Here are a few minimum viable security plans from Trail of Bits for your:

1. Application
2. Corporate network
3. Personal security
4. Cryptocurrency
5. Sextortion
6. X Brand Account

Suggestions or comments? Please mark up the doc or email dan@trailofbits.com

Related and recommended guides:

- Consumer Reports Security Planner
- DNC Security Checklist
- Starting Up Security

Application security

- ❏ Turn on all optional "Security & analysis" settings on Github
- ❏ Track the versions *and* licenses of 3rd party dependencies
- ❏ Choose cryptographic right answers
- ❏ Use Semgrep and CodeQL (w/ Trail of Bits Semgrep and CodeQL queries)
- ❏ Learn and follow the recommendations in our Testing Handbook
- ❏ Scan your web/mobile app with Data Theorem Web Secure, Mobile Secure, Checks

Language-specific

Semgrep and CodeQL have largely replaced individual language scanners and linters. However, specific tools may still offer deeper analysis in certain cases:

- ❏ C++: use a newer compiler, develop and test with ASAN (annotate custom containers/allocators), scan with scan-build and cppcheck
- ❏ Electron: Electronegativity
- ❏ Go: golangci-lint, develop and test with Race Detector, test cgo code with ASAN
- ❏ PHP: SonarSource, phpstan, psalm
- ❏ Python: Ruff, pip-audit, upgrade Django, follow their deployment checklist
- ❏ React: Follow security best practices
- ❏ Ruby: Brakeman Scanner
- ❏ Rust: dylint, cargo-audit, and miri
- ❏ Solidity: slither
- ❏ TypeScript: turn on strict type checking options, npm-audit, tsec
- ❏ WordPress: WPScan (but, try not to host your own WordPress)

Cloud security

- ❏ Reconsider whether you should run infrastructure at all: use Heroku or Fly.io
- ❏ Review your cloud security posture with Prowler or Steampipe (AWS, GCP, Azure)
- ❏ AWS-specific: Cloudsplaining
- ❏ GCP-specific: gcp_scanner

Purchase a license for Burp Suite Pro, add Active Scan++ and Backslash Powered Scanner, then train your QA staff with Web Security Academy. If you need to stem the bleeding immediately, consider deploying Signal Sciences.

Appsec program management: Apiiro, Tromzo

XXX Add Vulnerability Disclosure Program (VDP) guidance:

- Disclose.io Policymaker
- NCSC Vulnerability Disclosure Toolkit
- CISA Cybersecurity Incident & Vulnerability Response Playbooks

XXX https://github.com/tldrsec/awesome-secure-defaults

G Suite

Follow the G Suite Security Checklist and check your progress on the security dashboard.

Protect your accounts

- ❏ Make 2-step verification mandatory, and disable text and phone-based verification
- ❏ Create an organizational unit for "High-Risk Users" and require Security Keys
- ❏ Create a separate admin account from your personal account
- ❏ Allow users to enroll in Advanced Protection, and *require* that admins do

Secure your email

- ❏ Enable enhanced review of email: turn on enhanced attachment scanning, the security sandbox, pre-delivery scanning, and OCR to read images
- ❏ Disallow users from automatically forwarding their email, a common technique to "backdoor" Gmail accounts and accidentally lose sensitive data
- ❏ Prevent email spoofing by enabling SPF, DKIM, and DMARC, then send logs to DMARC Digests to identify attempted spoofing

On a regular basis, review DMARC logs for misconfigured email services or spoofing attempts and strengthen the DMARC policy from report-only, to quarantine, to reject with an increasing % of email. Consider BIMI and MTA-STS for higher security email transfer.

Prevent unintentional data loss

- ❏ Require external collaborators to sign into their Google account
- ❏ Enable warnings for out-of-domain sharing
- ❏ Review the settings recommended by the Security Health dashboard
- ❏ Disable Takeout for all individuals, and for all Google services

Restrict access by 3rd-party apps

- ❏ Restrict all Google services so only trusted apps can access them
- ❏ "Trust" individual apps only as needed to restore functionality
- ❏ Educate users to save and report the "client_id" to an admin if an app breaks

Control devices that access G Suite

Use Context-Aware Access to control devices that access G Suite:

- ❏ Create an access level that requires device encryption and a minimum patch level

- ❏ Apply the access level to all Google services available
- ❏ Require device approvals to individually review new user-owned devices
- ❏ Create an exemption organizational unit or group for certain users to bypass it

Office 365

See DHS CISA Alert AA20-120A for Office 365 security recommendations. Consider also reading their Ransomware Guide since many of the affected technologies are Microsoft-specific.

