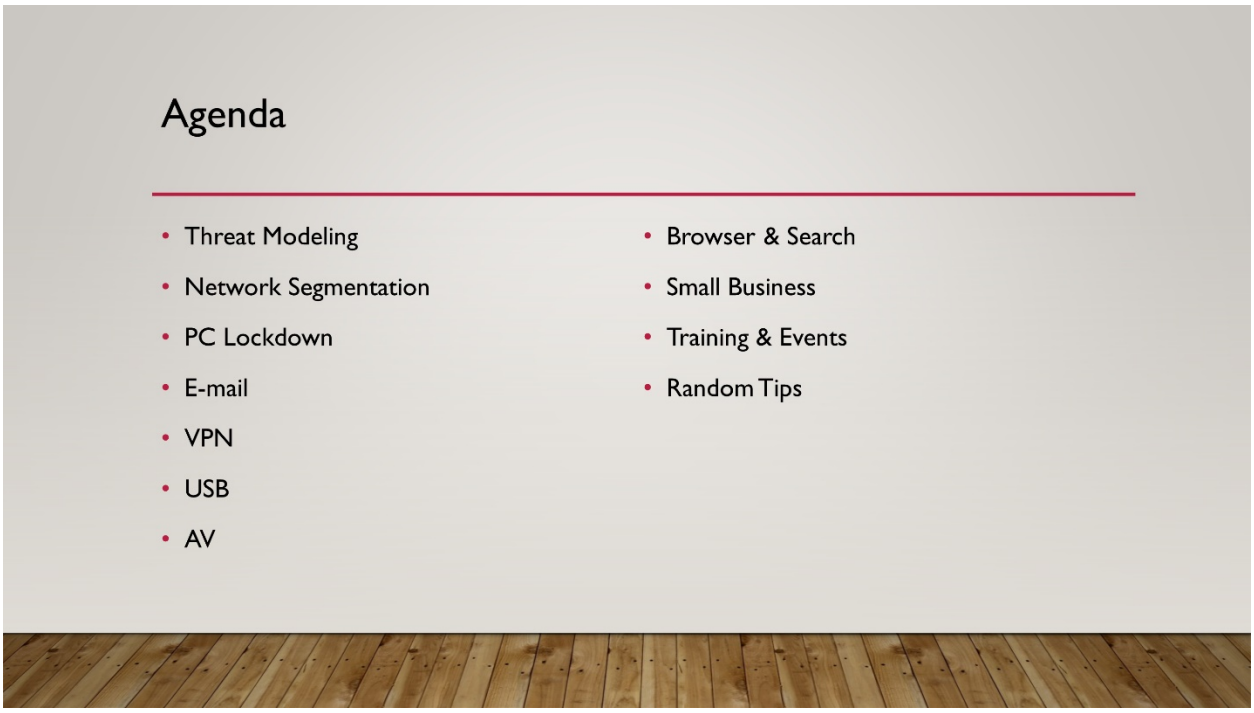

Maven
SECURITY CONSULTING
CYBER SELF-DEFENSE
For you,
your home,
and your small business.
By David Rhoades
https://MavenSecurity.com
@MavenSecurity


SPEAKER INFO
Bachelor of Science degree in Computer Engineering from the Pennsylvania State University (psu.edu).
Network, telecom, and web security assessments since 1996.
My email david.rhoades @ mavensecurity.com
Maven Security Consulting, Inc.
Assessments & training

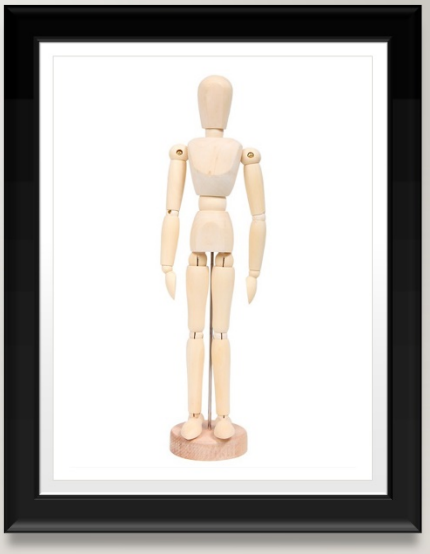


Staying secure in today's hyperconnected digital society requires more than anti-virus and software updates. This presentation will offer practical advice for **individuals**, **homes**, and **small businesses** with **actionable** steps to be more secure against current threats. Trendy buzzwords covered include: OPSEC, OSINT, privacy, PII, 2FA/MFA, IoT, Wi-Fi, Tor, VPN, and more (with plenty of lulz thrown in for good measure). The focus will be on free (or low cost) software and services, and operational security procedures that will enhance your ability to navigate an increasingly hostile digital landscape.

