Hedgehog

FREE COURSE WORKBOOK · 2026



Spot it. Stop it.

A free 7-part course on how website attacks really work, how to spot them, and the easy wins that stop them. All seven checklists in one place.

1	You're not a target. You're a match.	HOW ATTACKS FIND YOU
2	The front door: how passwords really get stolen	LOGINS AND PASSWORDS
3	The side doors: plugins, add-ons and old software	SOFTWARE HOLES
4	The email trick: scams that look real	PHISHING AND FAKE INVOICES
5	Your laptop is part of your website	INFOSTEALERS AND FAKE POP-UPS
6	The keys: your domain, your email and your backups	DOMAIN AND RECOVERY
7	Spot the signs, and the door that isn't there	DETECTION, RESPONSE AND PREVENTION

HOW ATTACKS FIND YOU · CHECKLIST

1 Make your site a bad match

From the lesson: You're not a target. You're a match.

Five easy steps. No tech skills needed.

THE PATTERN

- Robots scan millions of sites a day, looking for a match, not a name.
- They check three things: an old door, a lock to pick, a person to trick.
- When a site doesn't match, they move on. Small changes make you a bad match.

HOW TO SPOT IT

- You don't know what software or add-ons your site runs.
- Nobody would be told if Google found a problem on your site.
- Your site hasn't been looked at in months.

TICK AS YOU GO

- [ ] **Add your site to Google Search Console**
  search.google.com/search-console, then Add property. Pick the Domain option if your web person can add the record, or URL prefix if not.
- [ ] **Search Google for your own site**
  Type site:yourwebsite.com into Google. Look for pages you didn't write, in odd languages or selling pills, bags or betting.
- [ ] **Write down what your site runs on**
  WordPress, Wix, Squarespace, Shopify or something else. Not sure? Ask whoever built it, or take our quiz.
- [ ] **Find out who looks after it**
  You, a staff member, an agency, a freelancer or nobody. Write their name and how to reach them.
- [ ] **Take the 3-minute safety quiz**
  hedgehog.site/quiz gives you a score for each risk area and tips that fit your platform.

REMEMBER Robots don't choose you. They match you. Shut the doors they look for and they move on.

200 million password-guessing attempts a day on WordPress sites protected by one firm alone (Wordfence, Q2 2026).

hedgehog.site · © 2026 Hedgehog Site Limited

LOGINS AND PASSWORDS · CHECKLIST

2 Lock the front door

From the lesson: The front door: how passwords really get stolen

Start at the top. Email first, because it can reset every other password.

THE PATTERN

- Robots guess common passwords on public login pages.
- Leaked passwords from other sites get tried on yours (re-use).
- Malware copies saved passwords from your browser (lesson 5).

HOW TO SPOT IT

- "New sign-in" or "password changed" emails you didn't expect.
- Reset codes arriving by text or email that you didn't ask for.
- An admin user on your website you don't recognise.
- Being logged out of an account for no reason.

TICK AS YOU GO

- [ ] **Two-step login on your email**
  Gmail and Google Workspace: myaccount.google.com/security. Outlook and Microsoft 365: account.microsoft.com/security.
- [ ] **Two-step login on your domain account**
  Wherever you bought your web address: GoDaddy, Namecheap, Crazy Domains, 123 Reg and so on. Look under Account, then Security.
- [ ] **Two-step login on your hosting and website**
  Wix, Squarespace and Shopify have it in account settings. WordPress needs a two-step plugin or your host's login protection.
- [ ] **Use an authenticator app where you can**
  Google Authenticator, Microsoft Authenticator or your password manager. Codes by text message are better than nothing.
- [ ] **Set up a password manager**
  Apple Passwords, Google Password Manager, 1Password or Bitwarden. Let it create a new password for each account.
- [ ] **Change any password you've used twice**
  Start with email, domain, hosting and website. Your password manager can show you re-used ones.
- [ ] **Check who can log in to your website**
  Remove past staff, old agencies and anyone you don't recognise. Give everyone else the lowest access that works.

REMEMBER

If an unexpected login email arrives, don't click its link. Go to the account yourself and check.

99%+ reduction in account takeover risk with two-step login switched on (Microsoft Research).

hedgehog.site · © 2026 Hedgehog Site Limited

SOFTWARE HOLES · CHECKLIST

3 Close the side doors

From the lesson: The side doors: plugins, add-ons and old software

Works for WordPress, Joomla and Drupal. Builder users: see the last two items.

