VPNs are Internet Snake Oil

THE ORIGINAL CURE ALL
RELIEVES INSTANTANEOUSLY
And Cures: Headaches, Nueralgia, Cough, Cold, Sneezing, Hiccups, Gout, Gonorrhea, Dyptheria, Damplung, Mumps, Measles, Whooping cough, Tuberculosis, And even Bowden's Malady.
DOC MITCHELL'S
Providing the Finest in do-it-yourself health care since 2366
DOC MITCHELL'S
SNAKE OIL
101 PROOF
CURE ALL AND LINAMENT
FOR BLINDNESS TRY OUR RATTLESNAKE OIL!

Jim Troutman - jamesltroutman@gmail.com
@troutman

Jim Troutman, Internet “old timer”

- First online in 1982 with “paper TTYs” and acoustic coupler modems on BBSes. Using the Internet & UNIX since 1987. Tasked with building and running Internet infrastructure since the early 90s. Held a wide variety of senior roles in Internet operations, engineering, and management at various regional ISPs, telcos and cable companies, as well as founding some of them.

- Currently solving your broadband problems for hire. Volunteer Director of the regional Internet Exchange for Northern New England (NNENIX.NET), board member of the Maine Technology Users Group (MTUG.ORG).

Also dabbles in Information Security

SKYTALKS

- I come from the ancient times, in a land before the creation of the information security industry and silos of knowledge. Security was just part of doing your job in systems and network administration.

- Also part of the Skytalks Cabal - Director of Operations for the Skytalks Village at DEF CON (defcon.org), which are “off the record” talks more like the original days of the “computer underground” https://skytalks.info

Today’s Presentation

- History lesson on “snake oil” & Virtual Private Networks (VPNs).
- Why people may want to hide their identity online
- What a commercial Virtual Private Network (VPN) service can and cannot do for you.
- The surveillance problem in your pocket.
- Beyond VPNs: Recommendations to help limit online tracking and surveillance, for various levels of paranoia

snake oil noun

1. A worthless preparation fraudulently peddled as a cure for many ills.

2. Speech or writing intended to deceive; humbug.

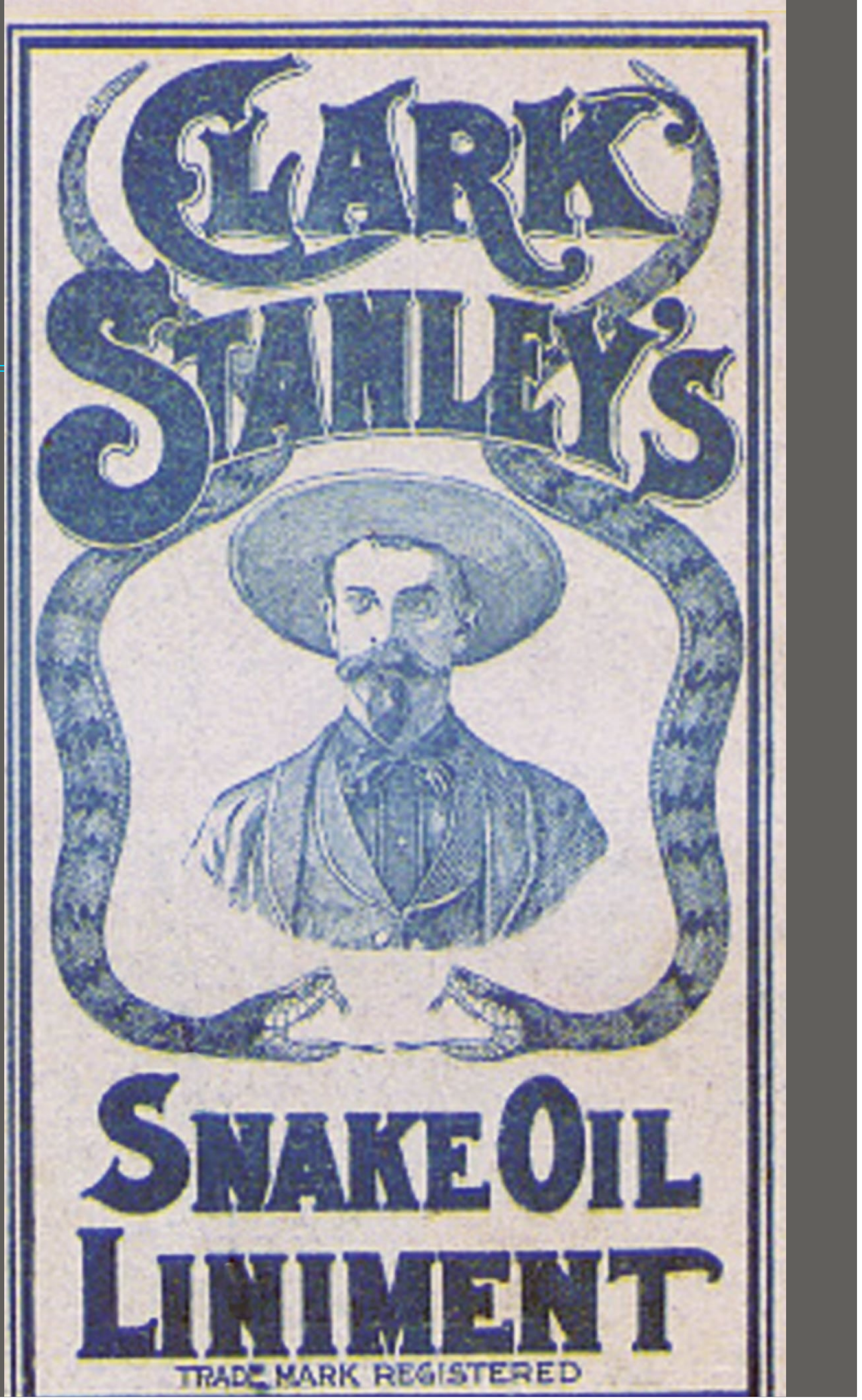
3. A traditional Chinese medicine used to treat joint pain.

snake oil noun

Real Chinese water snake oil has high concentrations of omega-3 fatty acids, and was used to treat joint pain like arthritis and bursitis. Was introduced to the USA by immigrants in the early 1800s.

