

Watch the lesson video on your dashboard, complete the task, then mark the lesson complete. Your artifact belongs in your Portfolio of Evidence.