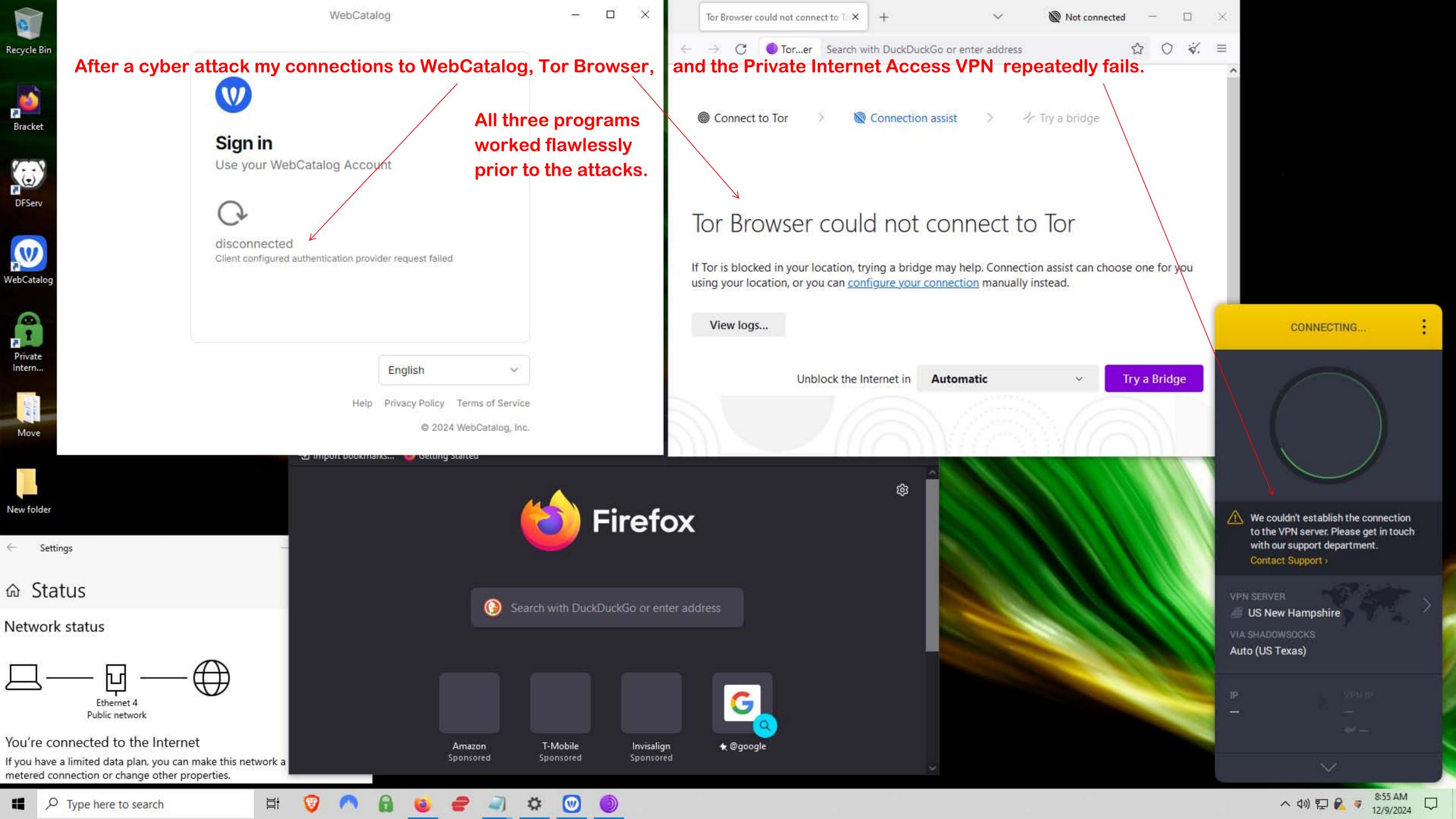## Continued Cyber Attacks Against My Network

