



TechCortado.com

Free ebook



# The Laptop Security Handbook

Stop the easy theft, protect your data and be back at work tomorrow



**TechCortado.com**

# The Laptop Security Handbook

*Stop the easy theft, protect your data and be back at work tomorrow*

---

Edition 1, October 2026

**TechCortado.com**

**Read the full online guide**

# About TechCortado

---

**TechCortado.com** publishes short, honest, insight-driven takes on the tech people use every day: phones, wearables, smart home, PC and gaming hardware, and everyday security. Each piece starts from the evidence, says what matters, and leaves out the rest.

**Why the name?** A cortado is a small espresso “cut” with a little steamed milk. The word comes from the Spanish *cortar*, to cut. It is strong, short and has no froth.

That is the idea behind our posts: the useful part first, just enough context to make it go down easily, and nothing puffed up. This handbook follows the same rule, and it is free to share.

Read more at **TechCortado.com**, and get new guides and updates to this book by email: **TechCortado.com/newsletter**.

## **The Laptop Security Handbook**

Edition 1, October 2026

Version 1.0 (first release, 30 October 2026)

Author: TechCortado.

[TechCortado.com](https://TechCortado.com)

**© 2026 TechCortado. All rights reserved. You may share this PDF free of charge in its complete, unmodified form. No modification, excerpting, resale, or reuse of the text, images or design (including for AI training datasets) without written permission.**

Third-party images remain under their own licences, as listed in Image credits at the back. Diagrams, cover art and design are by TechCortado.

Please read the disclaimers on the next page before you act on anything in this book.

Sources were checked on 29 and 30 October 2026. The online version of this guide is at [TechCortado.com](https://TechCortado.com).

Set in Literata, Inter Tight and IBM Plex Mono, under the SIL Open Font License.

# Disclaimers

---

**General information only.** This handbook gives general information about protecting a laptop and its data. It is not legal advice, insurance advice or professional security advice, and it does not replace advice for your own situation.

**No guarantee.** We work hard to be accurate, but we can't guarantee that the information is complete, correct or right for you. No step in this book can promise that a laptop won't be stolen or that data can't be reached.

**Use at your own risk.** You are responsible for how you use this information. Back up your data before you change security settings, and check the maker's own instructions for your device. To the extent the law allows, TechCortado is not liable for any loss or damage from using this book.

**Laws differ by country.** Rules on encryption, tracking, recording, border checks and reporting crime vary. Follow the law where you are, official guidance, the instructions of officials, and your employer's policies for work devices.

**Examples, not endorsements.** Products and services named in this book, mainly in Appendix B, are examples so you know what to look for. They are not endorsements. There are no affiliate links in this book and nobody paid to be included or sponsored it.

**Trademarks.** Product and company names are trademarks of their owners. Using them here does not mean any link with, or approval by, those owners.

**Current as of the edition date.** This is edition 1, October 2026. Sources were checked on 29 and 30 October 2026. Settings, products, prices and official advice change, so check the current version before you act.

**External links.** This book links to other websites. We don't control them and aren't responsible for their content, their privacy practices or whether they stay online.

# Contents

- 0 Start here .....7
- 1 What are you protecting? ..... 11
- 2 Stop the easy theft ..... 18
- 3 Locks and anchors ..... 23
- 4 Encryption and power states ..... 36
- 5 Firmware, boot and tampering ..... 49
- 6 Screen, sign-in and accounts..... 56
- 7 Backups and account recovery ..... 66
- 8 Find it, track it, mark it .....76
- 9 Tripwires ..... 86
- 10 Out and about ..... 93
- 11 Travel..... 99
- 12 When it goes wrong..... 106
- 13 Habits, setups and checklists ..... 112
- A Worksheets ..... 118
- B Example products (as of 2026) ..... 125
- Glossary ..... 133
- Sources ..... 136
- Image credits..... 141
- Index ..... 142
- Follow TechCortado ..... 144



CHAPTER 0

# Start here

*How to use this book*

---

## INSIDE

How the book is laid out

Pick your path

A few promises



TechCortado.com

**IN THIS CHAPTER**

- What this book covers: a laptop that leaves your hands, and how to be back at work soon after.
- How the boxes work: every chapter opens with this summary, and six coloured boxes mark tips, tricks, examples, warnings, stories and checklists.
- A table to pick the chapters that fit your life first.
- **Time needed:** 5 minutes.

This book is about one ordinary, painful event: a laptop that leaves your hands when you didn't mean it to. It might be a grab in a café, a bag lifted on a train, a break-in at home or a machine left in a taxi. It walks through what you can do before that day, what to do on the day, and how to be back at work soon after.

It doesn't ask you to buy much, and it doesn't assume you are a technical person. Most chapters start with things you can do in a few minutes with what your laptop already has.

---

## How the book is laid out

Every chapter opens with a short **In this chapter** box. If you only have a minute, read the boxes. Inside the chapters you'll meet six kinds of boxes, always in the same colours:

**TIP**

A small step that gives you a lot back.

**TRICK**

A less obvious way of doing something, or a shortcut.

**EXAMPLE**

A worked case: a table, a setting or a short walk-through.

**WATCH OUT**

A common mistake, a limit, or something a product page won't tell you.

**STORY**

*A short imagined scene that shows how things tend to go. The people in these boxes are made up. They are typical cases, not reports of real events.*

**CHECKLIST**

- ☐ Things to tick off.
- ☐ Printable versions are in the worksheets near the end.

## Pick your path

| If you are...              | Start with                            | Then read                  |
|----------------------------|---------------------------------------|----------------------------|
| Short on time today        | Chapter 13, the 15-minute quick start | Chapters 4 and 7           |
| Working mostly at home     | Chapters 1, 4 and 7                   | Chapters 3 and 8           |
| A student or a commuter    | Chapters 2, 6 and 10                  | Chapters 4, 7 and 12       |
| A frequent traveller       | Chapters 11 and 4                     | Chapters 5, 10 and 12      |
| Looking after a small team | Chapters 1, 3 and 7                   | Chapter 13, setups         |
| Reading this after a theft | Chapter 12                            | Then 7 and 4 for next time |

## A few promises

- **Methods, not shopping lists.** The chapters describe what to look for and how to check it. Brand names, models and prices date quickly, so a

small set of example products sits in Appendix B, clearly marked as examples as of 2026 and not endorsements.

- **Official advice first.** Where we give safety advice we lean on public guidance from police forces, national cyber security agencies and standards bodies. Numbers in small type point to the Sources list at the back.
- **No invented tests.** When a figure is a maker's own claim, we say so. When nobody has measured something, we say that too.
- **Dated facts carry their year.** Research and statistics come with the year they were published, so you can judge them yourself.



#### **WATCH OUT Before you act**

This is a general guide. Laws, insurance policies and workplace rules differ, so please read the Disclaimers page at the front. If your employer manages your laptop, its procedures come first.

---

#### **MORE ON THE SITE**

→ [Read the full online guide](#)



#### **Stay in the loop**

New guides, checklists and updates to this book, straight to your inbox.

**Get the TechCortado newsletter**

[Bluesky](#) · [Mastodon](#) · [Pixelfed](#) · [TechCortado.com](#)

# 01

## CHAPTER 1

# What are you protecting?

*Four losses in one theft*

---

### INSIDE

The ladder of protection

Match the effort to the threat





## IN THIS CHAPTER

- A stolen laptop is four separate problems: the hardware, your work, your data and your accounts.
- Each needs its own fix. No single gadget covers all four.
- Encryption, backups and account recovery come first. Do them today.
- Match the effort to the place you work and who might want the laptop.
- **Time needed:** 15 minutes to read and fill in the self-check.

Losing a laptop to a thief is several bad days rolled into one. The machine is gone. Work that lived only on that drive may be gone too. Someone else might now be able to open your documents, your browser sessions, or the accounts that control your other devices. And while you work out what was exposed, you still have to replace the hardware and rebuild a normal working day.

So we treat those as separate problems, because they need separate fixes. Keep the laptop under your control. Use a well-fitted physical lock when there is something solid to lock it to. Encrypt the storage, and know what happens to that protection when the lid closes. Keep a backup you can restore without the missing machine. Keep a way back into your important accounts. Add tracking as a possible help with recovery, not a promise.

What we are aiming for is a theft that costs money and patience but stays contained. A cable can't do that on its own. Neither can a perfect backup if the thief also walks off with an unlocked email account.

**Short version:** set up the basics before you buy clever accessories. That means encryption you have checked, a separate backup you have restored from, account recovery that doesn't depend on this laptop, and sensible habits in public. After that, a lock that fits your exact slot and something solid to anchor it to. A tracking tag is a good extra if it suits your phone and you know what it can and can't do.

A note on evidence. Product specs here come from the makers' own pages and manuals. When a number is a maker's pull test, compatibility list or battery estimate, we say so. We have not destroyed a pile of locks in a work-

shop, and we won't pretend otherwise. This is a researched guide, and the same rule runs through the whole book.

## The ladder of protection

These layers work together. Think of them as rungs that support each other. The list starts with not getting robbed in the first place, but please don't wait until your physical setup is perfect before you turn on encryption and backups.

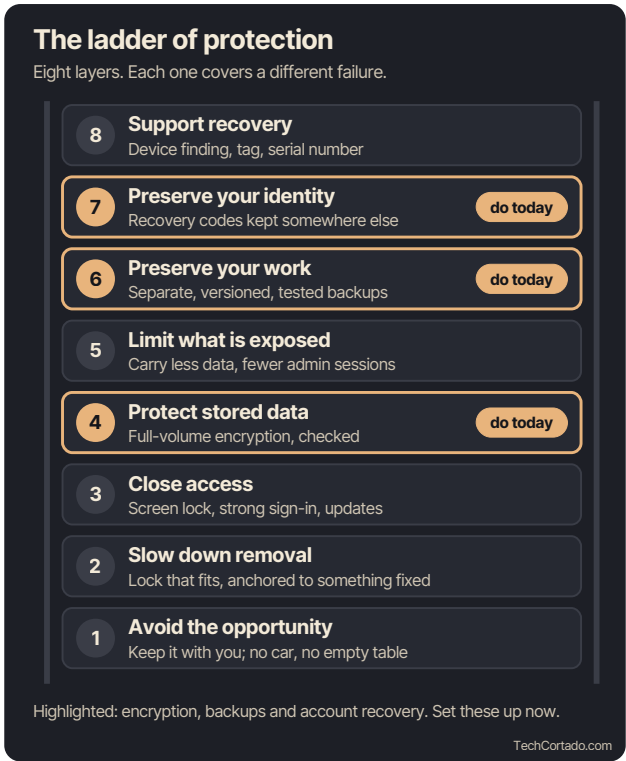


**Figure 1.1** Eight layers that support each other. Encryption, backups and account recovery are the ones to do today.

| Layer                    | What to do                                                                                   | What it can achieve            | What it can't promise                                        |
|--------------------------|----------------------------------------------------------------------------------------------|--------------------------------|--------------------------------------------------------------|
| 1. Avoid the opportunity | Keep the laptop with you; pick a sensible seat; don't leave it in a car or on an empty table | Fewer easy chances for a thief | No protection against robbery, burglary or your own slip-ups |

| Layer                     | What to do                                                                             | What it can achieve                                             | What it can't promise                                                   |
|---------------------------|----------------------------------------------------------------------------------------|-----------------------------------------------------------------|-------------------------------------------------------------------------|
| 2. Slow down removal      | Match the lock to the slot or bracket and fix it to something that really doesn't move | Interrupts a quick grab and makes removal more work             | Surviving every tool, or making an unattended spot safe                 |
| 3. Close access           | Lock the screen, use strong sign-in, keep updates current                              | Stops casual access through the normal login                    | Turning a running computer into a switched-off encrypted one            |
| 4. Protect stored data    | Turn on and check full-volume encryption; keep recovery material safe                  | Data at rest stays unreadable if the machine or drive is taken  | Protecting a session that was already unlocked, or files copied earlier |
| 5. Limit what's exposed   | Carry only the data you need; fewer admin sessions and stored secrets                  | Smaller consequences if something goes wrong                    | Pulling back copies already made                                        |
| 6. Preserve your work     | Independent, encrypted, versioned backups, with restores you've tested                 | Get your files back and lose less time                          | Stopping the theft or undoing a leak                                    |
| 7. Preserve your identity | Recovery codes and spare sign-in methods kept somewhere else                           | Get back into accounts even if laptop and phone vanish together | Helping if every recovery method was in the same bag                    |
| 8. Support recovery       | Turn on device finding, add a suitable tag, write down serial numbers                  | Leads, proof of ownership, support for a claim                  | A guaranteed location, remote wipe or police recovery                   |

The UK's National Cyber Security Centre gives the same core advice for devices: keep physical control, report a loss quickly, and don't store passwords alongside the device. Its data-security guidance also treats encryption, isolated backups and rehearsed restores as separate controls, which is how we've laid them out here. <sup>1,2</sup>



**TIP Start with three rungs**

Rungs 4, 6 and 7 (encryption, backups and account recovery) are free on almost every laptop and protect you whatever else happens. A lock or a tag is worth less until those are in place.

## Match the effort to the threat

If you work from cafés, the usual worry is a quick grab: the open laptop near the door, the bag on the back of a chair, a distraction while you're packing up. At a shared desk the window can be much longer. In an empty hotel room, a cable may be up against someone with privacy and plenty of time. And a person after your documents is a very different problem from someone who just wants to resell the hardware.

That difference should guide your spending. A plain bag, the habit of taking the laptop with you and a backup at home will often do more for you than swapping one decent cable lock for a slightly better one. A public workstation that stays exposed all day might justify an anchored enclosure or a proper locking station. Sensitive work might justify a separate travel laptop with less data on it and fewer powerful logins.

These are judgment calls about exposure. Nobody has a trustworthy figure for how much a given cable cuts your risk, so we won't invent one.

### Four kinds of loss

It helps to name the four losses separately, because each one has a different cure.

| Loss          | What it feels like                                                | Main fix                                        | Chapter  |
|---------------|-------------------------------------------------------------------|-------------------------------------------------|----------|
| The hardware  | Paying for a new machine and setting it up                        | Habits, locks, insurance records                | 2, 3, 8  |
| Your work     | Files that only lived on that drive                               | Separate, tested backups                        | 7        |
| Your data     | Someone reading your documents and messages                       | Encryption, a locked screen, less data carried  | 4, 5, 6  |
| Your accounts | Email, banking or cloud sessions still open on the stolen machine | Account recovery, signing out sessions remotely | 6, 7, 12 |

**EXAMPLE A quick self-check**

Answer five questions with a pen. There is a printable version in the worksheets.

1. Where does the laptop spend most hours away from home: café, office, campus, train, hotel, car?
2. Is the laptop encrypted, and have you **checked**, not assumed?
3. If it vanished right now, which files would you lose for good?
4. Could you get into your main email if your laptop **and** phone were gone?
5. Do you have the serial number written down somewhere else?

Every "no" or "not sure" points to a chapter. If question 4 makes you pause, start with Chapter 7.

**STORY Imagine two laptops stolen on the same day**

*Imagine two people who each lose a laptop from a café table on the same afternoon. The first had the drive encrypted, a backup at home and recovery codes in a drawer. Her evening is annoying: a police report, a call to the insurer, a few passwords changed. By the next afternoon she is working again on a borrowed machine. The second had none of that. His week goes on rebuilding files from email attachments and trying to prove to his email provider that he is who he says he is. The theft was the same. The preparation made the difference.*

**Who might want your laptop?**

Most laptop thieves want something quick to sell. They are not interested in your files, and they will wipe the machine or sell it on as it is. That is the case this book is built around.

A smaller group of people might care about what is on the drive: a business rival, someone who knows you, or a person who hopes to find saved passwords. If your work is sensitive, your employer probably has rules for this already, and Chapters 5 and 11 cover the extra steps official travel advice suggests.

**WATCH OUT Don't let rare threats crowd out common ones**

It is easy to spend an evening reading about clever attacks and still have no backup. The ordinary threats, a grab, a lost bag, a burglary, are far more likely. Cover them first.

**CHECKLIST Do this today**

- ☐ Write down your laptop's serial number and keep it away from the laptop.
- ☐ Check whether the drive is encrypted (Chapter 4 shows how).
- ☐ Make one backup to a drive that you then unplug (Chapter 7).
- ☐ Print or write down the recovery codes for your main email account.

**MORE ON THE SITE**

→ [The ladder of protection, online](#)

**Stay in the loop**

We update the guide when official advice changes. Hear about it first.

**Get the TechCortado newsletter**

[Bluesky](#) · [Mastodon](#) · [Pixelfed](#) · [TechCortado.com](#)

# 02

## CHAPTER 2

# Stop the easy theft

*Habits beat hardware*

---

### INSIDE

The moment it leaves your hands

Trains, buses and stations

Cars

Conferences, events and meal times

Bags, labels and records

Work laptops



**IN THIS CHAPTER**

- Most thefts happen in a few seconds: a distraction, a bag on a chair, a laptop left while you order.
- Keep the laptop in sight and in reach. Pack it away when you stand up.
- Never use a car as storage, not even the boot.
- Conferences and hotel meal times are known busy times for thieves.
- Keep the serial number, receipt and photos somewhere you can reach without the laptop.
- **Time needed:** a few minutes to change habits; nothing to buy.

Most laptop thieves need no tools and no skill. They need a few seconds when nobody is watching. This chapter is about taking those seconds away, and it costs nothing.

## The moment it leaves your hands

Start with the moment the laptop leaves your control. In a café, that's the walk to the counter. On a train, it's often the stop before yours. At a hotel, it can be the bag you set down by the reception desk. Police advice keeps returning to the same two openings: things left unattended, and distraction. A lock helps when you're working at one spot, but packing the laptop away when you get up is still the stronger everyday habit. <sup>3,4,5</sup>

**STORY Imagine the walk to the counter**

*Imagine a café on a busy morning. A student leaves her laptop open on the table by the door and walks the six steps to the counter for a refill. Someone comes in, asks the person at the next table for directions, and leaves. The whole thing takes less than ten seconds, and the laptop leaves with him. Nobody would call it a clever crime. It didn't need to be.*

Pick a seat where you can see both the bag and the computer, and keep the bag closed and next to you instead of hanging off the chair behind you. A stranger offering to "keep an eye on it" is being kind, but that isn't the same

as you having it. If someone stops you with a question, a leaflet or a bit of commotion, stay aware of your things. Most of those moments are innocent. This is simply how the Metropolitan Police describe distraction theft working.<sup>3</sup>

**TIP Make the laptop the first thing you pack**

When you get up, close the lid and put the laptop in the bag before anything else. Cables, cups and notebooks can wait. Done every time, this habit becomes automatic, and it covers the gap that most grabs use.

---

## Trains, buses and stations

On trains, glance at your bag at each station stop, and take valuables with you when you leave your seat or nod off. Don't run a laptop cable across an aisle or an emergency exit. A restraint that makes sense on a desk becomes a trip hazard in a moving carriage. And a cable doesn't make it fine to wander off to the café car with the laptop still on the table.<sup>4,5</sup>

**TRICK Use your feet**

On a seat, put the bag between your feet with a strap around your ankle or the chair leg. A thief who has to reach under you is far less likely to try, and you will feel the tug if someone does.

---

## Cars

In a car, the best place for the laptop is with you. Hiding the bag doesn't turn a parked car into safe storage. West Yorkshire Police specifically warn against leaving valuables or work equipment in vehicles, boot included. A car alarm is one more layer, and it does nothing for your data.<sup>6</sup>

**WATCH OUT Not the boot either**

A thief who sees you put a bag in the boot knows exactly where to look. Put things away before you arrive, or better, take them with you.

## Conferences, events and meal times

Busy events make easy hunting grounds. The US Cybersecurity and Infrastructure Security Agency (CISA) points out that meal times are a good time for thieves to check hotel rooms for unattended laptops, and that conferences and trade shows offer them a wide choice of devices, with owners who are distracted by talks and meetings. <sup>181,183</sup>

- Keep the laptop on you during breaks, or use a staffed cloakroom rather than a pile of bags by the door.
- At a stand or a speaker table, keep the laptop on your side of the table and lock it if you will be talking to people.
- When you present, have your slides on the laptop you can keep in sight, not on a machine you leave on the lectern overnight.

## Bags, labels and records

We like a plain, unbranded everyday bag because it doesn't advertise what's inside. That's our preference, not a measured drop in theft. The same thinking applies to luggage labels: give a way to reach you, not a public list of your name and home address. Keep the serial number, the receipt and a few clear photos somewhere you can reach without the laptop. Property registration or forensic marking can help identify a recovered machine, and what's available depends on your country. <sup>4,8</sup>



### **TIP A small alarm can help in a few places**

Some bags and small motion alarms make a loud noise if a bag is moved or opened. CISA mentions alarms and locks as options for portable devices.

<sup>181</sup> An alarm doesn't stop a determined thief, but it can make the grab louder and less attractive. Think of it as a habit helper, not a lock.

## Work laptops

If your employer manages the laptop, use their backup, recovery and incident procedures. Report a loss quickly. Don't switch off company security settings or install your own recovery software to work around them.<sup>1</sup>



### CHECKLIST Do this today

- ☐ Decide where your laptop goes when you stand up, and do it every time.
- ☐ Take a photo of the serial number label and the receipt, and store it away from the laptop.
- ☐ Check your bag: does it shout "laptop inside"?
- ☐ Never leave the laptop in the car, not even for a few minutes.

### MORE ON THE SITE

→ [Prevent the easy theft first](#)



### Stay in the loop

Short, honest takes on gadgets and how to keep them. No spam.

[Get the TechCortado newsletter](#)

[Bluesky](#) · [Mastodon](#) · [Pixelfed](#) · [TechCortado.com](#)

# 03

## CHAPTER 3

# Locks and anchors

*Slow the grab down*

---

### INSIDE

What a cable lock can do

Fit comes before strength

What to check when it arrives

Key, combination or both?

Cable thickness tells you something, but not everything

Read the test claim down to the fixture

Slotless laptops: three options, three compromises

Making the buying decision

**IN THIS CHAPTER**

- A cable lock is a delay and a deterrent, not a vault. Makers say so themselves.
- Think of a chain: furniture, anchor, cable, lock head, slot, laptop body. The weakest link decides.
- Fit comes before strength. There are three common slot shapes that look alike but don't swap.
- Keyed or combination is a matter of how you live. The anchor matters more than the choice.
- Laptops without a slot need an adapter, an adhesive plate or a locking station, each with a catch.
- **Time needed:** 20 minutes to identify your slot and plan a setup.

---

## What a cable lock can do

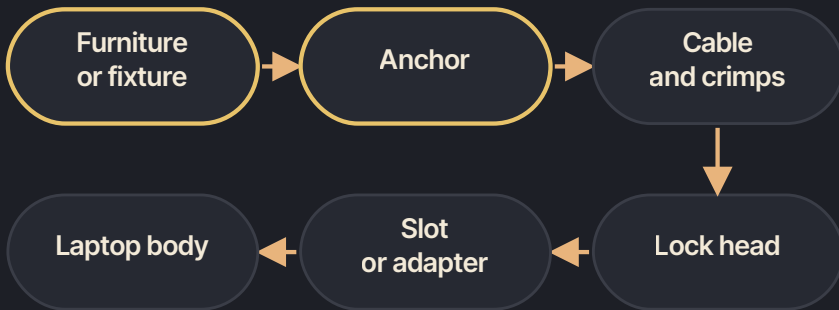
A cable lock earns its place anywhere someone could pick up your laptop and walk off before you notice. Its job is modest: make that grab slower, clumsier and more obvious. One laptop maker's security-cable manual says it plainly. The cable is a deterrent and can't guarantee the computer won't be stolen. We think that's the right yardstick for every glossy claim in this category. A lock can be useful without being unbeatable.<sup>9</sup>

It helps to picture the whole chain: **furniture or fixture → anchor → cable and crimps → lock head → laptop slot or adapter → laptop body**. That's a way of thinking about it, not a measured ranking. The strongest link doesn't make up for an anchor that the cable can slide off, a weak adhesive bond or a flimsy attachment point. An expensive lock looped around something that can leave with the laptop hasn't achieved much.

So before you buy, look at where you'll actually use it. A properly fitted desk anchor can work well in a home office. A fixed part of the building might do in a shared workspace. A light café chair won't. If there's nothing solid to lock to, keeping the laptop with you is the better call. And keep the cable out of walkways. Security shouldn't come with a trip hazard.

## A cable lock is a chain

The weakest link decides what it can do.



Outlined in yellow: the links people forget. A light chair or a desk part that lifts off undoes the best lock head.

TechCortado.com

**Figure 3.1** A cable lock is a chain. The furniture and the anchor are the links people forget.



**Figure 3.2** A combination cable lock in use. The loop around a fixed object matters as much as the head in the slot.

Photo: [Santeri Viinamäki](#), [CC BY-SA 4.0](#), via Wikimedia Commons.

