



Heirloom Software

The Idjits Guide to

No Trace Browser

Browse the web in private. Leave nothing behind.

Panic button, auto-erase, and a browser on a USB stick - one easy step at a time.

Disclaimer and Hold Harmless Agreement

The Idjits Guide to No Trace Browser • 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 Software, websites, prices, and menus change often; the information was believed accurate in October 2026 but may be out of date or incorrect when you read it.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. Two Kinds of Private	5
2. Getting No Trace Browser	7
3. Browsing in Private	9
4. The Panic Button	11
5. The Auto-Close Timer	12
6. Your Downloads	13
7. What Gets Erased	14
8. No Trace Browser on a USB Stick	15
9. What No Program Can Promise	16
10. The Free Trial and Your Key	17
11. Troubleshooting	18
Cheat Sheet	19
Glossary	20

Hi there! Read this first.

Every time you use the internet, your computer keeps notes: the places you went, little files called **cookies**, copies of pictures, and lists of programs you ran. This book shows you how to browse with **Heirloom No Trace Browser**, which keeps your trips on the web private and **erases those notes** every time you close it.

You don't need to know anything about computers. Each chapter is short. Read one, try it, and 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 your own computer.

FUN FACT

Something cool to know.

Grown-ups: this book is written at a 3rd to 5th grade reading level, but it covers everything the program does: how Tor Browser and the Tor network work, getting Tor Browser from torproject.org and the signature check, the three security levels, erase on close, the Panic button and Ctrl+Alt+X, the auto-close timer, the Downloads tab, cleaning Windows' records (UserAssist, MUICache, the Program Compatibility Assistant, Recent items), USB Copy, what no program can promise, the free trial and key, and troubleshooting.

CHAPTER 1

Two Kinds of Private

When people say "private browsing", they can mean two different things. No Trace Browser does **both**.

Kind of private	What it means	How No Trace Browser does it
Private on the internet	Websites and your internet company can't easily see who you are or where you went.	It uses Tor Browser and the Tor network.
Private on the computer	Nobody who uses this computer later can find out where you went.	It erases everything when the browser closes.

What is Tor?

Normally, your computer talks straight to a website. The website sees your computer's address, and your internet company sees which website you went to.

Tor works like passing a note through three friends. Your note goes to friend 1, then friend 2, then friend 3, and only then to the website. Each friend only knows the friend before and after. Nobody knows both who sent the note and where it went.

FUN FACT

Tor stands for **The Onion Router**. Your message is wrapped in layers, like an onion. Each of the three computers peels off one layer. The friends are real computers run by volunteers all over the world - thousands of them!

Who makes Tor Browser?

Tor Browser is made by **The Tor Project**, a group that gives it away free at torproject.org. No Trace Browser gets the real Tor Browser from them and adds the things it doesn't do on its own: the erasing, the Panic button, the timer, the downloads list, and the USB stick copy.

REMEMBER

Tor hides where you go on the internet. No Trace Browser also wipes the computer clean when you are done.

CHAPTER 2

Getting No Trace Browser

What you need

- A computer with **Windows 10 or Windows 11**. (Tor Browser doesn't work on Windows 7 or 8.)
- An internet connection.
- About **400 MB** of free space.

Installing it

No Trace Browser comes as one file named **Install Heirloom No Trace Browser.exe**.

1. Double-click **Install Heirloom No Trace Browser.exe**.
2. If a blue box says "Windows protected your PC", click **More info**, then **Run anyway**.
3. Click **Install**. You don't need a grown-up's password to install it.
4. Wait a few seconds. When it says it's installed, it opens by itself.

Now there is a **Heirloom No Trace Browser** icon on your Desktop and in the Start menu.

TIP

This book is on your computer too. In the program, click the **Help** tab, then **Open the Idjits Guide**.

The two agreements

The first time it opens, it shows two agreements: the **End User License Agreement** and the **Hold Harmless and Indemnity Agreement**. Ask a grown-up to read them with you. If you agree, click the agree button. You can read them again any time with the **Agreements** button.

