Things you should NEVER see from an ethical ISP (but witnessed AGAIN during last 24 hours from mine):

1. DNS lookups supplied by your ISP's DNS servers in <u>excess</u> of 10,000 milliseconds.

Failed or substantially delayed DNS lookups cause a substantially worse user experience...and it's <u>solely</u> at the hands of the ISP, not the website.

Delays of this magnitude can also be associated with distributed denial of service attacks (DdoS) on your home network. When a router (or server) is overloaded with requests from multiple servers (see #2 and #4) it is unable to respond timely to the requests.

2. DNS Leaks to several of your ISP's own servers:

DNS IP: 76.96.15.85

Hostname: sjos-cns11.nlb.sjc1.comcast.net

ISP: Comcast Cable

Country: United States

City: San Jose

Looks like your DNS might be leaking...

Your IP: 71.198.229.17

DNS IP: 76.96.15.83

Hostname: sjos-cns10.nlb.sjc1.comcast.net

ISP: Comcast Cable

Country: United States

City: San Jose

Looks like your DNS might be leaking...

Your IP: 71.198.229.17

DNS IP: 76.96.15.65

Hostname: sjos-cns01.nlb.sjc1.comcast.net

ISP: Comcast Cable

Country: United States

City: San Jose

Looks like your DNS might be leaking...

Your IP: 71.198.229.17

DNS IP: 76.96.15.69

Hostname: sjos-cns03.nlb.sjc1.comcast.net

ISP: Comcast Cable

Country: United States

City: San Jose

If you see this, sign up for a a VPN service immediately. This suggests your home network has been targeted for surveillance and distributed denial of service attacks.

3. Diagnosis from a packet scan on your home network using a tool such as wireshark that a "bot" has been installed on your home network and that it's executing packet overflow attacks:

https://static.golftraxx.com/newspress/Google_Pocket_COMCAST_Bot_Analysis.pdf

If this is discovered, IMMEDIATELY install a firewall router on your home network with ALL possible service patches to remediate the network, block the denial of service attacks wher possible by limiting inbound connections, and disable the bot as described by COMCAST:

https://static.golftraxx.com/newspress/rfc6561.pdf

4. Distributed Denial of Service Attacks:

When multiple servers connect to your network at the same time, they can execute what's known as a distributed denial of service attack. It basically overloads your network, or router or server with so many requests it cannot handle them. In step 2 you saw yesterday my home network was again connected to by no less than 5 COMCAST servers executing such an attack. Netflix is a quick and easy way to show your ISP you saw them doing it again when you have high speed internet.

5. Schedule an appointment from your ISP to come review your network security and privacy. You're paying them for it. Tell them you're experiencing terribly slow internet sometimes and sometimes DNS failures and believe that your internet activities are being surveilled.

6. If ISP chooses not to fix and cease and desist from such activities, report their activities to the FCC.

7. Suggest to the ISP that they start behaving like decent human beings and be accountable for their poor judgment and illegal and abusive actions.

8. Learn all you can about safeguarding your online experiences from surveillance, theft, and fraud. Take immediate action to limit your exposure:
https://www.zdnet.com/article/online-security-101-how-to-protect-your-privacy-from-hackers-spies-and-the-government/

Frank DeBenedetti
GolfTraxx.com