



Heirloom Software

The Idjits Guide to

Security Checks

Check a computer for who used it and what is on it.

Tidy up a computer the safe way - one easy step at a time.

Disclaimer and Hold Harmless Agreement

The Idjits Guide to Security Checks • October 2026 edition • Heirloom Software LLC

In plain words: This book is here to help you learn. We tried hard to get everything right, but we can make mistakes, and computers change. Save a copy of your important stuff before you try things. If something goes wrong, it is not our fault, and you agree not to blame or sue us. Kids: ask a grown-up before you install or change anything.

COPYRIGHT

Copyright © 2026 Heirloom Software LLC. All rights reserved. You may keep copies of this guide and print it for your own personal use. You may not resell it, share it publicly, or reproduce any part of it for others without written permission from Heirloom Software LLC.

TRADEMARKS

Product names, logos, and brands mentioned in this guide (including Microsoft, Windows, Linux, Ubuntu, Python, and the others named inside) are the property of their respective owners and are used only to identify their products. Heirloom Software LLC is not affiliated with, sponsored by, or endorsed by any of them, or by the publishers of any other book series.

DISCLAIMER

This guide is for general information and education only. It is provided "as is," without warranties of any kind, express or implied, including warranties of accuracy, completeness, merchantability, or fitness for a particular purpose. Software, websites, prices, and menus change often; the information was believed accurate in October 2026 but may be out of date or incorrect when you read it. Nothing in this guide is professional, legal, financial, or security advice. For important systems or data, consult a qualified professional.

YOUR RESPONSIBILITY

Installing operating systems, changing settings, typing commands, and working with computer hardware can erase data, make a computer unable to start, void warranties, or expose a computer or network to security risks. **Back up your data before you follow any instructions in this guide.** You alone decide whether to follow them, and you do so at your own risk. Always follow the manufacturer's and software maker's own instructions where they differ from this guide.

LIMITATION OF LIABILITY

To the fullest extent permitted by law, Heirloom Software LLC and its owners, authors, employees, and agents will not be liable for any direct, indirect, incidental, special, consequential, or punitive damages, or for any loss of data, profits, use, equipment, or business, arising out of or related to this guide or your use of it, even if advised of the possibility of such damages. If any liability is found despite this, it is limited to the amount you paid for this guide.

HOLD HARMLESS AGREEMENT

By reading or using this guide, you agree to release, hold harmless, defend, and indemnify Heirloom Software LLC and its owners, authors, employees, and agents from and against any and all claims, demands, losses, damages, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or related to your use of this guide, your following or failing to follow any of its instructions, or your use of any software, hardware, website, or service it mentions.

THIRD PARTIES

This guide mentions software, websites, and services made by others. Heirloom Software LLC does not control them and is not responsible for their content, safety, availability, or terms. Your use of them is governed by their own terms and policies.

AGREEMENT

If any part of this notice is found unenforceable, the rest remains in effect. **If you do not agree to these terms, do not use this guide.** Using it means you accept them.

What's Inside

1. What This Tool Is For	5
2. Starting the Program	6
3. The Security Checks (the main job)	7
4. Your Approved Software List	9
5. The Report (what you carry away)	10
6. Clean Up (the careful part)	11
7. The Key	13
8. If Something Goes Wrong	14
9. Quick Steps	15
Glossary	16

Hi there! Read this first.

Heirloom Security Checks is a tool for people who take care of other people's computers at work - the folks who keep the office running. You carry it on a **USB stick**. You plug it into a computer you are allowed to check, and it tells you what has been done on that computer and what is installed on it. It can also tidy the computer up, carefully, when you tell it to.

You don't need to be a computer expert. Each chapter is short. Read one, try it, then read the next.

Gray boxes show things you type. Words in **bold** are names of buttons you click.

TIP

Shortcuts and smart tricks.

WATCH OUT

Mistakes to watch out for.

REMEMBER

The big idea from a section.

TRY IT!

Something to try on a computer you are allowed to use.

FUN FACT

Something cool to know.

The most important rule: only use this tool on computers that belong to you, or that your boss or the owner has said in writing you are allowed to check. That is what it is for.

Grown-ups: this book is written at a 3rd to 5th grade reading level, but it covers everything the program does: running it from a USB stick, running as administrator, the four read-only checks (installed software vs an approved list, sign-ins and failed logons, USB device history, recently run and opened), where the reports are saved, the attended cleanup actions (temp, browsers, recent history, metadata stripping, and secure erase with its safety blocks), the license key, and the law about checking computers you are authorized to check.