THE PATTERN

- Each plugin, theme or app is someone else's code, and a possible door.
- Once a hole is public, robots try it within hours.
- Abandoned, "free paid" (nulled) and recently sold plugins are the riskiest.

HOW TO SPOT IT

- "Update available" badges that have sat there for weeks.
- Plugins or apps you don't remember adding.
- A plugin that hasn't been updated by its maker in over a year.
- A plugin that changed owner or name recently.

TICK AS YOU GO

- [ ] **List every plugin and theme**
  WordPress: Plugins, then Installed Plugins, and Appearance, then Themes. Write down the count.
- [ ] **Delete what you don't use**
  Deactivate, then Delete. Keep one spare default theme and delete the rest.
- [ ] **Replace anything abandoned**
  If a plugin page says it hasn't been updated in over a year, or it was closed, look for an alternative.
- [ ] **Remove any "free" copies of paid plugins**
  If you didn't buy it from the maker, assume it's unsafe. Replace it with the genuine version.
- [ ] **Turn on automatic updates**
  WordPress: Enable auto-updates on each plugin and theme. Ask your host to keep the PHP version current too.
- [ ] **Builders: review connected apps**
  Wix: Apps. Squarespace: Extensions. Shopify: Apps. Remove anything you don't use.
- [ ] **Builders: check pasted code**
  Look in custom code, header or embed settings for tracking or widget code you no longer need.

REMEMBER Every add-on is a door. The safest door is one you've removed.

11,334 new security holes found in WordPress add-ons and themes in 2025, up 42% (Patchstack).

hedgehog.site · © 2026 Hedgehog Site Limited

PHISHING AND FAKE INVOICES · CHECKLIST

4 Spot the email trick

From the lesson: The email trick: scams that look real

Keep this by your desk. Share it with anyone who opens the business email.

THE PATTERN

- Hurry: a deadline, a final notice, a threat.
- Someone official: Google, your bank, your host, a supplier.
- An action: click, open, log in or pay. All three together means stop.

HOW TO SPOT IT

- Domain renewal or "suspension" notices from companies you don't use.
- Links whose real address (hover or long-press) doesn't match the sender.
- A supplier asking to pay a new bank account.
- A login page that asks for your password after you clicked an email.

TICK AS YOU GO

- [ ] **Learn the pattern: Hurry + Official + Action**
  When an email has all three, don't click anything. Check the account yourself.
- [ ] **Bookmark your real logins**
  Domain, hosting, website, email, bank, Google Business Profile. Use the bookmarks, never email links.
- [ ] **Set a bank-details rule**
  Any change to payment details is confirmed by phone on a number you already have. Tell your team and your bookkeeper.
- [ ] **Check a link before you tap it**
  On a computer, hover over it. On a phone, press and hold. If the address doesn't match the sender, delete the email.
- [ ] **Ask for SPF, DKIM and DMARC**
  Send your email or web provider this line: "Please set up SPF, DKIM and DMARC for our domain."
- [ ] **Know your real renewal dates**
  Write down when your domain and hosting really renew, and who with. Fake renewal notices then stand out.

REMEMBER

If an email is urgent, official and wants an action, go to the account yourself. Real problems will be there too.

56% of phishing emails were written by AI in December 2025, up from under 5% (Hoxhunt).

hedgehog.site · © 2026 Hedgehog Site Limited

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

DOMAIN AND RECOVERY · CHECKLIST

6 Hold your own keys

From the lesson: The keys: your domain, your email and your backups

Mostly about knowing where things are. Once it's done, it's done.

THE PATTERN

- Whoever controls your domain controls your website and email.
- Most lost domains aren't hacked. They expire, or sit in someone else's name.
- Backups on the same hosting can be lost along with the site.

HOW TO SPOT IT

- You don't know which company your domain is registered with.
- Renewal emails go to an old address, or a past designer.
- Auto-renew is off, or the card on file has expired.
- Your only backup lives on your web hosting.