snake oil noun

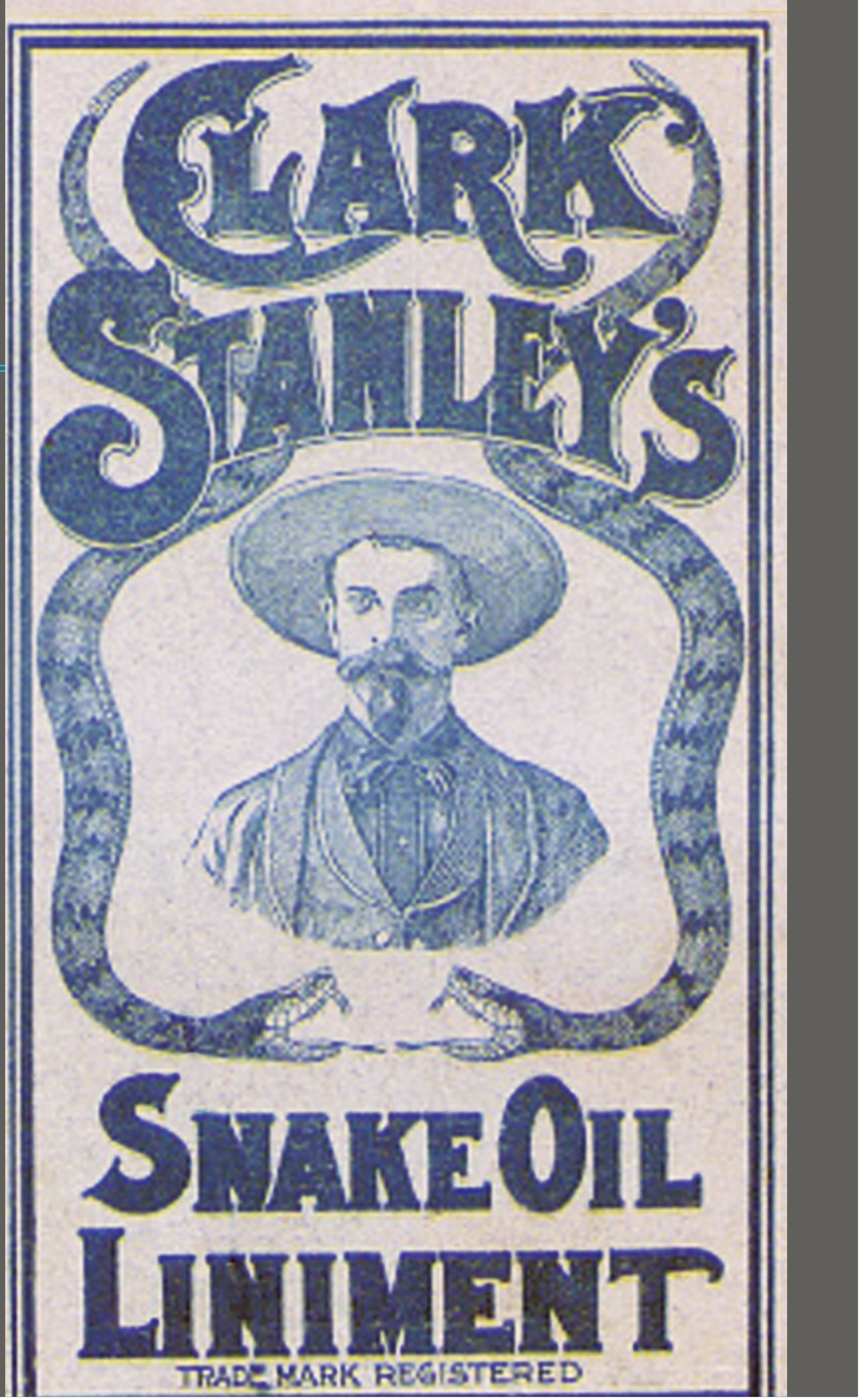
American businessman Clark Stanley created his Snake Oil Liniment circa 1880, and became successful by promoting and selling it in traveling medicine shows



snake oil noun

Product was tested in 1916 after the Pure Food & Drug Act of 1906 and was found to contain primarily mineral oil mixed with beef fat, capsicum, camphor and turpentine.

He was fined $20 by the government. The term became synonymous with fraudulent products or cures.



Virtual Private Networks (VPNs)

- Designed to securely connect a user to a remote local network over an untrusted public network, like the Internet.
- Work remotely, just like you were at the office.
- Original use in the 1990s at large corporate, government and education networks, often for IT and systems administration or for end-user access to “internal only” systems.

Virtual Private Networks (VPNs)

- Protocols have changed over the years, used to be PPTP or L2TP. Now generally IPsec, SSL TLS, or Wireguard based.
- If IPsec, see CNSSP 15 guidelines & NIST 800-41
  - ISAKMP/IKE minimum requirements shall be:
    - DH Group 16, AES-256, SHA-384 hash, or better.
  - IPsec minimum requirements shall be:
    - AES-256, SHA-384, CBC block cipher mode, or better

Consumer VPN services

- Commercial VPN services aimed at the home user started becoming available around 2005.
  - As the Internet became popular, so did on-line censorship, targeted advertising, and data mining of consumers.
  - Remember — back then nearly all websites and data transiting over the Internet was generally not encrypted.

Consumer VPN services

- VPNs became popular as a way for the average user to “protect themselves online”
  - public knowledge of expansive government surveillance due to Wikileaks and Edward Snowden’s leaks also helped
  - Also because often recommended by IT and information security staff as being somehow beneficial

Consumer VPN services

- in the late 2000s, media companies like Netflix, Hulu, and the BBC started putting video content online, but with geographic restrictions, which could be bypassed with VPNs
- Some countries have strict Internet usage and censorship policies, and VPN services have been able help users bypass those restrictions, historically.