CHAPTER 1

What This Tool Is For

Think about an office with lots of computers. Somebody has to make sure they are safe and are being used the right way. That person might check: Is there any software on this computer that should not be here? Did anyone try to sign in who shouldn't? Did someone plug in a USB stick and copy things?

Doing that by hand on every computer takes forever. **Heirloom Security Checks** does it for you in a minute, and writes down what it finds so you can keep it.

The golden rule

This tool is powerful. It can read what people did on a computer, and it can erase things. So there is one rule you must always follow:

REMEMBER

Only use Security Checks on computers you own, or that you have been given permission - in writing - to check. Checking someone's computer without permission can break the law.

WATCH OUT

Never use this tool to snoop on a person, to spy, or to hide or destroy proof of something. The first time you open it, it shows you an agreement that says all of this. You must say yes to use it.

If you take care of your company's computers and your boss has asked you to check them, you are exactly who this tool is made for.

CHAPTER 2

Starting the Program

There is nothing to install. The program lives on your USB stick.

- Plug your USB stick into the computer you want to check.
- Open the stick and find **Heirloom Security Checks.exe**.
- Double-click it.

Because the program is new, Windows might show a blue box that says it "protected your PC." That is normal. Click **More info**, then click **Run anyway**.

The first time

The very first time, the program shows you an **agreement**. Read it, scroll to the bottom, check the box, and click **I Have Read and Agree**. You only do this once per stick.

Run as administrator

Windows keeps some information locked up tight. To read the list of **sign-ins** (who logged in), the program needs extra permission, called being an **administrator**.

If you see a yellow bar near the top that says "Run as administrator," click it. Windows will ask "Do you want to allow this app to make changes?" Click **Yes**. The program starts over with the extra permission, and now it can read the sign-in list.

TIP

You can still run every other check without being an administrator. Only the sign-in list needs it.

CHAPTER 3

The Security Checks (the main job)

Click the **Security Checks** tab at the top. This is the part that looks at the computer. The best part: it only **reads**. It never changes anything on the computer you are checking.

You will see four boxes with check marks. Each one is a different thing to look at. Leave them all checked, then click the big green **Run Security Checks** button.

The program writes what it finds, line by line, right on the screen. When it is done, it also saves it all to your USB stick (more on that soon).

Check 1: Unapproved software

This lists every program installed on the computer. If you made an **approved list** (the next chapter shows how), the program marks anything that is NOT on your list with the words **NOT ON APPROVED LIST**. That is how you spot a program that shouldn't be there.

Check 2: Sign-ins and failed logons

This shows who signed in to the computer and when. It also shows **failed** sign-ins - times someone typed the wrong password and could not get in. A lot of failed sign-ins can mean someone was trying to break in.

WATCH OUT

If this check says it needs an administrator, go back to Chapter 2 and click "Run as administrator," then run the checks again.

Check 3: USB device history

Windows quietly remembers every USB stick and USB drive that was ever plugged into the computer. This check lists them all, with the date each was first seen. If you see a USB stick that nobody should have used, that is worth asking about.

Check 4: Recently run and opened

This shows programs that were run lately and files that were opened lately. It is a quick way to see what the computer was actually used for.

REMEMBER

All four checks only look. They change nothing. You can run them as many times as you like.

CHAPTER 4

Your Approved Software List

The program can't guess which software your company allows. You tell it, with a simple list.

- On the **Security Checks** tab, click **Edit approved-software list**.
- A text file called **approved_software.txt** opens.
- Type the programs your company allows, one on each line.
- Save the file and close it.

You can type just part of a name. If you type a line like this:

```
Chrome
```

then "Google Chrome" counts as approved. Here is what a list might look like:

```
Consign It  
Google Chrome  
Mozilla Firefox  
7-Zip  
QuickBooks  
Zoom
```

Now when you run the checks, any program that is NOT on your list - and is not normal Windows or driver software - gets flagged for you to look at.

TIP

Make the list once and keep it on the stick. It is used on every computer you check, so you don't have to make it again.

If you don't make a list, that's fine. The program just lists all the software and flags nothing.

CHAPTER 5

The Report (what you carry away)

Every time you run the checks, the program saves the findings to your USB stick. That way you walk away with the proof, right in your pocket.

Look on the stick for a folder called **Security Check Logs**. Inside is a file named after the computer and the date and time, like:

```
FRONTDESK-PC_2026-10-26_142530.txt
```

Open it any time to read what was found. At the very top is a short list called **SUMMARY OF CONCERNS** - the things worth a second look. The program also saves a second file (ending in **.csv**) with the full software list, which you can open in Excel.

