StreamBlur

The Streamer's Privacy Checklist

The complete guide to protecting your sensitive information before, during, and after every stream.

2026 Edition • 11 Pages • Print-Friendly

Why Privacy Matters for Streamers

Every year, streamers accidentally expose sensitive information on camera. The consequences can be severe—from stolen accounts to real-world harassment. This checklist will help you protect yourself.

12.8M

secrets detected in public GitHub commits in 2023[1]

67%

of security incidents involve credential exposure[2]

<1 min

time for bots to detect and exploit leaked AWS keys[3]

91%

of data breaches start with compromised credentials[4]

⚠️ **Real Talk:** Once something appears on stream, it's archived forever. Clips spread instantly. Automated bots actively scrape live streams and VODs looking for API keys, passwords, and personal info. Prevention is your only defense—but tools like **StreamBlur** can catch what you miss by automatically masking sensitive data in real-time.

What's At Risk?

- **API Keys & Tokens** — OpenAI, AWS, Stripe, Discord bots, etc.
- **Personal Information** — Email, phone, home address, real name
- **Financial Data** — Bank accounts, PayPal, crypto wallets
- **Private Communications** — DMs, emails, Slack messages
- **Account Credentials** — Passwords, 2FA codes, session tokens
- **Business Information** — Contracts, NDAs, client data

Sources:

[1] GitGuardian State of Secrets Sprawl Report 2024
[2] Verizon Data Breach Investigations Report 2023
[3] Truffle Security Research on AWS Key Exploitation
[4] IBM Cost of a Data Breach Report 2023

Pre-Stream Checklist

Complete this checklist before every stream. Make it a ritual.

Desktop & Environment

- [ ] **Close all unnecessary applications** — Email clients, messaging apps, file managers
- [ ] **Disable desktop notifications** — System-wide, not just individual apps
- [ ] **Hide desktop icons** — Or use a clean streaming desktop
- [ ] **Check your wallpaper** — No personal photos or identifying info
- [ ] **Clear recent files list** — In your OS and applications
- [ ] **Close password managers** — Or ensure they're locked
- [ ] **Log out of personal accounts** — In browsers you'll show on stream

Browser Preparation

- [ ] **Use a dedicated streaming browser profile** — Clean, no saved passwords
- [ ] **Clear autofill data** — Or disable autofill entirely
- [ ] **Check bookmarks bar** — Remove anything revealing
- [ ] **Review installed extensions** — Remove or hide personal ones
- [ ] **Close all tabs** — Start fresh
- [ ] **Disable tab previews** — They can reveal content on hover

Code & Development

- [ ] **Use environment variables** — Never hardcode secrets
- [ ] **Check .env files won't be shown** — Keep them closed/hidden
- [ ] **Review terminal history** — Clear it or use a fresh session
- [ ] **Hide IDE recent files** — They may show project paths
- [ ] **Use placeholder API keys** — For demos, swap real keys out

⚙️ OBS & Streaming Software

Scene Setup

- [ ] **Use Window Capture over Display Capture when possible** — Only shows what you choose
- [ ] **Set up a "BRB" or "Starting Soon" scene** — Switch when you need privacy
- [ ] **Create a "Privacy Mode" scene** — Instant switch for sensitive moments
- [ ] **Test scene transitions** — Ensure no frame leaks between switches
- [ ] **Add a small preview monitor** — See what viewers see in real-time

Audio Protection

- [ ] **Mute notification sounds** — System and app level
- [ ] **Set up a mute hotkey** — Instant audio cut for emergencies
- [ ] **Use voice activation threshold** — Cuts background noise
- [ ] **Check for audio leakage** — System sounds, other apps

Advanced OBS Settings

- [ ] **Enable "Hide OBS from capture"** — Prevents recursion and shows your preview
- [ ] **Set up source visibility hotkeys** — Quick show/hide for overlays
- [ ] **Use color sources as emergency covers** — Hotkey to black screen
- [ ] **Configure safe regions** — Crop captures to hide taskbar/dock

