
FROM THE MEHRUTHERM BLOG · CYBERSECURITY

A Laptop Left the Building. So Did Everything On It.

A missing laptop or phone doesn't have to become a lost week, or a breach. Here's how to make sure the one that goes astray is just hardware to replace, not a crisis.

October 5, 2026

You set the laptop on the roof of the truck for a second, loaded the last box, and drove off. Or it was in a bag on the passenger seat when the window got smashed in a parking lot. Or a phone slipped out of a pocket at the diner, and by the time you went back it was gone. However it happens, the first feeling is the same: a small, cold drop in the stomach.

The cost of the hardware is the part you will forget about fastest. A laptop or a phone is a few hundred dollars and an afternoon to replace. The real question, the one that decides whether this is an annoyance or a genuine problem, is simpler and scarier: what was on it, and can whoever has it now get in?

That answer is almost entirely decided before the device ever goes missing. A device that was set up properly is just a piece of hardware to replace. A device that was not can hand a stranger your email, your customer records, your saved passwords, and a way into everything those unlock. This is about making sure the one that walks off is the first kind.

The device is cheap. What's on it is not.

Think about what a single work laptop actually touches. It is usually signed into email, which is the master key to almost everything else, because most other accounts can be reset through it. It often has customer information, quotes, invoices, and files sitting right there. The web browser quietly remembers passwords to sites someone signed into months ago. For a town office, it may hold resident records and a way into the systems the office runs on.

Hardware is replaceable in a day. The trust of the people whose information was on that device is not. For a business or a town that handles sensitive records, a device in the wrong hands can become a reportable

breach with real consequences. That is the gap worth closing, and the good news is that closing it is mostly a one-time setup.

The difference is everything you do first

There is very little you can do in the moment a device goes missing that you did not already make possible beforehand. So the work is front-loaded. A handful of settings, put in place once, turn a lost device from a crisis into a shrug. None of them are complicated, and most are already built into the computers and phones you own. They just have to be switched on and set up correctly, which is exactly the sort of quiet, unglamorous groundwork that comes with having someone look after your equipment instead of leaving each machine to fend for itself.

A lock that actually stops someone

Start with the obvious one that is often half-done: the device should require a real sign-in to get past the lock screen, and it should lock itself quickly when left idle. A laptop that boots straight to the desktop, or a phone with no passcode, offers no resistance at all.

Just as important, and far less common, is encryption. In plain terms, encryption scrambles everything stored on the device so it is unreadable without the sign-in. Without it, a thief can pull the drive out and read your files on another machine, lock screen and all. With it, the hardware is a brick to anyone who does not have the sign-in. Encryption is built into modern business computers and phones at no extra cost. It simply needs to be turned on, which many devices do not do on their own.

So it can be found, locked, or wiped from afar

Modern devices can be located, locked, or completely erased from somewhere else, as long as that was set up ahead of time. A laptop left at a truck stop can be locked the moment you notice it is gone. A phone that is clearly lost for good can be wiped clean from a web browser back at the office, so whatever was on it goes with it.

When your devices are looked after as a group rather than one at a time, this becomes something that can be handled quickly, across every device your business or office owns, rather than something each person has to have remembered to set up alone. It is one of the clearest everyday payoffs of having your equipment managed, the same kind of before-it-breaks thinking behind [managed IT](#) generally.

So a lost device never means lost work

There is a second kind of loss hiding inside the first: the only copy of something important leaving with the device. Erasing a stolen laptop is a relief only if the work that was on it still exists somewhere else.

That is what reliable, tested backups are for. When the files a device holds are also saved somewhere safe and automatic, wiping the lost one costs you nothing but the hardware. We wrote about why a backup nobody has ever tested is not really a backup in [if you've never tested your backup, you don't have one](#).

The first hour, if one does go missing

Preparation decides most of the outcome, but the first hour still matters. Lock or erase the device remotely as soon as you are sure it is gone. Change the password on your email first, since it is the key to the rest, and turn on a second step to sign in if it is not already on, so a saved password by itself is not enough to get in. Then work outward to anything else that was signed in on the device.

If your passwords live in [one secured place](#) instead of saved in the browser on that laptop, this part is far faster and far less frightening. And tell whoever looks after your technology right away, because the sooner someone is tracing what that device could reach, the smaller the whole thing stays.

A device that wasn't ready

- × Boots straight in, or a passcode anyone could guess
- × Files readable by pulling the drive out
- × No way to lock or erase it from a distance
- × The only copy of some work was on it
- × Saved passwords hand over every other account

A device that was ready

- ✓ A real sign-in that locks itself when idle
- ✓ Everything on it encrypted and useless without that sign-in
- ✓ Can be located, locked, or wiped from afar in minutes
- ✓ Nothing lost, because the work is backed up elsewhere
- ✓ Passwords kept in one secured place, not the browser

KEY TAKEAWAYS

- A lost or stolen device is only as dangerous as what it can unlock. The hardware is the cheap part.
- Almost all of the protection is set up once, before anything goes missing.
- The essentials: a real sign-in that locks quickly, encryption turned on, and the ability to lock or wipe the device from afar.
- Tested backups mean erasing a lost device costs you the hardware and nothing more.
- If one does go missing, lock or wipe it, change your email password and turn on a second sign-in step, and tell whoever handles your technology right away.

A missing device is one of those risks that feels like pure bad luck in the moment, and is almost entirely a matter of preparation in hindsight. The businesses and towns that shrug it off are not luckier than the ones it wrecks. They just did the quiet setup first, back when nothing was wrong.

MEHRUTHERM · CRESTON, WA

Want to know what would happen if one of your laptops or phones went missing today? Get in touch and we'll look at how your devices are set up, and make sure a lost one is only ever a trip to the store, not a bad week.

mehrutherm.com/quote