   To expand their constant, illegal surveillance and cyber attacks on my devices and software, cyber criminals disabled my encrypted browser (Tor), a web application download program (WebCatalog), and my Virtual Private Network/VPN software (Private Internet Access/PIA)."cpf "Gzrtguu"XRP .
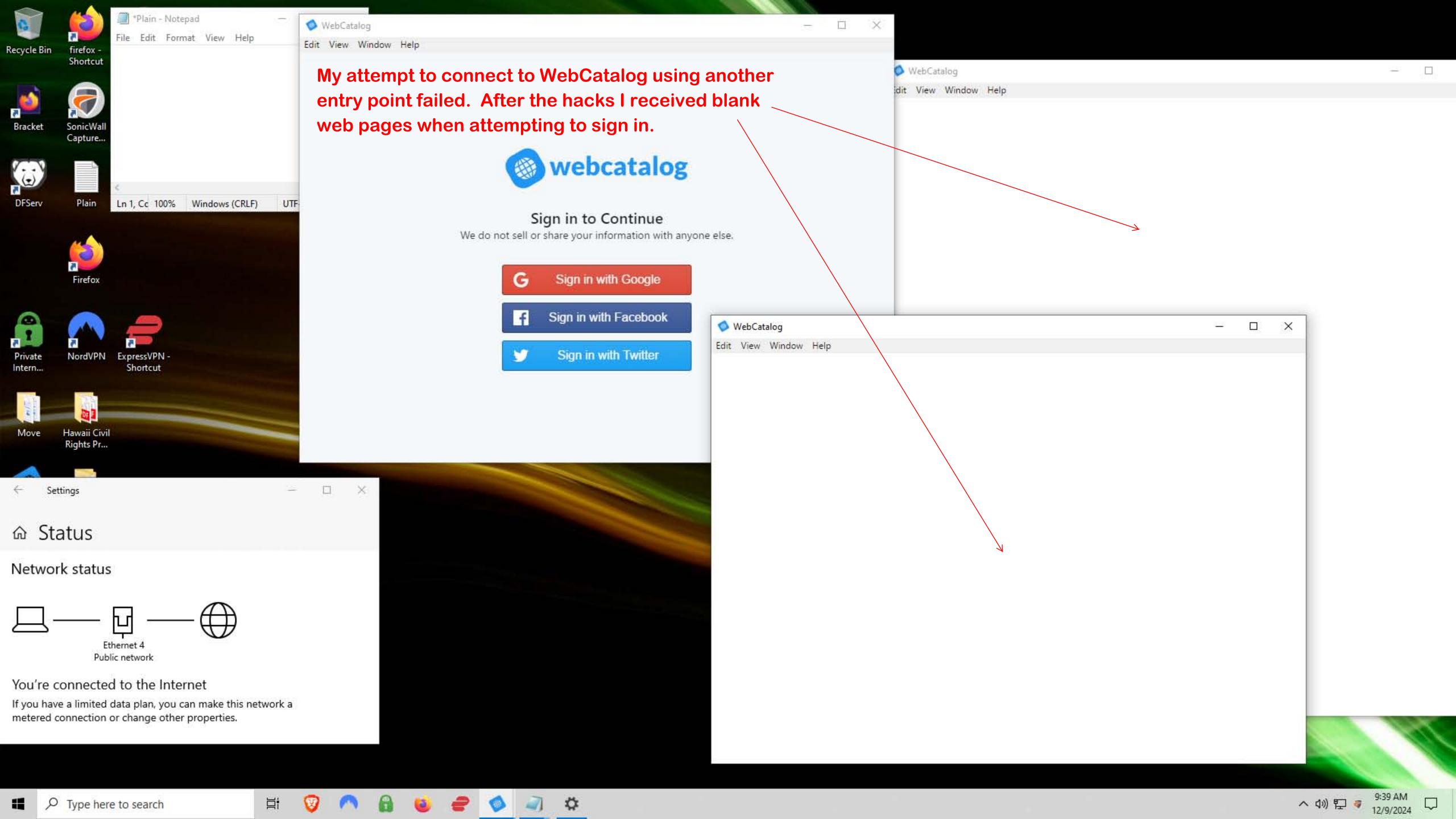
   By blocking these programs the criminals can see my website traffic and continue to block my connections to lawyers, media, whistleblower advocates, and others as desired.

   The next screen shot details my view after attempting to launch the three programs that failed. All worked flawlessly prior to being hacked. WebCatalog would allow me to install various, browser-free legal, social media, news, and other applications. The Tor browser and the PIA VPN cpf "Gzrtguu"XRP "hide website traffic from view.'"

'"Cffkkqpcn"uetggp"uj qu"uj qy "yj g"eqo rtqo kugu"yj cv'qeewttgf "chvgt"cwcemu"ci ckpuv'o { "Gzrtguu"XRP "rtqitco 0

   Again, cyber criminals blocked my software to allow their illegal surveillance to continue and to block me from exposing their crimes.