Essential Hotkeys

`F1` BRB • `F2` Mute • `F3` Black • `F4` Main — *Set in OBS → Settings → Hotkeys*

🎬 During Your Stream

Active Monitoring

- [ ] **Keep your preview visible** — On a second monitor if possible
- [ ] **Watch chat for warnings** — Viewers often catch leaks first
- [ ] **Set up trusted mod alerts** — They can DM you if something's showing
- [ ] **Use real-time protection software** — StreamBlur auto-detects and masks sensitive data
- [ ] **Take breaks between high-risk activities** — Check your setup

High-Risk Activities

- [ ] **Browsing email** — Switch to BRB or privacy scene
- [ ] **Opening terminals** — History, env vars, paths all visible
- [ ] **Logging into accounts** — Password managers, saved credentials
- [ ] **File navigation** — Folder names, recent files reveal info
- [ ] **Checking notifications** — DMs, emails, system alerts
- [ ] **Screen sharing in calls** — Double-check what's visible

Emergency Response

If you accidentally show something sensitive:

1. **Immediately switch scenes** — BRB or black screen
2. **Don't panic visibly** — Stay calm for viewers
3. **Rotate the exposed credential** — New API key, new password
4. **Check for active exploitation** — Monitor accounts/services
5. **Consider ending stream early** — If serious, take time to secure
6. **Submit DMCA for VOD** — Request platform remove the clip

Platform-Specific Privacy

Discord

- [ ] **Enable Streamer Mode** — Settings → Streamer Mode → Auto-enable
- [ ] **Hide personal info** — Email, linked accounts, phone
- [ ] **Disable link previews** — Can show unexpected content
- [ ] **Close DMs before sharing screen** — Notifications pop over
- [ ] **Use a streaming-only Discord account** — For showing on stream

Twitter/X

- [ ] **Log out of personal account** — Use brand account only
- [ ] **Disable DM notifications** — They preview message content
- [ ] **Check who you follow** — Can reveal personal interests
- [ ] **Review likes/bookmarks** — Visible in menus

Slack & Teams

- [ ] **Quit the application entirely** — Notifications bypass most blocks
- [ ] **Set status to DND** — If you must keep it open
- [ ] **Collapse all channels** — Hide channel names and unreads
- [ ] **Disable desktop notifications** — In app AND system

GitHub & Code Platforms

- [ ] **Check repository names** — Client names, secret projects
- [ ] **Review recent activity** — Shows what you're working on
- [ ] **Hide contribution graph** — Can reveal work patterns
- [ ] **Use anonymous/public repos only** — For streaming

Discord Streamer Mode Hides:

✓ Email addresses • ✓ Linked accounts • ✓ Server invite links

For Developers Who Stream

Environment & Secrets

- [ ] **NEVER open .env files on stream** — Use placeholder values
- [ ] **Set up .env.example files** — Show structure without secrets
- [ ] **Use secret managers** — AWS Secrets Manager, HashiCorp Vault
- [ ] **Use real-time screen masking** — StreamBlur detects API keys, tokens, and secrets automatically
- [ ] **Check git diff before commits** — May show secrets in changes

Terminal Safety

- [ ] **Clear command history** — `history -c` or new session
- [ ] **Hide prompt username/hostname** — Custom PS1 for streaming
- [ ] **Use aliases for sensitive commands** — Hide actual paths
- [ ] **Check for secrets in output** — API responses, error messages
- [ ] **Use a dedicated streaming terminal theme** — Clean, no personal info

IDE Configuration

- [ ] **Hide file paths in title bar** — Can reveal project locations
- [ ] **Clear recent projects list** — Shows what you've worked on
- [ ] **Disable telemetry popups** — They can show account info
- [ ] **Use "Zen Mode" or equivalent** — Cleaner, less UI clutter
- [ ] **Check extensions that modify UI** — Some show account info

> ⚠️ **API Key Alert:** Bots actively scan Twitch, YouTube, and social media for exposed API keys. An exposed OpenAI key can rack up thousands in charges within minutes. An AWS key can spin up crypto miners instantly.