Getting Tor Browser (the first time only)

1. Click the **Browse** tab.
2. Click **Get Tor Browser**.
3. Watch the bar fill up. Tor Browser is about 110 MB, so this takes a minute or two.
4. When the top says **Tor Browser ... is ready**, you're done.

No Trace Browser downloads Tor Browser **straight from torproject.org**. Then it checks The Tor Project's **digital signature** on it.

FUN FACT

A digital signature is like a wax seal on a letter. If anyone changed even one tiny piece of the file, the seal breaks. If the seal is broken, No Trace Browser throws the file away and installs nothing.

Keeping it up to date

Tor Browser gets better all the time. Once in a while, click **Check for Update** on the Browse tab. Tor Browser can also update itself while it's open.

CHAPTER 3

Browsing in Private

Step 1: pick a security level

Level	What it does	Good for
Safest	Turns off JavaScript (the part of websites that runs little programs) everywhere.	The most privacy. Some sites won't work right.
Safer	Turns JavaScript off on sites that aren't secure (no https).	Everyday browsing.
Standard	Every site works the usual way.	Sites that won't work any other way.

TIP

Start with **Safest**. If a site you need is broken, close the browser, pick **Safer**, and open it again.

Step 2: open the browser

1. Click the big green **Open Private Browser** button.
2. Tor Browser opens. It connects to the Tor network by itself. Give it a few seconds.
3. Type a website in the bar at the top, just like any browser.

Step 3: close it when you're done

Close the Tor Browser window the normal way (the **X** in the corner). A few seconds later, No Trace Browser erases everything. The **What happened** box tells you what was erased.

```
3:42 PM The browser closed - erased:
3:42 PM      Erased 57 files of history, cookies, site data, caches and
            temporary files.
3:42 PM      Emptied the clipboard.
3:42 PM      Took 3 records of this program out of Windows.
```

WATCH OUT

Don't sign in to your own accounts (email, shopping, social sites) in the private browser unless you have to. When you sign in, that website knows it's you - Tor can't hide that.

REMEMBER

Open it. Browse. Close it. Everything is erased by itself.

CHAPTER 4

The Panic Button

Sometimes you need the browser gone **right now**. That's what Panic is for.

Two ways to panic

- Click the red **PANIC - Close and Erase Now** button, or
- press **Ctrl + Alt + X** on the keyboard. This works from anywhere, even when the No Trace Browser window is hidden.

What Panic does

1. Closes the browser at once - every window and every tab.
2. Erases everything, the same as a normal close.
3. Empties the clipboard (anything you copied).
4. Drops the No Trace Browser window down to the taskbar.

TRY IT!

Open the private browser, go to any website, then press **Ctrl + Alt + X**. Count how fast it's gone!

WATCH OUT

Panic closes the browser without asking. Anything you were typing in a website is lost.

Erase Now

The **Erase Now** button does the same erasing as Panic, without hiding the window. Use it any time you want to be sure.

CHAPTER 5

The Auto-Close Timer

Worried you'll forget to close the browser? Set the timer. When it runs out, the browser closes and everything is erased.

1. On the **Browse** tab, find **Close and erase after:**.
2. Pick 10 minutes, 15 minutes, 30 minutes, 1 hour, or 2 hours.
3. Click **Open Private Browser**.

The time left counts down next to the buttons, like **Closes and erases in 14:59**. To turn the timer off, pick **Off** before you open the browser.

TIP

The timer is great on a shared computer - at the library, at work, or at a friend's house.

CHAPTER 6

Your Downloads

When you download a file in the private browser, it doesn't go into your normal Downloads folder. It goes into No Trace Browser's own hidden **Session** folder, so it doesn't leave a trail.

Downloads are **not** erased when the browser closes. They wait for you to decide. If any are waiting, the tab says **Downloads (2)** - the number is how many.

