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