## Fit comes before strength

Three slot shapes cover most of the market. Treat the sizes below as clues for identifying your slot. They aren't engineering drawings, and a tip of a similar size won't necessarily fit. <sup>10,11,12</sup>

| Slot family                                         | Approximate opening       | What it means when buying                                                                                    |
|-----------------------------------------------------|---------------------------|--------------------------------------------------------------------------------------------------------------|
| Standard slot (often called a K-slot or T-bar slot) | 7 × 3 mm                  | Ask for the standard slot by name. A brand name on its own is vague, because lock makers sell several heads. |
| Nano slot                                           | 6 × 2.5 mm                | Needs a head that's clearly Nano-compatible, or a universal head that lists Nano.                            |
| Wedge-shaped slot                                   | About 4.5 × 3.1 to 3.2 mm | Needs explicit wedge compatibility. Several makers sell heads for it.                                        |
| No security slot                                    | None                      | Look at a model-specific adapter, an adhesive adapter or an external locking station.                        |

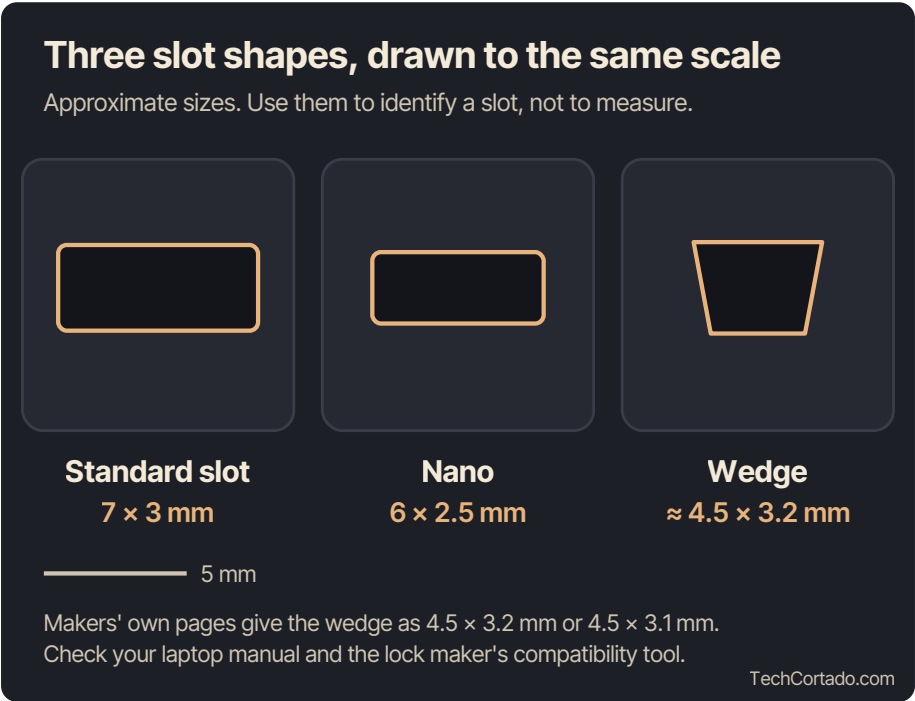


**Figure 3.3** The three common slots, drawn to scale. They look alike, and a lock for one won't fit another.



**Figure 3.4** A standard security slot on a thin laptop. Check yours against the model's manual before buying a lock.

Photo: [Bobulous](#), [CC BY-SA 4.0](#), via Wikimedia Commons.



#### **WATCH OUT Even the makers disagree by a fraction**

One lock maker's own pages give the wedge slot as  $4.5 \times 3.2$  mm in one place and  $4.5 \times 3.1$  mm in another. So don't settle the question with a ruler and a product photo. Start from your laptop's exact model and generation and its manual, then check against the lock maker's compatibility tool. The mismatch is a reason to check fit carefully. It doesn't mean there are two different wedge standards. <sup>10,11,13</sup>

One large laptop maker says outright that its machines don't all take the same lock. Some have standard slots, some have wedge slots, and some have none. Brand names and slot names have got thoroughly tangled over the years, so read the slot type and the exact product code, not the brand on the box. <sup>12,14</sup>

Universal locks make life easier in a household or office with several different laptops. But "universal" can't add a slot to a laptop that doesn't have one. Some heads need you to set the right tip position before you insert them, and some need a spacer chosen for your slot. Others use a single tip with no swappable parts. Read the instructions for the product you bought, not the older one that looks almost the same. <sup>15,16</sup>

## What to check when it arrives

Do the first fitting at home, while you can still return it. Find the slot, follow the lock's guide and use the right spacer. The head should go in without force and sit without levering the laptop up. Nearby ports should still be usable, and the lid should open and close normally. A head that looks compact in the listing can still get in the way on a laptop with a low slot. At least one maker lists the height to the slot's midpoint for its compact heads, which tells you clearance is a real design limit. <sup>15,17</sup>

Once it's locked, give it a gentle tug in the direction someone would pull it off. You're checking that it engaged, not testing its strength. Don't hang the laptop from it, yank the cable or copy a demo video. Leave enough slack to move the laptop a little, but not a loop that a passing bag or knee will catch.

With a combination lock, spin every dial away from the code once it's on. Lock manuals tell you to scramble all of them. Try out a new code while the lock is off the laptop, or at least where a mistake won't trap your working computer. Keep the code somewhere you can reach from another device. <sup>11</sup>



### **TRICK Photograph the fitted lock**

Once the head fits, take one photo of the slot, the spacer you used and the fitted head. When you replace the lock or buy one for a second laptop, that photo saves an evening of reading compatibility charts.

---

## Key, combination or both?

A keyed lock is easy if your keys stay in your pocket and a spare lives somewhere else. The way it goes wrong is a key kept in the laptop bag, which can disappear in the same theft. A combination gets rid of the key but gives you a code to remember or store. Skip birthdays, never keep the factory code, and don't write it on the laptop.

Four dials with ten digits each give 10,000 possible codes. That's not comparable to a strong password. A mechanical lock can fail in physical ways, and there's no honest way to turn a code count into "it would take a thief X minutes." How well the lock is made and installed still matters more. <sup>16</sup>

Hybrid locks need careful reading. Some open with a key **or** a combination. That's handy as a backup way in, but it isn't two-factor protection where you'd need both. On at least one such design the key doesn't reset the combination either. Product listings saying "key and combination" make this easy to misread. <sup>18</sup>

Set up recovery before you travel. Some lock makers run a registration service for replacement keys and stored combination recovery. If yours does, register, protect that account, and keep the lock's ID and receipt away from the laptop. For companies, master keys need just as much thought: they're convenient for the IT team, and they also change who can open every lock.

<sup>19</sup>

Keyed or combination, side by side

|                             | Keyed lock                                                                                                                      | Combination lock                                                                                                 |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Pros                        | Nothing to remember. Quick to open. Spare keys, keyed-alike sets and master keys are possible.                                  | No key to lose. Many models let you reset or share a code without handing over hardware.                         |
| Cons                        | The key can go missing, or leave in the same bag as the laptop.                                                                 | A code to remember and protect. Dials can be watched, guessed or decoded on weak designs.                        |
| Attacks we found documented | Shimming or forcing the head on older designs; cutting the cable. <sup>114</sup>                                                | Decoding the dials through design flaws; cutting the cable. <sup>113</sup>                                       |
| Lost key or code            | A replacement key through the maker's registration service, if you registered first. Otherwise the lock gets cut. <sup>19</sup> | Recoverable only if the maker stores codes or an admin can reset the model. Otherwise it gets cut. <sup>19</sup> |
| Shared desks                | Keyed-alike or master-keyed sets suit an IT team that hands out laptops. <sup>46</sup>                                          | Resettable codes suit hot-desking, as long as people really change them.                                         |
| Travel                      | Fine if the key lives on your keyring, never in the laptop bag.                                                                 | Nothing to forget at home. Scramble every dial each time.                                                        |

**EXAMPLE From the history books**

Two old reports are worth knowing, as history and not as tests of today's models. In 2004 a news agency reported that a security researcher had opened common laptop cable locks with the barrel of a ballpoint pen, thin plastic or rolled-up cardboard. In 2006 a technology site covered a combination laptop lock being decoded through flaws in its design. The makers have changed their designs since. The lesson that lasts: 10,000 codes on the box tells you very little about how long a lock holds. <sup>114,113</sup>

**Our pick:** keyed for one owner who always has their keys on them. Combination for hot desks, shared kit and anyone who loses keys. Either way, the fit of the head and the thing you anchor to matter more than the choice between the two.

## Cable thickness tells you something, but not everything



**Figure 3.5** A coiled cable lock. Thickness is one clue to strength, not the whole story.

Photo: [Fastily](#), CC BY-SA 4.0, via Wikimedia Commons.

A small coiled cable is easy to carry. A thick straight one may be annoying enough that you leave it at home. That trade-off is real. In 2024 one lock maker published minimum tensile figures for its cable families, and its coiled travel cables come in lower than its standard and heavy-duty ranges. Those are the maker's own family specs. We didn't test them, and they don't cover every product on sale now. <sup>20</sup>

Thickness includes how the cable is built and sometimes the coating, so compare like with like when the specs allow. The force that snaps a cable also isn't the force needed to beat every other part. A strong cable can sit on a weak laptop attachment. The plastic coating mostly protects surfaces. A thick jacket doesn't mean more steel.

A two-headed cable can secure two compatible devices, but check what's really held. Locking a USB-C dock doesn't lock the laptop plugged into it. Lock the laptop as well, unless the dock has a documented way of holding that exact computer. Cable traps for peripheral leads are a convenience, and how well they hold depends on the cable and connector shape. Don't assume everything in the product photo is protected on its own.

---

## Read the test claim down to the fixture

Published force numbers are worth reading, but the details decide what they mean. One maker describes a single pound-force test on its wedge heads. Another describes straight and side pull tests, with the slot held in a fixture in a machine, a set pull rate, and samples pulled until they fail. Those are different descriptions, without enough in common to say one brand is twice as hard to steal as the other. The fair summary is that both makers report testing. Nobody has handed us an independent league table.

<sup>21,20</sup>

The fixture makes a big difference. A head held in a lab fixture hasn't been tested inside every thin laptop it might end up in. Ask whether a figure refers to the cable, the head, the fixture or the complete assembly. Ask for the SKU, the pull direction, the number of samples, what counted as failure, and the report. And no pull-force result can back up a claim like "safe to leave for five minutes."

Durability is a separate question from resisting an attack. One maker's history of its own testing mentions temperature tests, repeated drops and rotation cycles. That matters for something you carry, bend and use daily. It doesn't turn a warranty into theft insurance, and it doesn't prove a particular thief can't beat your setup. Check the current warranty and any theft cover that's stated separately, rather than assuming either exists.<sup>22</sup>



#### **WATCH OUT** Labels that sound like ratings

Two other labels often get read as more than they are. **TAA compliant** is about US government purchasing rules on country of origin. **ISO/IEC 27001** is about how an organisation manages information security. Neither one, by itself, is a timed attack rating for the cable in your hand. A lock can be part of a company's physical security without carrying a "secure laptop" certificate.<sup>23,24</sup>

## Slotless laptops: three options, three compromises

A **model-specific adapter** clamps onto a slotless laptop and gives it a standard T-bar lock point without glue. Versions exist for many thin laptops, made for each model and size. Buy against the exact model identifier, because "fits this brand" isn't enough. Check case compatibility, clearance and the fitting instructions. An adapter maker's warranty statement isn't the same as approval from the laptop's maker.<sup>25</sup>

An **adhesive adapter** suits devices that have no dedicated adapter. It is a small plate stuck on with very high bond tape, often with a retractable lock point. Its advertised holding force is the maker's claim. It doesn't show that it holds as well on every coating, removable skin or older base cover. The surface and the bond become part of your security chain.<sup>26</sup>

With pressure-sensitive adhesive, prep and waiting time matter. A tape maker's general guidance calls for clean, dry surfaces and firm pressure, and says the bond builds over time. Its example room-temperature figures reach full strength after about 72 hours. Follow the adapter's own instructions, and only use surface prep that's safe for your laptop's finish. Don't sand a laptop or heat it because an industrial tape guide mentions those steps. Good glue on a poor surface is still a weak point.<sup>27</sup>

An **external locking station** holds the laptop with arms or a frame, without changing the computer. It suits a desk you use every day far better than a light travel bag. Check physical fit, not just screen size. Even the maker's size range and model list don't replace checking your exact laptop.

28

For a desk anchor, decide how it will be attached before you order. Some come with adhesive and one-way screws. Screws in the box only help if your desktop and your fitting can hold them. Ask before drilling a shared desk, and check a fitted anchor now and then. 29

| Option                 | Good for                                  | Watch for                                      |
|------------------------|-------------------------------------------|------------------------------------------------|
| Model-specific adapter | A slotless laptop you carry, with no glue | Exact model fit, cases, clearance              |
| Adhesive plate         | Devices with no adapter made for them     | Surface, prep, about 72 hours to full bond     |
| Locking station        | A desk you use every day                  | Size range, weight, cost of the station itself |
| Desk anchor            | Giving a lock something solid to hold     | How it's fixed, permission to drill            |

## Making the buying decision

For one laptop with a known slot, start with a head that clearly fits, has room to sit properly, comes with a suitable cable and goes on a good anchor. With several slot types in the house, a universal head can cut down on mistakes, as long as you understand how to adjust it. For a slotless travel laptop, compare how bulky each exact adapter is and what fitting it needs. For a fixed workspace, improve the anchor before you spend more on the head.

Keep the routine short: **anchor, engage, gentle check, take the key or scramble the dials, lock the screen**. When you leave, take the laptop with you whenever you can. The lock backs up your attention. It shouldn't become the reason you walk away. Its biggest value may be stopping a quick grab. Encryption and backups handle the much worse day when prevention fails.

# Questions worth asking before buying a lock

| Ask the seller or maker                                                    | Why the answer matters                                                                |
|----------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Does this exact product fit my exact laptop model and generation?          | "Works with brand X" is too vague.                                                    |
| Which slot type and spacer does it need?                                   | Openings that look alike aren't interchangeable.                                      |
| Will the laptop sit flat with charging and data cables plugged in?         | A lock you take off because it gets in the way does nothing.                          |
| Is the stated diameter for the head, the steel cable or the outer coating? | Listings often put unrelated measurements side by side.                               |
| What exactly was tested, and can I read the report?                        | Cable strength, fixture strength and holding a real laptop are different things.      |
| Is the code resettable, fixed, or recoverable by an admin?                 | This decides daily handling and what happens in an emergency.                         |
| Does the box include the cable, adapter and anchor?                        | Several products with similar names are parts or bundles.                             |
| What surface and curing conditions does fitting need?                      | Adhesive and screw anchors depend on what they're attached to and how.                |
| What are the local replacement-key, warranty and return terms?             | A global product page may not match what you buy locally.                             |
| Does any of the advertised protection include theft reimbursement?         | A product warranty usually covers the product; theft cover needs its own clear terms. |

In the end, one question settles it. Will this whole setup reliably stop someone picking up this particular laptop in the places you use it? Once you've answered that, encryption and a recovery plan you've rehearsed limit the damage if it disappears anyway.



**TIP** Example products live at the back

If you want names to start a search, Appendix B lists example locks, adapters and anchors as of 2026, by slot type. They are examples, not endorsements. Check fit for your exact model first.

**CHECKLIST Do this today**

- ☐ Find your laptop's slot and check its type in the manual.
- ☐ Look at the places you work: is there anything solid to anchor to?
- ☐ If you already own a lock, practise the routine: anchor, engage, gentle check, take the key or scramble the dials, lock the screen.
- ☐ Put the spare key or the code somewhere away from the laptop bag.

**MORE ON THE SITE**

→ [Physical locks in detail](#)

→ [Questions to ask before buying a lock](#)

**Stay in the loop**

Lock tests, new slot types and fresh buying notes, when we have them.

**Get the TechCortado newsletter**

[Bluesky](#) · [Mastodon](#) · [Pixelfed](#) · [TechCortado.com](#)

# 04

## CHAPTER 4

# Encryption and power states

*Make the drive useless to a thief*

---

### INSIDE

Know what state the laptop is in

Windows: check the protection, not the padlock icon

macOS: hardware encryption and FileVault aren't the same promise

Linux: check the storage layout, not the logo

Encrypted containers: a useful extra compartment

Recovery keys are part of your security

Which encryption, side by side

Fingerprint, face or PIN?





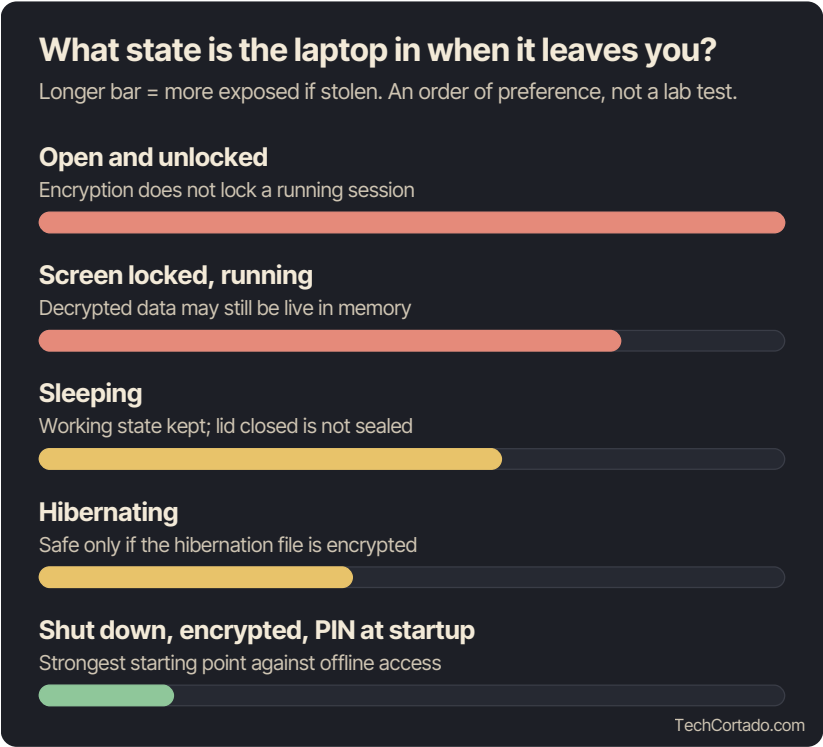
## IN THIS CHAPTER

- Encryption keeps stored data unreadable without your password or key. It doesn't protect a session that is already unlocked.
- The state the laptop is in when it leaves you matters: shut down is strongest, open and unlocked is weakest.
- Check, don't assume. On Windows, read both the encryption percentage and the protection status.
- A startup PIN or passphrase adds a step before the system starts. Worth it on a laptop that travels.
- A recovery key stored only on the stolen laptop is no recovery key.
- **Time needed:** 10 minutes to check; an evening if you need to turn it on.

A cable can stop someone walking off with your laptop. Encryption covers the next failure, when they have it anyway. Its job is to keep what's stored on the drive unreadable without an authorised way to unlock it. That means the obvious files, and also cached email, downloaded bank statements, browser data, app databases and half-finished work sitting in temporary folders. Windows and Ubuntu both describe full-volume encryption as protection for data at rest. Neither claims it hides whatever is already open on an unlocked screen. <sup>47,48</sup>

The goal is simple to say. The thief ends up with hardware you can replace, and you keep your work and your accounts. Getting there means checking a few real things: whether encryption is actually on, how the computer unlocks, what the encryption doesn't cover, and which recovery material you'll need after the theft. A recovery key saved only on the stolen laptop is a plan with the first step missing.

# Know what state the laptop is in



| Laptop state                                               | What it means if it's stolen                                                                                            | Sensible habit                                        |
|------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| Shut down, encrypted, with suitable startup authentication | The strongest starting point against offline access, though hardware, passwords and recovery-key handling still matter. | Make this your travel default for sensitive material. |

Treat this as a defensive order of preference, not a ranking that holds for every laptop design. For Windows machines facing skilled physical attacks, Microsoft specifically recommends a TPM plus a startup PIN, and shutting down or hibernating instead of using standby. TPM-only unlock is a fair baseline against opportunistic theft, but hibernating doesn't magically add a second startup factor.<sup>49</sup>



**EXAMPLE Old research, lasting lesson**

Back in 2008, the original cold-boot research showed memory could hold data long enough to undermine the encryption products of the time. That's why the power state belongs in any theft plan. It doesn't show that today's Apple-silicon Macs or every modern Windows laptop can be attacked the same way. Modern hardware needs its own evidence.<sup>50</sup>

## Windows: check the protection, not the padlock icon

Windows Home isn't automatically left out. Microsoft offers Device Encryption on eligible Home machines, while the more configurable BitLocker Drive Encryption controls come with Pro, Enterprise and Education. Whether it switches on by itself depends on setup. Microsoft says signing in with a Microsoft, work or school account can turn on Device Encryption and save a recovery key to that account, while setting up with a local account doesn't. So look at the actual machine rather than assuming the edition name tells you the answer.<sup>51</sup>

To check without changing anything, open Command Prompt as administrator and run:

```
manage-bde -status
```

It lists your drives and their encryption and protection status. Check every drive that holds anything you care about. Read the encryption percentage

together with **Protection Status**, because a percentage alone proves little. The system drive will normally show as unlocked while Windows is running. That's expected, not a fault. <sup>52</sup>



**TIP Two lines, read together**

In the output, look for **Percentage Encrypted** and **Protection Status** on every drive. "100%" with "Protection Off" means the data is scrambled but the key is sitting unprotected. You want 100% and Protection On.

The difference really matters after repairs or firmware updates. BitLocker protection can be suspended while the data stays encrypted, which leaves the key available without the usual protection. The laptop looks encrypted but isn't protected the way you think. Recheck after any servicing, and if protection is suspended, have whoever manages the machine fix it. Don't play with protector-deletion commands to tidy up the output. <sup>53</sup>

A TPM ties unlocking to the expected startup environment. A separate BitLocker startup PIN or startup key adds a step before Windows starts or resumes from hibernation. That's a different thing from the Windows sign-in PIN, which comes later. The extra step has a cost: unattended restarts and recovery get less convenient. We'd choose it for a travel laptop carrying sensitive material, if your organisation's setup allows it. <sup>54</sup>

The NCSC backed this up in August 2026. Writing about weaknesses in the Windows Recovery Environment, including an issue that has since been patched, it recommends authentication before Windows boots instead of assuming disk encryption alone closes every route. It also covers network unlock for companies and TPM-plus-startup-key setups where typing a PIN isn't realistic. Our takeaway: patch Windows and its recovery components, and keep the extra startup factor where you can. A PIN doesn't replace updates. <sup>55</sup>

Keep Secure Boot on and the firmware up to date. On hardware that supports it, look for Kernel DMA Protection in System Information (`msinfo32`) or in Windows Security's memory-access settings. DMA lets some external devices read memory directly, and Microsoft uses the IOMMU, a hardware gatekeeper for those devices, plus driver isolation to limit what they can reach. It depends on your hardware and firmware, it doesn't cover every

older port or physical attack, and it doesn't make random accessories trustworthy.<sup>56</sup>

Device Encryption doesn't automatically cover external USB drives, so encrypt your portable backup disk separately. If a second internal drive holds virtual machines or project archives, include it in your check too. An unprotected second drive can hold exactly what the thief is after.<sup>47</sup>

---

## macOS: hardware encryption and FileVault aren't the same promise

Macs with Apple silicon or the T2 chip encrypt their internal storage automatically. Turning on FileVault ties your login password into the protection of the keys. So "my Mac already encrypts its SSD" isn't a reason to leave FileVault off. Apple says FileVault keys on these machines are handled in the Secure Enclave, a separate security processor, and aren't directly exposed to the main CPU. Claims that every modern Mac's disk keys sit in ordinary memory are wrong. Older Intel Macs and external drives need their own attention.<sup>57</sup>

Check **System Settings → Privacy & Security → FileVault**. Pick the recovery option that suits the machine and keep it somewhere other than the computer. If you use a separate recovery key, store it safely away from the Mac. If you rely on account recovery, make sure you can get into that account without this laptop. Lose both the login and the recovery route and the files can be gone for good.<sup>58</sup>

A locked Mac is still a running computer. Apple's security documentation separates hardware generations, boot modes and data-protection classes, including data that stays available after the first unlock. So don't read "Secure Enclave" as meaning every document, session and app is sealed whenever the screen locks. For sensitive travel, shutting down is still a clear habit, without claiming every platform works the same inside.<sup>59</sup>

Turn on Find My before anything goes missing. On supported Macs, Activation Lock depends on the right account and startup-security settings. It can survive a remote erase and make the Mac less useful to a thief. That's a different job from FileVault, which keeps data private. Neither one stops someone physically taking the machine.<sup>60</sup>

Chapter 8 covers Find My's recovery actions and their limits. Set them up before you need them.

