LESSON 03 OF 05 · 7 MIN · ESSENTIAL

Updates, devices and the long tail

Most attacks use flaws that already have a fix. Here's how to make patching automatic and cover the devices everyone forgets.

The flaw is usually known

A patch is a software update that fixes a security flaw. When a fix is published, the details eventually become public, and attackers start scanning for machines that haven't applied it. An unpatched device isn't just old; it's a known way in.

This is good news. You don't need to predict the next attack. You need to apply the fixes that already exist, consistently.

Put the obvious things on autopilot

- **Windows and macOS:** automatic updates on, restarts outside working hours.
- **Browsers:** update automatically and restart weekly. An update that never restarts isn't applied.
- **Office and PDF apps:** usually handled by the platform; check.
- **Phones:** automatic OS and app updates.
- **Business apps:** accounting, payroll, booking, design tools, remote access.
- **Router and firewall firmware:** the device everyone forgets.

Retire what can't be fixed

A laptop that can't run a supported operating system will not receive security fixes. Keeping it on the network because it “still works” is a choice to accept risk. Either replace it, isolate it from business data, or accept it in writing with a plan to replace it.

Do a ten-minute monthly check: pending updates, expired protection licences, devices that haven't reported in, and anything that has reached end-of-life.

> **THE TEN-MINUTE HABIT**
>
> Once a month, open each platform's update or security dashboard. Look for devices with updates pending for more than a week. Restart them. That single habit closes more holes than most security products.

Key takeaways

- ✓ Most successful attacks exploit vulnerabilities that already have a fix.
- ✓ Automatic updates plus a weekly browser restart do most of the work.
- ✓ Include phones, routers and remote-access tools.
- ✓ Replace or isolate devices that no longer receive fixes.