After a cyber attack my connections to WebCatalog, Tor Browser, and the Private Internet Access VPN repeatedly fails.

All three programs worked flawlessly prior to the attacks.

*Plain - Notepad

File   Edit   Format   View   Help

Ln 1, Cc   100%   Windows (CRLF)   UTF

WebCatalog

Edit   View   Window   Help

My attempt to connect to WebCatalog using another entry point failed. After the hacks I received blank web pages when attempting to sign in.

webcatalog

Sign in to Continue
We do not sell or share your information with anyone else.

G   Sign in with Google

f   Sign in with Facebook

Sign in with Twitter

WebCatalog

dit   View   Window   Help

WebCatalog

Edit   View   Window   Help

Settings

⌂ Status

Network status

Ethernet 4
Public network

You're connected to the Internet

If you have a limited data plan, you can make this network a metered connection or change other properties.

Type here to search

9:39 AM
12/9/2024

Encrypted Browser Attack To Facilitate Illegal Surveillance

    The Tor browser uses a series of encrypted tunnels to provide online privacy. It prevents hackers from seeing your locations on the Internet. Cyber criminals attacked and disabled my Tor browser to facilitate their illegal online surveillance and cyber attacks. The criminals hacked my browser so sites I visited could be seen and communication blocked if a threat of exposure arose.

    My Tor browser operated flawlessly before the cyber attacks. The log that follows is from the browser. It details repeated failed connections after it was disabled. Each time I attempted to connect I received the same failures.

After being attacked and compromised, my Tor encrypted browser repeatedly failed to connect.