---

## Linux: check the storage layout, not the logo

Ubuntu's usual encryption uses LUKS and dm-crypt. In plain terms, LUKS locks the real encryption key behind one or more passphrases or unlock methods, and your login password is a separate layer from the disk passphrase. A familiar login screen doesn't tell you the disk underneath is encrypted. On a personal machine, the encryption option your distribution offers during installation is usually easier to trust than converting an existing system by hand. Back up first and follow the instructions for your release. An encryption installer isn't a harmless checking tool. <sup>48</sup>

Check the root filesystem, any separate home or data partitions, swap, and external drives. Hibernation writes your working state to storage. The kernel documentation explains that encrypted resume storage has to be unlocked before the system can resume. So "I encrypted my home folder" doesn't prove the hibernation image is safe. The kernel's old example scripts explain how it works; don't paste them into a current laptop. Use your distribution's supported setup. <sup>61</sup>

TPM-backed encryption on Linux needs careful reading of the documentation for your exact release. Some distributions have labelled their hardware-backed disk encryption as experimental in earlier releases, with limits around kernels and extra drivers. Newer releases document optional startup PINs or passphrases on top of the TPM, and describe that passphrase as an extra requirement that still holds even if the TPM protection is broken. Requirements usually include specific UEFI and TPM2 support plus Secure Boot. Having a TPM chip doesn't prove your whole setup is supported, and none of this is a knock on ordinary passphrase-based LUKS. <sup>62,63,64</sup>

Recovery steps also change between releases. One release may describe a stored recovery key you can read, while a later one describes replacing a lost key while you can still log in, which cancels the old one. Check the documentation for your version and sort out recovery before something breaks, not at the boot prompt. <sup>62,65</sup>

If you're comfortable with Linux, also keep a backup of the LUKS header, the small block at the start of the disk that holds the key slots, and understand what it can unlock. The cryptsetup FAQ warns that encrypted disks still need backups, and that cloning a LUKS image keeps the same underlying key. Changing the passphrase on a clone doesn't make it independent. That matters if you hand out VM or laptop images. Don't fix a theft problem by quietly giving several machines the same secret. <sup>66</sup>

---

## Encrypted containers: a useful extra compartment

An encrypted container is a single file that you open as a drive when you need it and close again afterwards. Open-source tools for this run on Windows, macOS and Linux. A container can keep a small set of sensitive files apart from everyday use, especially if it stays closed most of the time. It doesn't replace encrypting the system drive. Opening a document puts its contents in the app's memory, and that can end up in an unencrypted hibernation file if the system disk isn't protected. Encrypt the system drive as well, and check how your OS behaves. <sup>67</sup>

Closing the container doesn't guarantee the editor or viewer has wiped every trace from memory. Container tools document this limit themselves. Memory-protection features depend on the version and settings, so having a tool installed doesn't mean they're switched on. The habit that holds up: close the sensitive work, close the container, and shut down before the laptop leaves your control when the situation calls for it. <sup>68</sup>



### **WATCH OUT** Encryption doesn't stop malware

Encryption can't stop malware from reading documents your running system has opened, or from capturing passwords as you type them. Keep the OS, the browser and your key apps supported and updated. Encryption, app isolation and account security cover different failures, and you need all three. <sup>69</sup>

# Recovery keys are part of your security

A BitLocker recovery key is a 48-digit unlock code. Depending on how encryption was set up, it might be in your Microsoft account, your employer's account, on a printout or on a saved USB copy. Microsoft can't recreate it if every copy is lost. Before you travel, check you can reach it from a second trusted device. Never post it in a screenshot or a support forum. On a work laptop, use IT's key escrow and incident process instead of copying company recovery material into your personal cloud.<sup>70</sup>

The recovery code should be easy for you to reach and out of reach for whoever takes the bag. A password manager you can open on another trusted device is one option. A well-protected offline copy is another. Avoid the circle where your only password-manager access, your second factor and your recovery key all leave with the laptop. Encryption should make a theft survivable. It shouldn't turn an ordinary motherboard failure into permanent loss.



## TRICK The second-device test

Pick up your phone or another computer, not the laptop, and try to find your recovery key right now. If you can, good. If it takes more than five minutes or you can't, fix that before you travel.

# Which encryption, side by side

People often ask whether a free third-party tool beats the encryption built into the operating system. For the system drive, the honest answer is that each does a slightly different job. Here is how the main options compare on what changes daily life.

|      | Open-source system encryption (third party, Windows) | BitLocker (Windows Pro, Enterprise, Education)     | Device Encryption (Windows Home and others) | FileVault (macOS)               | LUKS (Linux)                                   |
|------|------------------------------------------------------|----------------------------------------------------|---------------------------------------------|---------------------------------|------------------------------------------------|
| Cost | Free and open source <sup>115</sup>                  | Included with those Windows editions <sup>47</sup> | Included on eligible devices <sup>51</sup>  | Included in macOS <sup>58</sup> | Free, offered by most installers <sup>48</sup> |

|                                          | Open-source system encryption (third party, Windows)                                                                | BitLocker (Windows Pro, Enterprise, Education)                               | Device Encryption (Windows Home and others)                                          | FileVault (macOS)                                                              | LUKS (Linux)                                                               |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|--------------------------------------------------------------------------------|----------------------------------------------------------------------------|
| <b>Which systems</b>                     | System drive: usually x64 Windows only. Containers: most desktop systems <sup>116,117</sup>                         | Windows                                                                      | Windows, including Home                                                              | Mac                                                                            | Linux                                                                      |
| <b>Password before the system starts</b> | Yes, at the tool's own boot loader, often on a US keyboard layout <sup>118,115</sup>                                | Optional startup PIN or USB startup key <sup>47</sup>                        | Unlocks automatically with the TPM; we found no documented startup PIN <sup>51</sup> | Your login password unlocks the disk at startup <sup>58</sup>                  | Passphrase at boot by default <sup>48</sup>                                |
| <b>TPM plus PIN</b>                      | No TPM use, by design <sup>115</sup>                                                                                | Yes, recommended for sensitive travel <sup>54,55</sup>                       | No PIN option found                                                                  | Apple hardware keys plus your password, not a TPM <sup>57</sup>                | Optional TPM2 plus PIN on supported setups <sup>122,63</sup>               |
| <b>If you forget the password</b>        | No recovery and no backdoor. A rescue disk repairs the boot loader but still needs your password <sup>115,119</sup> | 48-digit recovery key you save, print or store in your account <sup>70</sup> | Recovery key saved to your Microsoft account automatically <sup>51</sup>             | Online account or a recovery key. Lose both and the data is gone <sup>58</sup> | Spare passphrase slots and a header backup you make yourself <sup>66</sup> |
| <b>Effort</b>                            | Highest. You must make a rescue disk and read the notes before big Windows upgrades <sup>119,118</sup>              | A few settings, plus a PIN policy if you want one                            | Often already on                                                                     | One switch                                                                     | Easiest at install time                                                    |

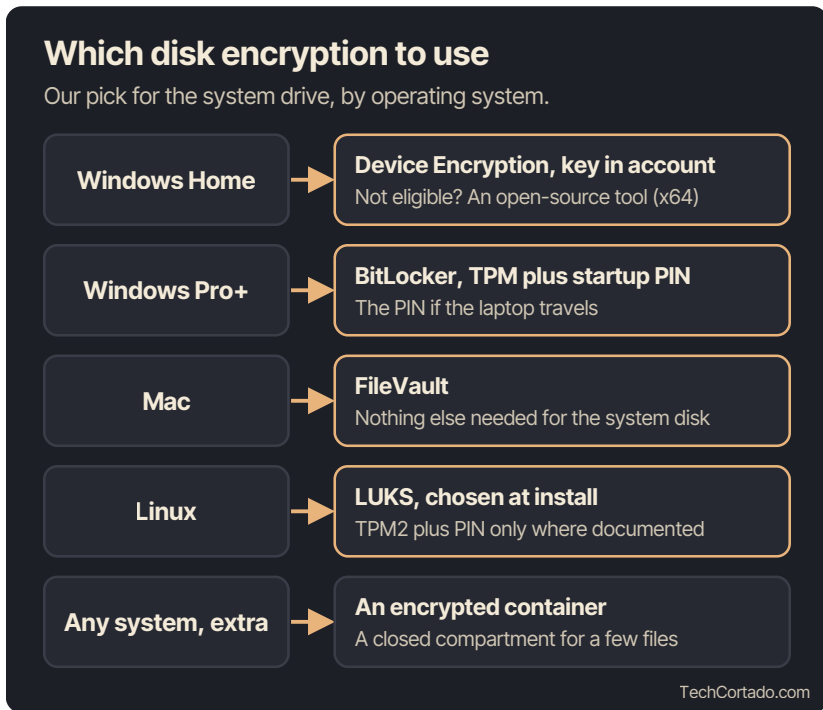


**Figure 4.2** Which encryption to use on each system, in one view.

## Our picks, by system

- **Windows Home:** check Device Encryption is on and that the recovery key is in your Microsoft account. If your laptop doesn't qualify, or you want a password before Windows starts, an open-source system encryption tool is the free option on most x64 laptops.
- **Windows Pro and up:** BitLocker with TPM plus a startup PIN if the laptop travels.
- **Mac:** FileVault. Nothing else is needed for the system disk.
- **Linux:** LUKS chosen at install. Add TPM2 plus PIN only where your distribution documents it.
- **Any system:** an encrypted container is a handy extra compartment for a few files.

## Fingerprint, face or PIN?

Fingerprint readers and face unlock make a locked laptop quick to open again, which makes people more willing to lock it. That is their real value. On most laptops they sit on top of a PIN or password rather than replacing it, and the full password is still the thing that protects the disk at startup.

- Keep a strong PIN or password behind any biometric. It is what unlocks the machine when the sensor can't.
- Restart your laptop once and see what it asks for. If it asks for the full password or startup PIN before the fingerprint works, your encryption is doing its job.
- Shutting down before a trip puts you back to "password first", whichever unlock you use day to day.



### STORY **Imagine the hotel desk**

*Imagine a consultant who works late in a hotel and closes the lid at midnight. The laptop sleeps. In the morning she goes to breakfast and leaves it on the desk. Her drive is encrypted, but a sleeping laptop has its keys ready in memory. Now imagine the same evening ending with a full shutdown. At breakfast, the laptop on the desk is just an encrypted brick that asks for a PIN before anything starts. One habit, a very different risk.*



### CHECKLIST **Do this today**

- ☐ Check encryption on every drive, not only the system drive.
- ☐ Find your recovery key from a second device.
- ☐ Decide on a startup PIN or passphrase if the laptop travels.
- ☐ Make "shut down" your habit before a trip, not "close the lid".

**MORE ON THE SITE**

→ Encryption and the state of the laptop



**Stay in the loop**

Settings move with every system update. We note the changes for you.

**Get the TechCortado newsletter**

[Bluesky](#) · [Mastodon](#) · [Pixelfed](#) · [TechCortado.com](#)

# 05

## CHAPTER 5

# Firmware, boot and tampering

*What the laptop agrees to start*

---

### INSIDE

Firmware passwords

Boot order, USB boot and Secure Boot

Fast ports and memory access

The "evil maid"

Tamper-evident seals, glitter included

If you suspect tampering



## IN THIS CHAPTER

- Firmware settings decide what a laptop will start, and who can change that.
- A supervisor (firmware) password protects those settings. Store it safely: forgetting it can mean a new system board.
- Keep Secure Boot on, put the internal drive first, and turn off USB and network boot if you don't use them.
- Shutting down rather than sleeping blunts several known attacks that need time alone with the laptop.
- Tamper-evident seals don't stop anyone. They tell you afterwards that something happened.
- **Time needed:** 15 minutes in the firmware menu, plus 2 minutes for a seal photo.

Encryption protects the data. The firmware settings decide what else the laptop will agree to start, and that matters most in the minutes a thief, or a curious stranger in a hotel, has alone with it.

---

## Firmware passwords

Most business laptops let you set passwords in the firmware (UEFI, often still called BIOS). One major business-laptop maker's guide describes a power-on password, asked for at every start, and a **supervisor password** that protects the firmware settings themselves. Two details from that guide are worth knowing. The laptop doesn't ask for these passwords when it wakes from sleep. And if you forget the supervisor password, the maker has no service procedure to remove it: an authorised provider replaces the system board, for a fee. Other PC makers use similar settings under different names, so check your own manual. <sup>125,126</sup>

**WATCH OUT The most expensive password to forget**

On some laptops a forgotten supervisor password means a new system board. Save it in your password manager **before** you leave the firmware screen, and check the entry opens from another device.

Macs differ by chip. On an **Intel Mac**, a firmware password stops anyone starting up from another disk or from Recovery without it. On **Apple silicon**, there is no firmware password. Apple says to turn on FileVault instead, and starting from an external system requires an authenticated change to the startup security policy. <sup>123,124</sup>

---

## Boot order, USB boot and Secure Boot

On a PC, set the internal drive first in the boot order and turn off booting from USB and the network if you don't use them. The supervisor password is what stops someone from simply switching those back. Keep **Secure Boot** on. Microsoft describes it as only letting trusted, signed software run while the PC starts, which makes swapping in a tampered boot loader harder. <sup>127,125</sup>

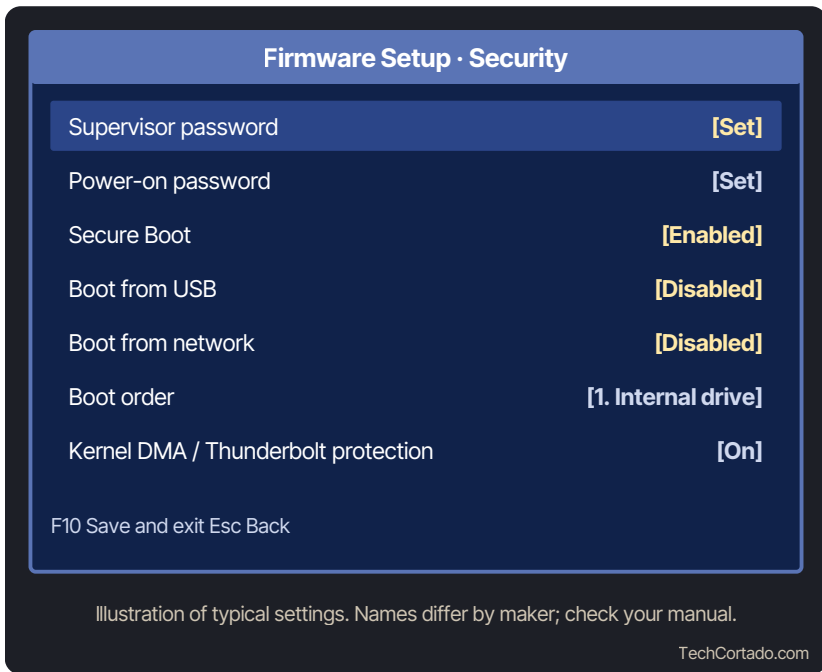


**Figure 5.1** The firmware settings worth checking. A generic illustration, not any one maker's screen.

## Fast ports and memory access

Some fast ports can read memory directly. Microsoft's Kernel DMA Protection blocks that from untrusted devices on supported hardware. The 2020 Thunderspy research showed how much time an attacker needs on older systems without that protection: "5 minutes alone with the computer, a screwdriver, and some easily portable hardware", even with Secure Boot, a firmware password and full-disk encryption on, if the laptop was left asleep. The defences are the ones this book keeps coming back to: shut down rather than sleep when you leave it, use a startup PIN, and keep firmware updated. <sup>56,128,49</sup>

## The "evil maid"

In 2009 a team of security researchers showed the "evil maid" attack on an encrypted laptop left in a hotel room. Someone boots it from a USB stick for a minute or two and plants code that records the password the next time

you type it. The demonstration targeted an earlier open-source encryption tool, but the idea is general. A firmware password, USB boot turned off, Secure Boot and TPM-based checks all make it harder. If BitLocker suddenly asks for its recovery key after the laptop was out of your sight, treat that as a warning sign rather than a glitch. <sup>129,49</sup>



#### STORY **Imagine an unexpected recovery prompt**

*Imagine a laptop that spends two days in a conference hotel room while its owner is at talks. On the third morning it asks for the 48-digit recovery key at startup, which it has never done before. Most of the time there is a dull reason: a firmware update, a changed setting, a dock. But the owner does the sensible thing anyway. She doesn't type her passwords on it, takes it to her IT team, and works from a spare until they have looked.*

## **Tamper-evident seals, glitter included**

A seal won't stop anyone. It can tell you afterwards that someone opened the case. In 2013 researchers Eric Michaud and Ryan Lackey suggested painting glitter nail polish over the case screws: the random pattern is very hard to copy, so you photograph it and compare later. Critics noted the limits. Glitter can shift, real polish is hard to remove when you need a repair, and painting it on a sticker over the screw works better. Commercial tamper-evident labels do the same job with less mess. Either way, it only helps if you actually take the photo and check it. <sup>130,131</sup>

## Glitter on the screws: a seal that tells, not stops



**Photo before the trip**

**Check after**

Paint glitter nail polish over a sticker on the case screws, photograph it, and compare when you get the laptop back. A changed pattern means someone may have opened it. Commercial tamper labels do the same job.

TechCortado.com

**Figure 5.2** Glitter nail polish over the screws. If the pattern changes, the case may have been opened.



### TRICK The two-photo routine

Before a trip, photograph the base of the laptop, screws and seal, in good light. When you get the laptop back after it has been out of your sight, take the same photo and compare the two side by side on your phone. It takes a minute, and a seal you never check is just decoration.

## If you suspect tampering

If a laptop you left unattended looks tampered with, stop using it and bring in whoever is responsible for security before typing any passwords. Concerns about who had it can linger even after it's back. The NCSC recommends stopping use and reporting suspected tampering.<sup>1</sup>

Official travel guidance from several national agencies gives the same advice in plainer terms: keep devices with you where you can, treat a device that was out of your control with more care, and report anything odd to whoever looks after your security.<sup>1,188</sup>

**CHECKLIST Do this today**

- ☐ Set a supervisor or firmware password and save it in your password manager.
- ☐ Check Secure Boot is on and USB and network boot are off.
- ☐ Look for DMA or Thunderbolt protection in your settings.
- ☐ Take a "before" photo of the laptop's base and screws.

**MORE ON THE SITE**

→ [Firmware, boot and tamper protection](#)

**Stay in the loop**

Plain-words security news, a few times a month at most.

**Get the TechCortado newsletter**

[Bluesky](#) · [Mastodon](#) · [Pixelfed](#) · [TechCortado.com](#)

# 06

## CHAPTER 6

# Screen, sign-in and accounts

*Close the doors a thief would try first*

---

### INSIDE

Lock it when you walk away

Privacy screens and shoulder-surfing

Keep the second factor off the laptop

Plan for the day you can't get in

Updates, antivirus and firewall

Shared and family laptops

Carry less





## IN THIS CHAPTER

- The screen lock is the cheapest protection you have. Use the shortcut every time you step away.
- A privacy screen stops people reading over your shoulder. It does nothing against theft.
- Keep at least one second factor off the laptop, ideally a security key on your keyring.
- Updates, the built-in antivirus and the firewall are part of physical security too: a stolen laptop is only as safe as its software.
- Shared and family laptops need separate accounts, each with its own password.
- **Time needed:** 20 minutes.

A thief who gets an unlocked laptop gets more than hardware: open email, saved passwords, signed-in accounts. The doors in this chapter are cheap to close, and most of them are already built into your laptop.

## Lock it when you walk away

The screen lock is the cheapest protection here. Windows key + L locks a PC, and Control-Command-Q locks a Mac. Two built-in features can help on the days you forget.

- **Windows Dynamic Lock** pairs with your phone over Bluetooth. Microsoft says it locks the PC within about a minute after the phone goes out of range, but only if the PC is also idle, and calls it an extra barrier, not a replacement for locking it yourself. <sup>139,140</sup>
- **Presence sensing** on some Windows laptops can turn the screen off when you leave, if the laptop has the sensor. Pair it with a short lock timeout so a dark screen also means a locked one. <sup>142</sup>
- **A paired watch** can unlock a Mac when you sit down. That is a convenience. Apple's page describes unlocking, needs two-factor authentication on your Apple Account and still asks for the password after a restart. We found no built-in feature that locks a Mac when the watch walks away, so keep the shortcut habit. <sup>141</sup>

**TRICK Teach your hand the shortcut**

For one week, lock the screen with the shortcut every single time you stand up, even at home. **Windows key + L** on a PC, **Control-Command-Q** on a Mac. After a week your hand does it without asking you.

What we couldn't find is a built-in consumer alert that tells you when someone types wrong passwords at your laptop's own login screen. Your Google, Microsoft and Apple accounts can warn you about new sign-ins to the account; the laptop itself generally won't. A canary token on the desktop of a decoy account, covered in Chapter 9, is one way to get an alert from the machine.

---

## Privacy screens and shoulder-surfing

Shoulder-surfing is the plain name for someone reading your screen or watching you type. It needs no skill: a seat beside you on a train, a queue behind you in a café, the row behind you on a plane. CISA's advice for portable devices is to pay attention to the people around you and shield yourself from shoulder surfers, so nobody can see you type passwords or read sensitive information on your screen. <sup>181</sup>

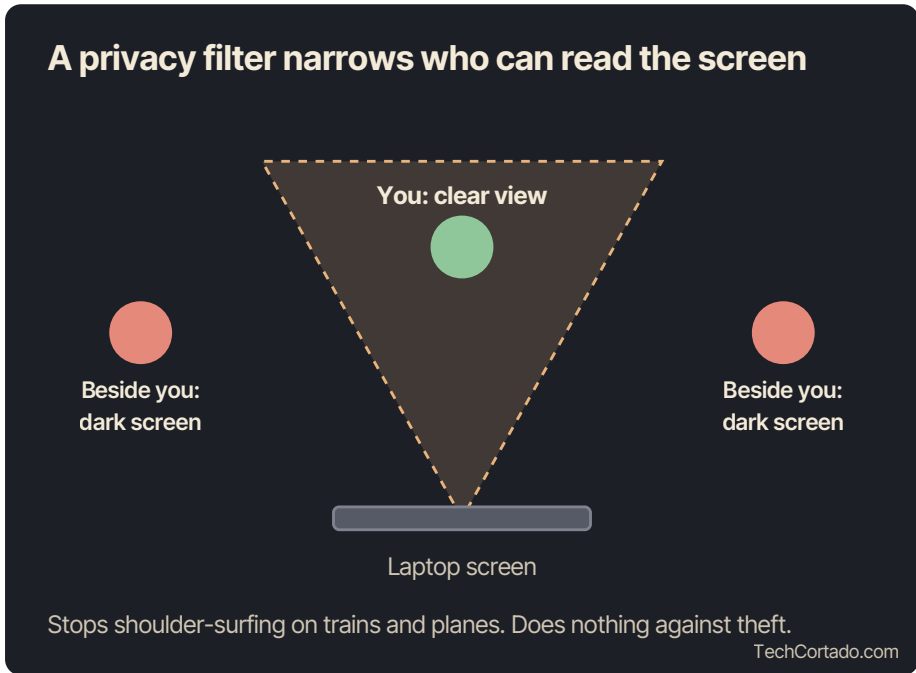


**Figure 6.1** A privacy filter narrows the viewing angle, so people beside you see a dark screen.

## How they work

Most privacy screens use a film with tiny vertical slats, like a set of micro-blinds or louvres, too small to see. Light from the screen passes straight through to you, but light heading off to the sides hits the slats and is blocked. People beside you see a dark or grey panel. Makers commonly quote a viewing cone of about 60 degrees in total (30 degrees either side of centre), which is a maker's figure and not something we measured. <sup>201,143</sup>

Most filters only narrow the view left and right. Someone standing directly behind you, or looking down from above in a crowded train, may still see the screen. A few filters narrow the view in all four directions; check the description if that matters to you.

The main types

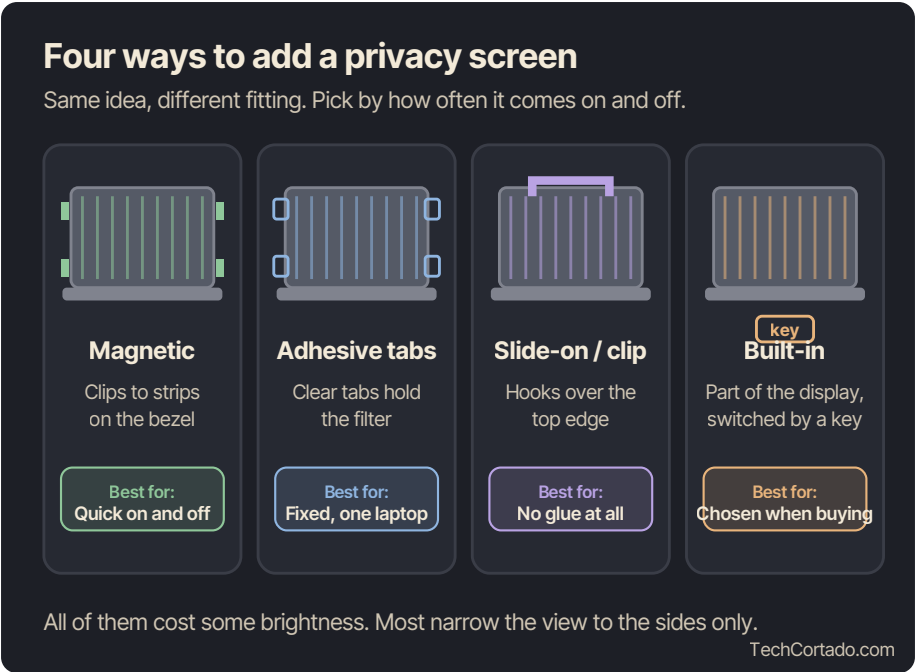


**Figure 6.2** Four ways to fit a privacy screen. Choose by how often it comes on and off.

| Type                  | How it fits                                                         | Good for                                                                               | Watch for                                                                             |
|-----------------------|---------------------------------------------------------------------|----------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| Magnetic              | Clips onto small metal strips or magnets in the bezel               | Laptops you use in public some of the time; easy to take off when you share the screen | Strips stuck to the bezel; some laptop lids have magnets, others need adhesive strips |
| Adhesive tabs         | Small clear tabs stuck to the bezel, filter slides in               | A fixed fit on one laptop                                                              | Tabs can leave marks; harder to swap between machines                                 |
| Slide-on or clip      | Hooks over the top of the screen, sometimes with side clips         | Shared or borrowed laptops; no glue at all                                             | Can shift in a bag; may cover the webcam if badly cut                                 |
| Built-in (switchable) | Part of the display; a key or setting turns privacy mode on and off | People who want privacy without adding anything                                        | Only on some models; chosen when you buy, not added later                             |

Built-in privacy displays use the display's own optics to send light mainly straight ahead when privacy mode is on, and widely when it's off. Display

researchers describe several ways of doing this, from a switchable liquid-crystal layer to a narrow backlight combined with a louvre film. <sup>202,203</sup> The big advantage is that you can switch it with one key when you want to show someone your screen.