TRY IT!

Run the checks on your own computer. Then open the Security Check Logs folder on the stick and read your report. See how the summary at the top points out the main things.

CHAPTER 6

Clean Up (the careful part)

The **Clean Up** tab tidies a computer: it can clear out junk files and old history, take hidden information out of files, and erase a folder for good. This part **does** change the computer, so it is very careful.

REMEMBER

Before anything is cleaned, the program shows you exactly what it will touch and asks **Yes or No**. Nothing happens until you click Yes.

WATCH OUT

What Clean Up removes is gone. It does NOT go to the Recycle Bin. Close your web browsers before you clean them.

The five cleanup buttons

- **Clear temp folders** - empties the computer's scratch folders (safe junk).
- **Clear browser cache & history** - clears Chrome, Edge, and Firefox.
- **Clear recent-files / Run / Jump List history** - clears the lists of lately opened things.
- **Strip metadata from a folder** - takes hidden information (like where a photo was taken) out of pictures and Office files.
- **Securely erase a folder** - overwrites a folder three times, then deletes it for good.

About stripping metadata

Pick a folder, and the program makes a clean copy of each picture and Office file with the hidden information taken out. The new copies have **(clean)** in their names. Your originals are not changed. For PDF files, use our other tool, **Heirloom Print Shield**.

About securely erasing

This one is serious. When you securely erase a folder, it writes over the files three times with random junk and then deletes them, so they can't be brought back - not even with recovery tools.

WATCH OUT

Use this only on a folder of files you truly want gone forever. To keep you safe, the program will NOT erase a whole drive, the Windows folder, or your main user folder. It also asks you twice.

Everything Clean Up does is written to a file called **cleanup log.txt** on the stick, so there is a record of what you tidied and when.

CHAPTER 7

The Key

The **Security Checks** - the part that looks at a computer and makes reports - are **always free**. You can use them forever.

The **Clean Up** part needs a **key** to work. A key is a line of letters and numbers that starts with **SC1-**. One key is **\$79**, paid one time - no monthly fee.

How to get a key

- Call or text **(606) 521-7093**, or order at **needfulthingssoftware.com**.
- The key is emailed to you.
- In the program, click the **License** tab, paste the key in the box, and click **Use this key**.

REMEMBER

Checking computers and saving reports never costs anything. Only the Clean Up tools need a key.

CHAPTER 8

If Something Goes Wrong

Problem	What to do
Windows says it "protected your PC"	Click More info, then Run anyway. The program is safe.
The sign-in check says it needs an administrator	Click the yellow "Run as administrator" bar, click Yes, and run the checks again.
No reports show up on the stick	The stick may be write-protected. The program then saves the reports to a folder on the Desktop instead, called Heirloom Security Checks.
Browser cleanup says a file is in use	Close the web browser all the way, then try again.
A program I know is fine got flagged	Add its name to approved_software.txt, then run again.
It won't open on an old computer	It works on Windows 7 and up. Make sure the stick is plugged in all the way.

Still stuck? Call or text **(606) 521-7093**. A real person answers. You can also let us see your screen for free with **Heirloom Help**.

CHAPTER 9

Quick Steps

I want to...	Do this
Check a computer	Security Checks tab, Run Security Checks
See sign-ins	Click Run as administrator first, then run the checks
Flag bad software	Edit approved-software list, add your allowed programs, run again
Find my report	Open the Security Check Logs folder on the stick
Clear out junk	Clean Up tab, Clear temp folders, click Yes
Clean a browser	Close it, then Clean Up tab, Clear browser cache & history
Take GPS out of photos	Clean Up tab, Strip metadata from a folder
Erase files for good	Clean Up tab, Securely erase a folder (asks twice)
Enter my key	License tab, paste the SC1- key, Use this key

QUICK REFERENCE

Glossary

Word	What it means
Administrator	Extra permission on a computer that lets you see and do more.
Approved list	Your list of software the company allows (approved_software.txt).
Audit	To carefully check something and write down what you find.
Cache	Leftover files a browser saves to load pages faster.
Failed logon	A time someone typed the wrong password and could not sign in.
Metadata	Hidden information stuck inside a file, like a photo's location.
Report / log	The file the program saves with what it found.
Securely erase	To write over files so they can't be brought back, then delete them.
USB stick	A small drive you plug in to carry files - this tool lives on one.
USB history	Windows' memory of every USB drive ever plugged into a computer.