TICK AS YOU GO

- [ ] **Find your domain registrar**
  Free lookup: lookup.icann.org. Type your web address and note the registrar name.
- [ ] **Check the domain is in your name**
  Log in to the registrar. The owner (registrant) should be you or your business, not a past designer.
- [ ] **Update the contact email**
  Use an address you read every day, not an old one or someone else's.
- [ ] **Auto-renew on, card up to date**
  And check the expiry date. Renew for a few years if you can.
- [ ] **Domain lock and two-step login on**
  Domain lock (also called transfer lock) stops it being moved without you.
- [ ] **Keep a copy of your site elsewhere**
  Text, photos and files, saved to your computer or cloud drive. WordPress: a backup plugin that stores off-site.
- [ ] **Write your key list**
  Where every login lives: domain, hosting, website, email, Google Business Profile, social. Keep it in your password manager.

REMEMBER **Whoever holds your domain holds your website and email. Make sure it's you.**

67 countries where Weebly began taking sites offline in September 2026 (Khaleej Times).

hedgehog.site · © 2026 Hedgehog Site Limited

DETECTION, RESPONSE AND PREVENTION · CHECKLIST

7 Spot the signs, and your first hour

From the lesson: Spot the signs, and the door that isn't there

Check the signs once a month. Keep the first-hour plan somewhere you'll find it.

IF YOU'VE BEEN HACKED: YOUR FIRST HOUR

1. Don't panic, and don't delete anything yet.
2. From a clean device, change passwords: email first, then domain, hosting, website.
3. Call your host. Ask for a holding page if visitors are at risk.
4. Get it cleaned properly, including backdoors and hidden admin users.
5. Ask Google for a review in Search Console once it's clean.
6. Check legal duties if customer details were exposed, and tell your insurer.
7. Report it: IC3 (US), the police fraud reporting service (UK), Canadian Anti-Fraud Centre, ReportCyber (AU), Own Your Online (NZ).

HOW TO SPOT IT

- Pages you didn't write in a site: search on Google.
- Customers saying they were sent somewhere else.
- Emails to customers landing in junk.
- A red warning in Google or the browser.

TICK AS YOU GO

- [ ] **Monthly: search for your own site**
  Type site:yourwebsite.com into Google. Look for pages you didn't write.
- [ ] **Monthly: check Search Console**
  Look under Security and Manual actions. Both should say no issues.
- [ ] **Monthly: check who has admin access**
  Remove anyone you don't recognise or who no longer needs it.
- [ ] **Ask a customer to test your site on their phone**
  Redirects often only show on phones coming from Google.
- [ ] **Save your first-hour contacts**
  Your host, your web person, your bank and your insurer, with phone numbers.
- [ ] **Check your insurance**
  Ask your broker if cyber incidents are covered, and what steps they expect you to have taken.
- [ ] **Consider taking the doors away**
  A static site has no plugins, database or login page to attack. Ask us for a free preview.

REMEMBER

If it happens: don't delete anything, change passwords from a clean device (email first), call your host, and get it cleaned properly.

A$56,600 average cost per cybercrime report for an Australian small business (Australian Signals Directorate).

hedgehog.site · © 2026 Hedgehog Site Limited

SOURCES

Where the numbers come from

1. Wordfence, Quarterly WordPress Threat Intelligence Report, Q2 2026: 18.2bn brute-force attempts blocked.
2. Microsoft Research, How effective is multifactor authentication at deterring cyberattacks?: 99.22% risk reduction.
3. UK DSIT, Cyber Security Breaches Survey 2025/2026: 43% of micro businesses require two-factor authentication.
4. Verizon, 2026 Data Breach Investigations Report: exploitation of software flaws 31% of initial access, ahead of credentials.
5. Patchstack, State of WordPress Security in 2026: 11,334 new vulnerabilities (+42%), 91% in plugins.
6. TechRepublic, Malicious WordPress plugins with backdoors (April 2026): 31 plugins backdoored after a sale.
7. Hoxhunt, Phishing Trends Report 2026: AI-written phishing 56% in December 2025.
8. Flashpoint, Global Threat Intelligence Report, midyear 2026: 7.4m infected devices, 1.7bn stolen logins.
9. Khaleej Times, Weebly websites to shut down in 67 countries (September 2026).
10. Sucuri, SiteCheck 2024 Threat Report: SEO spam 38.4% of infections.
11. Australian Signals Directorate, Annual Cyber Threat Report 2024-25: A$56,600 average small business cost per report.

Researched November 2026. Full references are in our free guide, "Is your website safe?". This workbook is general information, not legal or professional advice. You're welcome to share it unchanged.

NEXT STEP

The safest door is the one that isn't there. Hedgehog moves your existing site onto secure static hosting with no plugins, database or login page, and you change it by text or voice note. Get a free preview at hedgehog.site.