Fast Lane

Cybersecurity Core 4: Practice What Protects

A skills-first playbook to stop most breaches before they start, close the right gaps, outsmart phishing, and use AI with intent.

Fast Lane

Your Next Right Moves

By performing this checklist monthly during stand-ups or at the beginning of each sprint, and re-evaluating after significant changes, audits, or incidents, teams can turn good intentions into consistent, dependable habits that enhance overall security.

Passwords and MFA

- [ ] Phishing-resistant MFA is enabled for admins, finance, HR, VPN, and email; SMS/email OTP is disabled for high-risk use.
- [ ] Passkeys or FIDO2 security keys are rolled out for priority apps; device biometrics are enforced where supported.
- [ ] Unique credentials per system; access auto-revoked on role change; no untracked shared accounts remain.
- [ ] Centralized SSO with conditional access; step-up authentication on sensitive actionsor risky context.
- [ ] Approved password manager in use; secrets not stored in browsers or shared

Patch with Purpose

- [ ] Asset inventory is current, including internet-facing systems, versions, and owners; patch SLAs tie to severity and exploitability.
- [ ] Auto-update is enabled for OS, browsers, and critical apps; firmware and drivers included in the cadence.
- [ ] Patch validation is routine: vulnerability scans plus spot checks; exceptions have compensating controls and expiry.
- [ ] Change windows exist for fast-track criticals; rollback plans are documented and tested quarterly.

Phishing Awareness

- [ ] One-click "Report Phish" is live in mail and chat; reporting rates are tracked and celebrated to reinforce the habit.
- [ ] Verification habit is practiced: confirm requests for credentials, MFA codes, payments, or bank changes via a second channel.
- [ ] Staff can spot polished lures, lookalike domains, and MFA fatigue prompts; simulations include AI-crafted examples.
- [ ] Login discipline: do not follow links to sign in for key apps—use bookmarks or the SSO portal only.

Fast Lane

Your Next Right Moves

By performing this checklist monthly during stand-ups or at the beginning of each sprint, and re-evaluating after significant changes, audits, or incidents, teams can turn good intentions into consistent, dependable habits that enhance overall security.

AI in Security

- [ ] AI usage policy is clear on approved tools, allowed data, and red lines; no secrets or regulated data in public models.
- [ ] Detection mindset: teams know attackers use AI for personalization, voice cloning, and deepfakes; escalation paths are known.
- [ ] Human-in-the-loop: AI can triage logs and surface anomalies, but high-impact actions require analyst review.
- [ ] Training includes deepfake, voice-spoof, and vendor-invoice scenarios; tabletops cover AI-enabled incidents.

Manager's Quick Wins

- [ ] Enforce phishing-resistant MFA for admins and finance this week.
- [ ] Turn on browser auto-updates and set a 72-hour SLA for critical internet-facing patches.
- [ ] Launch the one-click phish report button and publish monthly reporting stats.
- [ ] Publish a one-page AI usage policy and remove unapproved AI tools from endpoints.

Talk to us, and discover what course fits best with your needs.

Contact Us

US CA