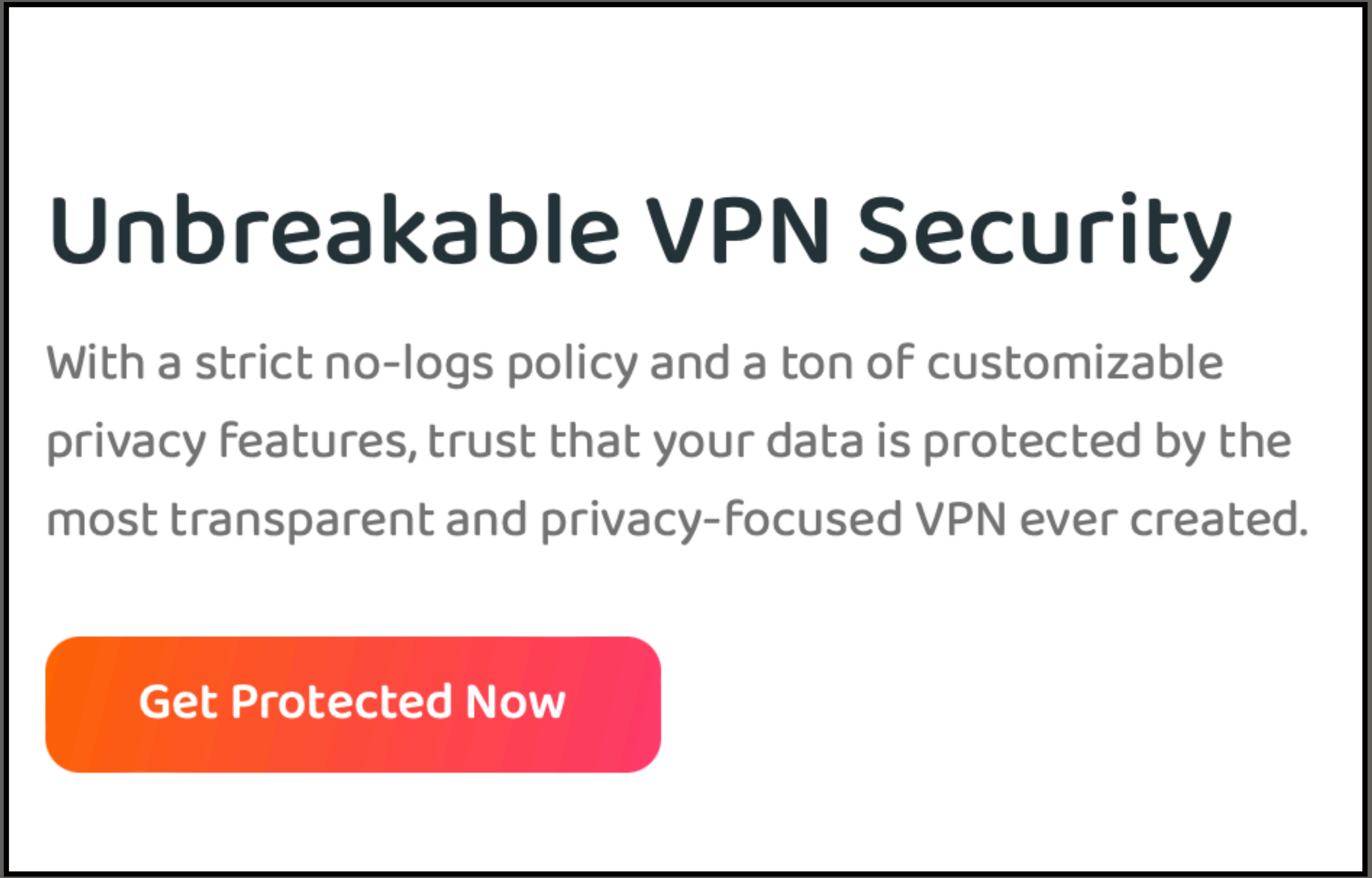
Consumer VPN Industry

- In 2023, the home user VPN industry is estimated at over $45 billion in size, with over 100 brands of paid services, and hundreds of “free” VPN services.

Consumer VPN Industry

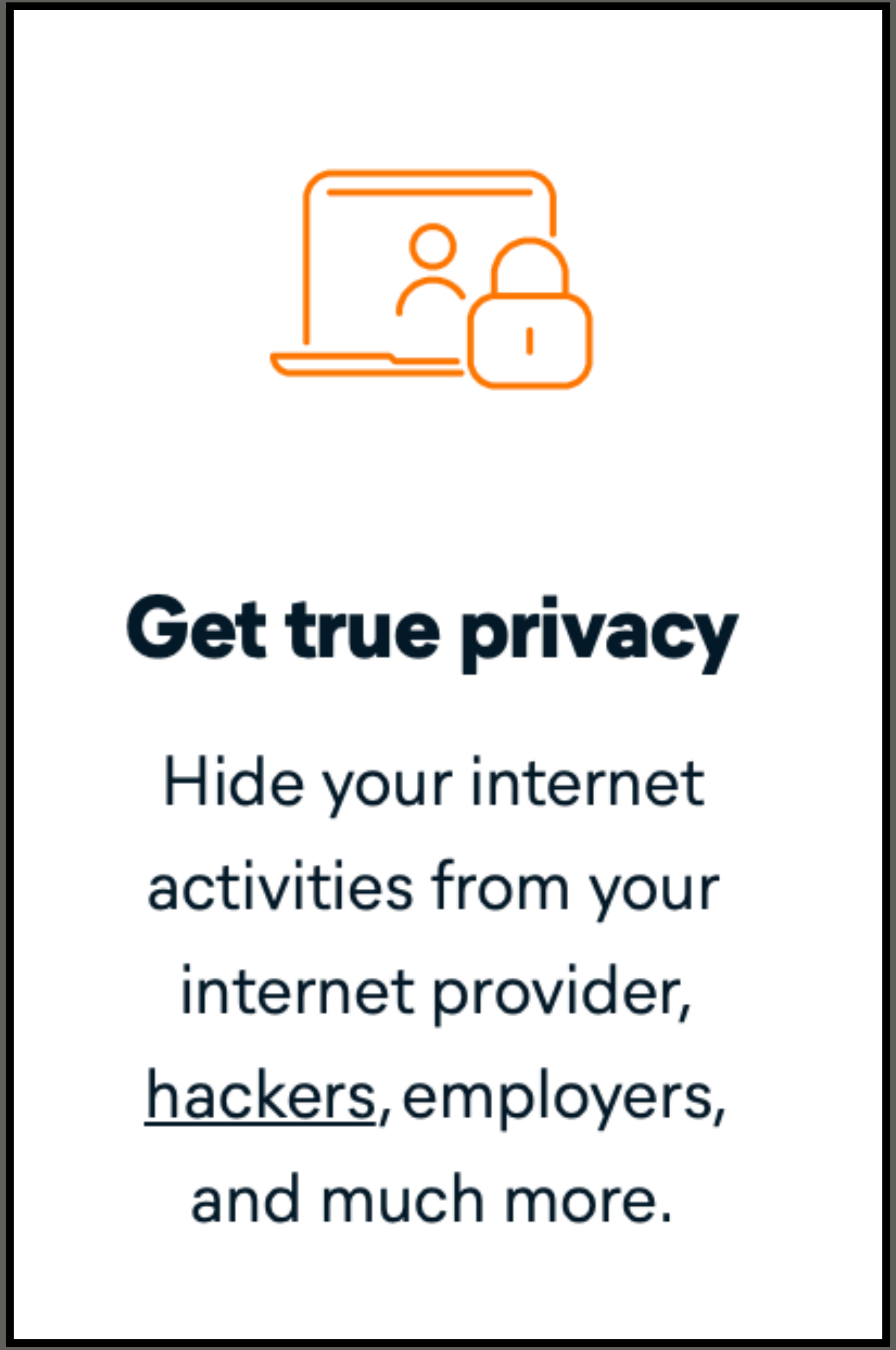
- The industry advertises heavily on advertising online and seems to sponsor most podcasts.
- Most VPN review websites are actually owned by a VPN provider and far from objective.

VPN marketing is “hyperbolic”



