

AI Security Starter Kit

Protect your AI accounts in just 5 minutes a week

3 Essential AI Security Habits

■ Regular Security Checks

Review connected apps and account permissions. Remove anything you no longer use.

■ Turn Off Model Training

Where available, stop your conversations from being used to improve future AI models.

■ Enable Two-Factor Authentication (2FA)

Add another layer of protection even if your password is compromised.

Quick Checklist

- Weekly security review
- Monthly full audit
- Remove unused apps
- Check connected devices
- Verify 2FA is enabled

Built by Sheryl Automates

Helping entrepreneurs build with AI—securely and efficiently.

Weekly AI Security Audit Prompt

Role

Act as my AI Security Auditor.

Objective

Review my current AI tool usage and help me identify any potential security or privacy risks.

- Third-party apps connected to my AI accounts that I no longer use.
- Browser extensions that have unnecessary permissions.
- AI tools that still have access to Google Drive, Dropbox, GitHub, Notion, Slack or other cloud services.
- API keys or tokens that should be rotated or revoked.
- Unused AI agents, automations or workflows.
- Whether 2FA is enabled on all important accounts.
- Devices currently signed in.
- Unusual login activity or security alerts.
- Sensitive files that remain unnecessarily accessible.
- ■ High-risk items

- ■ Medium-risk items
- ■ Everything that looks secure
- Checklist of actions to complete this week

Monthly AI Security Audit Prompt

Perform a complete monthly AI security and privacy review.
Help me verify that my AI ecosystem follows security best practices.

Account Security

- Password strength
- 2FA enabled
- Recovery methods updated
- Trusted devices

Connected Services

- Google Workspace
- Microsoft
- Dropbox
- GitHub
- Notion
- Slack
- Other connected apps
- Remove any integrations that are no longer required

API Security

- Review active API keys
- Rotate old keys
- Remove unused tokens
- Check permission scopes

AI Privacy

- Verify chat history settings
- Check model training settings (if available)
- Review shared conversations
- Remove conversations containing sensitive information if no longer needed

Automation Review

- Remove unused automations
- Review AI agents
- Check webhook permissions
- Verify external integrations

Device Security

- Review signed-in devices
- Remove unknown devices
- Check browser sessions

Return the report in this format:

- Overall Security Score (/100)
- Critical Issues
- Recommended Improvements
- Priority Actions for This Month

Monthly AI Security Scorecard

Category	Status
Account Security	■
Connected Apps	■
API Keys	■
Privacy Settings	■
AI Agents	■
Devices	■
Overall Score (/100)	_____