KEEPING YOU AND YOUR DEVICES SAFE ONLINE

Kyle Erickson
Sr. Solution Architect
ICT
University of Saskatchewan

BACKGROUND

- Started working at the University of Saskatchewan in 2009 with the Desktop Support group.
- Obtained certifications for Microsoft Windows, macOS, and GNU/Linux
- Significant experience professionally and informally working with end users on a variety of platforms.

WHAT DEVICES ARE WE TALKING ABOUT?

- Traditional computing devices such as desktops and laptops
- Modern computing devices such as phones and tablets.
- Smart TV’s or Appliances
- Smart home devices such as connected switches, light bulbs, or voice assistants.
- Personal network equipment such as a wireless router or access point.

KEEP YOUR DEVICES UP TO DATE

Keeping your devices up to date is one of the easiest ways to ensure your devices stay safe. A significant number of exploits target vulnerabilities that were already disclosed and fixed by the vendor.

Most devices have an option to automatically install updates, or at least regularly check for updates and notify you to install them.

WHAT DEVICES ARE WE TALKING ABOUT?

- Traditional computing devices such as desktops and laptops
- Modern computing devices such as phones and tablets.
- Smart TV’s or Appliances
- Smart home devices such as connected switches, light bulbs, or voice assistants.
- Personal network equipment such as a wireless router or access point.

QUESTIONS?

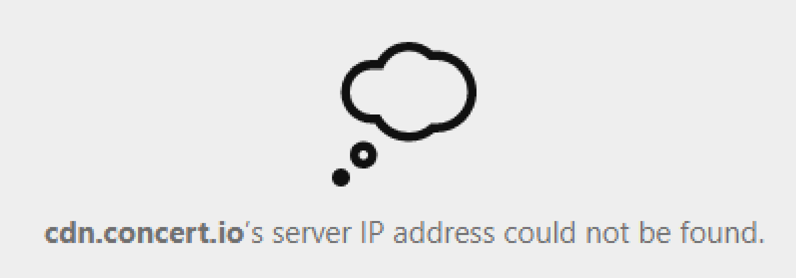
DNS FILTERING

Protect all* the devices in your home.

Some services go beyond malware and phishing and can also filter websites to make the internet more family friendly.

HOW DOES IT WORK?

- Your device asks a DNS server what the address is for phishing-website.com, and the server responds with a bogus address (like 0.0.0.0) and the connection fails.



cdn.concert.io's server IP address could not be found.