## Matte or glossy, and the brightness trade-off

Many add-on filters are reversible, with a matte side that cuts glare from windows and ceiling lights and a glossy side that looks sharper and more vivid. Try both: matte suits bright trains and offices, glossy suits a dim plane cabin. <sup>201</sup>

Every privacy layer costs some brightness, because the slats also block part of the light heading towards you. One maker's datasheet gives a light transmission of 65%, so roughly a third of the brightness is lost; filters sold as "bright" versions claim more. <sup>201</sup> In practice you'll turn the screen brightness up, which costs battery. Built-in privacy modes have a similar trade-off when switched on.



### TIP Choosing and using a privacy screen

- **Match the exact screen size and shape.** Measure the screen diagonal and check the aspect ratio (16:9, 16:10 or 3:2). A filter for the wrong shape leaves a gap or covers the webcam.
- **Pick the fitting for how you work.** Magnetic for on and off use, adhesive tabs for one laptop that always wears it, slide-on for no glue at all, built-in if you're buying a new laptop anyway.
- **Expect a darker screen.** Plan for higher brightness and a bit less battery life, and try the matte and glossy sides.
- **Sit with your back to a wall** on trains and in cafés when you can. A filter narrows the side view; it can't stop someone right behind you.
- **On planes, the aisle seat is the most exposed** to people walking past and standing nearby. A window seat with a filter is calmer for reading documents.
- **Keep it clean and flat.** Dust and a bent filter blur the view, and a scratched one is tiring to read.
- **Remember what it's for.** It protects what's on the screen, not the laptop. You still pack up when you stand up.

**STORY Imagine the 7:40 train**

Imagine a manager on a commuter train reviewing salary figures for her team. The person next to her has nothing to do and the spreadsheet is the brightest thing in the carriage. Nobody means any harm, but by the next stop a stranger knows what three people earn. With a filter on, the neighbour sees a dark rectangle. Even better, she saves that spreadsheet for the office.

**WATCH OUT Typing is visible too**

A filter hides the screen, not your hands. Someone watching your keyboard can still see a password being typed. Use a password manager to fill passwords, and cover the keys with your other hand for a PIN.



**Figure 6.3** Tape over a webcam. Like a privacy filter, a physical cover protects your privacy, not the laptop itself.

Photo: [Santeri Viinamäki](#), [CC BY-SA 4.0](#), via Wikimedia Commons.

---

## Keep the second factor off the laptop

If the laptop holds your password manager, your email and the app that makes your login codes, one theft hands over all three. Keep at least one

second factor somewhere else. A hardware security key on your keyring is the strongest common option, and passkeys built on the FIDO standards resist phishing. Major account providers list a second security key among the ways back in if you lose one, so register two and keep one at home.

144,145,88

---

## Plan for the day you can't get in

Password managers have recovery tools for exactly this. Some give you an emergency kit, a printable sheet with the secret you need to sign in on a new device. Others offer emergency access, where a trusted contact can request access after a waiting time you set, sometimes as a paid feature. Set up whichever yours offers, print what needs printing and keep it away from the laptop bag. <sup>89,146</sup>

---

## Updates, antivirus and firewall

A stolen laptop with old software is easier to get into, and an unpatched laptop at home is easier to attack over the network. Updates fix known holes, so the NCSC's top tips for staying secure online put installing the latest software and app updates near the top of the list and suggest turning on automatic updates. <sup>204</sup>

- **Turn on automatic updates** for the operating system, the browser and your main apps, and restart when asked rather than putting it off for weeks.
- **Use a supported system.** When a laptop no longer gets security updates, plan to replace it or move it to a supported system.
- **Leave the built-in protection on.** Windows includes antivirus, firewall and other protections in the Windows Security app, and macOS includes a firewall you can turn on in its settings. <sup>205,206</sup>
- **Update firmware too.** Laptop makers ship firmware updates that fix security issues, sometimes through the normal update tool, sometimes through their own app.

**EXAMPLE A once-a-month five minutes**

Pick a date, for example the first Sunday of each month. Open the update settings, install what's waiting, restart, then check the Windows Security or macOS settings show no warnings. Five minutes, twelve times a year.

---

## Shared and family laptops

A laptop that several people use is only as careful as its least careful user. Give each person their own account with their own password, and keep the account that can install software and change settings for the adult who looks after the machine.

- **Separate accounts** keep one person's browser sessions, saved passwords and files away from the others. A child who picks up the laptop can't open a parent's email.
- **Standard accounts for everyday use**, including your own if you can bear it. Use the administrator account only when you need to install or change something.
- **Use the system's family or parental settings** for children rather than sharing your own account with them.
- **Sign out of shared machines**, not just close the lid, especially in a shared house or a workplace kitchen.

**WATCH OUT Guests on your laptop**

If a visitor needs to look something up, use a guest account or a separate browser profile, not your signed-in account. It's not about trust. It's about not having to wonder later.

---

## Carry less

The less a laptop is signed into, the less a thief gets. For travel, a separate user profile, or a cheap travel laptop, with only the accounts you need for the trip is a calm middle ground. Chapter 13 shows where that makes sense.

**CHECKLIST Do this today**

- ☐ Set the screen to lock after a few minutes and practise the shortcut.
- ☐ If you work in public, measure your screen and decide on a privacy screen type.
- ☐ Register a second security key or a spare sign-in method and keep it at home.
- ☐ Set up your password manager's emergency kit or emergency access.
- ☐ Turn on automatic updates and check the built-in protection shows no warnings.
- ☐ Give each person who uses the laptop their own account.

**MORE ON THE SITE**

→ Screen, sign-in and account protection

**Stay in the loop**

More small habits that make a big difference.

**Get the TechCortado newsletter**

Bluesky · Mastodon · Pixelfed · TechCortado.com

# 07

## CHAPTER 7

# Backups and account recovery

*Be back at work tomorrow*

---

### INSIDE

Keep copies in places that fail separately  
Cloud, local drive or both, side by side  
Cloud sync helps, but read the recovery terms  
What the built-in tools really cover

A Linux route, with keys you can recover  
Test the restore, boring bits included  
Recover your accounts, not just your files  
Removable drives deserve the same care



## IN THIS CHAPTER

- Encryption stops others reading your data. Backups stop you losing it. You need both.
- Follow 3-2-1: three copies, two kinds of media, one offsite. Add one copy the laptop can't delete.
- Sync is not backup unless it keeps versions you can restore.
- Test a restore into an empty folder and open the files. A green tick proves little.
- Make sure you can get into your accounts with the laptop **and** the phone gone.
- **Time needed:** 30 minutes to set up; 10 minutes a month to test.

A stolen laptop causes at least two separate problems. Someone else may get your information, and you may lose access to it. Encryption deals with the first. Backups deal with the second. You need both. A perfectly encrypted laptop holding the only copy of a manuscript is still a disaster when it disappears. A flawless backup can't un-read documents someone already saw on an unlocked machine.

Here's the test we'd use. Could you borrow or buy another computer, get back into your essential accounts and pick up your most important work, all without touching the missing laptop? Try it for real rather than assuming. The Canadian Centre for Cyber Security names lost and stolen devices in its backup guidance, and it recommends multiple copies, offsite storage, encryption and test restores.<sup>71</sup>

**EXAMPLE The borrowed-computer test**

Imagine your laptop vanished this morning. On a borrowed computer, could you:

1. Sign in to your main email?
2. Open your password manager?
3. Find the project you worked on yesterday, in its latest version?
4. Read your disk recovery key?

Every "no" is a job for this chapter.

---

## Keep copies in places that fail separately

The well-known 3-2-1 rule is a good starting point: three copies counting the one you work on, on two different devices or kinds of media, with one copy offsite. For a laptop, that could be the internal SSD, an encrypted external drive kept at home, and a separately protected cloud or offsite backup. The right mix depends on your data and your risks. The home drive saves you when a travel bag goes missing. The offsite copy saves you if your home is burgled or damaged. These are examples, and no service is immune to failure. <sup>71</sup>

Then add the part the slogan leaves out. At least one useful copy should be safe from deletion by the laptop itself. The NCSC points out that 3-2-1 on its own doesn't require any copy to be offline. CISA recommends offline, encrypted backups and regular testing, because ransomware may go looking for reachable backups and destroy them. A network share that's always connected is another location, but whatever can wreck the laptop may be able to wreck that too. <sup>72,73</sup>

Physical distance matters as well. A backup SSD in the same sleeve as the laptop is handy on a trip, and it's gone the moment the sleeve is. Unplug a removable backup when it finishes and store it somewhere else. If you take a travel backup with you, keep another copy that stays home.



**Figure 7.1** 3-2-1: three copies, two kinds of media, one offsite, and one the laptop can't delete.

Cloud, local drive or both, side by side

|                         | Cloud backup service                                                                                  | Local SSD                                       | Local hard drive (HDD)                           | Both (the 3-2-1 idea)                          |
|-------------------------|-------------------------------------------------------------------------------------------------------|-------------------------------------------------|--------------------------------------------------|------------------------------------------------|
| Cost                    | A yearly or monthly fee, usually per computer or per amount of storage                                | A one-off purchase; SSDs cost more per terabyte | A one-off purchase; the lowest cost per terabyte | One drive plus one service                     |
| Restore speed           | Limited by your internet. Some services offer large downloads or will post you a drive with your data | Fastest                                         | Fast, slower than SSD                            | Restore from the drive, fall back to the cloud |
| Theft, fire, flood      | Survives anything that happens at home or in the bag                                                  | Lost too if it travels or sits with the laptop  | Same as SSD                                      | Survives                                       |
| Ransomware and mistakes | Version history helps; check how many days of versions are kept                                       | Safe while unplugged; at risk while connected   | Same as SSD                                      | One copy stays offline or versioned<br>72      |

|                 | Cloud backup service                                                                    | Local SSD                                                                                                               | Local hard drive (HDD)    | Both (the 3-2-1 idea)    |
|-----------------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|---------------------------|--------------------------|
| Encryption      | Check what the service offers; some let you hold a private key only you know            | Yours to turn on (BitLocker To Go, FileVault for Time Machine disks, LUKS or an encrypted container tool) <sup>77</sup> | Same as SSD               | Both                     |
| Version history | Built into the service                                                                  | Time Machine and File History keep versions; a plain copy doesn't <sup>76</sup>                                         | Same as SSD               | Both                     |
| Weak spots      | Needs internet; the first upload can take days; your account becomes a key to your data | Easy to forget to plug in; easy to lose                                                                                 | Dislikes drops and knocks | More to set up and check |

Cloud sync is not on this list on purpose. Synced storage mirrors your changes, deletions included. It is useful, but it is not a backup unless the service keeps versions you can restore.

**Our pick.** Most people: a hard drive for fast restores plus one cloud backup service for everything else. That is the 3-2-1 idea at the lowest cost. Pick an SSD over an HDD only if the drive travels or you restore often. If you can afford only one, choose the cloud backup for a laptop that travels, because a drive at home doesn't help when you need to restore abroad. If you have a slow connection, it's the other way round.



**WATCH OUT** Check drive prices over time

Storage prices move a lot from year to year, and a shop's "deal" may not be one. Look at a price history before you buy a backup drive.

## Cloud sync helps, but read the recovery terms

A synced folder can save your work when the hardware disappears, and that's valuable. It doesn't automatically give you a separate, protected history, though. Deletions and bad edits can sync across, a full storage quota can quietly stop uploads, and someone signed into your account may be able to change the remote copy. Judge a service by how many versions it

keeps, its deletion rules, its account controls and how restoring actually works.

Read the help pages of your own service. One large sync service, for example, lets eligible subscribers roll back a whole folder to any point in the last 30 days, while its deleted-files help gives different retention periods for personal and work accounts. Neither page promises recovery once something is permanently deleted from the recycle bin. So a sync service can help you recover without being your final copy that nobody can delete.<sup>74,75</sup>

Before a trip, open a few recently changed files from another trusted device. Check the dates and the contents. A green tick on a folder you rarely use says little about the project you worked on yesterday. If you use cloud-only files, make sure your backup tool copies their actual contents. A placeholder on disk doesn't contain the file.

---

## What the built-in tools really cover

On a Mac, Time Machine is a sensible first layer. Apple describes hourly, daily and weekly backups, with older ones removed as the disk fills. Check the date of the last successful backup, not just that Time Machine is on. Encrypt the backup disk as well as using FileVault on the laptop, since they protect different drives. Apple also warns that switching some network backups to encrypted can erase the existing backup set, so read the steps before changing it.<sup>76,77</sup>

Local snapshots are handy for undoing mistakes while you still have the Mac. They live on the same internal disk, though, so they won't help after a theft. Apple itself recommends a separate backup location even when you have local snapshots.<sup>78</sup>

On Windows, the name Windows Backup can suggest a full disk image. It isn't one. Microsoft describes backing up selected user folders through Microsoft's own cloud storage, some settings, and your pinned apps. Some apps will need downloading and installing again. Check folders outside the default locations, software licences, local databases and specialist app data separately.<sup>79</sup>

File History is another Windows option. It keeps older copies of personal files on an external drive or network location. Check which folders it covers

instead of assuming it gets everything. Its restore screen can save to a different location, which is the better choice for a test because it won't overwrite the file you're working on. Protect the backup drive against theft and prying eyes.<sup>80</sup>

---

## A Linux route, with keys you can recover

If you're comfortable running a Linux system, open-source command-line backup tools can give you versioned, encrypted backups to local or remote storage. None of them maintains itself. Check you're on a supported version, set the folders to include, schedule the jobs and set up alerts when they fail. A script that's been failing quietly for six weeks isn't a backup.

One popular tool warns that access to a repository depends on its password. Keep the password and the repository location reachable without the laptop. It lets you add several access keys to one repository, which can separate everyday access from emergency access. They all open the same repository, though, so they don't create an extra copy. Don't leave your only working credentials in a file that disappears with the computer.<sup>81,82</sup>

Another tool chooses its encryption mode when you create the repository, and its documentation recommends backing up the key separately. The exported key is itself encrypted, so you'll also need the passphrase to recover. Don't seal a key export in an envelope and forget that second part. The same documentation warns that if both the key and passphrase were exposed, changing the passphrase doesn't replace the underlying secrets. That's a job for moving to a new repository key.<sup>83,84</sup>

For more advanced setups, give the laptop's credentials only the backup permissions they need. An append-only server mode is one documented way to do this, but it has limits: direct filesystem access can get around it, and maintenance with full rights changes the protection. A remote repository with full delete rights saved on the laptop is a weaker arrangement. Check the real permissions before calling any backup immutable.<sup>85</sup>

## Test the restore, boring bits included

Checking a backup's integrity and actually restoring from it answer different questions. A tool's normal check may not read every stored piece of data; a full data check does, at a cost in time and bandwidth. Even a clean result doesn't prove you picked every folder that matters, or that your accounting software will open on a new computer. <sup>86</sup>

Do the test restore into a new, empty folder. Backup tools can overwrite existing files at the destination by default, which is a good reason not to experiment on your live work folder. Leave the originals alone while you test.

<sup>87</sup>

A monthly drill could be: restore one recent document, an older version of something, a photo and a small folder with subfolders. Then open them in their apps. Every few months, use another trusted computer or a clean, separate environment and follow your written recovery notes. If a local database export or a virtual machine is essential to your work, include it. Apps with databases may need their own backup method, because copying a running database or VM file isn't the same as a tested restore.

Write down the backup date, what you restored, how long it took and anything missing. That gives you two useful limits: how much recent work you could lose, and how long recovery really takes. It also catches forgotten passwords before a thief forces the issue.



### TRICK Restore to a different place

When a restore screen offers "restore to", pick a new folder on the desktop called "restore test" and the date. You can compare it with the original side by side, and nothing you're working on gets overwritten.

## Recover your accounts, not just your files

The missing laptop may have held your password manager, your email, your second factor and your backup console all at once. Avoid that circle. Register a spare security key or another recovery method before you need it, and keep it out of the travel bag. Google explains how to sign in with a

backup factor or key you registered earlier after losing your main one. Buying an unregistered spare afterwards won't get you back in. <sup>88</sup>

Password managers use several pieces for recovery, and each does a different job. An emergency kit records your account details. A secret key, where your manager uses one, works with your account password when you sign in on a new device, and it isn't a reset code. Recovery codes can restore access, but some processes also need access to the linked email account. Read how your own manager works, plan around those links and keep sensitive recovery material safely away from the laptop. <sup>89,90,91</sup>

After a theft, check and sign out the missing computer's sessions from a trusted device. Google notes that one device can have several sessions, and each may need attention. Also review service-specific tokens and backup credentials, depending on the risk and your provider's instructions. Changing a password and signing out remotely aren't always the same thing. <sup>92</sup>

And carry less. A travel laptop rarely needs your entire archive, every customer record, every server login and every exported password file. Take what the trip needs, set up a controlled way to reach the rest, and test it. The less that's on the machine, the less a failure elsewhere can cost you. Your backups get smaller and restores get faster, too.



#### **STORY** Imagine the bag with everything in it

*Imagine a freelancer who keeps everything in one tidy backpack: laptop, phone, backup SSD and a little notebook with her recovery codes. It's very organised. Then the backpack is stolen from a train luggage rack. Every copy, every code and both ways into her email leave together. The fix costs nothing: the SSD and the notebook live at home, and one recovery code sits with a family member.*

## **Removable drives deserve the same care**

A backup drive holds the same data as the laptop, often more of it, and it's small and easy to lose. NIST's guide to telework security treats removable media and backups as part of the device's protection, not an afterthought. Encrypt backup drives, label them without personal details, and store them away from the laptop. <sup>184</sup>

## An example maintenance schedule

| When                                          | What to do                                                                                                                                            | Worth remembering                                                                            |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| Before every trip                             | Run a fresh backup and confirm when it finished; open current essential files from another trusted device; leave at least one encrypted copy at home. | A routine like this helps, but it isn't continuous protection.                               |
| While you're working                          | Use automatic versioned backups, as often as matches how much work you could bear to lose; look into errors and storage warnings.                     | Hourly backups only limit loss to about an hour if the jobs finish and cover the right data. |
| Weekly (example)                              | Update the encrypted removable copy that lives elsewhere; confirm it finished; unplug it and put it back.                                             | A weekly offline copy could be up to a week behind if the others fail.                       |
| Monthly (example)                             | Restore a few typical files and an old version into a new empty folder, open them, and note the result.                                               | A small sample is useful, but it doesn't check everything.                                   |
| Every quarter, or after big changes (example) | Rehearse recovery on another trusted computer, including accounts, decryption keys, essential apps and real work files.                               | Test more deeply when the setup is more valuable or complicated.                             |



### CHECKLIST Do this today

- ☐ Start one backup today, even if it isn't the perfect setup.
- ☐ Encrypt the backup drive and store it away from the laptop.
- ☐ Restore one file into a new folder and open it.
- ☐ Run the borrowed-computer test from the start of this chapter.
- ☐ Print or write down recovery codes for your main email.

### MORE ON THE SITE

→ [Backups and account recovery](#)



### Stay in the loop

A reminder to test your restore now and then can't hurt.

[Get the TechCortado newsletter](#)

[Bluesky](#) · [Mastodon](#) · [Pixelfed](#) · [TechCortado.com](#)

# 08

## CHAPTER 8

# Find it, track it, mark it

*Leads, not promises*

---

### INSIDE

What a tag can and can't do

Pick the network your phone can manage

Separation alerts are reminders, not alarms

Built-in finding and remote actions

Anti-theft software and built-in finding, side by side

Stickers, labels and property marking

Your device record: serial, MAC address and photos



**IN THIS CHAPTER**

- A tag shows where something was last detected. Treat it as a lead for the police, not a reason to go yourself.
- Pick the tag network your phone already uses. No network has been shown to recover more laptops.
- A tag in the bag follows the bag. Decide which object you want to find.
- Turn on your laptop's built-in finding before you need it, and know what remote lock and erase can and can't do.
- Register the serial number. Marking helps prove ownership more than it deters.
- **Time needed:** 20 minutes.

When a laptop goes missing, the first question is "where is it now?" This chapter covers the tools that can give part of an answer, and why the answer is only ever partial.

---

## What a tag can and can't do

A tag can tell you where something was last detected. It can't hold the laptop to the desk, encrypt its files or rebuild your work. Treat the location and its timestamp as a lead. A dot on a map doesn't prove the laptop is still there, or that a particular person or flat has it. Bluetooth finding depends on radio conditions and on other people's devices passing by, and at least one tag maker says outright that its tags don't offer GPS or real-time tracking. <sup>93,94,95,96</sup>

Three quite different things get called "tags." An **asset label** shows who owns the item. A **QR recovery label** lets an honest finder get in touch. A **Bluetooth tracking tag** takes part in a finding network. A printed QR sticker doesn't send a location. And a tag in the laptop bag follows the bag, so if the laptop and bag get separated, so do their locations. Decide which object you actually want to find. <sup>8,97,96</sup>

## Pick the network your phone can manage

Tags join a finding network run by a phone platform or by the tag maker. The rule of thumb is simple: pick the network your phone already uses.

| Your phone                    | Network to look for                  | Worth knowing                                                                                                      |
|-------------------------------|--------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| iPhone                        | Apple's Find My network              | Tags are located in the Find My app; check what your phone and region support for precise finding <sup>98,93</sup> |
| Android                       | Google's Find Hub network            | Look for a tag that clearly says it works with Find Hub; check the offline finding settings <sup>99</sup>          |
| A phone maker's own ecosystem | That maker's own finding service     | Some tags only work with one maker's phones, not with Android in general <sup>101</sup>                            |
| Mixed household               | A tag that supports either network   | "Works with both" usually means one at a time, not both at once <sup>100,97</sup>                                  |
| Any                           | A standalone tag maker's own network | A separate app and network; check how well it works where you live <sup>102,95</sup>                               |

This is about fitting your phone. Nobody has shown one network recovers a measurably higher share of stolen laptops.

Check the exact model and generation before you buy, because older and similarly named tags can support different networks and features. Some tags use a replaceable coin cell, some are rechargeable, and battery-life figures are the makers' own estimates. Many recent tags also use UWB (ultra-wideband, the short-range radio behind precise "it's right here" finding) as well as Bluetooth. Range improvements in a launch announcement are the maker's figures, not test results. <sup>98,103</sup>



**TIP Test it without the laptop**

Pairing isn't the test. Leave the tagged bag at home, take your phone to a café, and check you can see the tag's last location and play its sound. If your only compatible device could vanish in the same bag, set up another way to reach the finding service now. <sup>93</sup>

On Android, Google documents several offline finding settings. "Without network" isn't the one for finding your belongings with tags. The crowd-based settings use detections from other Android phones nearby. The "busy

places" and "everywhere" options change how your phone takes part, but no setting can conjure up nearby phones or promise instant updates. Test your tag at home and on a normal journey, and recheck permissions after you change phones. <sup>99,94</sup>

## Separation alerts are reminders, not alarms

Some tag services offer alerts when you leave something behind. Read how they work. One standalone tag service says its paid alerts notify you when **your phone leaves** a set area, roughly five to ten minutes after you go. If the tagged laptop leaves and your phone stays put, you won't get that alert. Phone platforms offer similar "left behind" notices. These are "you forgot something" reminders, not reliable snatch alarms. Check notification permissions and the trusted locations where alerts are switched off, and test them on purpose. <sup>104,105</sup>

Anti-stalking protections matter too. Apple and Google both describe alerts when an unknown tag travels with someone over time. Those protections are right to have, and they also mean a thief may find out about a consumer tracker. Don't buy one expecting it to stay hidden forever, and don't tamper with its safety features. <sup>106,107</sup>



### WATCH OUT "Hidden" modes have a cost

At least one standalone tag service offers an anti-theft mode that hides registered tags from some scanning tools. It requires ID-and-selfie verification and regular re-checks. Read the terms before turning anything like it on. It isn't a guarantee of staying hidden, of getting the laptop back or of any payout, and the privacy cost is part of the decision. <sup>108,109</sup>

## Built-in finding and remote actions

Turn on your laptop's recovery features before you travel, and check it shows up in the right account. Microsoft's consumer Find My Device needs a personal Microsoft account, an administrator account and setting up in advance. The documented actions are locate and lock. Don't expect a consumer remote-wipe button on Windows because some corporate manage-

ment tool has one. Work laptops need your organisation's own procedure.  
110

On a Mac, turn on Find My beforehand. Apple says remote lock or erase only works when the Mac is powered on and online, even though an offline location may sometimes show. So a map update doesn't prove an erase command got through. Apple's Mac guidance for lost devices warns that erasing stops further finding, while its general Find My guidance has device-specific exceptions. To be safe, assume erasing may end your ability to locate it, and decide based on how sensitive the data is. 111,93

Eligible Macs can keep Activation Lock after a remote erase. Signing out a session or removing a lost Mac from a trusted-device list is not the same as removing it from your Find My account. Apple's removal instructions explain that removing Activation Lock lets someone else set the device up. Follow the lost-device steps exactly, and don't click the "remove device" option meant for selling or giving away a Mac when it's been stolen. 60,112

## Anti-theft software and built-in finding, side by side

Tags find bags. Software on the laptop itself can report where the laptop is, as long as it is switched on, signed in somewhere and online. Laptops have no GPS of their own, so these services estimate location from nearby Wi-Fi networks or the IP address.

|        | Built into macOS (Find My) | Built into Windows (Find My Device) | ChromeOS                                                     | Third-party anti-theft software             | Firmware-persistent agents      |
|--------|----------------------------|-------------------------------------|--------------------------------------------------------------|---------------------------------------------|---------------------------------|
| Cost   | Free                       | Free                                | Free                                                         | Usually a subscription, per device          | Paid, mostly sold to businesses |
| Locate | Yes 93                     | Yes, with location turned on 110    | Managed (work or school) devices only, through the admin 153 | Yes; some describe Wi-Fi based location 148 | Yes                             |

|                           | Built into macOS (Find My)                               | Built into Windows (Find My Device)                                               | ChromeOS                                                                | Third-party anti-theft software                                                  | Firmware-persistent agents                                                                                     |
|---------------------------|----------------------------------------------------------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------|----------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| <b>Lock</b>               | Yes <sup>111</sup>                                       | Yes <sup>110</sup>                                                                | Admin can disable a managed device <sup>153</sup>                       | Often a screen lock, alarm and on-screen message <sup>147</sup>                  | Depends on edition                                                                                             |
| <b>Erase</b>              | Yes <sup>111</sup>                                       | No consumer wipe documented <sup>110</sup>                                        | Not for consumers, as far as we found                                   | Sometimes, often on business plans <sup>147</sup>                                | Depends on edition                                                                                             |
| <b>Stays after a wipe</b> | Activation Lock on eligible Macs <sup>60</sup>           | No equivalent we could find                                                       | Enterprise enrolment ties the device to the organisation <sup>153</sup> | No                                                                               | A firmware module on supported laptops can bring the agent back after a reinstall or drive swap <sup>152</sup> |
| <b>Worth knowing</b>      | Erasing may end your ability to locate it <sup>111</sup> | Whoever is using the laptop sees a notification when you locate it <sup>110</sup> | Check your own device's options                                         | Some offer opt-in camera photos and screenshots; also covers Linux in some cases | Laptop model must support it                                                                                   |

**Our pick.** On a Mac, Find My plus Activation Lock covers most people at no cost. On Windows, turn on Find My Device, and add third-party anti-theft software if you want reports with photos, an alarm or finding on Linux too. Firmware-persistent agents are mostly business tools; their persistence is the one feature that survives a thief wiping the drive, if your laptop model supports it. Example products are listed in Appendix B.