THREAT MODELING

- Threat modeling – The first step

- 知彼知己，百戰不殆
(if you know your enemies and know yourself, you will not be imperiled)
- Sun Tzu, Art of War



Security Plan – Answer these five questions

- What do I want to protect?
- Who do I want to protect it from?
- How bad are the consequences if I fail?
- How likely is it that I will need to protect it?
- How much trouble am I willing to go through to try to prevent potential consequences?

- Source: https://ssd.eff.org/en/module/your-security-plan

When building a security plan answer these five questions:
What do I want to protect?
Who do I want to protect it from?
How bad are the consequences if I fail?
How likely is it that I will need to protect it?
How much trouble am I willing to go through to try to prevent potential consequences? — https://ssd.eff.org/en/module/your-security-plan

NETWORK SEGMENTATION

Typically reserved for companies with an IT budget, or high-end tech users that grok RFC. But there's an easier option already on your network, and it's easy to configure.

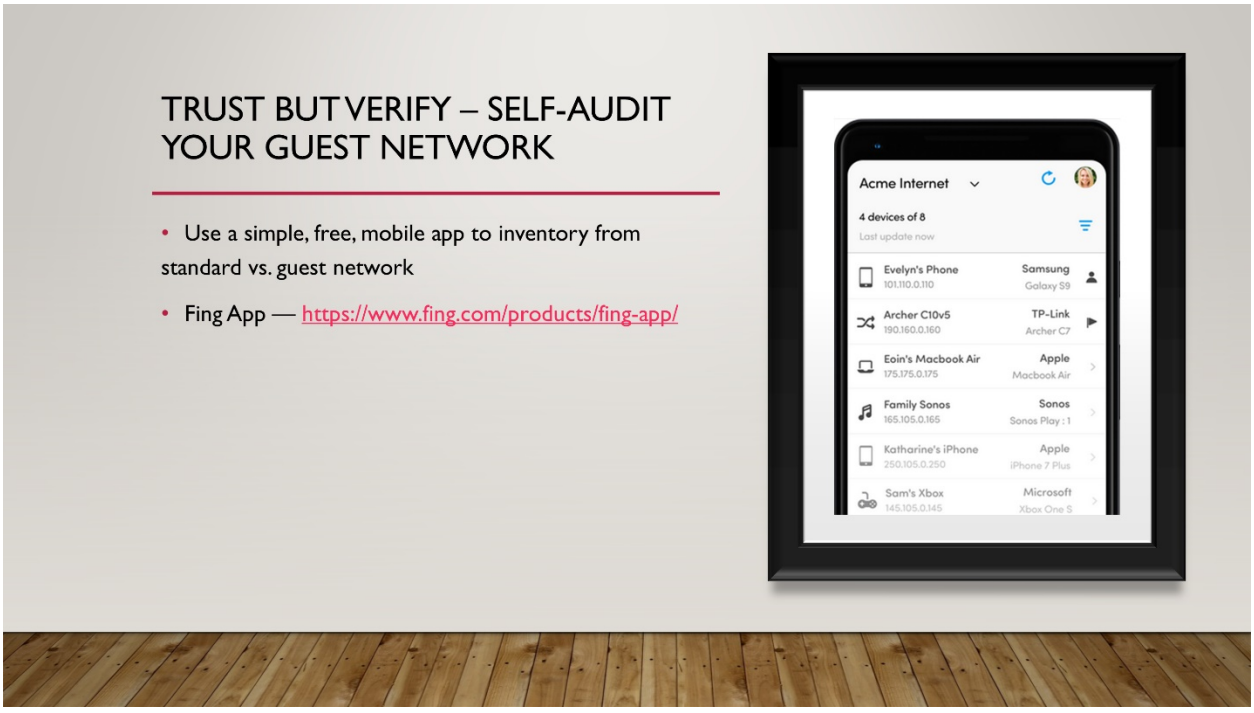
Network segmentation

- What: Put all your untrusted devices on a separate isolated VLAN segment…the easy way via Guest Network on your wireless router.
- Big win; small cost
- Guests can only talk to the Internet
- Guests can't
  - Talk to the router
  - Talk to each other
- Con: not appropriate for devices that need to talk to others (NAS, TV controlled via mobile app)

Guests can't

- Talk to the router – most routers have security issues, so it is best if network guests can't connect at al
- Talk to each other –

