Emergency Security Checklist for WooCommerce Store Owners

Print it. Save it. Tape it to your wall.

Use this checklist as your go-to reference to stay protected against AnonymousFox-style attacks and other common WooCommerce security threats.

🗓️ Daily Tasks

- ☐ Monitor site activity (logins, file changes, orders anomalies)
- ☐ Check email deliverability + no bounce alerts
- ☐ Review failed login attempts
- ☐ Log out unused admin sessions

📆 Weekly Tasks

- ☐ Backup full site + database (offsite, encrypted)
- ☐ Review installed plugins & themes for updates
- ☐ Scan site with Wordfence, MalCare, or similar
- ☐ Check for unknown user accounts or admin changes

🗓️ Monthly Tasks

- ☐ Test backups for integrity and recovery speed
- ☐ Audit cPanel & FTP credentials + update passwords
- ☐ Review file permissions (644/755 rule)
- ☐ Revoke access from former developers/team members

🚨 Signs You May Be Hacked

- ☐ Admin email or password changed without permission
- ☐ Unknown admin accounts appear (e.g. anonymousfox_1)
- ☐ Suspicious files like shell.php or data.php found
- ☐ Customers report password reset or phishing emails
- ☐ Emails stop sending or are flagged as spam

🧯 In Case of Emergency

- ☐ Change all passwords: WordPress, cPanel, FTP, email
- ☐ Disconnect site temporarily or set maintenance mode
- ☐ Contact your hosting provider security team
- ☐ Get professional help: https://w3-lab.com/ecommerce-maintenance/