**WATCH OUT Thief photos have a legal side**

Camera photos in anti-theft software should be opt-in and only for a device you own and have marked missing. In 2012 the US Federal Trade Commission settled with a software company whose product let rent-to-own shops secretly take webcam photos, log keystrokes and capture screens on computers people were renting. Use these features on your own laptop, tell anyone who borrows it, and hand the results to the police rather than acting on them yourself. <sup>154</sup>

**Remote wipe has limits.** Every service here needs the laptop to be on and online to receive the command. A thief who keeps it offline, or wipes it first, stops it. That is why encryption, done before the theft, does the real protecting, and why a decoy account that lets a thief reach the internet can help the finding services (Chapter 9). <sup>111</sup>

**Hiding a tag inside the laptop.** We don't recommend opening the case for this: warranties, batteries and heat are all good reasons not to. Anti-stalking alerts will also tell a thief's phone that an unknown tag is travelling with them, hidden or not. A slim tag in a zipped inner pocket of the sleeve is the gentler option, knowing that the laptop and the sleeve can part company. <sup>106</sup>

---

## Stickers, labels and property marking

You can buy stickers that say a laptop is GPS tracked, plates that leave a "stolen" mark when torn off, and invisible inks only a UV lamp shows. Do any of them stop a thief? We looked for real studies. Here is what we found, including where we found nothing.

### What the evidence says

- **Property marking with warning stickers, Wales, 1985.** Households that marked their property and showed a sticker had 40% fewer burglaries (128 down to 74). But not one stolen item was recovered thanks to the marking, and the author put the drop down to the publicity and stickers, not the marks themselves. <sup>155</sup>

- **Forensic marking kits, England, 2021 study.** Burglaries fell by about 82% in the first six months after kits and signs went out, then crept back to the old level by twelve months. <sup>156</sup>
- **Aarhus, Denmark, randomised trial.** 6,603 houses were offered forensic marking and stickers; only 32% took part. Burglaries were 21% lower over 15.5 months across everyone offered, and the effect faded. The authors thought the contact letters themselves may have done part of the work. <sup>157</sup>
- **North Zealand, Denmark, randomised trial, 12,000 households.** Burglary rates were 4.6% with marking, 5.1% with a placebo and 4.9% with nothing. No significant difference overall. Households that actually put the stickers up did slightly better, short of significance. <sup>158,159</sup>
- **Warning stickers on cars.** The US Problem-Oriented Policing Center says warning signs "generally do not act as a significant deterrent" to experienced offenders, and that in one survey 82% of car thieves said a vehicle watch sticker wouldn't put them off. <sup>160</sup>

All of these are about homes and cars. **We found no study of stickers or marking on laptops, and none at all on fake "GPS tracked" stickers.** A fake tracking sticker could put off a casual thief, or prompt a careful one to look for the tracker and switch the laptop off sooner. Nobody has measured which. The honest summary: marking may help for a while when it is publicised, it rarely gets things back on its own, and it works best as proof of ownership.



**EXAMPLE    Reading the studies fairly**

The North Zealand trial is a good lesson in why a single headline number can mislead. Marked homes (4.6%) did a little better than placebo homes (5.1%) and homes with nothing (4.9%), but the difference wasn't significant. Two numbers being different isn't the same as one thing working. <sup>158</sup>

**What each option is for**

| Type                                  | What it may do                                    | Limits                                                                           |
|---------------------------------------|---------------------------------------------------|----------------------------------------------------------------------------------|
| "Property of / reward if found" label | Helps an honest finder return it; shows ownership | No location; keep contact details minimal, such as an email made for the purpose |

| Type                              | What it may do                                                                                                                                                                                                         | Limits                                                                                                                |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Fake "GPS tracked" sticker</b> | May put off an opportunist                                                                                                                                                                                             | No evidence either way for laptops; can be peeled off; may make a thief more careful                                  |
| <b>Security plate</b>             | Hard-to-remove plate with an ID; some makers say removing it reveals an etched "stolen" mark, and run a recovery line <sup>161</sup>                                                                                   | Maker's claims only, no independent study found; the mark spoils resale, which is the point, and also your own resale |
| <b>UV pen marking</b>             | Invisible ID that police can read under UV light                                                                                                                                                                       | Ink may fade, so check it now and then; only helps if the laptop is found and checked                                 |
| <b>Forensic marking liquid</b>    | Unique traceable code; the trials above used kits like these                                                                                                                                                           | Effects seen for homes faded within about a year <sup>156,158</sup>                                                   |
| <b>Engraving the case</b>         | Permanent visible ID                                                                                                                                                                                                   | Lowers resale value; don't drill or engrave near batteries                                                            |
| <b>Serial number registration</b> | Police can match a found laptop to you. National property registers exist in some countries, and some police forces ask you to keep the serial so they can enter it into a national crime database. <sup>162,163</sup> | Only helps after a theft; schemes vary by country, so ask your local police                                           |

**Our pick.** Register the serial number (free and useful), add a small return label, and use UV or forensic marking if your local police scheme supports it. Buy a security plate if visible marking appeals to you, knowing the evidence is the maker's. Skip fake GPS stickers unless you simply like them; nothing shows they work.

## Your device record: serial, MAC address and photos

Police and campus safety offices ask for the same few details again and again. Universities in particular suggest recording the make, model and serial number, and some campus police departments run free registration for students' laptops. <sup>197,198,199</sup>

- **Serial number:** on the label underneath, in the system information, or on the box.
- **MAC address:** the hardware address of the Wi-Fi adapter, shown in network settings. Some campus and workplace networks can spot a known device when it connects, so it's worth recording. Many systems

now use a private, changing address on each network, so treat it as a helpful extra, not a tracker.

- **Photos:** the whole laptop, the serial label and any marks, scratches or stickers.
- **Receipt:** a photo or the email, saved away from the laptop.

The device record worksheet near the back has room for all of it.



#### CHECKLIST **Do this today**

- ☐ Turn on your laptop's built-in finding and check it appears in your account.
- ☐ If you use a tag, test it without the laptop.
- ☐ Fill in the device record worksheet, with serial number, MAC address and photos.
- ☐ Register the serial number with your local scheme, if there is one.
- ☐ Add a small return label with minimal contact details.

#### MORE ON THE SITE

- [Tracking tags and asset labels](#)
- [Built-in finding and remote actions](#)



#### **Stay in the loop**

Tracking features change often. We keep an eye on them.

**Get the TechCortado newsletter**

[Bluesky](#) · [Mastodon](#) · [Pixelfed](#) · [TechCortado.com](#)

# 09

## CHAPTER 9

# Tripwires

*Canary tokens and a decoy*

---

### INSIDE

What a canary token is  
The unencrypted honeypot

Setting it up, step by step  
Risks to keep in mind



## IN THIS CHAPTER

- A canary token is a file or link that emails you when someone opens it.
- It is a side project, not a core layer. It only works if someone goes online and pokes around.
- A decoy only works if a thief can reach it, and good encryption is designed to stop that.
- With a startup PIN, use a decoy USB stick. With automatic unlock, a standard decoy account can help finding services see the laptop.
- An alert is a lead for the police. Never act on it yourself.
- **Time needed:** 30 to 45 minutes, optional.

Everything so far tries to stop a theft or limit the damage. This chapter is about getting a signal from the laptop after it's gone. It is a side project, not a core layer, and it only works if the thief, or whoever buys the laptop from them, goes online and pokes around.

---

## What a canary token is

A canary token is a tripwire you can make for free with a public token service. You get a file or a link. When someone opens it, you get an email with the time and the address it came from. Appendix B names a free service and how to self-host it. <sup>164,165</sup>



Figure 9.1 How a canary token alert reaches you, and where it goes next.

| Token          | What fires it                                                                                            | Good for                                                                     | Limits                                                                                              |
|----------------|----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| Word document  | Opening it in Microsoft Office on Windows or macOS <sup>166</sup>                                        | "passwords.docx" on a decoy desktop                                          | Office may open files in Protected View, read-only, and the token may not fire there <sup>172</sup> |
| Excel workbook | Opening it in Office on Windows or macOS <sup>167</sup>                                                  | "bank-accounts.xlsx"                                                         | Same as Word                                                                                        |
| PDF            | Opening it in a "reasonably compliant" PDF reader, through a DNS lookup <sup>168</sup>                   | Works through strict networks                                                | Gives only a rough idea of where; some readers won't fire it                                        |
| Web bug (link) | Anyone visiting the URL <sup>169</sup>                                                                   | Browser home page or a bookmark called "Online banking" on the decoy account | Needs someone to click or load it                                                                   |
| Windows folder | Someone browsing a folder that holds the token's desktop.ini file, including inside a zip <sup>170</sup> | A folder named "Tax returns" on a decoy account                              | Windows only                                                                                        |

| Token       | What fires it                                 | Good for                                        | Limits                                       |
|-------------|-----------------------------------------------|-------------------------------------------------|----------------------------------------------|
| Self-hosted | Same tokens on your own server <sup>171</sup> | People who don't want a third party in the loop | Needs a domain and an internet-facing server |

What you get is a lead, not a location. The address may belong to a mobile network or a VPN. Hand it to the police with your report; don't go looking yourself.

## The unencrypted honeypot

A decoy only works if a thief can reach it, and full-disk encryption is designed to stop them reaching anything. That is the trade-off. Here is how it plays out on each system.

- **Mac with FileVault:** this works out of the box. With FileVault on, a Guest User can use Safari but can't reach your encrypted disk or create files, and anything a guest does is deleted at logout. Apple says guest access works with Find My, so you can locate the Mac if someone logs in as a guest and uses Safari. Canary files can't live in the guest account, so put them on a decoy USB stick instead. <sup>174</sup>
- **Chromebook:** guest browsing is built in and the owner can turn it on or off. Signing out of guest mode deletes the session's files. Work and school Chromebooks follow the admin's settings. <sup>173</sup>
- **Windows with BitLocker unlocking automatically (TPM only):** the laptop starts to the login screen, so a decoy account is reachable. Microsoft keeps the built-in Guest account off by default and calls it a security risk, so use an ordinary **standard, non-administrator local account** as the decoy instead. <sup>175</sup>
- **Windows with a startup PIN, or a boot passphrase from a third-party tool or LUKS:** nobody reaches a login screen without the PIN, so a decoy account on that drive does nothing. That's the protection doing its job. If you want a decoy here, use an **unencrypted USB stick** in the bag, labelled something dull like "Backup", holding only canary files.
- **A separate unencrypted decoy OS** in the boot menu is possible, but it fights with Secure Boot and boot settings and adds a lot of upkeep. We'd leave it to enthusiasts.

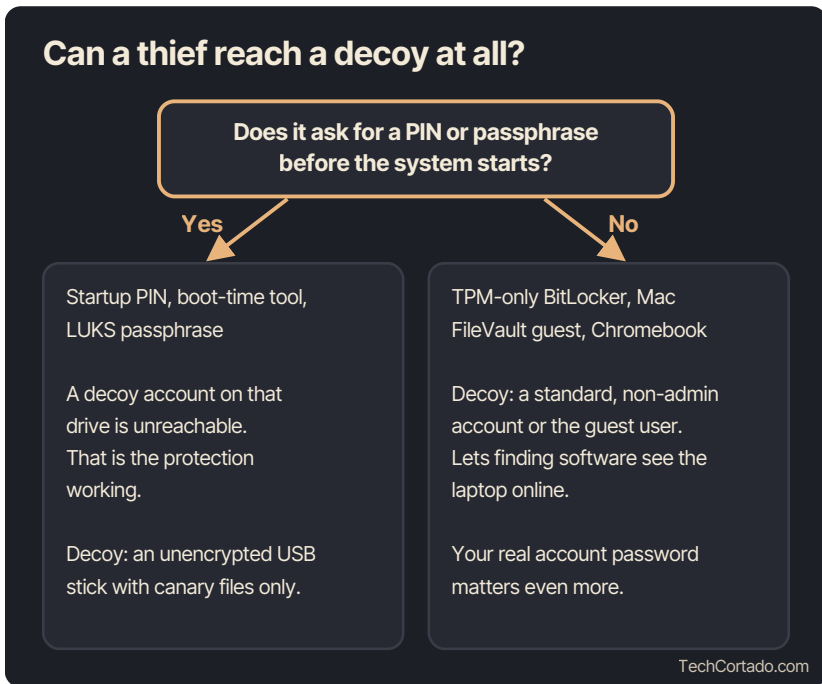


**Figure 9.2** Account or USB stick? It depends on whether the laptop asks for a password before it starts.

Our view on the trade-off: if your data is sensitive, keep the startup PIN and use the decoy USB stick. If your laptop already unlocks automatically to the login screen, a decoy account costs little and gives the built-in finding service, or your anti-theft software, another chance to see it online. Two honest cautions for that case. A decoy account gives a thief a running system where your encrypted drive is already unlocked, protected only by your own account's password and the system's permissions. And a strong password on your real account matters even more.

---

## Setting it up, step by step

- 1. Get the basics right first.** Encryption on, a strong password on your real account, and built-in finding or anti-theft software turned on and tested.
- 2. Make an alert email** that isn't your main address, so a forwarded alert can't reveal much about you.

3. **Create the tokens** with a token service: one Word, one Excel, one PDF and one web bug. Use the memo field to note which file goes where.
4. **Create the decoy.** Mac: turn on the Guest User. Chromebook: leave guest browsing on. Windows (TPM-only unlock): add a local standard account with an ordinary name and no admin rights, not linked to any Microsoft account. Linux: a separate user that isn't in the admin (sudo) group.
5. **Plant the files and link.** Put the documents on the decoy desktop with tempting names, set the web bug as the decoy browser's home page, and add a Windows folder token if you like. On a Mac, use the USB stick for the files.
6. **Test it.** Log in to the decoy, go online, open each file and the link, and check each alert arrives. Then put it back exactly as a stranger would find it.
7. **Recheck after big updates.** System upgrades can change guest settings or reset accounts.



#### TRICK Name files like a person would

"passwords.docx", "bank-accounts.xlsx" and a folder called "Tax returns" are more tempting than "decoy1". A bookmark called "Online banking" that points at your web bug is another quiet tripwire.

## Risks to keep in mind

- **Nothing real on the decoy.** No real documents, no saved passwords, no browser sync, no signed-in email.
- **No admin rights.** An admin decoy is simply a second door into your laptop.
- **Some systems limit it.** Windows discourages its Guest account, Mac guests are Safari-only with FileVault, and managed laptops follow the organisation's rules.
- **Alerts aren't guaranteed.** Offline machines, Protected View, file previews and blocked lookups all stop a token firing.

- **Keep it a tripwire.** Tokens only report that they were opened. Never plant anything that damages a computer, and never act on an alert yourself.



### STORY **Imagine the email two days later**

Imagine a laptop stolen from a car in a city centre. It unlocked automatically to the login screen, and the owner had set up a standard decoy account called "Sam". Two days later her phone shows an email: "passwords.docx opened". It gives a time and an internet address. She doesn't drive anywhere. She forwards the email to the officer handling her report and goes back to restoring her files. Sometimes that's all the lead is. Sometimes it's the piece that helps.



### CHECKLIST **Do this today (optional)**

- ☐ Decide: decoy account or decoy USB stick, based on your startup setup.
- ☐ Make a separate alert email address.
- ☐ Create and plant the tokens, then test that each alert arrives.
- ☐ Put a reminder in your calendar to recheck after big updates.

#### MORE ON THE SITE

→ [Canary tokens, decoy files and a honeypot](#)



### **Stay in the loop**

More low-cost tricks like these, when we find good ones.

**Get the TechCortado newsletter**

[Bluesky](#) · [Mastodon](#) · [Pixelfed](#) · [TechCortado.com](#)

# 10

## CHAPTER 10

# Out and about

*Cafés, trains, campuses and public Wi-Fi*

---

### INSIDE

The public-space routine

Public Wi-Fi

USB charging and found USB sticks

Bluetooth and other radios

Campuses, libraries and coworking spaces



**IN THIS CHAPTER**

- Most risk in public is simple: a laptop left for a minute, or a screen read by a stranger.
- On public Wi-Fi, prefer your phone's hotspot for anything personal or work-related, and turn off auto-join.
- Charge from your own plug and cable when you can. Public USB charging risk is mostly theoretical, but the fix is easy.
- Never plug in a USB stick you found.
- Turn off Bluetooth and Wi-Fi when you don't need them.
- **Time needed:** 15 minutes to change settings, then habits.

Working in a café, a library or on a train is mostly safe and often pleasant. The risks are small and ordinary, and so are the fixes.

---

## The public-space routine

Chapter 2 covers the theft habits: the laptop leaves with you, it stays in sight, and it doesn't sit on a table while you queue. In a public space, add three more.

1. **Choose your seat.** Back to a wall, laptop on the inside, bag strap under a chair leg or round your foot.
2. **Shield the screen.** Angle the screen away from the aisle, use a privacy screen (Chapter 6), and save sensitive documents for somewhere private.  
181
3. **Lock before you look away.** Turning to talk to someone counts.

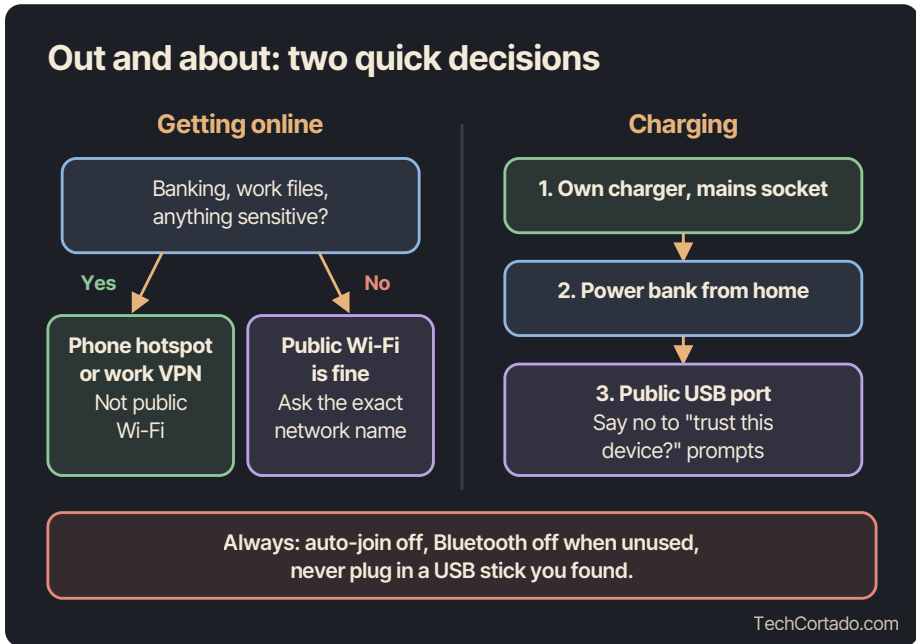


**Figure 10.1** Two quick decisions for working in public: how to get online, and how to charge.

## Public Wi-Fi

Free Wi-Fi in cafés, stations, hotels and airports is shared with strangers, and you can't easily tell a real network from a fake one with the same name. Official advice is consistent: avoid public Wi-Fi for personal or sensitive business where you can, and be careful what you do when you must use it.

182,183,188

Most websites now use encrypted connections, which protects what you type on those sites. Public Wi-Fi still exposes you to fake sign-in pages, a network that can see which sites you visit, and other devices on the same network. The simplest choices, in order:

1. **Use your phone's hotspot.** It's your own connection, protected by your own password.
2. **Use your organisation's VPN** for work, if it provides one. A VPN creates an encrypted tunnel from your laptop to a trusted network. <sup>192</sup>
3. **Use public Wi-Fi for low-stakes browsing**, and save banking, admin tasks and work files for a trusted connection.

**TIP Ask for the exact network name**

Ask staff for the exact name of the Wi-Fi network rather than picking the one that looks right. "Cafe\_Free" and "Cafe Free Wi-Fi" can be two different networks, and only one of them belongs to the café.

**Turn off auto-join**

Laptops remember networks and rejoin them automatically. That's handy at home, and less handy when a network with a familiar name, like a common hotel or airport name, appears somewhere else. CISA advises turning off settings that let your devices connect automatically to nearby networks.

183

- On Windows and macOS, open the Wi-Fi settings and turn off automatic joining for public networks you've used.
- Remove ("forget") old hotel, airport and conference networks after a trip.
- Mark public networks as public on Windows, which limits sharing with other devices on the network.
- Check that the system firewall is on (Chapter 6).

**USB charging and found USB sticks**

You may have seen warnings about "juice jacking", the idea that a public USB charging port could be rigged to install malware or copy data. The FCC gives sensible tips, and also says it is not aware of any confirmed cases.<sup>191</sup> So treat it as a low risk with an easy fix rather than something to fear.

- **Bring your own charger and plug it into a mains socket.** That avoids the question entirely.
- **Use a power bank** charged at home when sockets are scarce. [Our power bank buying guide](#) covers what to look for.
- **If your laptop or phone asks whether to trust a connected device, say no** when you're only charging.

**WATCH OUT Never plug in a found USB stick**

A USB stick left in a car park, a meeting room or a train seat is a classic trick: curiosity does the attacker's work. Hand it to staff or lost property. Don't plug it in "just to see who owns it". The same goes for free sticks and cables handed out by people you don't know.

---

## Bluetooth and other radios

Bluetooth makes your laptop visible and connectable to nearby devices. Official travel advice suggests turning it off when you're not using it. <sup>182,183</sup>

- Turn off Bluetooth when you don't need headphones, a mouse or a keyboard.
- Turn off file sharing features, such as nearby sharing or AirDrop, or set them to contacts only.
- Accept pairing requests only from devices you're holding.

**TRICK One switch for the whole trip**

Most laptops have a quick settings panel. Before you leave home, put Wi-Fi, Bluetooth and sharing toggles somewhere you can reach in one click, so turning them off becomes as quick as turning them on.

---

## Campuses, libraries and coworking spaces

Universities report the same pattern year after year: laptops taken from library desks, study rooms and cafés in a few minutes when the owner steps away. Their advice is the advice of this book: take it with you, lock it to something solid if you must stay at a desk, and record the serial number.

<sup>197,198</sup>



### STORY **Imagine the library seat**

*Imagine a student who leaves a coat on the chair and the laptop on the desk while she buys a coffee. The coat says "this seat is taken". To someone walking past, the laptop says "nobody is watching". She's back in six minutes. The coat is still there.*



### CHECKLIST **Do this today**

- ☐ Turn off auto-join for public networks and forget old ones.
- ☐ Set up your phone's hotspot and test it with the laptop.
- ☐ Pack a charger that plugs into a mains socket.
- ☐ Set Bluetooth and file sharing to off, or contacts only.
- ☐ Decide what you won't do on public Wi-Fi.

#### MORE ON THE SITE

- [Power bank buying guide](#)
- [Power bank calculator: how many charges?](#)



### **Stay in the loop**

Gadget guides for working on the move.

**Get the TechCortado newsletter**

[Bluesky](#) · [Mastodon](#) · [Pixelfed](#) · [TechCortado.com](#)

# 11

## CHAPTER 11

# Travel

*Airports, hotels, borders and coming home*

---

### INSIDE

Before you go

Airports and security screening

On the move

Hotels

Bags

At the border

Coming home



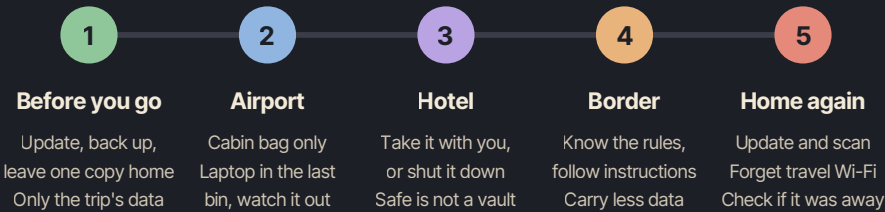
IN THIS CHAPTER

- Keep the laptop in your cabin bag, never in checked luggage.
- At the scanner, put the laptop on the belt last and watch it come out.
- In hotels, shut the laptop down when you leave it, and keep it with you when you can. Official advice says even hotel safes aren't a guarantee.
- At borders, know the rules for the country you're entering and follow officers' instructions. Carry only the data the trip needs.
- After the trip, update, check and reset what you used.
- **Time needed:** 20 minutes before a trip, 15 minutes after.

