



Part of the **tech4me2** series



PC SAFETY MADE SIMPLE WORKBOOK



Practical steps you can implement today to
protect your identity, your assets, and your
peace of mind



JOHN CLITES

PC Safety Made Simple Workbook

This workbook is designed to help you apply what you learn in the PC Safety Made Simple program.

This program stands upon a tripod:

1. The book explains the concepts.
2. The companion videos demonstrate the process.
3. This workbook guides you in securing your own computer and data.

I recommend that after reading each chapter and watching any companion videos, you go to the workbook to complete the exercises in the corresponding workbook section before moving on to the next chapter. Using this approach, when you've completed the chapters, your security plan will already be implemented on your computer.

You should be able to complete some exercises, such as listing your key accounts, quite quickly. Others, such as replacing duplicate passwords, will likely take some time. Just take your time and tackle each step in turn before moving on to the next section.

Ready? If you've read Chapter 1, move on to the exercises on the next page.

Section 1 — Your Current Safety Snapshot

Before making any changes, it helps to understand your current setup and habits.

For each statement below, check the box if the statement is true for you—and be honest.

- ☐ I know which browser I use, and how to access its settings.
- ☐ My (primary) email account is password protected.
- ☐ I currently use antivirus protection—or I consider Windows Defender sufficient in my case.
- ☐ I currently use 2FA for my accounts where money changes hands.
- ☐ I regularly back up important files (to the cloud, an external drive, or both).
- ☐ I currently use a password manager.

What concerns me most about online safety right now?

As you proceed through the program, give special attention to discussion of these areas of concern, and make a plan to address them.

Section 2 — Updates & Built-In Protection

Watch the companion video before completing this section.

☒ Do This Now

Open Windows Update and confirm your system is current.

- ☐ I checked Windows Update.
- ☐ I installed available updates.
- ☐ I restarted my PC if needed.
- ☐ Automatic updates are enabled.
- ☐ I checked for Chrome updates.
- ☐ I opened Windows Security.
- ☐ I saw green checkmarks.
- ☐ I ran a Quick Scan.

Did anything surprise or confuse me?

Section 3 — Extra Protection Tools

This section helps clarify the difference between built-in protection and optional tools.

My current protection setup consists of:

Antivirus software:

VPN:

Cleanup or optimization tools:

Do This Now

If you frequently use public Wi-Fi, subscribe to a VPN service.

Going Forward:

Windows Security is sufficient for many people. If you decide additional protection would give you greater peace of mind, choose a well-known antivirus program and avoid installing unnecessary "optimization" tools.

Section 4 — Passwords & Account Protection

Watch the companion video before completing this section.

Passwords

In a minute, you'll update the passwords for a few key accounts. The goal at the moment is simply to understand the process involved in creating and updating your passwords, and to begin protecting your most important accounts right away.

Do This Now

Earlier, you were asked to list several of your important or sensitive accounts. Now select the top three to use in this exercise.

My three most important accounts are:

Log in and update the passwords for each of these three accounts.

Password Manager

- ☐ Installed or opened my password manager
- ☐ Ran Password Checkup.
- ☐ Saved one new password
- ☐ Used the password generator when creating login credentials
- ☐ Successfully logged in using Autofill

Two-Factor Authentication

For the three accounts that you listed above, now go back and verify that 2FA is set up for each. While the exact process will of course vary, typically you will go into your security or sign-in settings. Then follow the prompts.

Recovery Methods

Recovery methods help you regain access if you forget your password or lose your phone. While you're in your account's security settings, verify that your recovery email address and recovery phone number are current.

- ☐ I verified my recovery email address.
- ☐ I verified my recovery phone number.
- ☐ I updated outdated recovery information.

Check Your Progress

- ☐ I remembered to log out of each account completely.
- ☐ I enabled 2FA on at least one account.
- ☐ I tested Autofill using a password manager.
- ☐ I reviewed recovery methods for important accounts

Did I discover reused passwords?

Going Forward:

As you naturally log into accounts over time, continue replacing weak or reused passwords with stronger ones.

Section 5 — Browsing, Emails & Scams

Watch the companion video before completing this section.

This section focuses less on technology and more on slowing down and recognizing warning signs.

Common phishing warning signs include:

- ☐ Urgent language
- ☐ Unexpected attachments
- ☐ Requests for passwords or payment
- ☐ Strange website addresses
- ☐ Spelling or formatting problems
- ☐ Messages creating panic or pressure

☒ Do This Now

Review your browser extensions and remove any you no longer use or do not recognize.

Reflection:

What situations make me most likely to rush online?

Without looking back, write down as many phishing warning signs as you can remember.

Going Forward:

Pause before clicking links in emails or texts from anyone you do not know.

When possible, go directly to important websites yourself.