IT security

Endpoint security

- ❏ Enforce minimum patch levels to access G Suite with Context-Aware Access
- ❏ Manage macOS and iOS devices with SimpleMDM or G Suite (mobile only)
- ❏ Outsource detection & response with Expel, Falcon Complete, or Red Canary

Network security

- ❏ Review your external network infrastructure with Asset Note
- ❏ Review your internal network infrastructure (if any) with Rumble Network Discovery
- ❏ Host your domain, locked, at a provider with a track record of security and 2FA

Common 3rd party services

- ❏ Slack: Require apps are approved by administrators before installation
- ❏ Github: Restrict access to third-party applications

Compliance

- ❏ Avoid overcomplicating SOC2, study up, and get tested by A-LIGN or Schellman

XXX
Microsoft Office macro blocking
PDF JavaScript blocking
Outsourced IT: NetGenius, NetworkRight

Personal security due diligence

Online Services

1. Setup 2-factor authentication (2FA) on your Google account. Use the Google Authenticator app or a U2F Security Key. Avoid the use of SMS as a second factor.
2. Run a Security Checkup on your personal Google account.
3. Setup 2FA on your Apple ID, Github, Facebook, and other online services.
4. Turn on Find My iPhone. You'll be able to recover your phone if lost or stolen, or wipe the phone remotely if you can't recover it.

Laptop

1. Change your default browser to Chrome. Install Password Alert and either uBlock or Ghostery. Ads are frequently a source of malicious content.
2. Use a unique Chrome Profile for every identity you have (work, personal, etc). Do not sign into multiple accounts simultaneously in the same browser instance.
3. Turn on full-disk encryption with FileVault and backup your keys to iCloud. If on Linux, ensure you encrypt the whole disk and not only your home directory.
4. Install BlockBlock on your Mac. It will prompt you when applications attempt to silently install themselves to run at startup.

Phone

1. Call your cell phone provider and add additional authentication to your account:
    a. Instructions for AT&T, T-Mobile, Verizon, Google Fi
    b. Background about why from Forbes, the FTC, and Krebs
2. Set an alphanumeric passcode on your iPhone. 4 and 6-digit PINs are trivial to brute force with commonly available forensic software.
3. If using Android, use *only* Google-branded devices (e.g., Pixels) running the latest major version of Android.
4. In Signal Messenger, turn on the Registration Lock. Hacked SMS can be used to impersonate you without it.

Operational Security

1. Review the FBI Elicitation Guide and be aware of the methods others may use to gather information about your company or projects.
2. Don't be Maria Butina. Familiarize yourself with public projects or clients you can reference in conversation.
3. If you notice any suspicious activity, immediately report it to an appropriate person at your company.

XXX Password managers: Use 1Password, not LastPass

Retail-grade cryptocurrency security

Device security

Use a strictly separate Chrome profile, user account, or entirely separate device (e.g., a single-purpose "Secure Access Workstation" or SAW) to access your cryptocurrency.

Use bookmarks to access online services. Do not follow links from email, Twitter, Discord, etc. Any use of social media or email should be separated from your cryptocurrency.

Use only Chrome. Visit `chrome://settings/security` and further enable:

1. *HTTPS-Only Mode*. Visit `chrome://settings/security` and, in the Advanced section, set "Always use secure connections."
2. *DOM Sanitizer*. Visit `chrome://flags#enable-experimental-web-platform-features` and enable the setting. This setting eliminates DOM-based XSS.
3. *Secure DNS*. Use DNS-over-HTTPS with Google Public DNS or Cloudflare, which are more resistant to DNS poisoning and filter malicious domains.
4. *Enhanced Safe Browsing*, which will more aggressively check websites you visit and warn you if it is not safe.

Avoid using SMS text message-based two-factor authentication. SIM swap attacks are common for cryptocurrency thefts. Add additional authentication to your cellular account.

Strongly prefer services that support hardware security keys (FIDO U2F). Purchase a YubiKey (directly from Yubico) and use it everywhere possible. If desired, the YubiKey Bio can additionally authenticate with a fingerprint.

Enroll in Google's Advanced Protection Program to limit third-party app access to your data, put stronger checks on suspicious downloads, and tighten account recovery security.