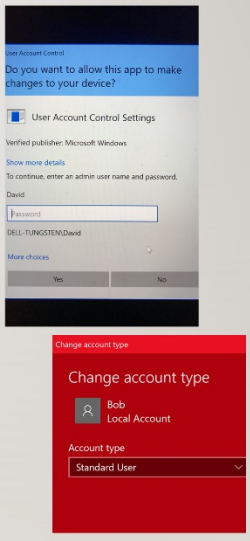
"Guest network" isolation is not to be confused with a similar feature that might be offered on your main network called 'AP isolation' or "wireless isolation".
But that means none of your devices can talk to each other, nor can they reach wired device (such as printers). It's probably best to use the Guest Network feature and put untrusted and one-way devices there.
You can use a simple network scanner app, such as Fing, on your mobile device to test that your guest network is isolating each connected device.
Lock Down Your Wi-Fi Network With Your Router's Wireless Isolation Option — https://www.howtogeek.com/179089/lock-down-your-wi-fi-network-with-your-routers-wireless-isolation-option/
Network segmentation - Wikipedia — https://en.wikipedia.org/wiki/Network_segmentation



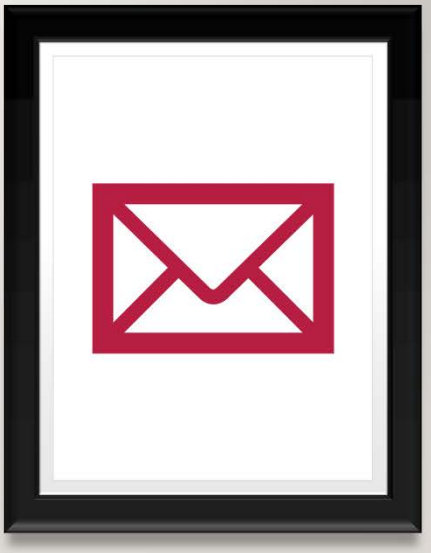
The best thing you can do for those in your (cyber) care is to disable their ability to destroy their own computer by mistake.
In Microsoft Windows this means removing

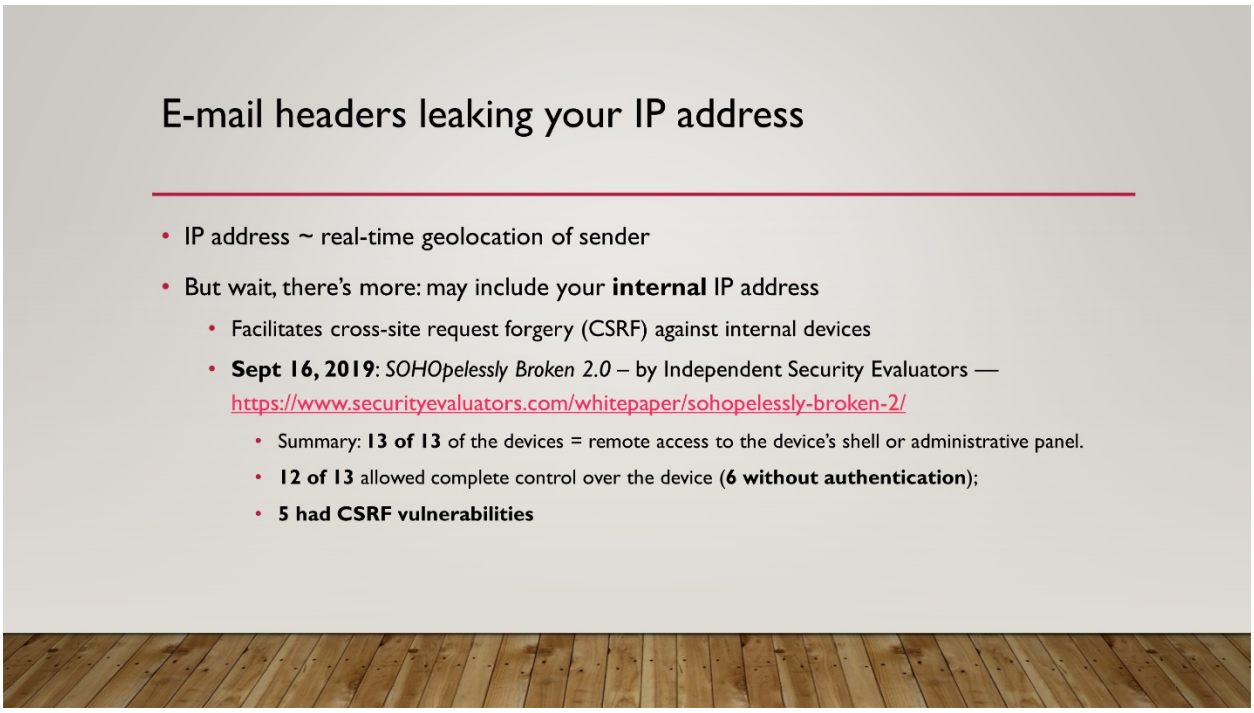
STANDARD USER

- If the PC only needs one account then create two:
- Admin one for periodic use (i.e. remote support person)
- Standard (non-admin) one for the actual user



E-MAIL





Summary: **13 of 13** of the devices (SOHO router and NAS devices) had vulnerability that **allowed remote access to** the device's **shell** or device's **administrative panel**.
12 of 13 of the devices **allowed complete control** over the device (**6 without authentication**);
5 had CSRF. Knowing the internal IP scheme – if changed from the default – is super helpful during the attack…thanks e-mail headers!

