STRETCHLEARN · WORKBOOK

# Password Management & Digital Security Basics — Workbook

This workbook turns the course into a hands-on security setup you complete in a few focused sessions. You will inventory your accounts and rank them by risk, stand up a password manager, enable phishing-resistant 2FA on what matters, drill your phishing detection, and lock in a maintenance routine. Work one section per module, fill the worksheets, and run the checklists against your real accounts. By the end you will have a configured vault, 2FA on your tier-one accounts, and a tested recovery plan, all captured in the templates at the back.

## Mapping Your Risk and Priorities

Inventory your accounts, sort them into tiers, and find where you are exposed so your effort targets what matters most.

### Exercise: Run Your Personal Breach Check

Go to haveibeenpwned.com and enter each email address you use. Record which breaches appear and which accounts may share an exposed password. This is your starting risk picture; you will fix the worst items first.

• Which of your email addresses appear in known breaches, and how many breaches each?

• For any breached account, where else did you reuse that same password? List every site you can recall.

• Which single password, if stolen, would unlock the most other accounts of yours? Why?

### Worksheet: Account Inventory and Tiering

List your important accounts and assign each a tier. Tier 1 = can reset or seize everything else (email, password manager, phone carrier, primary bank, government and tax). Tier 2 = sensitive (secondary email, payment apps, cloud storage, identity-linked social, business tools). Tier 3 = everything else. Fix tier 1 first.

Account name and login URL

Email or username used

Tier (1, 2, or 3)

Current password unique? (yes/no)

2FA enabled? (none / SMS / app / hardware / passkey)

Recovery method set (email/phone/codes)

Action needed and target date

### Checklist: Crown-Jewel Identification Checklist

[ ] Identified my primary email as a tier-one crown-jewel account
[ ] Listed every account that uses that email for password resets
[ ] Identified my phone carrier account and whether it has an account PIN set
[ ] Flagged my primary bank and any government or tax logins as tier one
[ ] Confirmed my password manager itself is on the tier-one list once chosen

## Standing Up Your Password Manager

Choose a manager, create a strong master passphrase, migrate your logins, and replace reused passwords in priority order.

### Exercise: Generate a Diceware Master Passphrase

Create a six-word passphrase using the EFF Diceware word list (physical dice or the list's selection method), aiming for at least 77 bits of entropy. Write it on paper, store it securely, and type it daily this week to memorize it. Do not store it inside the vault it protects.

• What six random words make up your master passphrase, and where will the paper backup live?

• If using 1Password, where will you store your Secret Key and Emergency Kit PDF separately from the master password?

• On which devices have you installed the manager app and browser extension, and did the vault sync on each?

### Worksheet: Password Rotation Tracker

As you replace weak and reused passwords, log each one. Work top-down: tier one first, then any account flagged as breached, then tier two and three. Mark done only after you confirm a successful logout and login with the new password.

Account name

Tier

Old password reused elsewhere? (yes/no)

New password generated and saved? (yes/no)

New password length (target 16 to 20)

Login re-tested successfully? (yes/no)

Date completed

### Checklist: Manager Setup and Migration Checklist

[ ] Chose a manager (1Password, Bitwarden, or KeePassXC) and installed it on phone, computer, and browser
[ ] Created and memorized a six-word Diceware master passphrase, with a secure paper backup
[ ] Imported existing logins, then deleted the exported CSV and emptied the trash immediately
[ ] Turned off the browser's built-in password saving so the manager is the single source of truth

[ ] Ran the manager's audit (Watchtower or Reports) and started fixing reused, weak, and breached passwords by tier
[ ] Created separate vaults or folders for Personal, Business, and Finance

## Turning On Strong 2FA

Enable the strongest available second factor on each account, set up recovery codes, and add a backup hardware key.

### Exercise: Enable Hardware or App 2FA on Email First

Start with your primary email. In its security settings, enable the strongest method it offers (hardware key or passkey if available, otherwise an authenticator app). Save the recovery codes into your password manager, then log out and back in to confirm the second factor is requested.

• What is the strongest 2FA method your email provider offers, and did you enable it?

• Where did you store the email account recovery codes, and did you verify they are saved correctly?

• Did you set a carrier account PIN to defend against SIM swapping on your phone number?