Safe Streaming Terminal Prompt

```
# Add to .bashrc/.zshrc for streaming
```

✓ Post-Stream Checklist

Immediate Actions

- [ ] **Review your VOD** — Scrub through for any accidental exposures
- [ ] **Check chat logs** — Did anyone mention seeing something?
- [ ] **Monitor clip creation** — Delete any problematic clips
- [ ] **Re-enable notifications** — Now that you're off air
- [ ] **Close streaming-specific apps/profiles** — Return to normal setup

If Something Was Exposed

- [ ] **Rotate credentials immediately** — Don't wait to see if it's exploited
- [ ] **Delete the VOD** — Remove from your channel
- [ ] **Request clip deletion** — Contact platform if others clipped it
- [ ] **Check service logs** — For any unauthorized access
- [ ] **Enable additional 2FA** — On affected accounts
- [ ] **Document the incident** — For future reference and prevention

Regular Maintenance

- [ ] **Audit your API keys monthly** — Rotate proactively
- [ ] **Review connected applications** — Revoke unused access
- [ ] **Update your checklist** — Add items for new tools/workflows
- [ ] **Practice emergency procedures** — Know your hotkeys cold
- [ ] **Backup security settings** — OBS profiles, browser configs

> **Monthly Security Ritual:** Set a calendar reminder to rotate API keys, review OAuth connections, and update your streaming security setup. Prevention is infinitely easier than damage control.

🛠️ Privacy Tools for Your Workflow

🔒 Real-Time Protection

- [ ] **StreamBlur** — AI-powered screen masking for API keys, passwords, emails, and sensitive data in real-time
- [ ] **Muzzle (Mac)** — Auto-disable notifications during screen share
- [ ] **Hush (Windows)** — Notification silencer for streaming

🔐 Password & Secret Management

- [ ] **1Password / Bitwarden** — Auto-lock when idle
- [ ] **AWS Secrets Manager** — Cloud secret storage
- [ ] **HashiCorp Vault** — Enterprise secrets
- [ ] **dotenv-vault** — Encrypted .env files

🎬 Streaming Software

- [ ] **OBS Studio** — Free, open-source
- [ ] **Streamlabs** — All-in-one streaming
- [ ] **Stream Deck** — Hardware scene control
- [ ] **Touch Portal** — Mobile deck alternative

🌐 Browser Privacy

- [ ] **Firefox Multi-Account** — Isolated browser containers
- [ ] **uBlock Origin** — Block targeted ads
- [ ] **Privacy Badger** — Stop invisible trackers
- [ ] **Temporary Containers** — Disposable sessions

💻 Developer Security

- [ ] **git-secrets** — Block secret commits
- [ ] **GitGuardian** — Scan for exposed keys
- [ ] **truffleHog** — Audit git history
- [ ] **pre-commit hooks** — Catch leaks locally

🔊 Audio & Communication

- [ ] **VoiceMeeter** — Audio routing control
- [ ] **Krisp** — AI noise cancellation
- [ ] **SoundSwitch** — Quick audio switching

StreamBlur — Your Safety Net

Even with perfect preparation, mistakes happen. StreamBlur watches your screen 24/7 and automatically masks sensitive data before viewers see it. Think of it as your last line of defense.

📋 Quick Reference Card

Print this page and keep it at your streaming desk.

🚨 EMERGENCY ACTIONS

1. Hit your BRB/black screen hotkey
2. Stay calm—don't draw attention
3. Rotate the exposed credential
4. Delete VOD when stream ends
5. Monitor for exploitation

✓ BEFORE EVERY STREAM

1. Close email & messaging apps
2. Disable all notifications
3. Check browser tabs & bookmarks
4. Clear terminal history
5. Test your emergency hotkeys

⌨️ ESSENTIAL HOTKEYS

F1 — BRB Scene
F2 — Mute All
F3 — Black Screen
F4 — Return to Main
Configure in OBS Settings

HIGH-RISK MOMENTS

- Opening email
- Terminal commands
- Logging into anything
- File browsing
- Checking notifications

Stream Blur

Protecting creators, one stream at a time.

streamblur.com