Unbreakable VPN Security

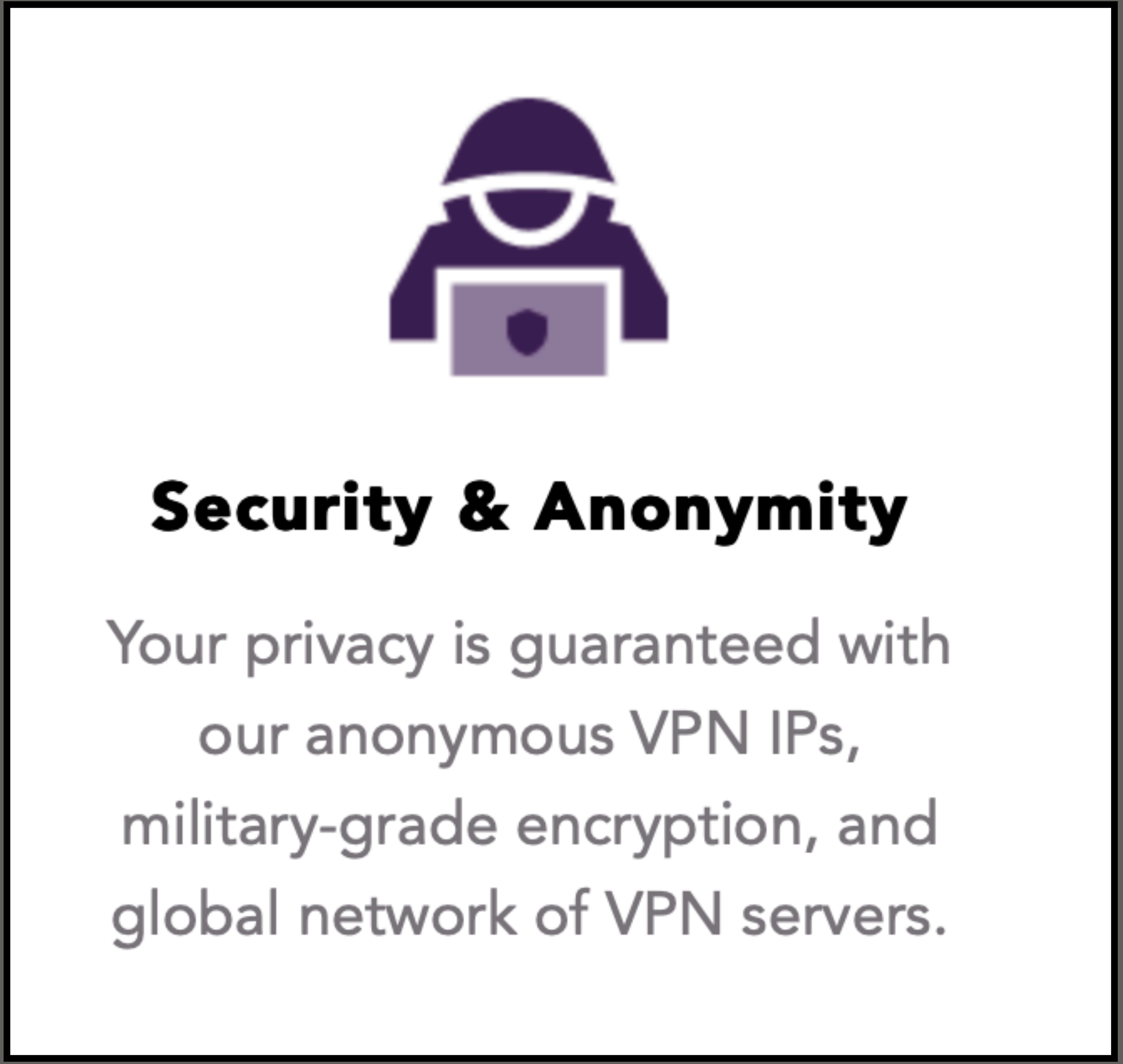
With a strict no-logs policy and a ton of customizable privacy features, trust that your data is protected by the most transparent and privacy-focused VPN ever created.



Get true privacy

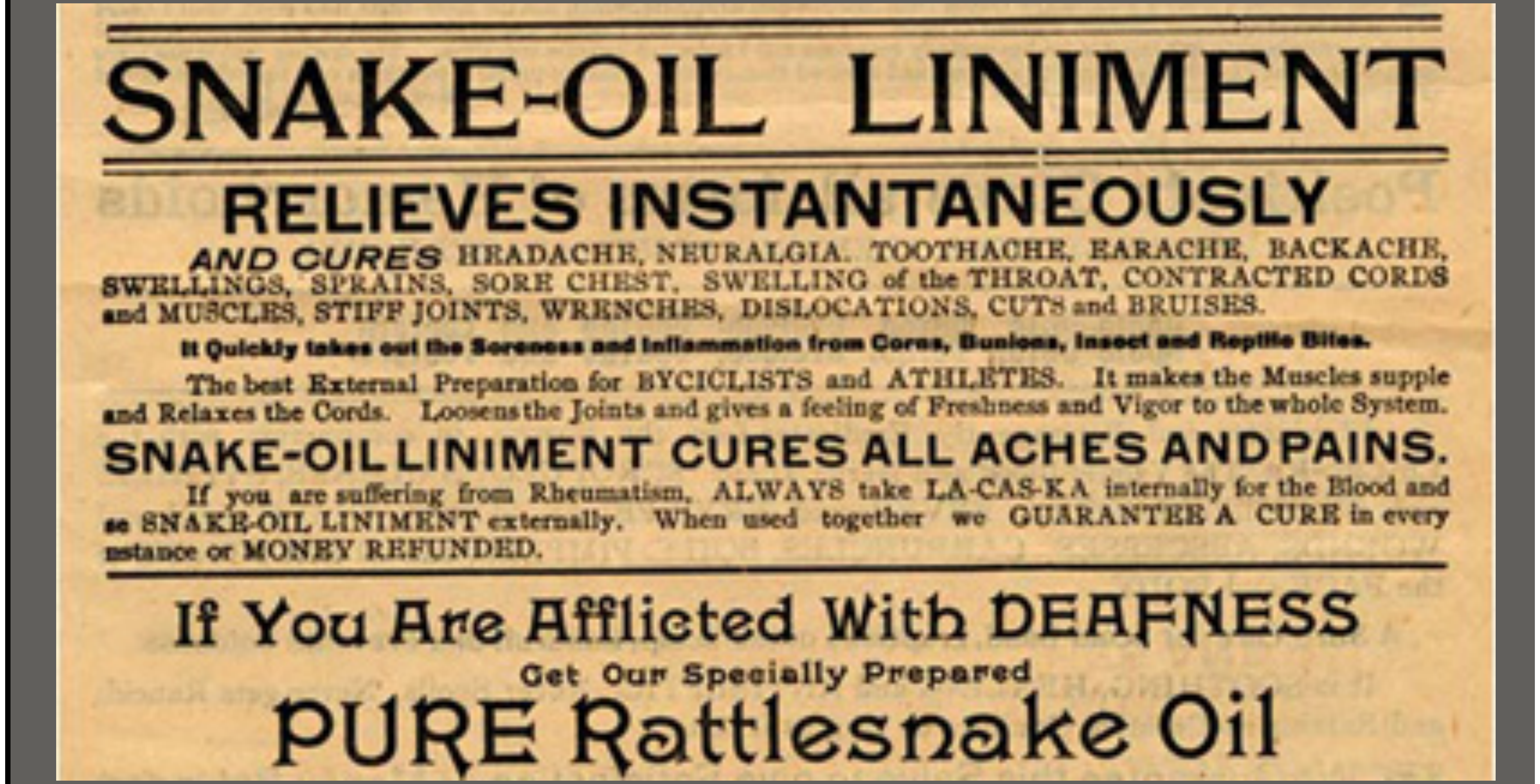
Hide your internet activities from your internet provider, hackers, employers, and much more.

VPN marketing is “hyperbolic”



Security & Anonymity

Your privacy is guaranteed with our anonymous VPN IPs, military-grade encryption, and global network of VPN servers.



SNAKE-OIL LINIMENT

RELIEVES INSTANTANEOUSLY

AND CURES HEADACHE, NEURALGIA. TOOTHACHE, EARACHE, BACKACHE, SWELLINGS, SPRAINS, SORE CHEST, SWELLING of the THROAT, CONTRACTED CORDS and MUSCLES, STIFF JOINTS, WRENCHES, DISLOCATIONS, CUTS and BRUISES.