Travel packs the risks of the last few chapters into a few days: crowds, queues, unfamiliar rooms, tired evenings and other people's networks. Most of the protection happens before you leave home.

### A trip in five steps

What to do at each stage. Official travel advice from several countries agrees.



Not legal advice: border rules differ by country. Read the official guidance first.

TechCortado.com

**Figure 11.1** A trip in five steps, from packing to coming home.

## Before you go

The best travel security happens at home. Official travel guidance from several countries gives the same short list: update everything, back up, encrypt, and take as little data as the trip needs. <sup>183,186,187,190</sup>

- **Update** the system, browser and apps (Chapter 6).

- **Back up** and leave one copy at home (Chapter 7).
- **Encrypt**, and shut down rather than sleep when you travel (Chapter 4).
- **Turn on finding** and test it (Chapter 8).
- **Note down** the serial number, and pack a photo of it separately (Appendix A).
- **Check your insurance** for travel, business use and the countries you're visiting (Chapter 12).
- **Check your employer's rules** if it's a work laptop. Many organisations have a travel policy, and some lend travel laptops.

## A travel laptop or a travel profile

**A travel laptop.** For trips where losing the laptop would hurt most, a cheaper machine or a separate profile signed into only what you need limits what a thief gets. Carry a backup of what you need on the trip, encrypted, and keep the main backup at home.

Government travel guidance for business travellers goes further: some suggest a separate "clean" laptop or a loaner device with only the data needed for the trip, especially for high-risk travel. <sup>185,186,187</sup> For most people a separate user profile, signed in to only what the trip needs, is a sensible middle ground.



### TIP Sign out of what you won't need

Before a trip, sign out of accounts you won't use while away, such as work admin consoles, old projects and shopping sites with saved cards. Your password manager still has the details. A stolen laptop that's signed in to less gives away less.

---

## Airports and security screening

Keep the laptop in your cabin bag. Australia's cyber security agency advises against putting devices in checked luggage. <sup>188</sup> Checked bags pass through many hands out of your sight, and airlines often limit lithium batteries in the hold.

**Airport security.** Washington DC police describe a two-person trick at the scanner: one thief walks through quickly, the other holds up the line, and your laptop rolls off the belt to the first one. Their advice is to put the laptop on the belt only when you're next in line and to watch it come out. Canada's airport security agency suggests putting the things you most want to watch in the last bin you send through. <sup>163,176</sup>



#### TRICK The last bin

Send your coat, shoes and bag through first, and the laptop in the very last bin, so it reaches the far end when you do. Then pack the laptop first, before your belt and shoes.

---

## On the move

Planes, trains and airport lounges mix long waits with tired people. Keep the laptop in the bag at your feet rather than in an overhead rack where you can't see it, and use a privacy screen if you work on board (Chapter 6). Lounges and gate areas count as public Wi-Fi (Chapter 10).

---

## Hotels

Hotels need a decision each time. Take the machine with you when that makes sense, or use the room safe or the hotel's secure storage. Check that the laptop actually fits and that the safe closes without pressing on the lid. Keep doors and windows shut, and don't leave the bag unattended while you check in. A cable to the furniture adds some delay, but we can't vouch for hotel furniture or hotel safes as secure. <sup>7</sup>

Official guidance from several governments goes a step further on safes. The US National Counterintelligence and Security Center notes that capable actors can get into hotel safes, and Australia's cyber security agency advises never leaving devices unattended, even in hotel safes. <sup>186,188</sup> So treat the safe as protection against casual theft, and let encryption do the rest.

If the laptop has to stay in the room, NSA guidance says it should be powered down with full-disk encryption on. <sup>194</sup> That's the same advice as Chapter 4: shut down, don't sleep.



#### EXAMPLE A good hotel routine

1. On arrival, check the laptop fits the safe without pressing on the lid.
2. When you go out for the day, take the laptop if you can.
3. If it stays, shut it down, lock it in the safe, and put the "do not disturb" sign out if you don't need cleaning.
4. If you use tamper-evident seals or the two-photo trick (Chapter 5), check them when you return.

---

## Bags

"Anti-theft" backpacks with hidden zips, lockable pulls or cut-resistant panels are designed to slow down pickpockets and bag thieves. The claims are the makers'; we found no independent test against laptop theft, and we haven't tested any ourselves. A plain bag that doesn't look like it holds a laptop may draw less attention. RFID-blocking pockets protect contactless cards and passports; laptops have no RFID chip to read, so that feature does nothing for the laptop.

---

## At the border

Border officers in many countries can inspect travellers' belongings, including laptops and phones, under their national rules. The rules, and your rights, differ from country to country, so read the official guidance for each country you're entering before you travel.

As one example of published rules, US Customs and Border Protection explains on its website that all travellers crossing the US border are subject to inspection, that device searches happen rarely (less than 0.01 percent of arriving international travellers had their devices searched in fiscal year 2025, by its figures), and that travellers are expected to present devices in a condition that allows them to be examined. It also says it gives travellers an in-

formation sheet explaining the purpose of a search and how to raise concerns. <sup>195,196</sup>

The calm approach is the same everywhere:

- **Know the rules** for the country you're entering, from its official government website.
- **Follow officers' instructions** and be polite. Ask for any written information they provide.
- **Carry less.** A laptop with only the trip's data has less on it to worry about at any checkpoint, and less to lose to a thief.
- **For work devices**, follow your employer's travel policy and know who to contact if a device is held.



#### **WATCH OUT** Where to check the rules

Border rules change and depend on your nationality and where you're going. This section explains where to look, not what the law says. For a specific question, ask the country's official authorities or a lawyer.

## Coming home

Official guidance recommends a short reset after travel, especially after business trips. <sup>185,190</sup>

- **Install updates** and run a check with the built-in antivirus.
- **Forget** hotel, airport and conference Wi-Fi networks (Chapter 10).
- **Change passwords** you used on shared or public computers, and sign out sessions you don't recognise.
- **Copy back** new work to your normal backup.
- **If the device was out of your control**, for example lost and returned, left with others or taken away for a while, Australia's cyber security agency advises treating it as possibly compromised. <sup>188</sup> For a work laptop, tell your IT team. For a personal one, see Chapter 12.

**STORY** **Imagine the conference week**

Imagine a small business owner at a trade fair abroad. She took a second laptop with only her slides, price lists and email. On the fourth evening it disappears from a stand while she's talking to a customer. It's a bad hour, not a disaster: the laptop was encrypted and shut down, her main laptop is at home, and the trip's files were already in her backup. She reports it to the venue and the police, changes two passwords and carries on with her phone.

**CHECKLIST** **Before every trip**

- ☐ Update, back up and leave one copy at home.
- ☐ Encryption on; shut down rather than sleep.
- ☐ Finding turned on and tested.
- ☐ Serial number and photos saved separately.
- ☐ Only the trip's data and accounts on the laptop.
- ☐ Charger that plugs into a mains socket packed.
- ☐ Insurance and employer rules checked.
- ☐ Official border guidance read for each country you're entering.

**MORE ON THE SITE**

- [Travel, bags and hotel rooms](#)
- [Power bank calculator for the trip](#)

**Stay in the loop**

Travel rules change. Get the updates before your next trip.

**Get the TechCortado newsletter**

[Bluesky](#) · [Mastodon](#) · [Pixelfed](#) · [TechCortado.com](#)

# 12

## CHAPTER 12

# When it goes wrong

*After a theft, and when you sell*

---

### INSIDE

The first hour

Insurance, serial numbers and second-hand listings

If it comes back

Selling or giving away a laptop safely





## IN THIS CHAPTER

- Safety first: tell staff and the police. Never confront anyone or follow a tracker yourself.
- Then contain: lock or erase, secure accounts, sign out sessions, tell your employer.
- Save proof and call your insurer.
- Restore onto a trusted replacement right away. Don't wait for the laptop to turn up.
- A device that comes back after being out of your control may need checking or resetting.
- Selling a laptop is a planned "loss": back up, remove it from your accounts, erase it properly.
- **Time needed:** keep the after-theft log in Appendix A ready now; it takes 10 minutes.

If you are reading this with an empty desk in front of you, start at "The first hour" and work down. If you are reading ahead, the checklist at the end of this chapter is what to prepare now.



**Figure 12.1** What to do after a theft, in order.

## The first hour

Your first moves are about safety and containment, not a recovery mission of your own. Tell the venue staff and the police, save the last known location and its time, and give them identifying details. Never confront a suspected thief, or go into a building because a tracker points there. Even tag makers recommend involving local police when you suspect theft. <sup>3,108</sup>

From a trusted device, use the relevant lost or lock feature, and think back to whether the laptop was off, screen-locked, asleep or unlocked and in use. If it held work material, tell your employer straight away. Then secure the accounts and credentials that were on it, starting with the order in the box below. Signing out existing sessions and revoking tokens matters as much as changing passwords. Neither can pull back files that were already cached or copied offline.

**EXAMPLE Which accounts first?**

A sensible order for most people:

1. **Email.** It resets everything else.
2. **Password manager.** Check its own recovery and session options.
3. **Cloud storage and backups.**
4. **Anything with admin access:** work systems, websites, servers.
5. **Banking and shopping** sites with saved cards.

That order is a suggestion. Each provider's own recovery steps come first.

Save proof before anything changes: the laptop's serial number, receipt, model, any distinguishing marks, the time and place of the theft, the police reference number and timestamped screenshots. Report it to your insurer promptly, following the policy's rules. Before you travel, ask your insurer about business use, which countries are covered, conditions for items left in cars, single-item limits, the excess and how replacements are valued. That's a list of questions to ask, not a description of any particular policy. <sup>8,110</sup>

A remote erase can be an urgent step when the data at risk justifies it. You don't have to wait until every attempt to get the hardware back has failed. Don't assume it ran while the laptop was offline, and a tracker update doesn't prove it finished. Start restoring onto a trusted replacement from your tested backups right away, instead of waiting to see if the laptop turns up. Write down what was lost and which security settings were already on. That preparation turns a theft into a contained interruption instead of guesswork about every account and file. <sup>111</sup>

---

## Insurance, serial numbers and second-hand listings

Before anything happens, write down the serial number and take a few photos of the laptop, including any marks or stickers. With make, model and serial number, police can enter a stolen device into their records straight away. Some police forces, such as Washington DC's, say so on their theft advice pages, and some countries have free national property registers police can search. <sup>163,162</sup>

Check your insurance before you need it. In the US, the Insurance Information Institute says most renters policies include off-premises cover, so belongings stolen away from home, including from your car, can be covered. Policies differ in whether they pay the actual cash value, after depreciation, or the replacement cost. A two-year-old laptop can be worth much less on paper than it costs to replace. Ask about single-item limits and business use too. <sup>177</sup>

After a theft, it can be worth searching local second-hand listings for your model for a few weeks. If you think you've found it, see the box below. <sup>3</sup>



#### **WATCH OUT** Don't buy it back yourself

If you think you've found your laptop for sale, it's tempting to arrange a meeting. Don't. Send the listing, serial number and photos to the police and let them decide what to do.

## If it comes back

Sometimes a lost laptop turns up: handed in by a finder, returned by the venue, or recovered by the police. That's good news, but think before you sign in. Australia's cyber security agency advises treating a device that has been out of your control as possibly compromised. <sup>188</sup>

- **Work laptop:** hand it to your IT team before using it.
- **Personal laptop:** check for signs of tampering (Chapter 5). If you have any doubt, erase it and reinstall the system, then restore your files from your backup.
- **Either way:** keep the passwords you changed after the theft. Don't change them back.



#### **STORY** Imagine the phone call

*Imagine a laptop left in a taxi. The driver hands it to the taxi office, and the office calls the owner three days later. It was shut down and encrypted, the screws look untouched and nothing about it seems odd. The owner still erases it and restores from her backup before signing in. It takes an evening. In return she never has to wonder.*

## Selling or giving away a laptop safely

A laptop you sell is a laptop that leaves your hands on purpose, so the same thinking applies.

1. **Back up and check the backup opens** on another device.
2. **Sign out and remove it from your accounts.** On a Mac, remove it from Find My so the buyer isn't stuck behind Activation Lock. <sup>112</sup>
3. **Erase it properly.** On Windows, use Reset this PC with "Remove everything" and turn on "Clean data", which Microsoft recommends when you sell, donate or recycle. On a Mac, use Erase All Content and Settings. <sup>178,179</sup>
4. **Know why encryption helps here too.** NIST's media sanitisation guide lists cryptographic erase, destroying the encryption key, as a recognised method. A drive that was encrypted from day one is far easier to clean with confidence. <sup>180</sup>
5. **Remove stickers, labels and plates** that point back to you, and update any property register you used.



### CHECKLIST Keep ready now

- ☐ Fill in the after-theft log in Appendix A and store it away from the laptop.
- ☐ Note your insurer's claim number and policy details.
- ☐ Bookmark your laptop's lost-device page on your phone.
- ☐ Know who to call at work if it's a work laptop.

### MORE ON THE SITE

- [What to do after a theft](#)
- [Selling or giving away a laptop safely](#)



### Stay in the loop

We hope you never need this chapter. Stay in touch anyway.

[Get the TechCortado newsletter](#)

[Bluesky](#) · [Mastodon](#) · [Pixelfed](#) · [TechCortado.com](#)

# 13

## CHAPTER 13

# Habits, setups and checklists

*Put the layers together*

---

### INSIDE

Twenty habits that make the layers work  
Three setups

Quick start: a 15-minute checklist

**IN THIS CHAPTER**

- Twenty small habits make the layers in this book actually work.
- Three example setups show how much to do for an everyday laptop, a travelling one and a fixed desk.
- If you only have 15 minutes, use the quick start at the end of this chapter.
- **Time needed:** 15 minutes for the quick start.

By now you have met every layer. This chapter turns them into routines you can keep, shows three example setups, and ends with a quick start for the days you only have fifteen minutes.

## Twenty habits that make the layers work

1. **Pack up by default when you stand up.** Then the cable never becomes an excuse to leave the laptop behind. <sup>3</sup>
2. **Check the anchor before you uncoil the lock.** A chair that moves, a desk part that lifts off or a fitting the cable can slide off will undo the whole setup.
3. **Note the exact laptop model and lock SKU together.** Add a photo of the right slot, spacer and fitted head. Buying a replacement gets much easier. <sup>12,13,15</sup>
4. **Keep the key on you.** Store the spare away from the laptop bag. A combination should also be recoverable without the computer.
5. **Practise the lock routine at home.** Engage it, give it a gentle tug, take the key or scramble every dial, then lock the screen. <sup>11</sup>
6. **Don't carry or lift the laptop by the lock.** It's a restraint, not a handle or a strength demo.
7. **Check the laptop still sits flat.** Try the charger, the ports you use most and the full lid movement before the return window closes. <sup>17,34</sup>
8. **Give adhesive the prep and time that product asks for.** A plate stuck on in a rush the night before a trip may not have bonded properly yet. <sup>27,44</sup>

9. **Set a short screen-lock timer and check it asks for a password on wake.** Use the lock shortcut when you step away rather than waiting. The timer is a fallback.
10. **Before travel, watch it shut down fully.** A closed lid may only mean sleep. For sensitive data, check startup authentication as well as encryption. <sup>49,54</sup>
11. **Check every drive.** A well-protected system drive doesn't help much if all your work sits on an unencrypted second SSD. <sup>47,48</sup>
12. **Recheck protection after repairs or firmware updates.** In Windows, "encrypted" and "BitLocker protection on" are separate status lines. <sup>52,53</sup>
13. **Keep the backup out of the theft.** If the laptop and its only backup travel in one bag, they can be lost together. <sup>71</sup>
14. **Restore a file, then open it.** A "backup complete" message is nice. A restored project you can open answers the harder question. <sup>86,87</sup>
15. **Test recovery without your laptop or your phone.** Register a spare sign-in factor in advance and keep recovery material safely elsewhere. <sup>88,89</sup>
16. **Review admin access before a trip.** Sign out of admin consoles you won't need, and delete old exports of passwords or recovery secrets. Keep server and backup logins limited to their job.
17. **Name tags after what they're attached to.** "Laptop bag" is more honest than "Laptop" if the tag stays in the bag when the laptop comes out.
18. **Test alerts after changing phones or permissions.** A paired tag and a working alert aren't the same thing. <sup>104,105</sup>
19. **Keep an incident sheet somewhere else.** Note the serial number, proof of purchase, support contacts, recovery portal and insurer details. Never put decryption keys on a sheet other people can open. <sup>8</sup>
20. **Review the setup after any change.** A new laptop, bag, desk, phone, backup drive or password manager can quietly break something that used to work.

**TIP Pick three**

Twenty habits is a lot. Pick the three you skip most often and practise only those for a month. Then pick three more.

## Three setups

These are example setups. They aren't price tiers or certifications. Each assumes supported software, current updates and a healthy machine. Match the extra effort to how sensitive the work is and how the laptop travels.

### Everyday personal laptop

Start with BitLocker or Device Encryption, FileVault, or a supported encrypted Linux install, and check it's really on. Use a strong sign-in, automatic screen lock, an encrypted external backup kept somewhere else, and another offsite copy. Test account recovery and write down the serial number. Add a lock made for your exact slot if there's somewhere solid to anchor it. A compatible tracker helps with bags you forget.

Often the purchase that matters most is a backup drive, not a fancier lock. If your files only exist on the laptop, fix that first. If you already have a dependable backup, focus on being able to restore it and on whether the laptop you carry around is signed into too much.

### Frequent travel or shared workspaces

Keep the same baseline, then pick a lock you'll actually bring, with a head that fits the machine and a cable long enough to reach the anchors you usually find. For sensitive work on Windows, use a supported startup PIN. Shut down for travel, back up before you leave, and keep recovery material and at least one backup at home. Test that you can reach the finding service from another device. <sup>49,55</sup>

Carry fewer local files and fewer signed-in accounts. If one powerful browser session opens everything, an unlocked theft costs far more than the laptop. A limited travel profile or a separate travel laptop can make sense, as long as you have a working way to reach what you actually need. If you're also sorting out power for the trip, our [power bank guide](#) covers the laptop-sized ones.

### Fixed desk or higher-sensitivity work

Improve the anchor and the storage around it, think about a compatible cradle or enclosure where the machine stays put, and decide who holds the keys. For managed fleets, write down who can use master keys and recover

combinations. Use centrally managed encryption recovery, approved backups and an incident process that suits the organisation. <sup>46</sup>



#### EXAMPLE One household, three setups

Imagine one household. The family laptop on the kitchen table gets the everyday setup. The parent's work laptop, which goes on trains twice a week, gets the travel setup with a startup PIN and a privacy screen. The reception PC in the family's small office gets a locking station and a firmware password. Same book, three different amounts of effort.

## Quick start: a 15-minute checklist

If you do nothing else today, do these. Each takes a minute or two.

1. **Check encryption is on.** Windows: Settings, search "encryption". Mac: FileVault in Privacy & Security. Linux: check at install or with your distribution's tools.
2. **Find your recovery key** and save it somewhere that isn't this laptop.
3. **Turn on Find My or Find My Device**, then check the laptop shows up from your phone.
4. **Set the screen to lock after a few minutes** and learn the shortcut: Windows key + L, or Control-Command-Q on a Mac.
5. **Start a backup** to a drive or a cloud backup service. A first one running beats a perfect plan.
6. **Write down the serial number** and take two photos of the laptop.
7. **Check your email and password manager** have a second factor that isn't on this laptop.
8. **Turn on Dynamic Lock** on Windows if you carry your phone everywhere, or practise the lock shortcut on any system.



#### CHECKLIST The full checklist

The complete checklist, with chapter numbers, is in Appendix A. Tick it off once, then again after any big change: a new laptop, phone, bag, backup drive or password manager.

---

**MORE ON THE SITE**

- [Twenty habits that make the layers work](#)
- [The full checklist](#)



### **Stay in the loop**

Get the next edition of this handbook when it is out.

**Get the TechCortado newsletter**

[Bluesky](#) · [Mastodon](#) · [Pixelfed](#) · [TechCortado.com](#)



## APPENDIX A

# Worksheets

*Fill in, print, keep away from the laptop*

---

### INSIDE

Device record

Threat self-check

Recovery-kit record

Travel checklist

After-theft log

The full checklist





## IN THIS CHAPTER

- Six worksheets: device record, threat self-check, recovery-kit record, travel checklist, after-theft log and the full checklist.
- Fill them in on paper or in a copy of this file. Keep them somewhere the laptop isn't.
- Never write decryption keys or passwords on a sheet other people can open. The recovery-kit record says **where** things are, not what they are.

## Device record

| Item                                                   | Your details |
|--------------------------------------------------------|--------------|
| Make and model                                         |              |
| Serial number                                          |              |
| Wi-Fi MAC address                                      |              |
| Date bought, and where                                 |              |
| Receipt stored at                                      |              |
| Photos taken (whole laptop, serial label, marks)       |              |
| Distinguishing marks, stickers, engraving              |              |
| UV or forensic mark code                               |              |
| Tracking tag name and network                          |              |
| Property register or campus registration and reference |              |
| Insurer, policy number and claim phone number          |              |
| Employer IT contact (work laptops)                     |              |
| Lock model, key number or code location                |              |

# Threat self-check

Tick the answers that fit, then read the chapters in the right-hand column first.

| Question                                                             | Yes                      | No                       | If yes, start with |
|----------------------------------------------------------------------|--------------------------|--------------------------|--------------------|
| Do you use the laptop in cafés, trains or libraries every week?      | <input type="checkbox"/> | <input type="checkbox"/> | Chapters 2, 6, 10  |
| Does it hold the only copy of anything important?                    | <input type="checkbox"/> | <input type="checkbox"/> | Chapter 7          |
| Would someone reading its files hurt you, a client or your employer? | <input type="checkbox"/> | <input type="checkbox"/> | Chapters 4, 5      |
| Does it often sleep instead of shutting down when you travel?        | <input type="checkbox"/> | <input type="checkbox"/> | Chapter 4          |
| Is it signed in to email, banking and work admin all at once?        | <input type="checkbox"/> | <input type="checkbox"/> | Chapters 6, 11     |
| Does it sit in hotel rooms, cars or shared offices?                  | <input type="checkbox"/> | <input type="checkbox"/> | Chapters 3, 5, 11  |
| Do other people use it?                                              | <input type="checkbox"/> | <input type="checkbox"/> | Chapter 6          |
| Would you know what to do in the first hour after a theft?           | <input type="checkbox"/> | <input type="checkbox"/> | Chapter 12 (if no) |

# Recovery-kit record

Write **where** each item is kept, never the secret itself.

| Item                                                | Where it's kept (not on the laptop) | Last checked |
|-----------------------------------------------------|-------------------------------------|--------------|
| Disk encryption recovery key                        |                                     |              |
| Password manager emergency kit or emergency contact |                                     |              |
| Spare security key or backup codes for email        |                                     |              |
| Backup drive and its password                       |                                     |              |
| Cloud backup login and any private key              |                                     |              |
| Firmware or supervisor password                     |                                     |              |
| Spare lock key or combination                       |                                     |              |

## Travel checklist

| Before you go                                                  | Done                     |
|----------------------------------------------------------------|--------------------------|
| System, browser and apps updated                               | <input type="checkbox"/> |
| Backup run and one copy left at home                           | <input type="checkbox"/> |
| Encryption on, startup PIN set if needed, shut down for travel | <input type="checkbox"/> |
| Finding turned on and tested from another device               | <input type="checkbox"/> |
| Only the trip's data and accounts on the laptop                | <input type="checkbox"/> |
| Serial number and photos saved separately                      | <input type="checkbox"/> |
| Insurance and employer travel rules checked                    | <input type="checkbox"/> |
| Official border guidance read for each country you're entering | <input type="checkbox"/> |
| Charger for mains sockets, privacy screen, lock packed         | <input type="checkbox"/> |
| Auto-join off, Bluetooth and sharing off                       | <input type="checkbox"/> |

| After you return                                        | Done                     |
|---------------------------------------------------------|--------------------------|
| Updates installed and a security scan run               | <input type="checkbox"/> |
| Travel Wi-Fi networks forgotten                         | <input type="checkbox"/> |
| Passwords changed if used on shared computers           | <input type="checkbox"/> |
| New work copied to your normal backup                   | <input type="checkbox"/> |
| Device checked, or reset, if it was out of your control | <input type="checkbox"/> |

## After-theft log

| Step                                               | Time and notes |
|----------------------------------------------------|----------------|
| Where and when it was last seen                    |                |
| State at the time: off, asleep, locked or unlocked |                |

| Step                                                | Time and notes |
|-----------------------------------------------------|----------------|
| Venue staff told (name)                             |                |
| Police report number                                |                |
| Last known location and its time (screenshot saved) |                |
| Lock or erase sent from (device)                    |                |
| Employer told (name, time)                          |                |
| Email password changed, sessions signed out         |                |
| Password manager secured                            |                |
| Cloud storage and backups secured                   |                |
| Admin, banking and shopping accounts checked        |                |
| Insurer told, claim number                          |                |
| Restore started on replacement                      |                |
| Second-hand listings checked (dates)                |                |

## The full checklist

| Area          | What to do                                                                               | Chapter | Done                     |
|---------------|------------------------------------------------------------------------------------------|---------|--------------------------|
| Habits        | Pack up when you stand up; keep the bag closed and in sight                              | 2       | <input type="checkbox"/> |
| Lock          | Match the head to your slot; anchor to something fixed; keyed or combination to suit you | 3       | <input type="checkbox"/> |
| Encryption    | System and second drives encrypted; protection status checked                            | 4       | <input type="checkbox"/> |
| Startup       | PIN or passphrase before the system starts on travel laptops                             | 4       | <input type="checkbox"/> |
| Recovery keys | Saved away from the laptop; tested                                                       | 4       | <input type="checkbox"/> |
| Firmware      | Supervisor or firmware password stored safely; USB and network boot off; Secure Boot on  | 5       | <input type="checkbox"/> |
| Tamper checks | Seal or photo of the screws if the laptop sits in hotel rooms                            | 5       | <input type="checkbox"/> |

| Area             | What to do                                                      | Chapter | Done                     |
|------------------|-----------------------------------------------------------------|---------|--------------------------|
| Screen lock      | Short timeout; Dynamic Lock or presence sensing where available | 6       | <input type="checkbox"/> |
| Privacy          | Privacy screen for trains, cafés and planes                     | 6       | <input type="checkbox"/> |
| Second factor    | Security key or passkey kept off the laptop; spare at home      | 6       | <input type="checkbox"/> |
| Password manager | Emergency kit or emergency access set up                        | 6       | <input type="checkbox"/> |
| Updates          | Automatic updates on; built-in antivirus and firewall on        | 6       | <input type="checkbox"/> |
| Shared use       | Separate accounts; standard accounts for daily use              | 6       | <input type="checkbox"/> |
| Backups          | 3-2-1: drive plus cloud backup, versioning on                   | 7       | <input type="checkbox"/> |
| Restore test     | Restore and open a file each month                              | 7       | <input type="checkbox"/> |
| Account recovery | Works without this laptop or phone                              | 7       | <input type="checkbox"/> |
| Finding          | Built-in finding or anti-theft software on and tested           | 8       | <input type="checkbox"/> |
| Tags             | Tag matched to your phone, in the sleeve or bag                 | 8       | <input type="checkbox"/> |
| Marking          | Serial registered; return label; UV or plate if you like        | 8       | <input type="checkbox"/> |
| Tripwires        | Optional canary tokens or decoy account, tested                 | 9       | <input type="checkbox"/> |
| Public Wi-Fi     | Hotspot or VPN for anything sensitive; auto-join off            | 10      | <input type="checkbox"/> |
| Radios           | Bluetooth and sharing off when not needed                       | 10      | <input type="checkbox"/> |
| Travel           | Belt last, laptop shut down, cabin bag only, travel profile     | 11      | <input type="checkbox"/> |
| Insurance        | Off-premises cover and replacement cost checked                 | 12      | <input type="checkbox"/> |
| After a theft    | Police, lock or erase, sign out sessions, insurer               | 12      | <input type="checkbox"/> |
| Selling          | Remove from your accounts, reset with clean data, remove labels | 12      | <input type="checkbox"/> |

**MORE ON THE SITE**

→ Quick-start: a 15-minute checklist



**Stay in the loop**

Printable checklists and updates, as they come.

