

You probably have more online accounts than you can remember. The forgotten ones still hold your **personal data, saved payment details, and old passwords.**

The 30-Minute Digital Life **Audit**

Free Starter: the first two audits from the Complete Edition. Find your forgotten accounts and your reused passwords in about 15 minutes, score your exposure, and know exactly what to fix first.

FREE STARTER · 5 PAGES

Tim O.

safepasswordgenerator.net

The Account Inventory

Minutes 0 to 8

You can't protect accounts you forgot you have. Attackers love the ones you forgot: same old password, no two-factor, nobody watching.

☐ List your Tier 1 accounts (the crown jewels).

Primary email, banking, phone carrier, Apple/Google ID, and anything with a saved card. Your email is the master key: whoever controls it can reset everything else.

☐ Search your inbox for the ones you forgot.

Search your email for "welcome to", "verify your email", and "your account has been created". Skim the results and add anything you still recognize. Give this five minutes, not twenty.

☐ Check your browser's saved password list.

Chrome: Settings > Passwords. Safari: Settings > Passwords. This is often the most complete record of your accounts that exists. Count the entries:

☐ Mark the dead ones.

Put an X next to anything you haven't used in over a year. You'll deal with these in Part 9. Don't delete anything yet.

☐ Star the money accounts.

Anything holding funds, cards, or credit: banks, PayPal, Venmo, Amazon, crypto exchanges. These get priority in every later step.

Reality check: expect to find at least a few accounts you'd completely forgotten existed. Every one of them is still running whatever password you gave it years ago.

The Password Check

Minutes 8 to 16

Reused passwords cause more account takeovers than any hack. One breached site leaks your password, and criminals try it everywhere else within hours. It's automated, and it works because surveys consistently find that a majority of people reuse passwords across accounts.^[1]

☐ **Check if your email has been breached.**

Go to haveibeenpwned.com and enter your main email addresses. Write down how many breaches each appears in:

☐ **Count your password reuse honestly.**

Look at your Tier 1 list. How many share a password with any other account, even a variation like adding "1" or "!"? Variations count as reuse. Attackers try those first.

☐ **Run your browser's built-in password checkup.**

Chrome: Settings > Passwords > Checkup. Safari: Passwords > Security Recommendations. It flags reused, weak, and breached passwords for free. Flagged count:

☐ **Change the worst offender right now.**

Whichever Tier 1 account has a reused or breached password, fix it before moving on. Use a generated password of 16+ random characters, not one you invent. Invented passwords follow patterns, and cracking tools know all the patterns.

☐ **Retire your "system".**

If your method is one base word plus the site name (hello, "Netflix2019!"), acknowledge it's a system a bored teenager could reverse-engineer. You don't have to fix everything today. You do have to stop creating new passwords this way.

The uncomfortable math: if you can remember all your passwords, they're weak. Human-memorable and machine-resistant are opposite properties. The fix is not a better memory, it's not needing one.

YOUR RESULTS

The Quick Exposure Score

Answer honestly; the score only means something if the answers are true. Points are penalties: higher means more exposed.

This score is a practical prioritization tool created for this workbook, not a standardized or statistically validated security-risk assessment.

QUESTION	POINTS
My primary email password is reused anywhere else	+5
My primary email has no two-factor authentication	+5
Any money account shares a password with another account	+4
My email appears in 3+ breaches on haveibeenpwned.com	+3
I use a "base word plus site name" password system	+3
I found 3+ accounts I forgot existed	+2

Your total: _____ / 22

12 to 22: Open Door

You're relying on luck, and luck is not a control. The +5 items are the emergency list: fix them this week.

6 to 11: Soft Target

Better than most. Your gaps are specific, listed above, and fixable in one more sitting.

0 to 5: Hard Target

Strong on the basics this starter measures. The Complete Edition checks the seven areas this version doesn't.

Whatever you scored: the two fixes with the highest impact per minute are 2FA on your primary email and a unique generated password for it. Everything else builds on that foundation.

KEEP GOING

You've audited 2 of 9 areas

The starter covers accounts and passwords, which are where most takeovers begin. The Complete Edition covers where they continue: your second factors, recovery paths, devices, browser, home network, and family.

☐ **The MFA Audit + a second-factor decision guide.**

Apps vs SMS vs keys vs passkeys, honestly ranked, plus the carrier PIN that blunts SIM-swapping.

☐ **The Recovery, Device, Browser, and Wi-Fi Audits.**

The back doors, the unlocked laptop, the forgotten extensions, and the router with the sticker password.

☐ **The Family Security Audit + shared credentials worksheet.**

Shared logins, ex-access, and phone-scam defenses for the people you love.

☐ **A breach response plan, printable worksheets, and the full 50-point scorecard.**

Plus a 10-minute triage version, a 6-month re-audit tracker, a glossary, and cited sources.

The Complete Edition is \$9

26 pages, nine audits, three worksheets, one score, free updates for the life of the edition, and a 14-day no-questions refund. It exists because articles don't get finished and checklists do.

Get the Complete Edition

Instant PDF download · safepasswordgenerator.net/digital-life-audit

And the recommendation the audit makes throughout: a password manager automates the slowest parts of what you just did. I currently recommend NordPass; compare alternatives before choosing, since the audit works the same whichever you pick.

[Try NordPass](#). Paid affiliate link: I may earn a commission if you purchase NordPass through this link, at no additional cost to you.