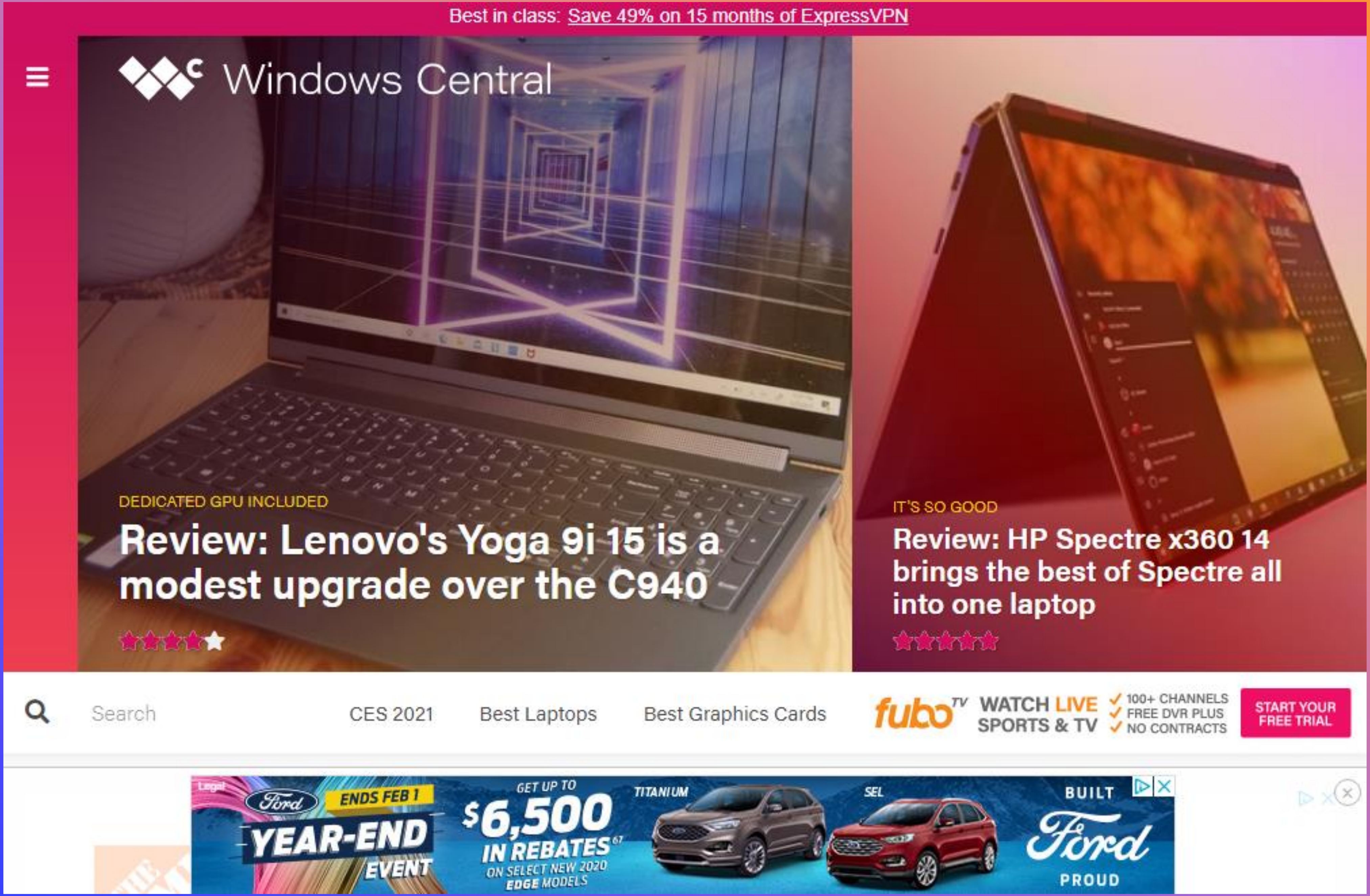
FILTERING SERVICES

- CIRA Canadian Shield - https://www.cira.ca/cybersecurity-services/canadian-shield
- Shaw BlueCurve Protected Browsing - https://support.shaw.ca/t5/internet-articles/bluecurve-home-faq-protected-browsing/ta-p/5455
- CloudFlare - https://developers.cloudflare.com/1.1.1.1/1.1.1.1-for-families
- Quad 9 - https://www.quad9.net/about/

QUESTIONS?

AD-BLOCKING

- Generally only possible on computers, phones, or tablets.
- Why?
  - Ad servers are targeted regularly and when compromised can serve malicious ads from trustworthy domains across thousands of websites at once.
- How do they work?
  - Usually installed as an “extension” to your web browser they filter content before it is loaded.