Self-Audit E-mail for IP leaks

- Determine if you are giving up your
  - External IP address (~ real-time geolocation)
  - Internal IP address
- Self-Audit: Email Leak Tests — http://emailipleak.com/

E-mail Security Checklist

- Disable auto-accept of calendar invites
  - Gmail - http://bit.ly/350Lw9Y
  - Outlook - http://bit.ly/34Q1Gmn
- Consider e-mail with better security & privacy options [Top 5]
  - Proton Mail https://protonmail.com/security-details
  - CounterMail, Hushmail, Mailfence, Tutanota: http://bit.ly/34R940L

Calendar spam has been in the news lately (Aug 2019).
Oh snap, Gmail didn't make the top 5 of email solutions focused on privacy. Oh well, maybe next year. ;-)
https://youtu.be/oPwrodxghrw – Missed it by that much

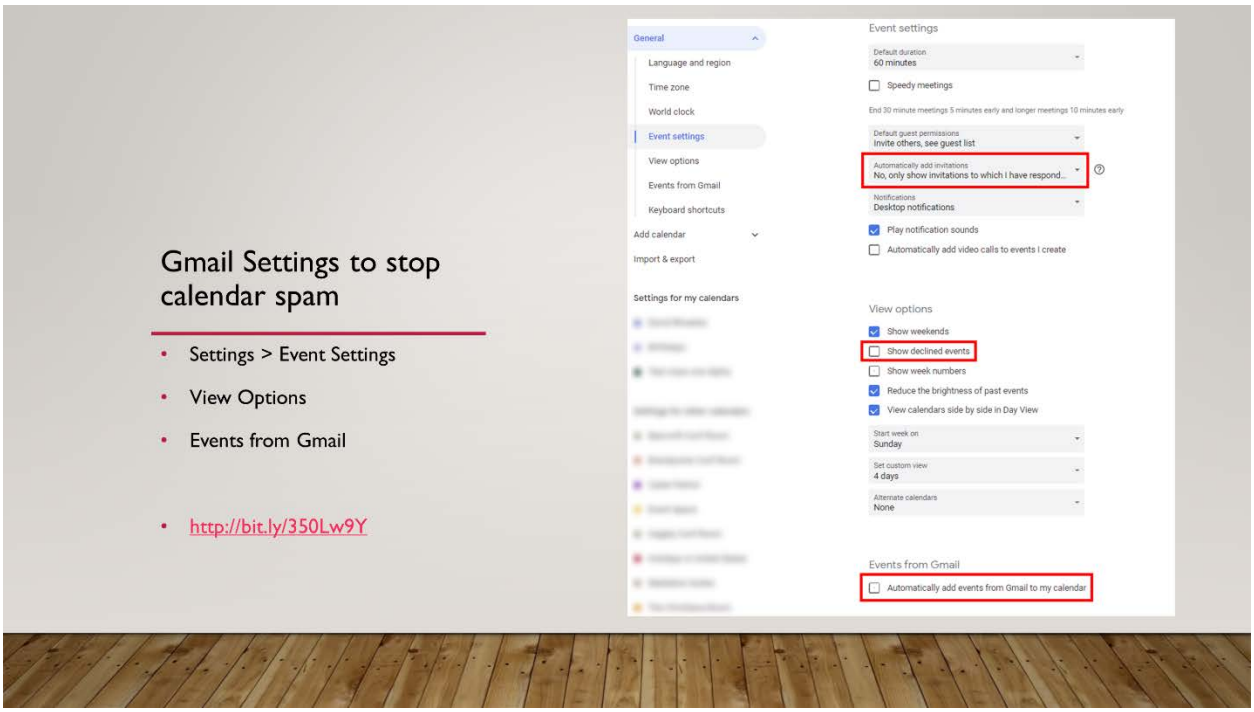


Image: David Rhoades
Instructions: http://bit.ly/350Lw9Y

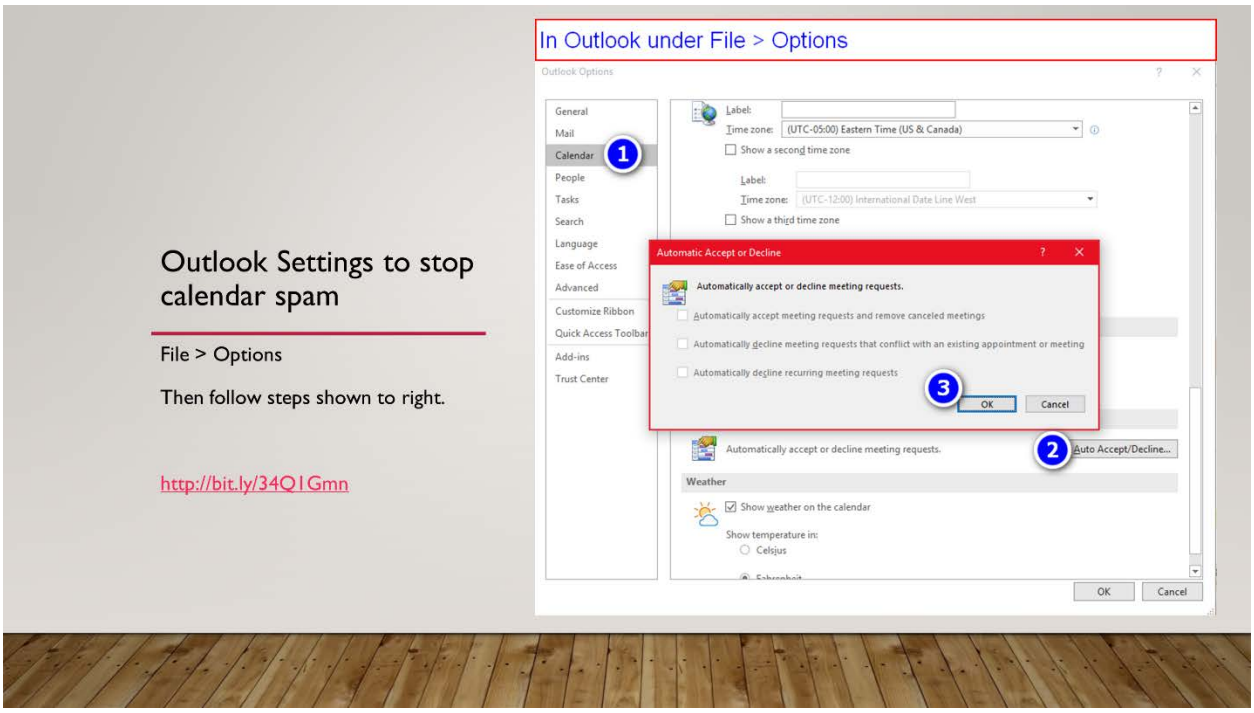
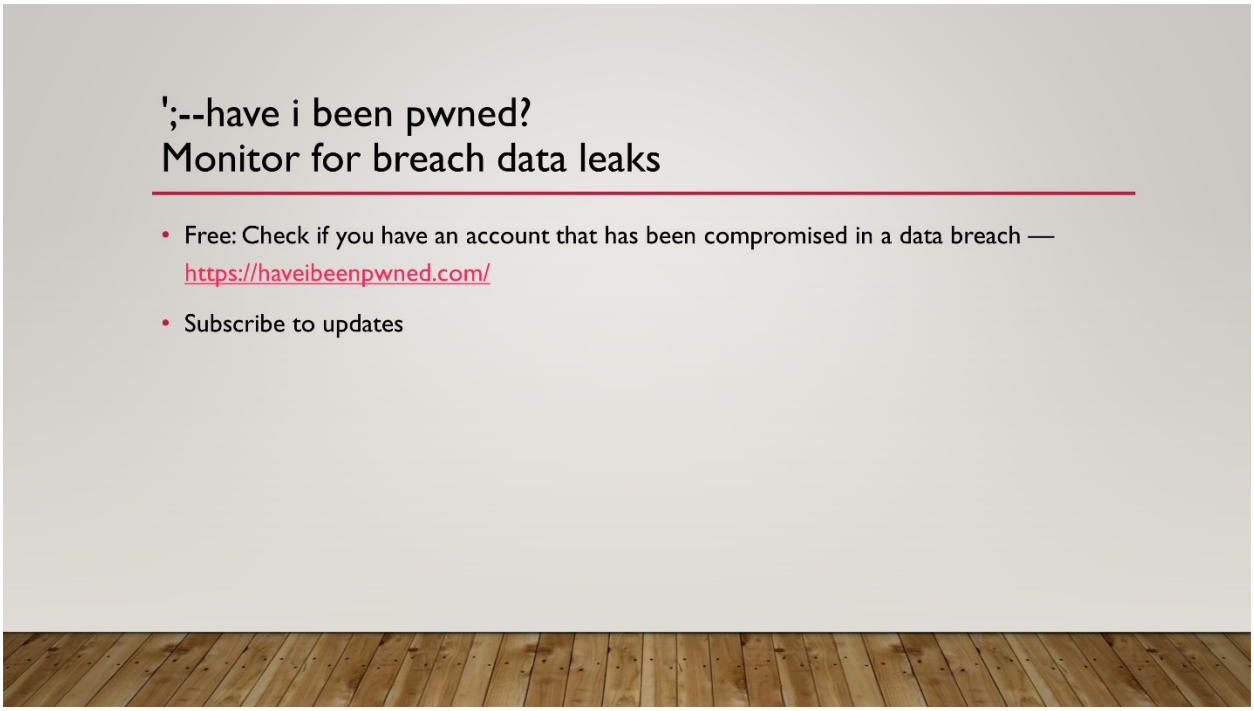