**Get the TechCortado newsletter**

Bluesky · Mastodon · Pixelfed · TechCortado.com

# B

## APPENDIX B

# Example products (as of 2026)

*Names, so you know what to search for*

---

### INSIDE

Locks and anchors (Chapter 3)

Encryption (Chapter 4)

Privacy screens (Chapter 6)

Backups and password managers (Chapters 6 and 7)

Tracking tags (Chapter 8)

Finding and anti-theft software (Chapter 8)

Marking and registration (Chapter 8)

Canary tokens (Chapter 9)



IN THIS CHAPTER

- The chapters describe methods and features. This appendix names example products so you know what to look for.
- These are examples we read about while researching, **not endorsements** and not test results. We didn't test any of them ourselves.
- Product names, models and features change. Everything here was checked on 29 and 30 October 2026. Check the maker's current page before you buy.
- No prices: they change too often to print.



**WATCH OUT** How to read this appendix

Names, model numbers and maker claims are copied from the makers' own pages. A product appearing here doesn't mean it's better than one that doesn't. Check the exact model fits your laptop, your phone and your country.

## Locks and anchors (Chapter 3)

This table compares documented fit and features. It isn't a strength ranking from our own tests. Check the exact SKU, your laptop model, local stock, the full price at checkout, the return terms, and whether the cable or adapter is in the box. We didn't put together a like-for-like price comparison for any single country, so prices aren't listed.

| Product and SKU                                                          | Interface                                        | Documented cable or fitting                       | Who it suits, and the catch                                                                                                              |
|--------------------------------------------------------------------------|--------------------------------------------------|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Kensington Universal 3-in-1 2.0 Keyed</b> , K63389WW <sup>30,31</sup> | Standard/K-slot, Nano, wedge; one adjustable tip | 1.8 m coated carbon steel; diameter not confirmed | Mixed laptops, or if you might switch laptop. "Universal" still needs a model and clearance check; slotless laptops need something else. |

| Product and SKU                                                                                      | Interface                                                        | Documented cable or fitting                              | Who it suits, and the catch                                                                                                                          |
|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Kensington Universal 3-in-1 (previous generation),</b> K62318WW <sup>32,33</sup>                  | Standard/K-slot, Nano, wedge; swappable tips                     | 1.8 m carbon steel                                       | Keeping or repairing a lock you already have. Spare tips get lost; don't mix it up with 2.0.                                                         |
| <b>Kensington Slim NanoSaver 2.0 EQ,</b> K60630WW <sup>34</sup>                                      | Nano                                                             | 1.8 m stainless steel                                    | Thin Nano-slot laptop where clearance matters. Not for standard or wedge slots; check local stock and laptop shape.                                  |
| <b>Kensington MicroSaver 2.0,</b> K65020WW (regional variants exist) <sup>35</sup>                   | Standard Kensington/T-bar                                        | 6 ft carbon steel; the 10 mm figure is the HEAD diameter | Standard-slot business laptop. Won't fit Nano or wedge; the website's availability notices are unclear.                                              |
| <b>Kensington MicroSaver 2.0 Portable,</b> K64423 / K67989 variants; check your region <sup>36</sup> | Standard                                                         | Coiled; extends to 6 ft, packs to about 3 in             | Travellers who want small packing. Coiled portability isn't evidence it resists as well as a full desk cable.                                        |
| <b>Noble low-profile flat-key wedge,</b> TZ18T <sup>37</sup>                                         | Wedge, for listed Dell consumer/gaming/Alienware models          | 1.8 m, 4 mm PVC-coated braided steel; 105 g              | Compatible low-profile Dell gaming laptop. Check the model, not just the Dell logo; the 150 lbf figure is the maker's own claim, not a theft rating. |
| <b>Noble compact barrel-key wedge,</b> TZ04T <sup>38</sup>                                           | Wedge, for listed Dell Latitude and other models                 | 1.8 m, 4 mm; 98 g per maker's table                      | Compatible Latitude, if you prefer a barrel key. A different key type doesn't make it more secure than the flat-key one.                             |
| <b>Targus DEFCON Ultimate Universal resettable,</b> ASP96RGLX <sup>39</sup>                          | Standard/Nano/wedge, including what Targus calls oversized wedge | 2 m galvanised, sleeved steel                            | Someone who wants to set their own code. Four digits can be watched over your shoulder; code count isn't attack time; ignore "cut-proof" marketing.  |
| <b>Targus DEFCON Ultimate Universal serialised,</b> ASP96GLX-S <sup>40</sup>                         | Standard/Nano/wedge                                              | 2 m galvanised, sleeved steel                            | IT teams that want managed code recovery. Serialised isn't the same as user-resettable; check local warranty and recovery process.                   |

| Product and SKU                                                                                                                       | Interface                                          | Documented cable or fitting                         | Who it suits, and the catch                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------|-----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>StarTech Universal serialised</b> , UNIVCS-LAPTOP-LOCK <sup>41</sup>                                                               | Standard/Nano/wedge                                | 2 m, 4.4 mm carbon steel                            | Managed fixed-code rollouts that need slot-specific test figures on paper. Preset code can't be changed; listed pull figures differ by slot.                            |
| <b>Compulocks Ledge MacBook adapter/bundle</b> , MBPR14LDG01KL / MBPR16LDG02KL / MBALDG04KL / MBALDG05KL by exact model <sup>25</sup> | Adds a lock point to supported MacBooks            | Depends on bundle; check whether a lock is included | Compatible slotless MacBook, travel or desk. Needs an exact chassis match; the load is carried by a small part of the laptop.                                           |
| <b>Compulocks Blade</b> , BLD01 bracket; BLD01KL keyed bundle; BLD01CL combination bundle <sup>26</sup>                               | Adds a standard lock point with an adhesive plate  | Depends on bundle                                   | Slotless, flat-backed device with no mechanical adapter. Surface prep, curing and adhesion carry the load; don't block vents; maker's force claim isn't a chassis test. |
| <b>Kensington Laptop Locking Station 2.0</b> , K64453WW with lock / K64451WW without <sup>28</sup>                                    | External adjustable arms around a supported laptop | Lock included only in one bundle                    | A permanent desk with a slotless laptop. Bulky, and needs an exact physical fit; screen size alone tells you little.                                                    |
| <b>Targus dedicated T-Lock</b> , ASP48USX <sup>42</sup>                                                                               | Standard T-bar                                     | 6 ft galvanised steel                               | A dedicated standard-slot alternative. No universal tip; EU version and stock not confirmed.                                                                            |
| <b>StarTech large anchor</b> , LTANCHORL <sup>43</sup>                                                                                | Desk anchor, not a laptop lock                     | Ring opening 35 × 19 mm                             | Permanent desk where you're allowed to mount it properly. The screws are only as strong as the desk; not portable.                                                      |
| <b>Targus base plate</b> , PA400P <sup>44,45</sup>                                                                                    | Desk anchor accessory                              | Compatible cable sold separately                    | A compatible DEFCON setup with proper mounting. The manual itself calls adhesive-only fitting marginal security.                                                        |

None of the recent public comparisons we found tested every lock on this list to destruction under one shared method. The makers' reports back up their own specs. They don't crown an independent winner.

For a **confirmed Nano slot**, compare the Slim NanoSaver 2.0 EQ with other heads that clearly list Nano, and pay close attention to clearance. For a **standard slot**, a dedicated MicroSaver 2.0 or a Targus T-bar lock is the simple route. For a **wedge slot**, compare a Noble lock listed for your exact model with Kensington's N17 range. For **mixed slot types**, the 2026 Kensington 3-in-1 2.0 does away with loose tips, while the Targus and StarTech models give you different ways of handling codes. <sup>34,35,42,37,38,14,30,40,39,41</sup>

For a **slotless MacBook**, start with a mechanical adapter made for your exact chassis, or a desk station that fits. Only consider an adhesive option if you have a suitable surface and a plan for fitting it. At a **regular desk**, give the anchor at least as much thought as the lock head. <sup>25,28,44,43</sup>

---

## Encryption (Chapter 4)

- **Built into the operating system:** BitLocker and Device Encryption (Windows), FileVault (macOS), LUKS (most Linux distributions). These are the methods Chapter 4 describes.
- **Open-source third-party tool for Windows system encryption and encrypted containers:** VeraCrypt is one well-known example. Its documentation covers supported systems, the rescue disk and its limits.

<sup>115,116,119</sup>

---

## Privacy screens (Chapter 6)

- **Add-on filters:** several accessory makers sell louvre-type filters with magnetic, adhesive-tab or slide-on fittings. One maker's datasheet, used in Chapter 6, lists a microlouver filter with a 60-degree viewing angle, magnetic strips and a reversible matte and glossy side. <sup>201</sup>
- **Built-in switchable displays:** some business laptops offer an integrated privacy screen switched with a key, for example HP's Sure View, described in the maker's white paper. <sup>203</sup> Other makers offer similar options on some models; check the specification of the exact model.

## Backups and password managers (Chapters 6 and 7)

| Kind                                         | Examples                                                              | What to check                                                                              |
|----------------------------------------------|-----------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Cloud backup service                         | Backblaze Computer Backup, IDrive <sup>132,134</sup>                  | Versions kept, private key option, how restores work, whether external drives are included |
| Cloud sync storage (not a backup on its own) | iCloud+, Google One, OneDrive <sup>135,136,74</sup>                   | Version history and deleted-file retention                                                 |
| Portable drives                              | Common portable SSD and hard drive ranges from the big storage makers | Price history; encryption support                                                          |
| Open-source command-line backup              | restic, Borg <sup>81,83</sup>                                         | Supported version, key backup, scheduling and alerts                                       |
| Password manager recovery                    | 1Password Emergency Kit, Bitwarden emergency access <sup>89,146</sup> | What each recovery piece does; what it depends on                                          |

## Tracking tags (Chapter 8)

| Tag or label                                                  | Phone ecosystem and network                                                                          | Power              | What to check                                                                                                           |
|---------------------------------------------------------------|------------------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------|
| <b>AirTag (2nd generation, 2026)</b> <sup>103,98,93,106</sup> | iPhone/Apples household; Apple Find My                                                               | Replaceable CR2032 | Your phone, OS, UWB and regional support; Find My app needed to locate it; anti-stalking alerts; no guaranteed recovery |
| <b>Chipolo POP</b> <sup>100</sup>                             | iPhone or Android with Google Find Hub; Apple Find My or Google Find Hub                             | Replaceable CR2032 | Exact model compatibility; choosing a network isn't a proven security advantage                                         |
| <b>Pebblebee Clip 5</b> <sup>97</sup>                         | Android or iPhone user who wants a rechargeable tag; Apple Find My OR Google Find Hub, one at a time | Rechargeable       | Remember to charge it; set up the finding network before the companion app; a bag tag follows the bag                   |
| <b>Samsung SmartTag2</b> <sup>101</sup>                       | Compatible Samsung Galaxy owner; Samsung ecosystem                                                   | Replaceable CR2032 | Not for Pixel or other Android phones; UWB needs compatible Galaxy hardware                                             |

| Tag or label                           | Phone ecosystem and network                                                                                   | Power            | What to check                                                                                                                        |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------|------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Tile</b><br>102,95,96,108,109,104   | Households already using Tile/Life360, after checking how well it works locally; Tile network                 | Depends on model | Core finding free; Smart Alerts are a paid extra and don't warn you when the item moves without you; Anti-Theft Mode needs ID checks |
| <b>Asset/QR recovery label</b> 8,97,96 | Proof of ownership and a way for honest finders to reach you; none for a plain label, QR service as described | None             | No location tracking of its own; share as little contact info as possible                                                            |

The table above lists what the makers' pages said in October 2026. Apple launched a second-generation AirTag on 26 January 2026; check you are reading about the current model of any tag. 103



**Figure B.1** A tracking tag. Pick the tag whose network your phone already uses.  
Photo: [ajay\\_suresh](#), [CC BY 2.0](#), via Wikimedia Commons.

## Finding and anti-theft software (Chapter 8)

| Kind     | Examples                                                                                          | Worth knowing           |
|----------|---------------------------------------------------------------------------------------------------|-------------------------|
| Built in | Find My (macOS), Find My Device (Windows), admin tools for managed ChromeOS devices<br>93,110,153 | Free; set up in advance |

| Kind                            | Examples                                  | Worth knowing                                                                                                                                          |
|---------------------------------|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| Third-party anti-theft software | Prey <sup>147,149</sup>                   | Missing reports with opt-in photos and screenshots; also runs on Linux; check current plans, as a free tier was unclear in October 2026 <sup>150</sup> |
| Firmware-persistent agent       | Absolute Home & Office <sup>151,152</sup> | Needs a supported laptop model; the premium edition advertised a recovery guarantee in some countries in 2026                                          |

## Marking and registration (Chapter 8)

- **Security plates:** STOP (Security Tracking of Office Property). <sup>161</sup>
- **Property registers:** in the UK, Immobilise is a free register police can search, and it alerts the CheckMEND second-hand check. <sup>162</sup> Other countries have their own schemes; ask your local police.
- **Forensic marking kits:** several brands sell kits like those used in the studies in Chapter 8.

## Canary tokens (Chapter 9)

- **Canarytokens.org**, run by Thinkst, makes free tokens: Word, Excel, PDF, web bug, Windows folder and more. <sup>164,165</sup>
- **Self-hosted:** the same tokens can run on your own server using the published canarytokens-docker project. <sup>171</sup>

### MORE ON THE SITE

- The full online guide, with every product table
- Lock and anchor shortlist
- Frequently asked questions



### Stay in the loop

Example products change every year. We refresh the list.

Get the TechCortado newsletter

Bluesky · Mastodon · Pixelfed · TechCortado.com

# Glossary

---

**Account recovery.** The ways back into an account when you lose a password or a device: recovery codes, a recovery email or phone, or trusted contacts.

**Admin account.** A user account that can install software and change system settings. Daily work is safer in a standard account.

**Anchor.** The fixed point a cable lock loops around, such as a desk leg or a screwed-down anchor plate.

**Auto-join.** A setting that lets a laptop connect to a known Wi-Fi network name without asking. Off is safer for public networks.

**Backup.** A separate copy of your files that you can restore without the original laptop.

**Biometrics.** Signing in with a fingerprint or a face instead of typing a PIN or password.

**Boot order.** The list of drives a laptop tries to start from, set in the firmware.

**Canary token.** A file or link that sends you an alert when someone opens it.

**Cloud storage.** Files kept on a provider's servers and reached over the internet.

**Decoy.** A deliberately visible account or USB stick meant to be found and opened by a thief, so a canary token can fire.

**Device record.** Your note of a laptop's make, model, serial number, MAC address, photos and marks. See Appendix A.

**Dynamic lock.** A Windows feature that locks the screen when your paired phone moves out of range.

**Emergency kit.** A printed or stored note that holds what you need to get back into a password manager after losing your devices.

**Encryption.** Scrambling data so it can only be read with the right key, PIN or password.

**Evil maid attack.** Tampering with a laptop left unattended, for example in a hotel room, to capture data later.

**Factory reset.** Erasing a laptop and returning it to its original software, before selling or giving it away.

**Finding service.** Software that shows a lost laptop's location and can lock or erase it when it goes online.

**Firewall.** A filter that controls which network connections a computer accepts.

**Firmware.** The low-level software that starts the laptop before the operating system loads. Also called BIOS or UEFI.

**Full-disk encryption.** Encryption that covers the whole system drive, so a removed drive shows only scrambled data.

**Hibernation.** A power state that saves memory to the drive and switches off. It is safe only if that saved file is encrypted.

**Immutable backup.** A backup copy that can't be changed or deleted for a set time, even by the account that made it.

**Juice jacking.** Using a tampered public USB charging port to reach a connected device. Reported as a risk; confirmed cases are rare.

**MAC address.** A hardware identifier for a network adapter. Useful in a device record and for campus registration schemes.

**Offsite copy.** A backup kept in a different place from the laptop, so one fire or burglary can't take both.

**Password manager.** An app that stores strong, unique passwords and fills them in for you.

**Passkey.** A sign-in method that uses a key stored on your device instead of a password, unlocked by a PIN or biometrics.

**Privacy screen.** A filter or built-in display mode that narrows the viewing angle, so people beside you see a dark screen. Also called a privacy filter.

**Recovery code.** A one-time code that lets you into an account when your usual second factor is gone.

**Recovery key.** A long key that unlocks an encrypted drive when the normal sign-in fails. Keep it away from the laptop.

**Second factor.** A second proof of identity at sign-in, such as an app code, a security key or a passkey.

**Secure Boot.** A firmware feature that only starts software signed by a trusted maker.

**Security key.** A small hardware device used as a second factor or passkey.

**Security slot.** The small opening in a laptop's case for a cable lock. Common shapes are standard, Nano and wedge.

**Serial number.** The maker's unique number for one laptop. Police and insurers ask for it.

**Shoulder surfing.** Reading a screen or watching someone type from beside or behind them.

**Sleep.** A low-power state that keeps the working session in memory. Closing the lid is not the same as switching off.

**Standard account.** A user account without admin rights, safer for daily use and for shared laptops.

**Startup PIN.** A PIN asked for before the system starts, so the encrypted drive stays locked until it is typed.

**Tamper-evident seal.** A sticker or mark that shows if a case has been opened, such as glitter nail polish over screws.

**Tracking tag.** A small tag that reports its location through nearby phones on a maker's network.

**TPM.** Trusted Platform Module. A chip that stores encryption keys and checks that the startup chain hasn't changed.

**VPN.** Virtual private network. An encrypted tunnel from your laptop to a trusted network, often provided by an employer.

# Sources

---

The small numbers in the text point to this list. Sources 1 to 180 are the ones used for the TechCortado laptop security guide on the website; 181 to 206 were added for this book. All were checked on 29 and 30 October 2026. Makers' figures are the makers' own claims.

- 1 NCSC Advice for End Users [nsc.gov.uk](https://nsc.gov.uk)
- 2 NCSC 10 Steps to Cyber Security: Data security [nsc.gov.uk](https://nsc.gov.uk)
- 3 Metropolitan Police: Crime Prevention Advice: Distraction Theft [metengage.co.uk](https://metengage.co.uk)
- 4 British Transport Police: Travel safely by rail [btp.police.uk](https://btp.police.uk)
- 5 British Transport Police: Be Aware [btp.police.uk](https://btp.police.uk)
- 6 West Yorkshire Police: Theft from motor vehicles [westyorkshire.police.uk](https://westyorkshire.police.uk)
- 7 Police.uk: How to stay safe while visiting London [police.uk](https://police.uk)
- 8 Police.uk: Mark your property to deter burglars [police.uk](https://police.uk)
- 9 HP Compaq 6720t Mobile Thin Client: End-User Reference Guide, security-cable section [h10032.www1.hp.com](https://h10032.www1.hp.com)
- 10 Types of Laptop Locks: K-Slot, Nano & Wedge Explained [kensington.com](https://kensington.com)
- 11 Simple Solutions Combination Laptop Lock: K60213/K60214/K60215 installation guide [accoblobstorage.us.blob.core.windows.net](https://accoblobstorage.us.blob.core.windows.net)
- 12 How to Physically Secure Your Dell Computer, Monitor or Docking Station [dell.com](https://dell.com)
- 13 Kensington laptop lock selector [customer.kensington.com](https://customer.kensington.com)
- 14 N17 Keyed Laptop Lock for Wedge-Shaped Slots [kensington.com](https://kensington.com)
- 15 StarTech UNIVCS-LAPTOP-LOCK Quick Start Guide: Spanish [sgcdn.startech.com](https://sgcdn.startech.com)
- 16 Universal 3-in-1 2.0 Combination Laptop Lock: K63394WW [kensington.com](https://kensington.com)
- 17 TZ03TC Ultra Compact Wedge Combination Lock [noblelocks.com](https://noblelocks.com)
- 18 TZ06T Keyed & Resettable Combination Wedge Lock [noblelocks.com](https://noblelocks.com)
- 19 Register & Retrieve Program [kensington.com](https://kensington.com)
- 20 What is Pull Strength and Why Does it Matter? [kensington.com](https://kensington.com)
- 21 Noble Wedge Lock Technology [noblelocks.com](https://noblelocks.com)
- 22 30 Years of Kensington Locks [kensington.com](https://kensington.com)
- 23 Trade Agreement Act Compliance: GSA Vendor Support Center [vsc.gsa.gov](https://vsc.gsa.gov)
- 24 ISO/IEC 27001:2022: Information security management systems [iso.org](https://iso.org)
- 25 Compulocks MacBook M5 Lock: Ledge adapters [compulocks.com](https://compulocks.com)
- 26 Universal Laptop Lock: The Blade [compulocks.com](https://compulocks.com)
- 27 Surface Preparation for 3M VHB Tape Applications [3m.com](https://3m.com)
- 28 Kensington Laptop Locking Station 2.0 with MicroSaver 2.0, UK: K64453WW [kensington.com](https://kensington.com)
- 29 Desk Mount Security Anchor Point: K64613WW [kensington.com](https://kensington.com)
- 30 Kensington launches Universal 3-in-1 2.0 laptop locks, 24 March 2026 [kensington.com](https://kensington.com)
- 31 Kensington Universal 3-in-1 2.0 Keyed Laptop Lock [kensington.com](https://kensington.com)
- 32 Kensington Universal 3-in-1 Keyed Laptop Lock, K62318WW [kensington.com](https://kensington.com)
- 33 Kensington replacement lock-head tips, K62315WW [kensington.com](https://kensington.com)
- 34 Kensington Slim NanoSaver 2.0 EQ Keyed Laptop Lock, K60630WW [kensington.com](https://kensington.com)
- 35 Kensington MicroSaver 2.0 Keyed Laptop Lock, K65020WW [kensington.com](https://kensington.com)
- 36 Kensington MicroSaver 2.0 Portable Keyed Laptop Lock [kensington.com](https://kensington.com)
- 37 Noble TZ18T Low Profile Wedge Lock for Dell Consumer and Gaming Laptops [noblelocks.com](https://noblelocks.com)