Section 6 — Home Wi-Fi & Public Networks

Your Wi-Fi network is your first line of defense against online threats. Review yours following these steps:

Step 1: Find Your Wi-Fi Network Name

Go into Settings > Network & internet > Wi-Fi > Show available networks.

Find the network that you use. Note that you may see several listed, such as your neighbors' network names.

My Home Wi-Fi Network Name:

Step 2: Find Your Wi-Fi Password

Still in Settings, click on Show available networks. Find yours and click on it, then click the Show button beside Wi-Fi network password and record it.

Alternatively, find your physical router and look for a label on it showing the network name and password. This label is typically either on the back or underside of the unit.

My Wi-Fi Password:

Note: If you can't locate your password using these steps, don't worry. Watch the companion video for additional methods.

Step 3: Confirm Your Network Is Password-Protected

You should have just confirmed that your network is password-protected

(although if you've checked the "Connect automatically" button, you won't have to enter it each time you access your Wi-Fi.)

⚠ If no password is required, your network is "Open" and it is not secure. Your network may be easily breached, and a strong password should be assigned right away.

Step 4: Check If You're Using the Default Password

If your Wi-Fi is password-protected, but the password was assigned by the ISP and never updated, you can increase your network's security by creating a password or passphrase.

Using public Wi-Fi:

Extra care should be exercised when using public Wi-Fi, even if it is password-protected. Follow this routine:

- ☐ Be sure that your VPN is turned on. (VPN really is a must when using public Wi-Fi.)
- ☐ In your browser, open an incognito session.
- ☐ Avoid logging into banking, credit card, or other financial websites.

If you must use a public computer:

- ☐ Open an incognito session.

- ☐ Absolutely avoid logging into financial or sensitive accounts.
- ☐ When finished, go into the browser menu and delete your browsing data..

Going Forward:

Avoid sensitive activities on unfamiliar public networks, which is simply never as secure as your home Wi-Fi.

Section 7 — Backup Planning & Protection

Watch the companion video before completing this section.

Important files I most want to protect:

Where are those files currently stored?

My chosen backup method:

☐ OneDrive or cloud backup

☐ External drive

☐ Both

Backup drive: _____

Cloud service: _____

☒ Do This Now

Turn on one backup method and verify that your files are actually being backed

up. Be sure to verify by spot-checking a few folders and a few files within those folders.

- ☐ I verified OneDrive is syncing.
- ☐ I created a manual backup.
- ☐ I confirmed files are accessible.

Going Forward:

Backups work best when important files are stored in a few organized folders such as Documents and Pictures.

If your files are scattered everywhere, consider gradually reorganizing them over time. The upcoming File Organization Action Guide will help with this process.

Section 8 — Banking, Shopping & Sensitive Activities

Earlier in this workbook, you identified some of your most important accounts.

Let's now focus specifically on accounts and activities involving financial or sensitive information.

Additional sensitive accounts to review:

- ☐ I avoid logging into sensitive accounts through email links.
- ☐ I understand the importance of HTTPS and avoid sites without the -S.
- ☐ I reviewed where payment information is stored.
- ☐ I created bookmarks for important financial websites (to ensure that I always return to the legitimate website).

Data Breaches

Even if you adhere religiously to best security practices, your data can still be exposed in a data breach of a site which stores your personal information. If you are notified that your data was or may have been exposed in a breach, do the following:

Data Breach Response Checklist:

- ☐ Go directly to the company website and log in, then:
 - ☐ Change your password, after first recording it. You'll need it in a moment.
 - ☐ Enable 2FA if it is not already.
- ☐ In Password Manager, search on the password you recorded above. If you find that it was reused on other websites, log into those and change the password there as well.
- ☐ Be on the alert for follow-up scams, which often follow notifications of data breaches.

Going Forward:

- ☐ Always use secure passwords or passphrases on banking or other sites where financial information might be exposed.
- ☐ Be sure that 2FA is activated on these same sites.
- ☐ Do not access financial accounts on public Wi-Fi unless using a VPN.
- ☐ If you must use a public Wi-Fi, do not access financial accounts. (You may be able to use your cell phone as a hotspot, which is much more secure.)

Section 9 — My Personal Safety Plan

You now have a secure online safety system. To maintain it, cultivate good habits, including:

- ☐ Keep updates enabled (and restart your PC regularly)
- ☐ Use strong passwords, even if you must...
- ☐ Use a password manager
- ☐ Enable 2FA, even if it seems a bit inconvenient at times
- ☐ Back up important files according to a schedule
- ☐ Avoid websites which do not begin with HTTPS
- ☐ Slow down before clicking
- ☐ Monitor important accounts periodically

Helpful reminders I may add to my calendar:

My Next Safety Improvements:

1.

2.

3.