Image: David Rhoades
Instructions: http://bit.ly/34Q1Gmn



Series of tubes - Wikipedia — https://en.wikipedia.org/wiki/Series_of_tubes

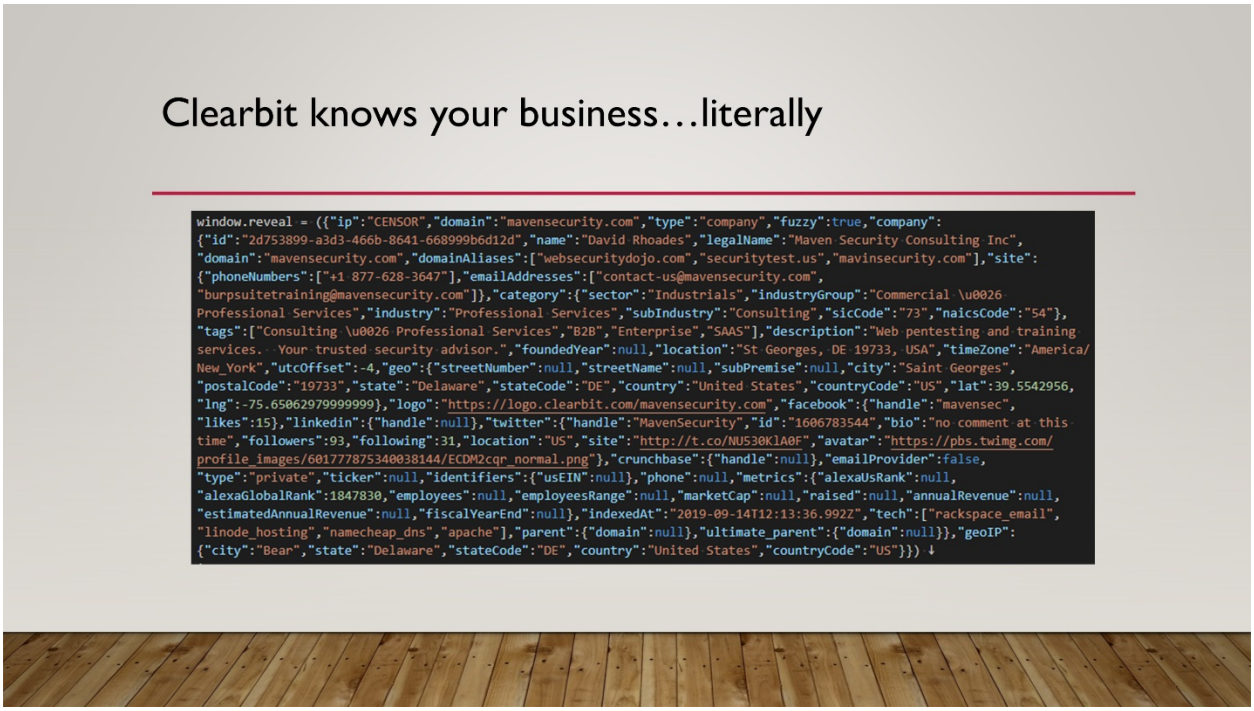
VPN – Virtual Private Network

- Your own private tube.
- Pipes all your traffic (e.g. DNS) from the weakest location (your LAN/Wi-Fi) to another location before dumping it out onto the Internet.
  - Adds integrity and confidentiality to non-encrypted traffic (e.g. DNS)
  - Add privacy to you by hiding your Ip address (i.e. ~ geo-location)
- Objection: I don't need a VPN because…reasons.