### Worksheet: 2FA Enrollment and Recovery Log

For each tier-one and tier-two account, record the 2FA method you enabled, where the codes live, and whether a backup key is registered. Prefer hardware keys or passkeys for tier-one accounts and authenticator apps over SMS everywhere.

Account name

2FA method enabled (app / hardware key / passkey / SMS fallback)

Authenticator location (Authy / Microsoft Authenticator / in password manager)

Recovery codes saved? (yes/no) and where

Backup hardware key registered? (yes/no)

Passkey created? (yes/no)

Date completed

### Checklist: Phishing-Resistant 2FA Checklist

[ ] Enabled app-based or hardware 2FA (not SMS) on email, bank, and password manager
[ ] Saved per-account recovery codes into the password manager as secure notes
[ ] Enabled cloud backup or seed export in my authenticator app so a lost phone is not catastrophic
[ ] Bought and registered two hardware keys on tier-one accounts, keeping one as a safe backup
[ ] Created passkeys on the major accounts that support them, while keeping a strong password and 2FA as fallback
[ ] Set a PIN or passcode on my mobile carrier account to block SIM-swap attacks

# Spotting Threats and Staying Secure

Drill your phishing detection, harden your devices and business accounts, and lock in a maintenance and recovery routine.

## Exercise: Dissect Three Suspicious Messages

Find three real emails or texts from your spam or junk folder that ask you to log in, pay, or share information. Apply the inspection checklist to each: reveal the true sender address, preview the real link destination, and identify the urgency tactic. Decide for each whether it is phishing and why.

• For each message, what is the real sender address and the true destination domain of its main link?

• What specific urgency, fear, or reward tactic does each message use to make you act quickly?

• Which red flags appeared, and how would your password manager's autofill behavior have helped you catch the fake site?

## Worksheet: Device and Account Hardening Worksheet

Go device by device and account by account, confirming the core protections are in place. Complete this for each computer and phone you use, and for each tier-one account's recovery settings.

Device or account name

Strong passcode or password set? (yes/no)

Full-disk encryption on? (FileVault / BitLocker / device encryption)

Automatic OS and browser updates enabled? (yes/no)

Find My Device / remote wipe enabled? (yes/no)

Recovery email and phone reviewed and current? (yes/no)

Unknown connected apps or devices removed? (yes/no)

## Checklist: Business Account Offboarding Checklist

[ ] Moved team credentials into a business plan with shared vaults scoped by role (least privilege)
[ ] Enforced 2FA across the team and required hardware keys or passkeys for admin and financial accounts
[ ] Set a verification step for any change to vendor or payroll payment details to prevent business email compromise
[ ] When someone leaves: revoked vault access, reset shared passwords, and removed them from email and tools the same day
[ ] Separated duties so no single login can both initiate and approve a money transfer

## Checklist: Ongoing Maintenance Routine Checklist

[ ] Monthly: run the manager audit and fix any newly flagged reused, weak, or breached passwords (about 15 minutes)
[ ] Quarterly: review tier-one recovery settings, connected apps, active devices, and 2FA backups (about 30 minutes)
[ ] Annually: rotate the most critical passwords and re-read the recovery plan
[ ] Registered email addresses with Have I Been Pwned breach notifications

[ ] Tested at least one recovery path (such as a backup code) to confirm it works before it is needed
[ ] Set up emergency access or a legacy contact so a trusted person can reach critical accounts

## Your Action Plan

1. Run a Have I Been Pwned check on every email address and list which accounts are exposed.
2. Complete the account inventory and tier each account; mark your tier-one crown jewels.
3. Choose a password manager (1Password or Bitwarden), install it everywhere, and create a six-word Diceware master passphrase with a secure paper backup.
4. Import your logins, delete the exported CSV, turn off browser password saving, and run the built-in audit.
5. Replace reused and weak passwords in priority order using the Password Rotation Tracker, starting with tier one and any breached accounts.
6. Enable the strongest 2FA each tier-one account offers, starting with email, and save every recovery code into the vault.
7. Buy and register two hardware keys on tier-one accounts, and create passkeys where supported while keeping fallbacks.
8. Harden each device: strong passcode, full-disk encryption, auto-updates, auto-lock, and remote wipe.
9. Drill phishing detection on three real messages and set a personal rule to navigate to sites directly when in doubt.
10. Schedule the monthly, quarterly, and annual maintenance routine and test one recovery path today.