CICADA | RESOURCES

DEVICES | 45 MIN | ESSENTIAL | UPDATED NOVEMBER 2026

A patch routine that actually happens

Set updates to automatic, cover the software people forget, and replace devices that no longer get fixes.

The short version

- ✓ Most attacks use vulnerabilities that already have a fix.
- ✓ Turn on automatic updates for the OS, browser and office apps.
- ✓ Include phones, routers and remote-access software.
- ✓ Retire devices that no longer receive security updates.

What to update

- **Operating systems:** Windows, macOS, iOS, Android.
- **Browsers:** Chrome, Edge, Safari, Firefox, often the most exposed software.
- **Office apps:** Microsoft 365, Google Drive, PDF readers.
- **Business software:** accounting, payroll, booking, design and remote-access tools.
- **Network gear:** router and firewall firmware.
- **Security software:** endpoint protection and any management agent.

Make it automatic

Windows: Settings → Windows Update → keep updates on, set active hours and restart outside working time. macOS: System Settings → General → Software Update → automatic updates. Phones: enable automatic app and OS updates. Browsers: restart them at least weekly. An update that never restarts isn't applied.

For line-of-business apps, check whether they update themselves. If not, put a monthly calendar reminder on the person who owns them.

The monthly ten-minute check

01 Open the security or update dashboard for each platform.

02 Look for devices with updates pending for more than seven days.

03 Check that endpoint protection is active and reporting.

04 Look for apps and devices that have reached end-of-life.

05 Restart anything that has been waiting; confirm the version changed.

> **END-OF-LIFE KIT**
>
> A laptop that can't run a supported OS is not secure, however well it still works. Budget to replace it, or isolate it from business data.

Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.

Action checklist

- [ ] Automatic updates enabled on every work device
- [ ] Browsers restart at least weekly
- [ ] Phones included in the routine
- [ ] Router and firewall firmware checked
- [ ] Monthly dashboard review scheduled
- [ ] No end-of-life devices holding business data

0 of 6 done