Myth – Private Mode Browsing

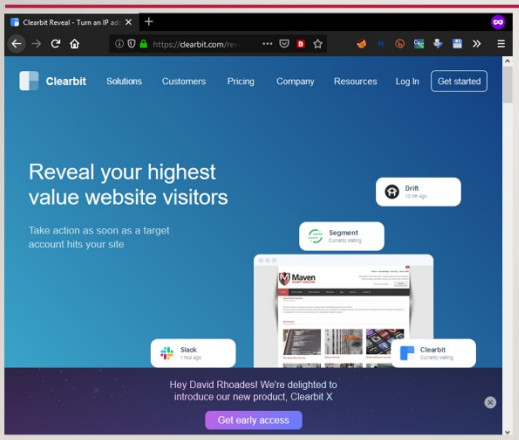
- Claim: You are using a web browser in Incognito/Private mode. So now your anonymous, right?
- Busted: There are various ways to fingerprint and identify you while you're in "private" more [note the "air" quotes]
  - Your **source IP address** is also being tracked, correlated, and sold. https://clearbit.com/reveal
  - Various browser "features" can be leveraged to track you (besides cookies)
    - [more details under **Browser** section]

Your IP history for sale (sort of):



This is from my home office IP, which does change periodically. Yet Clearbit is still able to find and track me based on my current IP address.
Not only do they know my name, they know my business info.
93 followers on Twitter #HumbleBrag ;-)

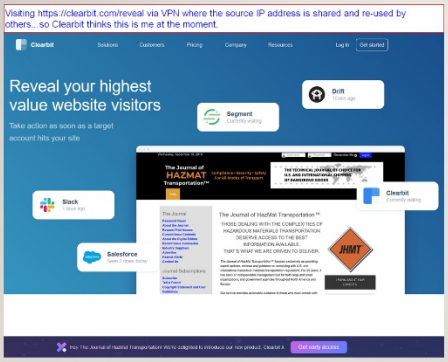
Clearbit – Look ma' cookie-free ~~stalking~~ tracking



- Based only on my source IP address.

Winning hearts and minds…not! #Creepy

Clearbit – Fun with VPNs



- See who used your VPN IP address recently.