It Quickly takes out the Soreness and Inflammation from Corns, Bunions, Insect and Reptile Bites.

The best External Preparation for BYCICLISTS and ATHLETES. It makes the Muscles supple and Relaxes the Cords. Loosens the Joints and gives a feeling of Freshness and Vigor to the whole System.

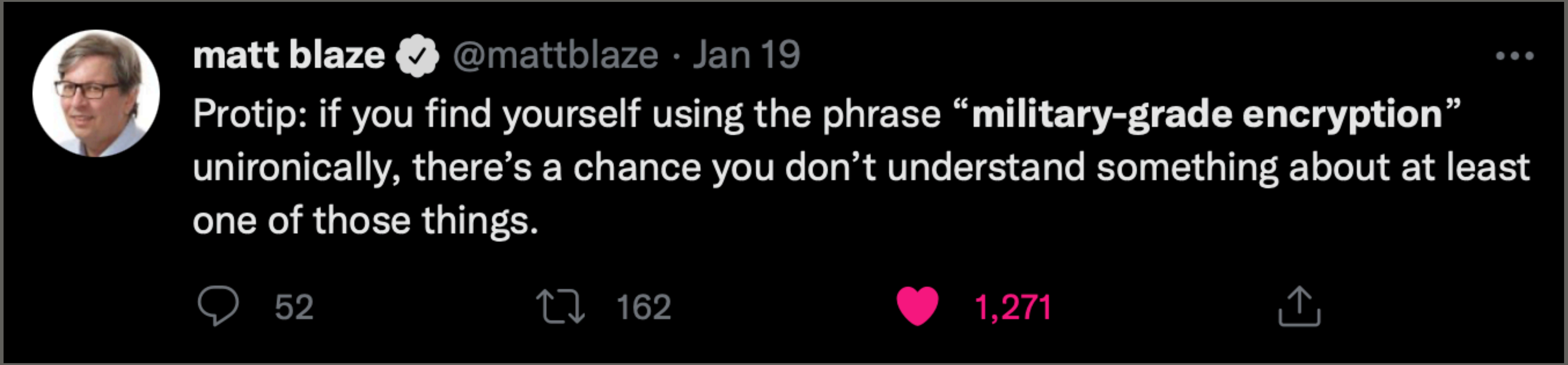
SNAKE-OIL LINIMENT CURES ALL ACHES AND PAINS.

If you are suffering from Rheumatism, ALWAYS take LA-CAS-KA internally for the Blood and se SNAKE-OIL LINIMENT externally. When used together we GUARANTEE A CURE in every nstance or MONEY REFUNDED.

If You Are Afflicted With DEAFNESS

Get Our Specially Prepared

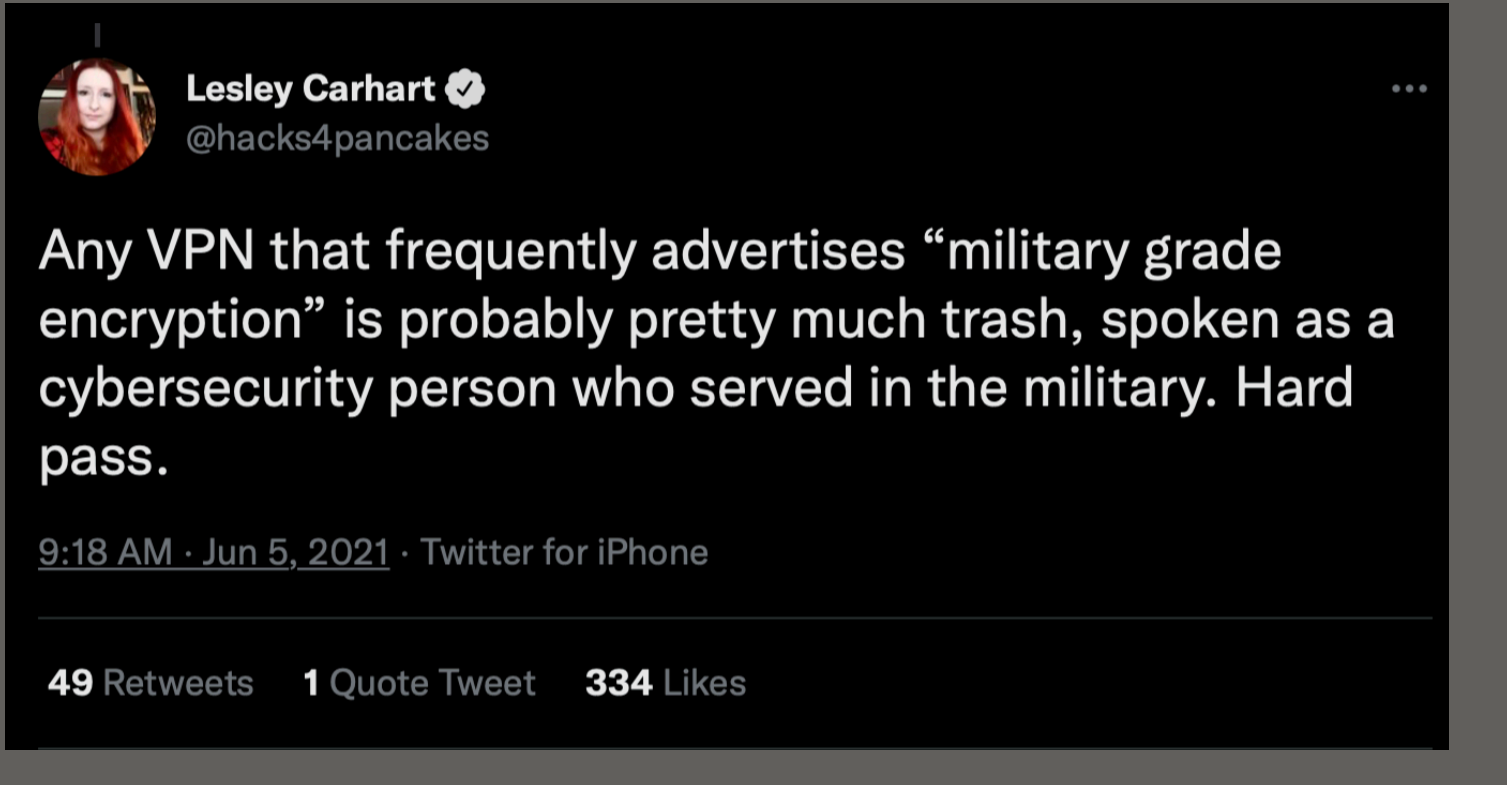
PURE Rattlesnake Oil



matt blaze @mattblaze · Jan 19

Protip: if you find yourself using the phrase “**military-grade encryption**” unironically, there’s a chance you don’t understand something about at least one of those things.