2024-12-07 02:58:55.250 [NOTICE] Opening Socks listener on 127.0.0.1:9150
2024-12-07 02:58:55.250 [NOTICE] Opened Socks listener connection (ready) on 127.0.0.1:9150
2024-12-07 02:58:56.242 [NOTICE] Bootstrapped 5% (conn): Connecting to a relay
2024-12-07 02:59:17.620 [NOTICE] Bootstrapped 10% (conn_done): Connected to a relay
2024-12-07 02:59:38.492 [WARN] Problem bootstrapping. Stuck at 10% (conn_done): Connected to a relay.
(Connection timed out [WSAETIMEDOUT]; TIMEOUT; count 10; recommendation warn; host
AAA083A03F9EAF563A5FAF08C5A54A1156677BD5 at 178.211.147.22:6839)
2024-12-07 02:59:38.492 [WARN] 9 connections have failed:
2024-12-07 02:59:38.492 [WARN] 5 connections died in state handshaking (TLS) with SSL state SSLv3/TLS write
client hello in HANDSHAKE
2024-12-07 02:59:38.493 [WARN] 4 connections died in state connect()ing with SSL state (No SSL object)
2024-12-07 02:59:38.505 [NOTICE] Closing no-longer-configured Socks listener on 127.0.0.1:9150
2024-12-07 02:59:38.505 [NOTICE] DisableNetwork is set. Tor will not make or accept non-control network
connections. Shutting down all existing connections.
2024-12-07 02:59:38.603 [NOTICE] Delaying directory fetches: DisableNetwork is set.
2024-12-07 02:59:49.146 [NOTICE] Renaming old configuration file to "C:\Users\Luke\Desktop\Tor
Browser\Browser\TorBrowser\Data\Tor\torrc.orig.1"
2024-12-07 02:59:54.754 [NOTICE] Opening Socks listener on 127.0.0.1:9150
2024-12-07 02:59:54.754 [NOTICE] Opened Socks listener connection (ready) on 127.0.0.1:9150
2024-12-07 02:59:56.156 [WARN] Problem bootstrapping. Stuck at 10% (conn_done): Connected to a relay.
(CONNECTRESET; CONNECTRESET; count 11; recommendation warn; host **Retry failed to connect.**
24E2F139121D4394C54B5BCC368B3B411857C413 at 204.13.164.118:443)
2024-12-07 02:59:56.157 [WARN] 11 connections have failed:
2024-12-07 02:59:56.157 [WARN] 6 connections died in state handshaking (TLS) with SSL state SSLv3/TLS write
client hello in HANDSHAKE
2024-12-07 02:59:56.157 [WARN] 5 connections died in state connect()ing with SSL state (No SSL object)
2024-12-07 02:59:56.165 [NOTICE] Closing no-longer-configured Socks listener on 127.0.0.1:9150
2024-12-07 02:59:56.165 [NOTICE] DisableNetwork is set. Tor will not make or accept non-control network
connections. Shutting down all existing connections.
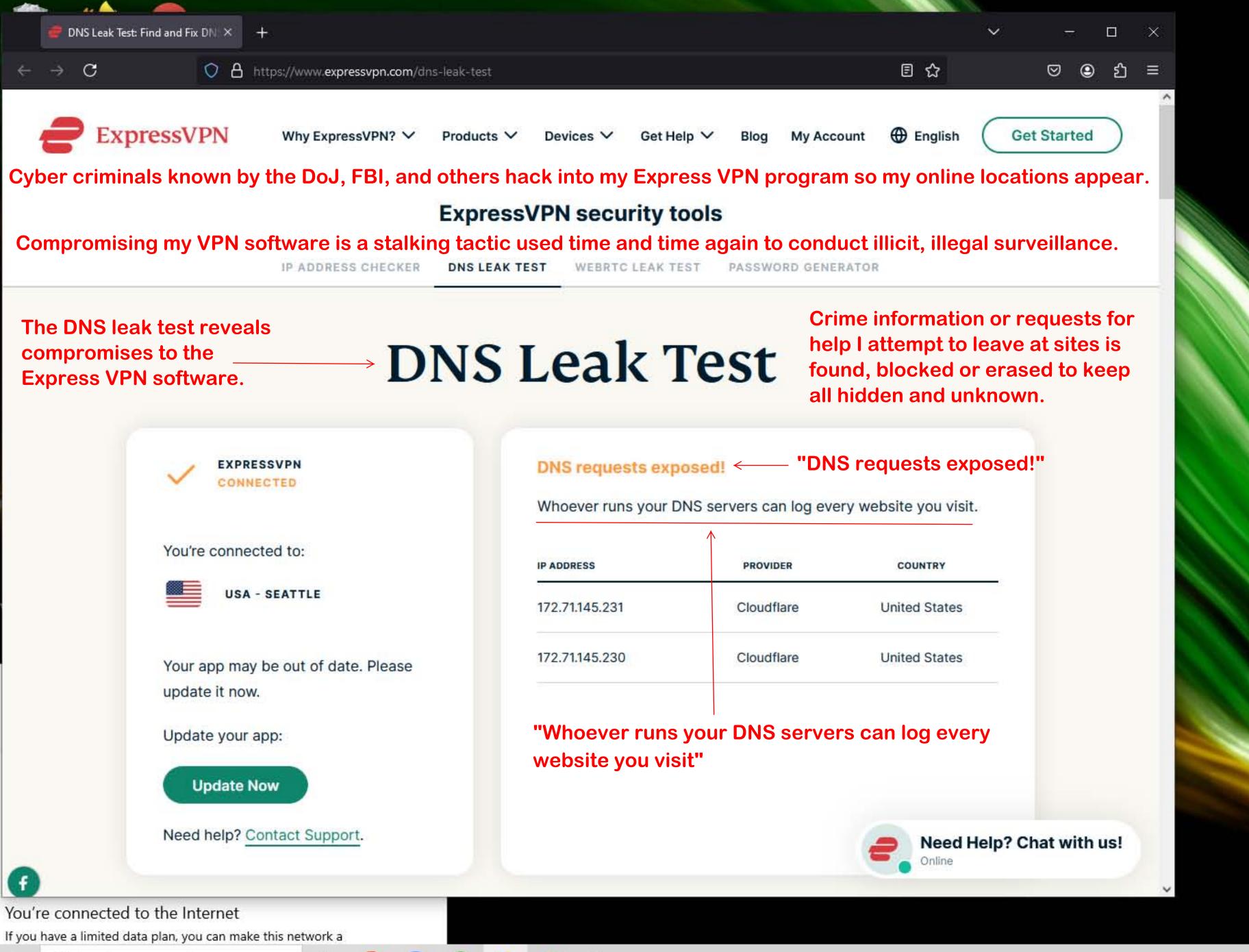2024-12-07 02:59:56.743 [NOTICE] Delaying directory fetches: DisableNetwork is set.