Windows Central

DEDICATED GPU INCLUDED

Review: Lenovo's Yoga 9i 15 is a modest upgrade over the C940

★★★★☆

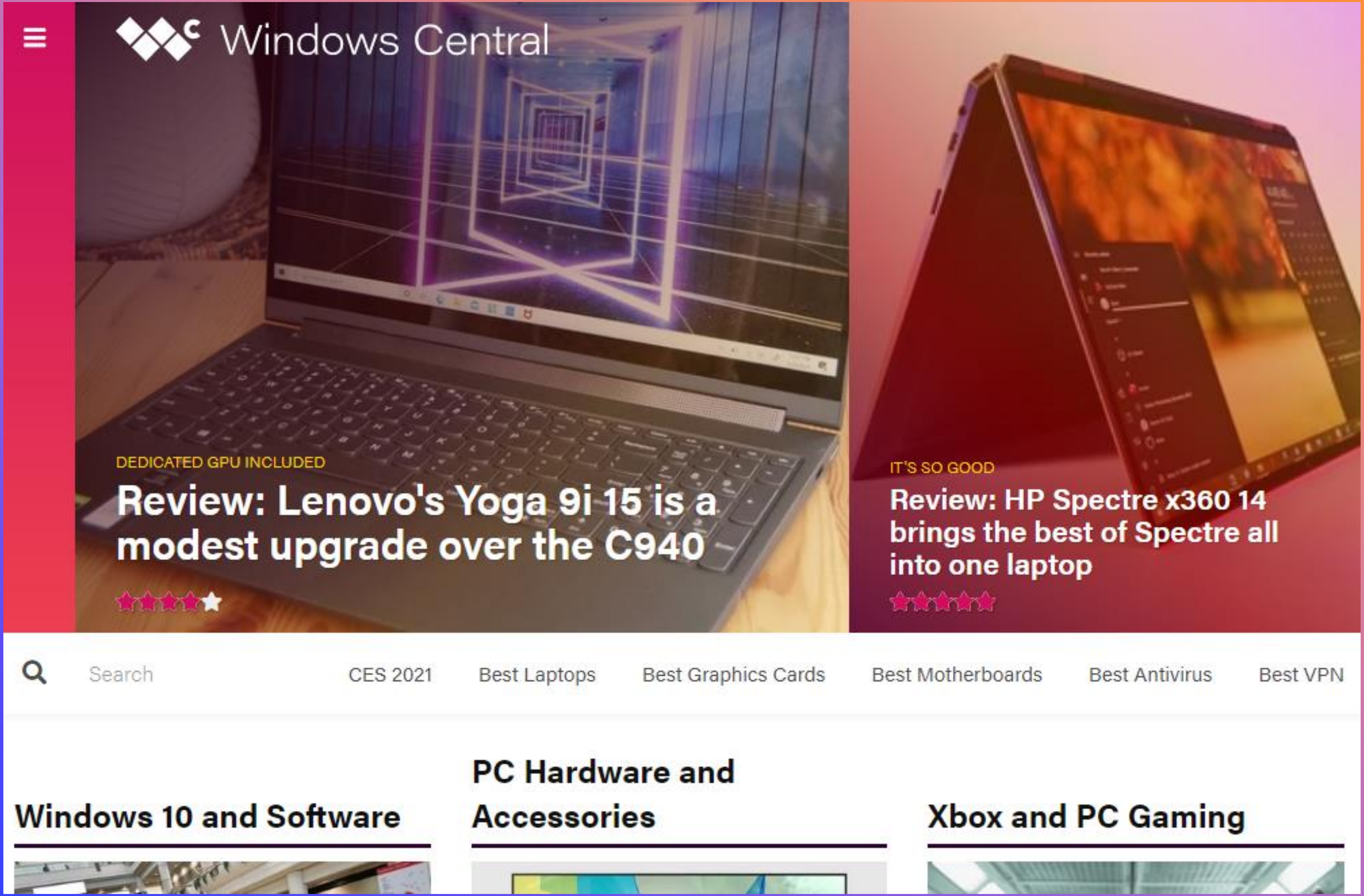
IT'S SO GOOD

Review: HP Spectre x360 14 brings the best of Spectre all into one laptop

★★★★★

Search

CES 2021 Best Laptops Best Graphics Cards



DEDICATED GPU INCLUDED

Review: Lenovo's Yoga 9i 15 is a modest upgrade over the C940

★★★★☆

IT'S SO GOOD

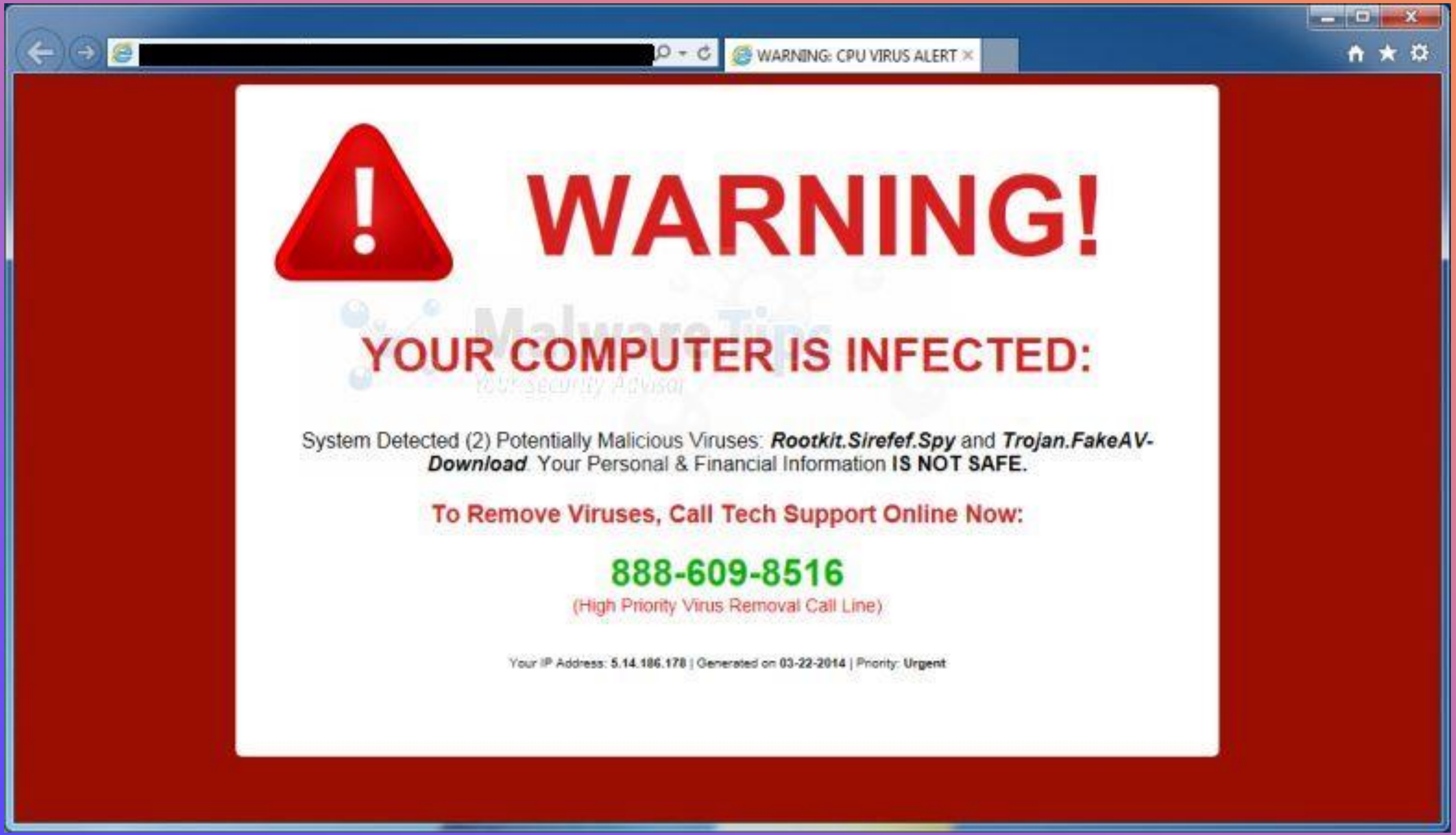
Review: HP Spectre x360 14 brings the best of Spectre all into one laptop

★★★★★

Windows 10 and Software

PC Hardware and Accessories

Xbox and PC Gaming



WARNING!

YOUR COMPUTER IS INFECTED:

System Detected (2) Potentially Malicious Viruses: ***Rootkit.Sirefef.Spy*** and ***Trojan.FakeAV-Download***. Your Personal & Financial Information **IS NOT SAFE.**

To Remove Viruses, Call Tech Support Online Now:

888-609-8516

(High Priority Virus Removal Call Line)

Your IP Address: **5.14.186.178** | Generated on **03-22-2014** | Priority: **Urgent**

AD-BLOCKING

- What about sites that rely on ads for revenue?
    - Blocking by default and adding websites to an “allow” list still provides additional protection for your device.