52 162 1,271

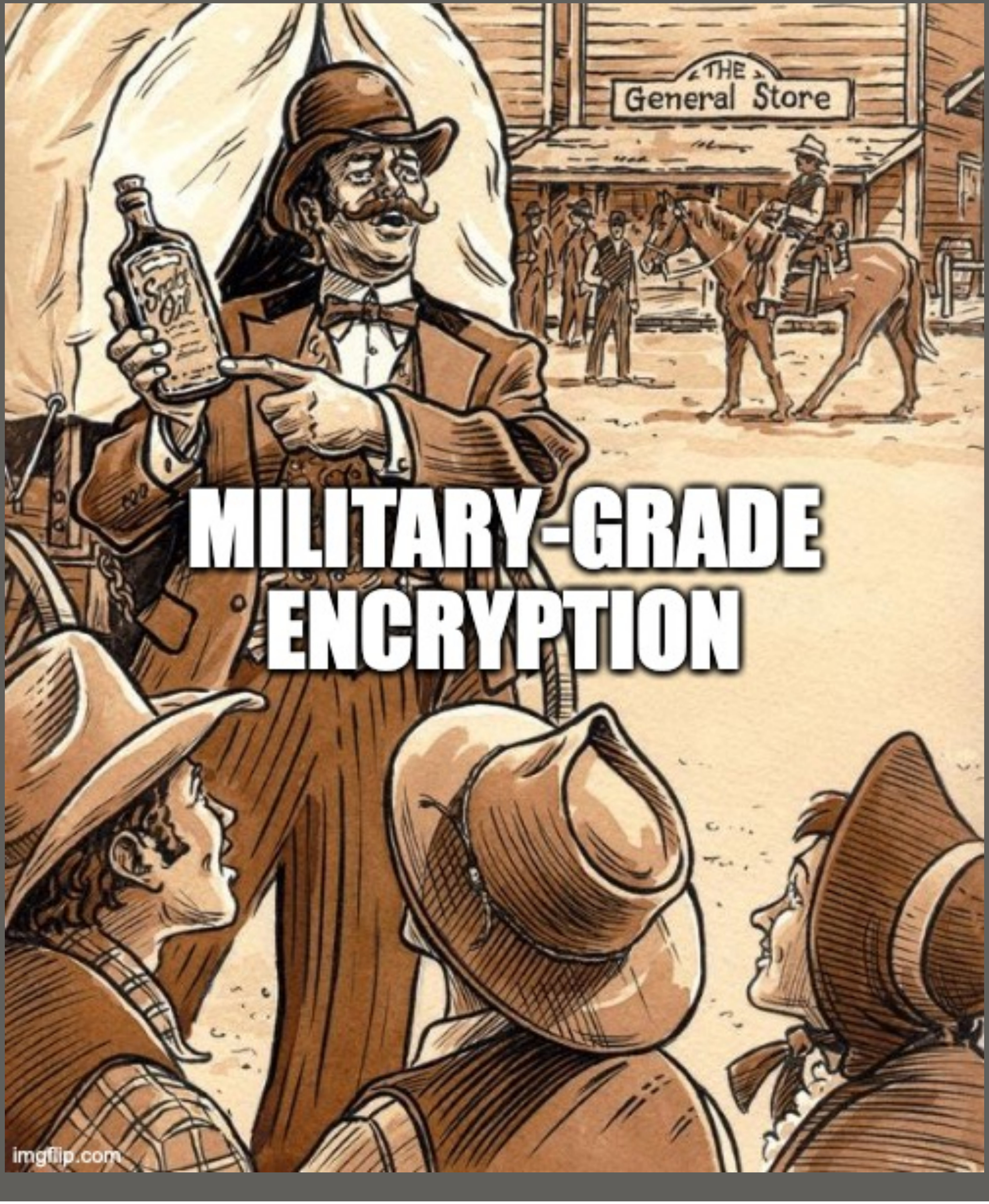


Lesley Carhart
@hacks4pancakes

Any VPN that frequently advertises “military grade encryption” is probably pretty much trash, spoken as a cybersecurity person who served in the military. Hard pass.

9:18 AM · Jun 5, 2021 · Twitter for iPhone

49 Retweets **1** Quote Tweet **334** Likes


THE General Store
Snake Oil
MILITARY-GRADE ENCRYPTION
imgflip.com

@TROUTMAN

VPN falsehoods

- prevents social media and advertising tracking
- avoid data breaches
- protect your passwords and “information”
- hide your mobile phone location (GPS)
- defend against “cyber threats”
- privacy is guaranteed !

YOU KEEP USING THAT PHRASE "PRIVACY IS GUARANTEED"
I DO NOT THINK IT MEANS WHAT YOU THINK IT MEANS
memegenerator.net

@TR

VPNs can help with

- VPNs can and do help protect again "Man the Middle" attacks on vulnerable unsecured networks like public Wi-Fi access points often found in hotels and coffee shops.
- encrypts traffic so that your local ISP cannot monitor it or track you, which includes DNS requests
- Masks your public IPv4 address from websites and services
- May help you evade geographic content restrictions

VPN service use cases

- For the perceived benefits of security and privacy enhancements, including hiding your online activities from your ISP.

- To get around geolocation blocks to access content
  - “whack-a-mole” game with content providers, as new IPv4 blocks are used, indentified as being used by VPNs and then blocked.

VPN service drawbacks

- You will get a lot of CAPTCHAs
- Some websites may not work at all
- Your ability to access geolocation locked content will vary wildly and may disappoint you
- Your Internet experience may be quite a bit slower

Shady Free VPN Apps

- Stats from Top10VPN study in 2021:
  - Chinese VPN ownership: 59% of the most popular free VPN mobile apps have links to China
  - Weak VPN privacy policies: 86% of free VPN apps had substandard privacy policies

Shady Free VPN Apps

- Poor professionalism: 55% of free VPN apps had privacy policies hosted in amateur fashion.

- 52% offered customer support via personal email accounts (Gmail, Hotmail or Yahoo).

Shady Free VPN Apps

- Scant company information: 64% of free VPN apps had no dedicated website. Almost all made it very difficult to properly identify individuals providing the VPN service

- 85% of 150 Android VPNs had unsafe permissions.
  - 25% of those exposed data via DNS, WebRTC, or IP address leakage.

RFC7721

Security and Privacy Considerations for IPv6 Address Generation

"3.1. Correlation of Activities over Time

As with other identifiers, an IPv6 address can be used to correlate the activities of a host for at least as long as the lifetime of the address. The correlation made possible by IEEE-identifier-based IIDs is of particular concern since they last roughly for the lifetime of a device's network interface, allowing correlation on the order of years."

What is your risk model?

- Why are you using the VPN? Trying evade being caught for doing something deemed illegal in your jurisdiction?

- Illegal acts can range from just accessing information, file sharing of copyrighted materials, attacking and breaking into systems & services, purchasing controlled drugs or products on-line, to criminal conspiracy and terrorism.

What is your risk model?

- Many ISPs are monitoring and monetizing your DNS traffic from all your devices, tied to your IP address.

- Some sell this data to brokers, which is often purchased by government entities to add to their databases.

- Even if your ISP doesn’t sell DNS data, they usually have the right to use it to provide target ad services.

What is your risk model?

- Many ISPs keep DHCP logs for years
- ISPs can tie your home or business physical location and account to your Ethernet MAC of your router.
- Also directly to your smartphone.
  - ISPs answer subpoenas regularly.
    - Big ones have entire departments dedicated

What is your risk model?

- A commercial VPN service can absolutely help hide your DNS traffic and other activity from YOUR ISP, but not from the Internet as a whole.
- requires much additional precautions.

