INFOSTEALERS AND FAKE POP-UPS · CHECKLIST

5 Protect the devices that run your site

From the lesson: Your laptop is part of your website

Do this on every computer and phone that logs in to your website, email or hosting.

THE PATTERN

- Fake downloads, cracked apps, extensions and fake updates install infostealers.
- They copy saved passwords and logged-in sessions in seconds.
- A stolen live session can skip two-step login altogether.

HOW TO SPOT IT

- A "verify you're human" box asking you to press keys or paste something.
- Browser extensions you don't remember adding.
- Antivirus or Windows Security turned off, or warnings ignored.
- Logins to your accounts from places you've never been.

TICK AS YOU GO

- [ ] **Automatic updates on**
  Windows: Settings, then Windows Update. Mac: System Settings, then General, then Software Update. Phones: turn on automatic updates.
- [ ] **Built-in protection on**
  Windows Security (Virus and threat protection) or the Mac's built-in protection, switched on and current.
- [ ] **Passwords out of the browser**
  Move saved passwords into a password manager, then clear them from the browser.
- [ ] **Tidy your browser extensions**
  Remove any you don't use or don't recognise. Fewer extensions, fewer risks.
- [ ] **A separate business browser profile**
  Chrome, Edge and Firefox all let you add a profile. Use it only for business admin.
- [ ] **Log out of admin areas**
  Website, hosting and domain accounts, when you've finished.
- [ ] **Lock your phone**
  A PIN or face unlock. Your phone holds your email, and your email can reset everything.

REMEMBER If a website asks you to press keys or paste something to prove you're human, close it. Real sites never do.

1.7 billion logins stolen by infostealer malware in the first half of 2026 (Flashpoint).

hedgehog.site · © 2026 Hedgehog Site Limited