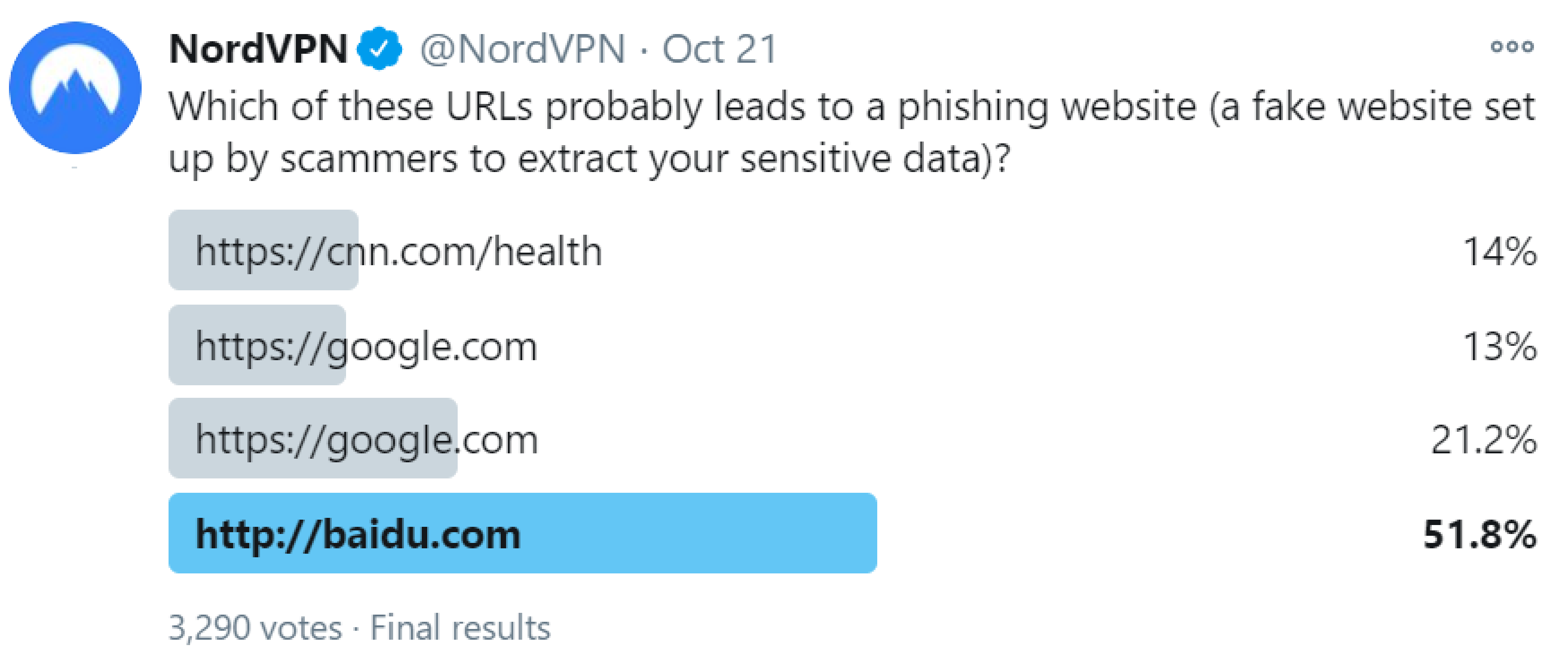
- Recommendations?
    - uBlock Origin
    - AdBlock Plus by Eyeo GmbH
    - AdGuard

QUESTIONS?

PASSWORD MANAGERS

- Can help prevent you from entering your credentials on a look-alike (phishing) website.
- Can help to eliminate password re-use across websites.

Which URL looks the most suspicious to you?



NordVPN @NordVPN · Oct 21

Which of these URLs probably leads to a phishing website (a fake website set up by scammers to extract your sensitive data)?

https://cnn.com/health 14%

https://google.com 13%

https://google.com 21.2%

http://baidu.com 51.8%

3,290 votes · Final results

RECOMMENDATIONS

- The password manager built into your web browser is okay to use, however these may be limiting.
  - For example, if you use Safari and iCloud Keychain it will synchronize your passwords across a Mac and iPhone, but you wouldn't be able to access them on an Android phone or tablet, or a Chromebook. Similarly, if you use Google Chrome's password manager you will only be able to access them when using the Chrome browser.
- Third party services like LastPass or BitWarden have free options that work in multiple browsers and can sync to multiple platforms. They also offer additional features at a cost. 1Password is a Canadian company based in Ontario that is extremely popular as well, and the cost is roughly $4 CAD per month (1password.ca).

QUESTIONS?

MULTI-FACTOR AUTHENTICATION

- Combines something you know (e.g. your password) with something you have (e.g. your cell phone).
- Even if you don’t use it everywhere, using it on high value accounts such as your email account can help to limit the damage if your password is compromised.

QUESTIONS?

WHAT ABOUT ANTIVIRUS?

- Windows and macOS include built-in protections that combined with DNS filtering and ad-blocking are likely sufficient.
  - These can be supplemented or replaced by free, freemium, or paid for solutions (e.g. Sophos Home, MalwareBytes).
- Google and Apple both scan their respective app stores for malicious content, and while malicious applications can get through, the best advice is to avoid installing unnecessary applications to reduce your risk.
- Keep the operating system and applications up to date!

OTHER ADVICE?

- Be skeptical of pop ups, alerts, text messages, emails, and phone calls.
  - Grammar or spelling mistakes are good indicators something is fake.
  - Demands (or offers) involving money or gift cards require additional caution.
  - Ask yourself if you were expecting a notification, email, etc., particularly for legitimate services such as Interac email transfers (or a shipping notification).
  - Don’t click links if you’re unsure. Navigate to the appropriate website, or call the company to ensure something is legitimate first.

QUESTIONS?