FACTS

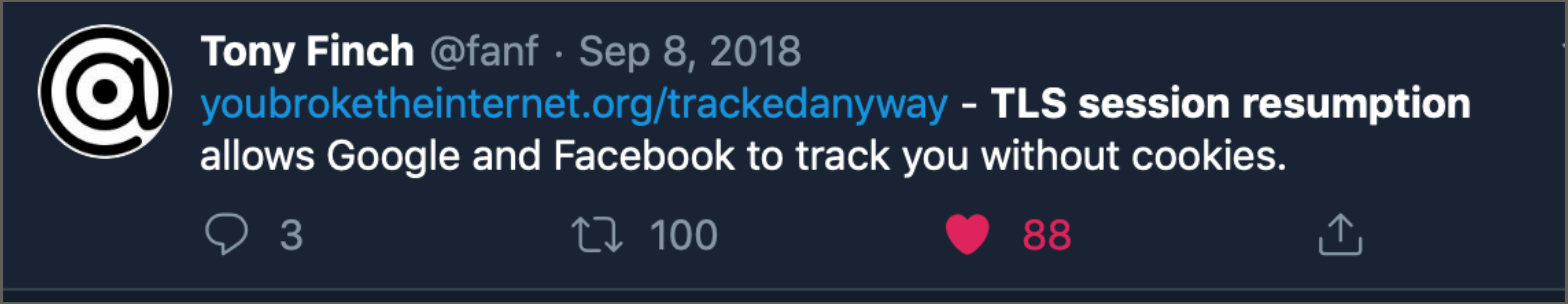
- VPNs by themselves will not save you from these risks
- Determined adversaries have resources you cannot imagine to correlate traffic.

FACTS

- The real problem is the browser and the apps in your pocket.
- Pervasive and sophisticated online user activity surveillance

FACTS

- Yes, this means tracking cookies and pixels from hundreds of advertising networks and social media companies
- But there is a lot more sophisticated methods



Tony Finch @fanf · Sep 8, 2018

youbroketheinternet.org/trackedanyway - **TLS session resumption** allows Google and Facebook to track you without cookies.

- TLS Session Resumption Tickets
- A nearly unblockable “cookie” that can be used to track you everywhere when resuming previous TLS sessions (all HTTPS apps including DoH) over a long period of time (up to 7 days with TLS 1.3)

FACTS

- Browser & device fingerprinting
  - screen size, software versions, fonts installed, many other data points
  - Can be unique down to about 1:256000 users on average

FACTS

- Plus the enormous amount of telemetry from apps on your smart phone that you agreed to.
- Common for multiple advertising SDKs to be compiled into the apps

FACTS

- You are only as secure as you are patient.
- It is very hard to anonymize human behavior. We all have habits and patterns.

REALITY - AVERAGE USER

- Using a VPN service at home or on your device can help hide your Bittorrenting or website visits from *your* ISP, but not beyond that.
- Some VPNs add software that can help reduce tracking, but only on that device.

Recommendations

- Harden the browser you use and install tracking blocker plug-ins like Privacy Badger, uBlock Origin and others as recommended
- Use a DNS service that blocks common ad networks (Pi-Hole, others).

Hardcore Recommendations

- The best way to do shady things is use other people's computers over stacked covert channels from other untraceable locations.
- Why do you think botnets are so popular?

ADVANCED USER Recommendations

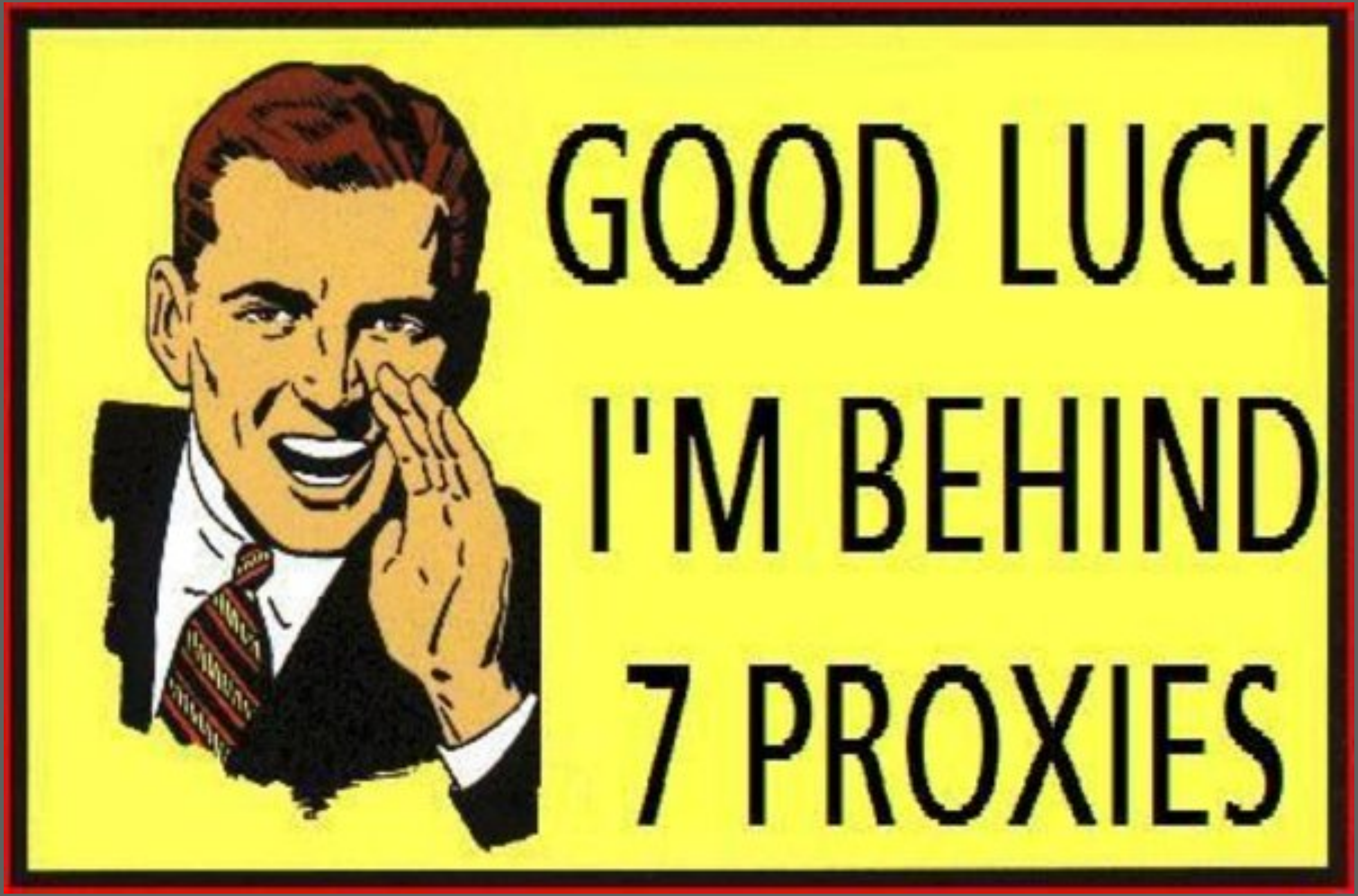
- Combine using a reputable VPN with a dedicated virtual machine for your sketchy browsing needs
  - Reset the VM state after every use, don’t store any cookies
  - Pro-tip: VMs can be easy to identify if you allocate a single CPU core

Hardcore Recommendations

- Don’t do any shady things from your home, work or anyplace else that can be traced to you.
- Use TAILS with Tor from a USB drive
- Use dedicated old hardware that the purchase cannot be tracked back to you
  - Disable/Remove Wi-Fi and bluetooth from the machine
  - Disable/Remove cameras and audio.