- 38 Noble TZ04T Compact Wedge Lock with Barrel Key [noblelocks.com](https://noblelocks.com)
- 39 Targus DEFCON Ultimate Universal Resettable Combination, ASP96RGLX [us.targus.com](https://us.targus.com)
- 40 Targus DEFCON Ultimate Universal Serialized Combination, ASP96GLX-S [es.targus.com](https://es.targus.com)
- 41 StarTech UNIVCS-LAPTOP-LOCK official datasheet [media.startech.com](https://media.startech.com)
- 42 Targus DEFCON T-Lock Keyed Cable Lock, ASP48USX [us.targus.com](https://us.targus.com)
- 43 StarTech LTANCHORL large laptop cable-lock anchor [datasheet media.startech.com](https://media.startech.com)
- 44 Targus DEFCON N-KL Mini Keyed Cable Lock installation guide, PA400P [instructions cdn.targus.com](https://cdn.targus.com)
- 45 Targus Security Anchor Base Plate, PA400P [us.targus.com](https://us.targus.com)
- 46 StarTech Universal Laptop Locks for Deployments [guide media.startech.com](https://media.startech.com)
- 47 BitLocker overview: Microsoft Learn [learn.microsoft.com](https://learn.microsoft.com)
- 48 Full disk encryption (FDE): Ubuntu security documentation [documentation.ubuntu.com](https://documentation.ubuntu.com)
- 49 BitLocker countermeasures [learn.microsoft.com](https://learn.microsoft.com)
- 50 New Research Result: Cold Boot Attacks on Disk Encryption [blog.citp.princeton.edu](https://blog.citp.princeton.edu)
- 51 Device Encryption in Windows [support.microsoft.com](https://support.microsoft.com)
- 52 manage-bde status [learn.microsoft.com](https://learn.microsoft.com)
- 53 manage-bde protectors [learn.microsoft.com](https://learn.microsoft.com)
- 54 BitLocker planning guide [learn.microsoft.com](https://learn.microsoft.com)
- 55 How BitLocker PINs help protect your data and devices: NCSC [ncsc.gov.uk](https://ncsc.gov.uk)
- 56 Kernel DMA Protection [learn.microsoft.com](https://learn.microsoft.com)
- 57 Volume encryption with FileVault in macOS [support.apple.com](https://support.apple.com)
- 58 Protect data on your Mac with FileVault [support.apple.com](https://support.apple.com)
- 59 Protecting keys in alternate boot modes [support.apple.com](https://support.apple.com)
- 60 Activation Lock for Mac [support.apple.com](https://support.apple.com)
- 61 How to use dm-crypt and swsusp together [docs.kernel.org](https://docs.kernel.org)
- 62 Hardware-backed disk encryption: Ubuntu 24.04 [ubuntu.com](https://ubuntu.com)
- 63 Hardware-backed disk encryption: Ubuntu 26.04 [ubuntu.com](https://ubuntu.com)
- 64 Hardware-backed disk encryption requirements: Ubuntu 26.04 [ubuntu.com](https://ubuntu.com)
- 65 Configure hardware-backed disk encryption: Ubuntu 26.04 [ubuntu.com](https://ubuntu.com)
- 66 Frequently Asked Questions: Cryptsetup/LUKS [gitlab.com](https://gitlab.com)
- 67 VeraCrypt: Hibernation File [veracrypt.io](https://veracrypt.io)
- 68 VeraCrypt: Unencrypted Data in RAM [veracrypt.io](https://veracrypt.io)
- 69 VeraCrypt: Malware [veracrypt.io](https://veracrypt.io)
- 70 Find your BitLocker recovery key [support.microsoft.com](https://support.microsoft.com)
- 71 Tips for backing up your information (ITSAP.40.002) [cyber.gc.ca](https://cyber.gc.ca)
- 72 Offline backups in an online world [ncsc.gov.uk](https://ncsc.gov.uk)
- 73 CISA / MS-ISAC Ransomware Guide [cisa.gov](https://cisa.gov)
- 74 Restore your OneDrive [support.microsoft.com](https://support.microsoft.com)
- 75 Restore files deleted from your OneDrive [support.microsoft.com](https://support.microsoft.com)
- 76 Back up your Mac with Time Machine [support.apple.com](https://support.apple.com)
- 77 Keep your Time Machine backup disk for Mac secure [support.apple.com](https://support.apple.com)
- 78 Back up your files with Time Machine on Mac [support.apple.com](https://support.apple.com)
- 79 Back up and restore with Windows Backup [support.microsoft.com](https://support.microsoft.com)
- 80 Backup and restore with File History [support.microsoft.com](https://support.microsoft.com)
- 81 restic: Preparing a new repository [restic.readthedocs.io](https://restic.readthedocs.io)
- 82 restic: Encryption [restic.readthedocs.io](https://restic.readthedocs.io)
- 83 Borg: Quick Start [borgbackup.readthedocs.io](https://borgbackup.readthedocs.io)
- 84 Borg: key commands (change-passphrase, export, import) [borgbackup.readthedocs.io](https://borgbackup.readthedocs.io)

- 85 Borg: Additional Notes, append-only mode [borgbackup.readthedocs.io](https://borgbackup.readthedocs.io)
- 86 restic: Working with repositories [restic.readthedocs.io](https://restic.readthedocs.io)
- 87 restic: Restoring from backup [restic.readthedocs.io](https://restic.readthedocs.io)
- 88 Sign in if you lost your security key [support.google.com](https://support.google.com)
- 89 Get to know your Emergency Kit [support.1password.com](https://support.1password.com)
- 90 Find your Secret Key or Setup Code [support.1password.com](https://support.1password.com)
- 91 Generate and use recovery codes [support.1password.com](https://support.1password.com)
- 92 See devices with account access [support.google.com](https://support.google.com)
- 93 Apple: Use Find My to locate your lost Apple device or AirTag [support.apple.com](https://support.apple.com)
- 94 Google: How Find Hub protects your data [support.google.com](https://support.google.com)
- 95 Life360: Tile Network [support.life360.com](https://support.life360.com)
- 96 Life360: How Tile Works [support.life360.com](https://support.life360.com)
- 97 Pebblebee: Get started with Clip 5 [help.pebblebee.com](https://help.pebblebee.com)
- 98 Apple: AirTag (2nd generation) technical specifications [support.apple.com](https://support.apple.com)
- 99 Google: Be ready to find a lost Android device [support.google.com](https://support.google.com)
- 100 Chipolo POP product page [chipolo.net](https://chipolo.net)
- 101 Samsung Galaxy SmartTag2 official specifications [samsung.com](https://samsung.com)
- 102 Life360: Use My Tile without a Subscription [support.life360.com](https://support.life360.com)
- 103 Apple introduces new AirTag with expanded range and improved findability [apple.com](https://apple.com)
- 104 Life360: Set Up Tile Smart Alerts [support.life360.com](https://support.life360.com)
- 105 Apple: Set separation alerts for an AirTag or item [support.apple.com](https://support.apple.com)
- 106 Apple: Alerts for unknown AirTag and compatible tracking devices [support.apple.com](https://support.apple.com)
- 107 Google: Find unknown trackers [support.google.com](https://support.google.com)
- 108 Life360: Tile Anti-Theft Mode [support.life360.com](https://support.life360.com)
- 109 Life360 Product and Services Terms [legal.corp.life360.com](https://legal.corp.life360.com)
- 110 Microsoft: Find or lock a lost Windows device [support.microsoft.com](https://support.microsoft.com)
- 111 If your Mac is lost or stolen [support.apple.com](https://support.apple.com)
- 112 Apple: Remove a device from Find My on Mac [support.apple.com](https://support.apple.com)
- 113 Engadget: Targus Defcon CL lock hacked (2006) [engadget.com](https://engadget.com)
- 114 SecurityInfoWatch / Associated Press: Laptop locks are often easy pickings for thieves (2004) [securityinfowatch.com](https://securityinfowatch.com)
- 115 VeraCrypt: Frequently Asked Questions [veracrypt.io](https://veracrypt.io)
- 116 VeraCrypt: Supported Systems for System Encryption [veracrypt.io](https://veracrypt.io)
- 117 VeraCrypt: Supported Operating Systems [veracrypt.io](https://veracrypt.io)
- 118 VeraCrypt: System Encryption [veracrypt.io](https://veracrypt.io)
- 119 VeraCrypt: Rescue Disk [veracrypt.io](https://veracrypt.io)
- 120 VeraCrypt: Hidden Volume [veracrypt.io](https://veracrypt.io)
- 121 VeraCrypt: Hardware Acceleration [veracrypt.io](https://veracrypt.io)
- 122 systemd-cryptenroll manual [freedesktop.org](https://freedesktop.org)
- 123 Apple: Set a firmware password on your Mac [support.apple.com](https://support.apple.com)
- 124 Apple Platform Security: Startup disk security policy control [support.apple.com](https://support.apple.com)
- 125 Lenovo ThinkPad user guide: UEFI BIOS passwords [download.lenovo.com](https://download.lenovo.com)
- 126 Lenovo: What to do if you forget your supervisor password [download.lenovo.com](https://download.lenovo.com)
- 127 Microsoft: Windows 11 and Secure Boot [support.microsoft.com](https://support.microsoft.com)
- 128 Thunderspy (Björn Ruytenberg, 2020) [thunderspy.io](https://thunderspy.io)
- 129 Invisible Things Lab: Evil Maid goes after TrueCrypt! (2009) [theinvisiblethings.blogspot.com](https://theinvisiblethings.blogspot.com)
- 130 Wired: Nail polish as a tamper seal (2013) [wired.com](https://wired.com)

- 131 Vice: It'll take more than glitter nail polish to stop snooping [vice.com](https://www.vice.com)
- 132 Backblaze: Computer Backup pricing [backblaze.com](https://www.backblaze.com)
- 133 Backblaze: Extended Version History [backblaze.com](https://www.backblaze.com)
- 134 IDrive: Pricing [idrive.com](https://www.idrive.com)
- 135 Apple: iCloud+ plans and pricing [support.apple.com](https://support.apple.com)
- 136 Google One plans [one.google.com](https://one.google.com)
- 137 Pangoly: Samsung T7 2TB price history [pangoly.com](https://pangoly.com)
- 138 Pangoly: WD 5TB My Passport price history [pangoly.com](https://pangoly.com)
- 139 Microsoft Learn: Dynamic lock [learn.microsoft.com](https://learn.microsoft.com)
- 140 Microsoft: Sign-in options in Windows [support.microsoft.com](https://support.microsoft.com)
- 141 Apple: Unlock your Mac with Apple Watch [support.apple.com](https://support.apple.com)
- 142 Microsoft: Managing presence sensing settings in Windows 11 [support.microsoft.com](https://support.microsoft.com)
- 143 Lenovo: What is a privacy filter? [lenovo.com](https://lenovo.com)
- 144 Google: Use a security key for 2-Step Verification [support.google.com](https://support.google.com)
- 145 FIDO Alliance: Passkeys [fidoalliance.org](https://fidoalliance.org)
- 146 Bitwarden: Emergency access [bitwarden.com](https://bitwarden.com)
- 147 Prey: Pricing [preyproject.com](https://preyproject.com)
- 148 Prey: home page [preyproject.com](https://preyproject.com)
- 149 Prey for individuals [preyproject.com](https://preyproject.com)
- 150 Prey help: How to protect your devices with Prey [help.preyproject.com](https://help.preyproject.com)
- 151 Absolute Home & Office: FAQ [homeoffice.absolute.com](https://homeoffice.absolute.com)
- 152 Absolute: Persistence [absolute.com](https://absolute.com)
- 153 Google: Disable or deprovision ChromeOS devices [support.google.com](https://support.google.com)
- 154 Federal Register: DesignerWare, LLC; analysis of proposed consent order (2012) [govinfo.gov](https://govinfo.gov)
- 155 Laycock: Property Marking: A Deterrent to Domestic Burglary? (Home Office, 1985) [popcenter.asu.edu](https://popcenter.asu.edu)
- 156 Forensic property marking and burglary, quasi-experimental study (Security Journal, 2021) [doi.org](https://doi.org)
- 157 Aarhus randomised trial of forensic marking (Journal of Experimental Criminology) [link.springer.com](https://link.springer.com)
- 158 North Zealand randomised trial of burglary prevention (Cambridge Journal of Evidence-Based Policing, 2022) [doi.org](https://doi.org)
- 159 Danish Ministry of Justice: Burglary prevention report (2022) [justitsministeriet.dk](https://justitsministeriet.dk)
- 160 POP Center: Thefts of and from cars on residential streets and driveways [popcenter.asu.edu](https://popcenter.asu.edu)
- 161 STOP (Security Tracking of Office Property) [stoptheft.com](https://stoptheft.com)
- 162 Immobilise [immobilise.com](https://immobilise.com)
- 163 Metropolitan Police Department (Washington DC): Tips for preventing theft of laptops and personal electronics [mpdc.dc.gov](https://mpdc.dc.gov)
- 164 Canarytokens documentation: Guide [docs.canarytokens.org](https://docs.canarytokens.org)
- 165 Canarytokens: Getting started [docs.canarytokens.org](https://docs.canarytokens.org)
- 166 Canarytokens: MS Word token [docs.canarytokens.org](https://docs.canarytokens.org)
- 167 Canarytokens: MS Excel token [docs.canarytokens.org](https://docs.canarytokens.org)
- 168 Canarytokens: Adobe PDF token [docs.canarytokens.org](https://docs.canarytokens.org)
- 169 Canarytokens: HTTP token (web bug) [docs.canarytokens.org](https://docs.canarytokens.org)
- 170 Canarytokens: Windows Directory token [docs.canarytokens.org](https://docs.canarytokens.org)
- 171 thinkst/canarytokens-docker [github.com](https://github.com)
- 172 Microsoft: What is Protected View? [support.microsoft.com](https://support.microsoft.com)
- 173 Google: Browse as a guest on your Chromebook [support.google.com](https://support.google.com)
- 174 Apple: Change Guest User settings on Mac [support.apple.com](https://support.apple.com)
- 175 Microsoft Learn: Local accounts [learn.microsoft.com](https://learn.microsoft.com)
- 176 CATSA: Tips for stress-free screening [catsa-acsta.gc.ca](https://catsa-acsta.gc.ca)

- 177** Insurance Information Institute: Renters insurance [iii.org](https://www.iii.org)
- 178** Microsoft: Reset your PC [support.microsoft.com](https://support.microsoft.com)
- 179** Apple: Erase your Mac and reset it to factory settings [support.apple.com](https://support.apple.com)
- 180** NIST SP 800-88 Rev. 2: Guidelines for Media Sanitization [csrc.nist.gov](https://csrc.nist.gov)
- 181** CISA: Protecting portable devices, physical security [cisa.gov](https://cisa.gov)
- 182** CISA: Securing portable electronic devices during travel (2019) [cisa.gov](https://cisa.gov)
- 183** CISA: Cybersecurity while traveling (tip card) [cisa.gov](https://cisa.gov)
- 184** NIST SP 800-114 Rev. 1: User's guide to telework and bring your own device security [doi.org](https://doi.org)
- 185** FBI: Business travel brochure [fbi.gov](https://fbi.gov)
- 186** US National Counterintelligence and Security Center: Travel security guidance (October 2024) [dni.gov](https://dni.gov)
- 187** UK NPSA: Secure Innovation travel security guidance [npsa.gov.uk](https://npsa.gov.uk)
- 188** Australian Signals Directorate: Travelling with mobile devices [cyber.gov.au](https://cyber.gov.au)
- 189** Australian Signals Directorate: PROTECT, travelling overseas with electronic devices (October 2021). Further reading [cyber.gov.au](https://cyber.gov.au)
- 190** Australian Signals Directorate: Personal cyber security handbook, travelling overseas [cyber.gov.au](https://cyber.gov.au)
- 191** FCC: Juice jacking, tips to avoid it [fcc.gov](https://fcc.gov)
- 192** [business.gov.uk](https://business.gov.uk): Protect your data abroad [business.gov.uk](https://business.gov.uk)
- 193** NSA: Best practices for securing your home network (2023). Further reading [media.defense.gov](https://media.defense.gov)
- 194** NSA: Best practices for keeping your home network secure (transcript) [nsa.gov](https://nsa.gov)
- 195** US CBP: Border search of electronic devices [cbp.gov](https://cbp.gov)
- 196** US CBP: Border search of electronics at ports of entry, FY2025 statistics [cbp.gov](https://cbp.gov)
- 197** UC Berkeley Information Security Office: Preventing laptop theft [security.berkeley.edu](https://security.berkeley.edu)
- 198** Harvard University Police Department: Laptop theft prevention [hupd.harvard.edu](https://hupd.harvard.edu)
- 199** VCU Police: Computer registration [police.vcu.edu](https://police.vcu.edu)
- 200** University of Exeter: Cyber security when travelling. Further reading [exeter.ac.uk](https://exeter.ac.uk)
- 201** StarTech.com: 14 inch laptop privacy screen datasheet [media.startech.com](https://media.startech.com)
- 202** Society for Information Display: SID Symposium Digest, volume 64, issue 1 [sid.org](https://sid.org)
- 203** HP: HP Sure View white paper [ftp.hp.com](https://ftp.hp.com)
- 204** NCSC: Install the latest software and app updates [ncsc.gov.uk](https://ncsc.gov.uk)
- 205** Microsoft: Stay protected with the Windows Security app [support.microsoft.com](https://support.microsoft.com)
- 206** Apple: Use a firewall on Mac [support.apple.com](https://support.apple.com)

# Image credits

---

All diagrams, the cover art and the chapter openers are by TechCortado. All rights reserved. Some diagram text was simplified for the book.

Third-party images remain under their own licences, shown with each photo below. The book licence does not change their terms.

- **A combination cable lock in use.** Photo by Santeri Viinamäki, [CC BY-SA 4.0](#), from Wikimedia Commons: [Laptop Kensington lock.jpg](#). Resized and recompressed.
- **A standard security slot on a thin laptop.** Photo by Bobulous, [CC BY-SA 4.0](#), from Wikimedia Commons: [Kensington lock slot on an Acer Swift 3 laptop.jpg](#). Resized and recompressed.
- **A coiled cable lock.** Photo by Fastily, [CC BY-SA 4.0](#), from Wikimedia Commons: [Kensington Laptop Lock 1 2019-05-06.jpg](#). Resized and recompressed.
- **Tape over a webcam.** Photo by Santeri Viinamäki, [CC BY-SA 4.0](#), from Wikimedia Commons: [Tape over laptop webcam.jpg](#). Resized and recompressed.
- **A tracking tag.** Photo by ajay\_suresh, [CC BY 2.0](#), from Wikimedia Commons: [Apple AirTag \(51334123725\).jpg](#). Resized and recompressed.

Fonts: Literata, Inter Tight and IBM Plex Mono, used under the SIL Open Font License 1.1.

# Index

---

## A

Account recovery [12](#), [14](#), [15](#), [41](#), [44](#), [74](#), [75](#), [115](#), [123](#)

Adhesive adapter [24](#), [26](#), [32](#), [128](#)

Admin account [64](#), [79](#)

Airports [95](#), [101](#), [102](#), [104](#)

Anchor, desk [12](#), [24](#), [30](#), [33](#), [34](#), [113](#), [115](#), [122](#), [126](#)

Auto-join [94](#), [96](#), [98](#), [121](#), [123](#)

## B

Backup [12](#), [13](#), [15](#), [22](#), [29](#), [33](#), [41](#), [43](#), [45](#), [67](#), [68](#), [69](#)

Backup, offsite [67](#), [68](#), [115](#)

Biometrics [47](#)

Bluetooth [57](#), [77](#), [78](#), [94](#), [97](#), [98](#), [121](#), [123](#)

Border searches [100](#), [103](#), [105](#), [121](#)

## C

Cable lock [15](#), [24](#), [30](#)

Campus registration [16](#), [84](#), [97](#), [119](#)

Canary token [58](#), [87](#), [123](#), [132](#)

Charging, public USB [94](#), [96](#)

Combination lock [28](#), [29](#)

## D

Decoy [58](#), [82](#), [87](#), [88](#), [89](#), [91](#), [123](#)

Device record [84](#), [119](#)

Dynamic Lock [57](#), [116](#), [123](#)

## E

Emergency kit [63](#), [65](#), [74](#), [120](#), [123](#), [130](#)

Encryption, full-disk [14](#), [37](#), [38](#), [40](#), [42](#), [52](#), [89](#), [103](#), [120](#)

Evil maid [52](#)

## F

Finding service [41](#), [78](#), [80](#), [87](#), [89](#), [111](#), [115](#), [116](#), [130](#), [131](#)

Firewall [57](#), [63](#), [96](#), [123](#)

Firmware password [50](#), [51](#), [52](#), [53](#), [55](#), [116](#), [120](#), [122](#)

## G

Glitter seal [53](#)

## H

Hibernation [38](#), [40](#), [42](#), [43](#)

Hotel safe [100](#), [102](#)

Hotels [15](#), [19](#), [21](#), [47](#), [50](#), [53](#), [96](#), [100](#), [102](#), [104](#), [120](#)

## I

Insurance [10](#), [15](#), [32](#), [101](#), [105](#), [107](#), [109](#), [111](#), [114](#), [119](#), [121](#)

## K

Keyed lock [24](#), [28](#), [122](#), [126](#)

## L

Locking station [15](#), [24](#), [26](#), [33](#), [116](#), [128](#)

## M

MAC address [84](#), [119](#)

Marking, UV and forensic [21](#), [59](#), [82](#), [119](#), [123](#), [129](#), [132](#)

## N

Nano slot [26](#), [126](#)

## P

Passkey [63](#), [123](#)

Password manager [44](#), [51](#), [55](#), [62](#), [63](#), [65](#), [68](#), [73](#), [101](#), [109](#), [114](#)

Police report [16](#), [109](#), [122](#)

Power states [39](#)

Privacy screen [57](#), [58](#), [65](#), [94](#), [102](#), [116](#), [121](#), [123](#), [129](#)

Public Wi-Fi [94](#), [95](#), [98](#), [102](#), [123](#)

**R**

Recovery key **37, 39, 41, 42, 44, 45, 47, 53, 68, 116, 120, 122**

Remote wipe **14, 41, 80, 82, 109**

**S**

Second factor **29, 44, 57, 62, 73, 116, 123**

Secure Boot **40, 42, 50, 51, 52, 53, 55, 89, 122**

Security key **57, 63, 65, 73, 120, 123**

Selling a laptop **16, 80, 107, 111, 123**

Serial number **14, 16, 19, 21, 22, 77, 84, 97, 101, 105, 109**

Shared laptops **57, 64, 116, 121**

Shoulder surfing **57, 58, 127**

Sleep mode **38, 47, 50, 52, 101, 103, 105, 114, 120**

Slot types **26, 127**

Standard account **64, 87, 91, 92, 123**

Startup PIN **37, 39, 40, 42, 45, 47, 52, 87, 89, 115, 121**

**T**

Tamper-evident seal **50, 51, 53, 54, 79, 103, 110, 122**

Thunderbolt **40, 52, 55**

TPM **39, 40, 42, 45, 53, 89, 91**

Tracking tag **12, 77, 79, 83, 85, 107, 108, 115, 119, 130**

Trains **8, 16, 19, 20, 58, 74, 94, 97, 102, 116, 120, 123**

**U**

Updates **14, 40, 53, 57, 63, 65, 75, 79, 80, 91, 92, 100**

USB stick, found **52, 87, 89, 91, 92, 94, 96**

**V**

VPN **89, 95, 123**

**W**

Webcam cover **60, 82**

Wedge slot **26, 31, 126**

# Follow TechCortado

---

The easiest way to hear from us is our own newsletter. We send it from TechCortado.com, and you can unsubscribe with one click.

**Get the TechCortado newsletter**

Website: [TechCortado.com](https://TechCortado.com)

The full online guide: [Laptop security: locks, encryption and backups](#)  
Power bank calculator: [TechCortado.com/tools/power-bank-calculator](https://TechCortado.com/tools/power-bank-calculator)

## Social and reading

|           |                                                                                |
|-----------|--------------------------------------------------------------------------------|
| Bluesky   | <a href="https://techcortado.bsky.social">@techcortado.bsky.social</a>         |
| Mastodon  | <a href="https://techcortado@mastodon.world">@techcortado@mastodon.world</a>   |
| Pixelfed  | <a href="https://techcortado@pixelfed.social">@techcortado@pixelfed.social</a> |
| Tumblr    | <a href="https://techcortado.tumblr.com">techcortado.tumblr.com</a>            |
| Substack  | <a href="https://techcortado.substack.com">techcortado.substack.com</a>        |
| Medium    | <a href="https://medium.com/@techcortadohq">medium.com/@techcortadohq</a>      |
| Pinterest | <a href="https://pinterest.com/techcortado">pinterest.com/techcortado</a>      |
| Flipboard | <a href="https://flipboard.com/@TechCortado">flipboard.com/@TechCortado</a>    |
| Sharkey   | <a href="https://techcortado@sharkey.world">@techcortado@sharkey.world</a>     |
| Misskey   | <a href="https://techcortado@misskey.gg">@techcortado@misskey.gg</a>           |

Spotted a mistake or something out of date? Tell us through any of these accounts and we will fix it in the next edition.



**TechCortado**

# A laptop can be replaced. A week of your life is harder.

Most laptop thefts are quick and ordinary: a café table, a train seat, a car, a hotel room. This short handbook shows how to make the grab harder, keep a stolen machine from becoming a stolen life, and be back at work the next day.

- Locks that fit, and what they can and can't do
- Encryption, sleep and the startup PIN, in plain words
- Backups and account recovery you can restore without the laptop
- Privacy screens, public Wi-Fi and charging on the move
- Travel, hotels and borders, using official public guidance
- What to do in the first hour after a theft

**Newsletter · Bluesky · Mastodon · Pixelfed · Full online guide**

General information only, not legal or professional security advice. No guarantee; use at your own risk. Follow local law and official guidance. Product mentions are examples, not endorsements, with no affiliate links or sponsorship. Current as of October 2026, edition 1.