Choosing a wallet

If possible, store cryptocurrency at a reputable centralized exchange (e.g., Coinbase, Kraken, or Gemini). Their full-time security staff will protect your assets better than you can.

If you plan to use a web wallet: Install MetaMask, then immediately back up your "Secret Recovery Phrase" to a secure location (off your computer). Never share it with anyone.

If you plan to use a mobile wallet: Install Argent. Argent has innovative account recovery and transaction approval features that make it safer.

Consider exclusively using aggregators like Zapper or Zerion. These services may help reduce your exposure to scams and offer greater information about transactions.

Hardware wallets are less secure than advertised:

1. Their typically tiny screens obfuscate crucial information about transactions
2. Backdoored software or malware on your computer is still a threat
3. Pre-initialized devices and pre-selected recovery words are common attack vectors
4. Devices poorly attest to their own firmware or hardware integrity
5. Claims of security about the underlying hardware have not panned out

Using a dedicated computer with a software wallet will effectively build your own hardware wallet. If a hardware wallet is a must, consider that GRID+ wallets have a large screen to review transactions and offer simple backups to credit card-like "SafeCards."

Revoke approvals immediately after they are no longer needed. If your wallet does not include built-in support for managing approvals, consider using Revoke.cash.

If you get hacked:
https://x.com/CFInvestigators
https://x.com/NAXOLabs
https://x.com/zeroshadow_io

XXX Purchase direct from manufacturer, avoid using Amazon
XXX More about backups
XXX More about approvals
XXX What are common attacks? What are we protecting against? Let's list a few classics.
XXX Recommended due diligence for new investments:

- Identified team w/ strong corporate governance
- Security roles identified on team and audit available
- Vulnerability disclosure process described on the website
- Intuitive UX and account recovery features
- Easy tech indicators: HSTS with CAA (SSL Labs, Hardenize) and strict DMARC

XXX Things to avoid: Don't use a VPN, don't use ProtonMail, don't use Tor
https://www.bvp.com/atlas/how-to-hire-and-build-your-cybersecurity-team

Sextortion

If you know someone experiencing sextortion, nonconsensual/revenge pornography, or similar harassment, send them this list:

1. Don't comply with the blackmailer. It emboldens them to continue making demands.
2. Save evidence. Collect all the screenshots, emails, usernames, etc as meticulously as possible.
3. Report and block them on whatever platform they contact you through
    a. Using “Report” will capture the messages and send them to the company for review.
    b. Instagram: Click their profile, click the three dots above "Options", choose Report.
    c. Snap: Press and hold their name, tap the three dots on the top right, tap Report.
    d. Facebook
    e. Facebook Messenger
4. There are tools that prevent your images and video from being shared online:
    a. If you’re under 18, file a report with TakeItDown
    b. If you’re over 18, begin a case at StopNCII.org
5. Protect your accounts.
    a. Setup two-factor authentication on Google and Apple.
    b. Set your social media accounts to private and change your passwords.
6. Monitor the web and respond to what you find.
    a. Setup Google Alerts for your name
    b. Consider PimEyes monitoring for your image
    c. Remove your images from Google Search
    d. Issue takedown notices via Rulta, DMCA.com, BranditScan, or an attorney

Reporting to authorities

- Visit your local police station or their website to file a report. Provide all your evidence.
- If you know they’re operating from another country, report the case to the FBI IC3.

Other resources

- StopSextortion.org
- Revenge Porn Hotline (UK)

Recommended attorneys

Start at the Cyber Civil Rights Legal Project: A nationwide project through the K&L Gates law firm providing pro bono legal assistance to victims of nonconsensual pornography. They

maintain a roster of attorneys across the US who volunteered to assist victims on a pro or low bono basis.

Here are others:

- Goldstein & Orr (Texas)
- Katherine O'Brien (NY/NJ)
- Andrew M. Stengel (NY)
- Schiffer Law (TX)
- Werksman Jackson & Quinn (CA)
- Dordulian Law Group (CA)

XXX: Review privacy settings with Block Party

Online harassment

1. Setup Blockparty to filter your social media
2. Walk through Security Planner to lockdown your devices and accounts
3. Remove your personal info with EasyOptOuts, Kanary, Optery, and/or Yael's DIY list
4. Report credible threats to law enforcement. Establish a paper trail.

If you're an enterprise, consider using GetPicnic or Kanary for your team and Brightlines for your executives.

More resources: https://www.tallpoppy.com/resources