Hardcore Recommendations

- Try to use a last mile access method that is as untraceable to you as possible.
  - Long-distance Wi-Fi use in areas without surveillance cameras


GOOD LUCK
I'M BEHIND
7 PROXIES

Recommendation for your users

- DO NOT use any “free” VPN products
- Look to independant product reviews like Consumer Reports for purchasing VPN services.
- “Keeping safe online” is not an easy fix.

Thank you!

- This slide deck will be available to download.
- jamesltroutman@gmail.com
- Twitter: @troutman
- @jtroutman.bsky.social

Selected Bibliography & Resources

- An in-depth guide to choosing a VPN - https://freedom.press/training/choosing-a-vpn/
- Are you really invisible when you use a VPN?- https://www.tomsguide.com/features/are-you-really-invisible-when-you-use-a-vpn
- MSN Article: VPNs Are Snake Oil Because HTTPS Exists - https://www.freezenet.ca/msn-article-vpns-are-snake-oil-because-https-exists/
- Don't use VPN services - https://gist.github.com/joepie91/5a9909939e6ce7d09e29
- Scams and SnakeOil In the VPN Industry - https://vpnftw.com/scams-and-snakeoil-in-the-vpn-industry-984/
- $10/month VPN services – snake oil or not? - https://nohats.ca/wordpress/blog/2012/06/08/10month-vpn-services-snake-oil-or-not/

Selected Bibliography & Resources

- Free VPN Ownership Investigation - https://www.top10vpn.com/research/free-vpn-investigations/
- Many free mobile VPN apps are based in China or have Chinese ownership - https://www.zdnet.com/article/many-free-mobile-vpn-apps-are-based-in-china-or-have-chinese-ownership/
- Top VPNs secretly owned by Chinese firms - https://www.computerweekly.com/news/252466203/Top-VPNs-secretly-owned-by-Chinese-firms/
- China owns half of all VPN services - https://www.csoonline.com/article/3335480/china-owns-half-of-all-vpn-services.html
- Free VPN Risk Index - https://www.top10vpn.com/research/free-vpn-investigations/risk-index/
- These VPN “Review” Websites are Actually Owned by VPNs - https://restoreprivacy.com/

Selected Bibliography & Resources

- Should You Use a VPN? https://www.consumerreports.org/vpn-services/should-you-use-a-vpn-a5562069524/
- VPN Testing Reveals Poor Privacy and Security Practices, Hyperbolic Claims - https://www.consumerreports.org/vpn-services/vpn-testing-poor-privacy-security-hyperbolic-claims-a1103787639/
- VPNalyzer: Crowdsourced Investigation into Commercial VPNs - https://vpnalyzer.org
- Mullvad, IVPN, and Mozilla VPN Top Consumer Reports' VPN Testing - https://www.consumerreports.org/vpn-services/mullvad-ivpn-mozilla-vpn-top-consumer-reports-vpn-testing-a9588707317/
- Security and Privacy of VPNs Running on Windows 10 - https://digital-lab-wp.consumerreports.org/wp-content/uploads/2021/12/VPN-White-Paper.pdf

Selected Bibliography & Resources

- Seven 'no log' VPN providers accused of leaking – yup, you guessed it – 1.2TB of user logs onto the Internet - https://www.theregister.com/2020/07/17/ufo_vpn_database/

- Know your cookies: A guide to internet ad trackers - https://digiday.com/media/know-cookies-guide-internet-ad-trackers/

- Tracking Users across the Web via TLS Session Resumption - https://svs.informatik.uni-hamburg.de/publications/2018/2018-12-06-Sy-ACSAC-Tracking_Users_across_the_Web_via_TLS_Session_Resumption.pdf

- TLS Session Resumption https://www.venafi.com/blog/tls-session-resumption

- Advertisers can track users across the Internet via TLS Session Resumption - https://www.zdnet.com/article/advertisers-can-track-users-across-the-internet-via-tls-session-resumption/

Selected Bibliography & Resources

- Wikipedia - Device fingerprint - https://en.wikipedia.org/wiki/Device_fingerprint
- Cover Your Tracks — See how trackers view your browser - https://coveryourtracks.eff.org
- What Is Browser Fingerprinting and How Can You Prevent It? - https://www.avast.com/c-what-is-browser-fingerprinting
- Browser Fingerprinting: What Is It And What Should You Do About It? - https://pixelprivacy.com/resources/browser-fingerprinting/
- What Is Browser Fingerprinting & How Does It Work? - https://seon.io/resources/browser-fingerprinting/
- Cross device tracking - An FTC Staff Report - https://www.ftc.gov/system/files/documents/

Selected Bibliography & Resources

- 4 geolocation technologies compared - https://www.sensolus.com/four-geolocation-technologies-compared-how-can-they-improve-your-operational-efficiency/
- Wikipedia - Room 641A - https://en.m.wikipedia.org/wiki/Room_641A
- 5 Things You Need to Know About Beacon Technology - https://www.wordstream.com/blog/ws/2018/10/04/beacon-technology
- What is a Bluetooth beacon? - https://www.beaconstac.com/what-is-a-bluetooth-beacon
- How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did - https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=c7df19266686
- Toll payment devices used to track vehicles on toll-free roads - https://papersplease.org/wp/2015/04/28/toll-payment-devices-used-to-track-vehicles-on-toll-free-roads/

Selected Bibliography & Resources

- IPv6 and Internet Privacy - https://blogs.infoblox.com/ipv6-coe/ipv6-and-internet-privacy/]
- Understanding IPv6 EUI-64 Bit Address - https://community.cisco.com/t5/networking-documents/understanding-ipv6-eui-64-bit-address/ta-p/3116953
- Security and Privacy Considerations for IPv6 Address Generation Mechanisms - https://datatracker.ietf.org/doc/html/rfc7721
- SLAM - Strategies for Large-Scale IPv6 Active Mapping - https://www.caida.org/funding/cns-slam/cns-slam_proposal/
- SLAM - Strategies for Large-Scale IPv6 Active Mapping - https://www.internetsociety.org/blog/2014/12/ipv6-privacy-addresses-provide-protection-against-surveillance-and-tracking/
- Follow the Scent: Defeating IPv6 Prefix Rotation Privacy - https://arxiv.org/pdf/2102.00542.pdf

Selected Bibliography & Resources

- EFF - Privacy Badger - https://privacybadger.org
- EFF - Privacy Badger source - https://github.com/EFForg/privacybadger
- Best Practices: Firefox Hardening - https://wevpn.com/blog/best-practices-firefox-hardening/
- Firefox configuration hardening - user.js - https://github.com/pyllyukko/user.js