Keeping a download

1. Click the **Downloads** tab.
2. Click the file. (Click nothing to pick all of them.)
3. Click **Move To a Folder...** and pick where it should go.

Getting rid of a download

1. Click the **Downloads** tab.
2. Click the file. (Click nothing to pick all of them.)
3. Click **Erase**, then **Yes**.

WATCH OUT

Erased means gone for good. No Trace Browser writes random junk over the file before deleting it, so not even an "undelete" program can bring it back.

FUN FACT

Most programs only delete a file's name and leave the file itself on the disk. Overwriting it first is like shredding a paper instead of just throwing it in the trash can.

CHAPTER 7

What Gets Erased

Erased every time	What it is
History	The list of places you went
Cookies	Little files websites leave to remember you
Site data and caches	Copies of pages and pictures saved to load faster
Saved form entries and passwords	Things you typed into boxes
The saved session	Which tabs were open
Temporary files	Scrap files the browser made while it worked
Folders it remembered	Where you last saved or opened a file
The clipboard	Anything you copied
Windows' records	Windows' own lists of programs you ran (see below)

Windows' own lists

Windows keeps lists of the programs you run, so it can show them in the Start menu and help them run better. Those lists would show that you used No Trace Browser. With the box **Also take this program out of Windows' records of programs run** checked, No Trace Browser takes itself out of them:

- **UserAssist** - the list behind "most used" programs,
- **MUICache** - a list of program names,
- the **Program Compatibility Assistant** list,
- and **Recent items** that point at its files.

What is kept

- Tor Browser itself and its add-ons.
- Your security level and timer choice.
- Tor's own settings, like bridges and the first Tor computer it uses. They don't show anything you looked at, and keeping the same first computer actually makes Tor safer.

- Your downloads, until you move or erase them.

CHAPTER 8

No Trace Browser on a USB Stick

You can carry No Trace Browser in your pocket. **USB Copy** puts the whole thing on a USB stick: the program, Tor Browser, your key, and this book.

1. Plug in a USB stick with at least **1 GB** free.
2. Click the **USB Copy** tab.
3. Click **Choose...** and pick the USB stick.
4. Click **Copy to USB**. It takes a few minutes.
5. When it says **Done!**, the stick has a folder named **Heirloom No Trace Browser**.

Using the stick

1. Plug the stick into any Windows 10 or 11 computer.
2. Open the **Heirloom No Trace Browser** folder on the stick.
3. Double-click **Heirloom No Trace Browser.exe**.

The copy on the stick keeps **everything on the stick** - its settings, its downloads, and Tor Browser. It doesn't save its free-trial date or settings on the computer. The window's title says **running from** and the stick's letter, so you know which copy you're using.

WATCH OUT

Close the browser and wait for the erase to finish before you pull out the stick.

CHAPTER 9

What No Program Can Promise

No Trace Browser does a lot. But no program in the world can make you invisible. Here's the truth:

- **Websites you sign in to know it's you.** Tor hides where you are, not who you tell them you are.
- **A computer you don't trust can still watch you.** A work or school computer may record the screen or the keyboard. Use a computer you own.
- **Windows keeps a few records only a grown-up administrator can clear,** like Prefetch files and system logs. Windows' page file and sleep file can also hold scraps of memory.
- **Solid-state drives (SSDs) move data around** to stay healthy, so overwriting a file doesn't always hit the same spot. The file is still deleted.
- **Your internet company can see you are using Tor** - just not what you do with it. If that's a problem where you are, turn on a **bridge** in Tor Browser's settings.

TIP

For the most privacy of all, grown-ups can use **Tails** (tails.net) - a whole private computer system that starts from a USB stick and never touches the computer's own drive.

Using it the right way

- Using Tor is legal in the United States.
- Private does not mean "anything goes". Never use it to threaten, bully, cheat, or hurt anyone, or to buy or sell anything illegal.
- Only use it on computers you own or are allowed to use.
- Following your school's or workplace's rules is still your job.