My encrypted browser was compromised to continue illegal online surveillance of my online activities,.
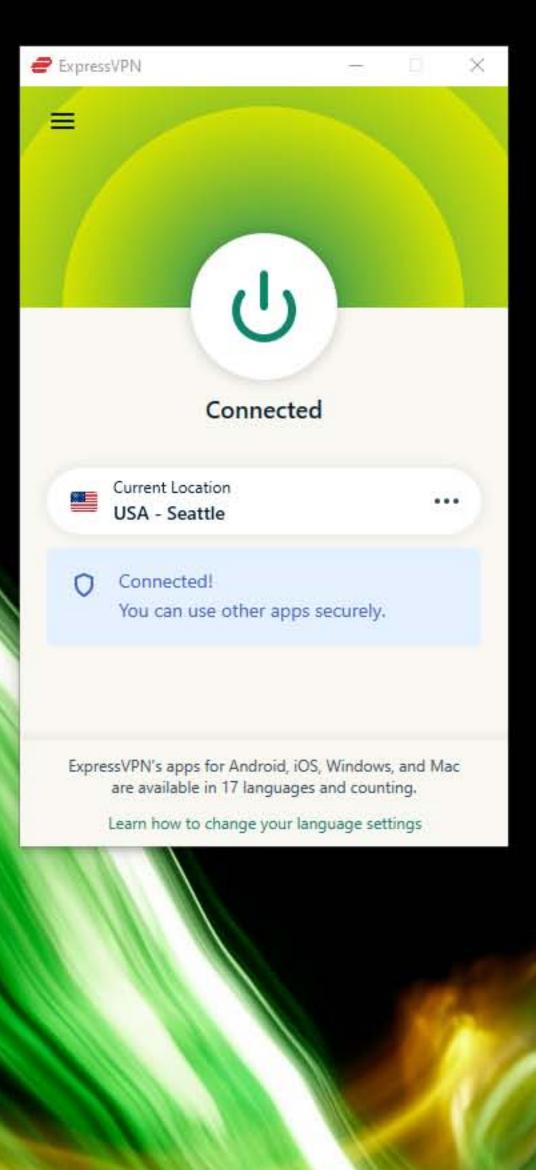
Encrypted Virtual Private Network Attack to Facilitate Illegal Surveillance and Cyber Attacks

Disabling my Virtual Private Network (VPN) has been a common tactic taken by the cyber criminals to facilitate their illegal online surveillance. Once again cyber criminals attacked my Express VPN program causing it to fail securely. Their attack disabled the function that hides my online location. The program is configured with a setting titled "DNS Leak Test" which reveals compromises which allow website addresses to be seen by prying eyes.

A DNS leak test exposed a breach rendering the VPN program useless for security. After their attack my Internet Protocol (IP) addresses previously hidden became visible, allowing every website I connected to be discovered. After their hack, every website I viewed became known and communication blocked if a threat of exposure arose.

Disabling my VPN has been a repeated tactic of the cyber criminals, having made attacks dozens of times.   As I have documented in great detail, law enforcement at all levels ignored my pleas for intervention.

Cyber criminals known by the DoJ, FBI, and others hack into my Express VPN program so my online locations appear.

Compromising my VPN software is a stalking tactic used time and time again to conduct illicit, illegal surveillance.

The DNS leak test reveals compromises to the Express VPN software.

Crime information or requests for help I attempt to leave at sites is found, blocked or erased to keep all hidden and unknown.

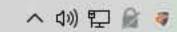"DNS requests exposed!"

"Whoever runs your DNS servers can log every website you visit"

ExpressVPN security tools

IP ADDRESS CHECKER   DNS LEAK TEST   WEBRTC LEAK TEST   PASSWORD GENERATOR

DNS Leak Test

EXPRESSVPN
CONNECTED

You're connected to:

🇺🇸 USA - SEATTLE

Your app may be out of date. Please update it now.

Update your app:

Update Now

Need help? Contact Support.

DNS requests exposed!

Whoever runs your DNS servers can log every website you visit.

IP ADDRESS	PROVIDER	COUNTRY
172.71.145.231	Cloudflare	United States
172.71.145.230	Cloudflare	United States

Need Help? Chat with us!
Online

ExpressVPN

Connected

Current Location
USA - Seattle

Connected!
You can use other apps securely.

ExpressVPN's apps for Android, iOS, Windows, and Mac are available in 17 languages and counting.

Learn how to change your language settings

You're connected to the Internet
If you have a limited data plan, you can make this network a

Blocked From Connecting to ExpressVPN Support

This screen shot reveals my failed attempt to contact the Express VPN support staff seeking help to repair the DNS leak. Cyber criminals blocked my connection to the support portal through the Express VPN software.

"Unable to send"

Cyber criminals blocked my attempt to contact ExpressVPN support to report the DNS leak.

The cyber attack prevented me from sending this report explaining the disabling cyber attack to ExpressVPN support.