REMEMBER

Privacy is good. Breaking the law is not. No Trace Browser is only for the first one.

CHAPTER 10

The Free Trial and Your Key

Every part of No Trace Browser is free for **30 days**. The top of the window says how many days are left. After that, **browsing and erasing when the browser closes are still free**. The Panic hide, the auto-close timer, erasing Windows' records, and USB Copy need a **key**. A key costs **\$53 one time** - it never runs out.

To buy one, call or text **(606) 521-7093**, or order at **needfulthingssoftware.com**. The key comes in an email.

1. Save the file from the email that ends in **.lic**.
2. In No Trace Browser, click **Enter Your Key** at the top.
3. Click **Load License File** and pick the .lic file. (Or paste the key. A No Trace Browser key starts with **NT1-**.)
4. Click **Save Key**. The top of the window now says **Licensed to** and your name.

TIP

Make your USB copy after you enter your key. The key goes onto the stick too.

Taking it off the computer

Click **Uninstall** at the top of the program. It erases Tor Browser and everything the browser left, then takes the program off. Or open Windows **Settings**, then **Apps**, find **Heirloom No Trace Browser**, and click **Uninstall**.

CHAPTER 11

Troubleshooting

"It says Tor Browser needs Windows 10 or 11."

Tor Browser doesn't run on Windows 7 or 8 anymore. Use a newer computer, or ask a grown-up about **Tails** (tails.net).

"Get Tor Browser says it couldn't reach torproject.org."

- Check that the computer is on the internet.
- Some work and school networks block torproject.org. Try at home.
- Try again in a few minutes.

"It says the download is NOT correctly signed."

Something changed the file on the way to your computer, so No Trace Browser threw it away to keep you safe. Try again on a different network. If it keeps happening, call us.

"The browser is stuck on Connecting."

Your network may block Tor. In Tor Browser, open **Settings**, then **Connection**, and turn on a **bridge**. Bridges are kept between visits, so you only do this once.

"A website looks broken."

Close the browser, pick **Safer** (or **Standard**), and open it again. Some websites also block Tor - that's the website's choice, not a problem on your computer.

"Ctrl + Alt + X doesn't do anything."

Another program is using those keys. The **What happened** box will say so. Use the red **PANIC** button instead.

"The buttons say I need a key."

The 30-day trial is over. Browsing and erasing when the browser closes are still free. For the rest, click **Enter Your Key** (Chapter 10).

Still stuck?

Call or text Heirloom Software at **(606) 521-7093**, or visit **needfulthingssoftware.com**.

QUICK REFERENCE

Cheat Sheet

To do this	Do this
Get Tor Browser the first time	Browse tab, Get Tor Browser
Browse in private	Pick Safest, click Open Private Browser
Erase everything	Just close the browser (or click Erase Now)
Get out fast	Red PANIC button, or Ctrl + Alt + X
Close by itself later	Close and erase after: pick the minutes, then open the browser
Keep a download	Downloads tab, Move To a Folder...
Shred a download	Downloads tab, Erase
Carry it on a USB stick	USB Copy tab, Choose..., Copy to USB
A site is broken	Close, pick Safer, open again

QUICK REFERENCE

Glossary

Word	What it means
Bridge	A secret Tor computer that helps you connect when Tor is blocked.
Browser	The program you use to visit websites.
Cache	Copies of pages and pictures a browser keeps so they load faster.
Clipboard	Where Windows keeps what you copied, until you paste it.
Cookie	A little file a website leaves on your computer to remember you.
Digital signature	A seal that proves who made a file and that nobody changed it.
History	The list of websites a browser visited.
Internet company	The company that brings the internet to your home or phone.
JavaScript	Little programs that websites run inside the browser.
Panic	Close the browser and erase everything, right now.
Tor	The Onion Router. Sends your connection through three volunteer computers.
USB stick	A small drive you plug into a computer to carry files.