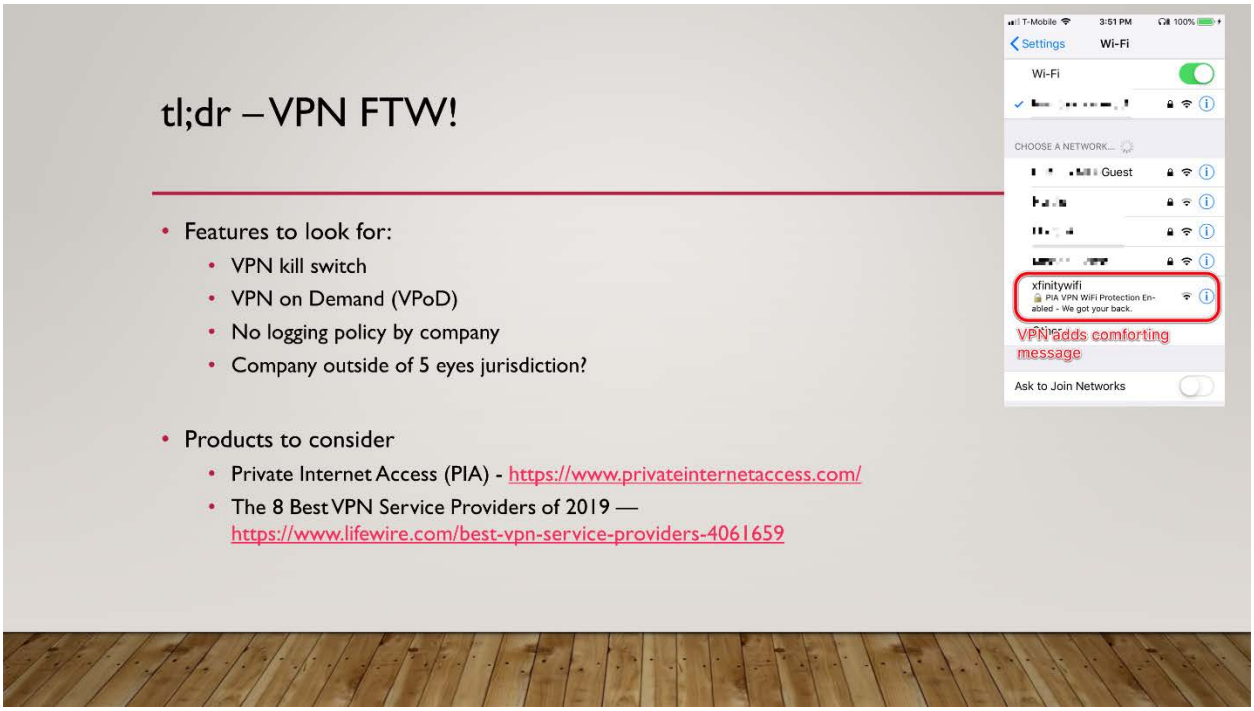
Myth – HTTPS

- Claim: I use HTTPS for everything so I'm fine, right?
- Busted: Nope. Sensitive traffic is not always encrypted
  - Are you sure your **email** is encrypted in transit?
  - DNS is not (currently) encrypted = privacy and integrity (spoofing) risks
  - Evil twin (wireless networks) - Wikipedia — https://en.m.wikipedia.org/wiki/Evil_twin_(wireless_networks)
  - Besides it only takes one piece of non-https CDN content on a site to spoil the whole thing

Myth – "Secure" public Wi-Fi is secure

- Claim: It's like…network segmentation…encrypted…unique initialization vector (IV)…like a VLAN
- **Seriously?**
- Busted: Common tools (Wireshark) if they observe your wireless handshake can then decrypt all your traffic...
- …unless you are using transport encryption (HTTPS, SSH, SFTP) **or a VPN**.

Pop Quiz – Name the two types of wireless networks
Answer: Bad (most “encrypted” ones) and worse (open; no encryption)
HowToDecrypt802.11 - The Wireshark Wiki — https://wiki.wireshark.org/HowToDecrypt802.11
Wireshark can be configured to observe a Wi-Fi handshake and then decrypt subsequent traffic.
To capture a four-way WPA handshake the attacker will have to temporarily de-authenticate the victim from the wireless network. That's easy, and left as an exercise for the reader. ☺
Only traffic with transport-layer security (e.g. HTTPS, SSH, SFTP) are safe at this point.
A VPN can help protect you against this situation when using public (or private) Wi-Fi.



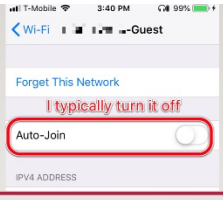
A VPN kill switch (or Internet kill switch) is a feature where the device will not pass traffic if the VPN is not present. This presents the user from accidentally exposing insecure traffic.
VPN on Demand (VPod) is a feature that enables the VPN connection whenever there is a request for traffic.
Traditionally, neither of these were an option for typical VPN settings on an iPhone. The user had to manually start the VPN (via several clicks into the device Settings). In addition, the device would happily continue to pass traffic even after the VPN crashed. Often the user would not notice the small [VPN] icon along the top edge of their screen had disappeared until after their traffic had been exposed across the network with the additional protection provided by a VPN.
Now, several VPN providers offer these features, even for iPhones.

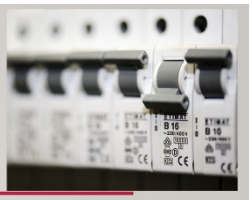
Myth: I use a VPN on my smart phone, so now I'm anonymous

- Nope
- OS and various/numerous background apps are authenticated – they know who you are, and now they know your new, temporary IP address.

- Next Level Solution: burner phone that you never use with your real identity.
- *Tinfoil hat sold separately*

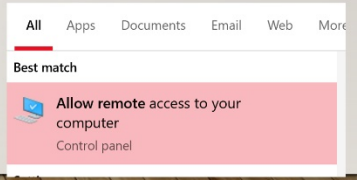
More Wi-Fi Tips





- Wire your devices were possible (e.g. printer).
- Turn off wireless access on wired devices (e.g. printers).
- Don't auto-join (public) wireless.
- DIY network segmentation = ~VLAN

- Windows OS:
  - treat all new networks as Public (so you don't share resources)
  - Settings > "Allow Remote Access" is off for Public networks



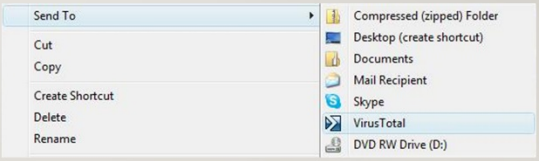
The fewer wireless access points means less interference from overlapping channels and better bandwidth.
Auto-joining wireless. I prefer manually joining specific networks as needed. I'm less likely to get punked by an evil twin impersonating a popular SSID (e.g. xfinitywifi).
If you don't use "Remote Access" then it's off. But if you do use it (while on a secure network of course) then turn it off when you travel.
Settings > "Allow Remote Access" is off for Public networks, or simply off when you are outside your office (assuming you use Remote Desktop to connect to that system)
Evil twin (wireless networks) - Wikipedia — https://en.wikipedia.org/wiki/Evil_twin_(wireless_networks)

Resource: Independent AV Reviews

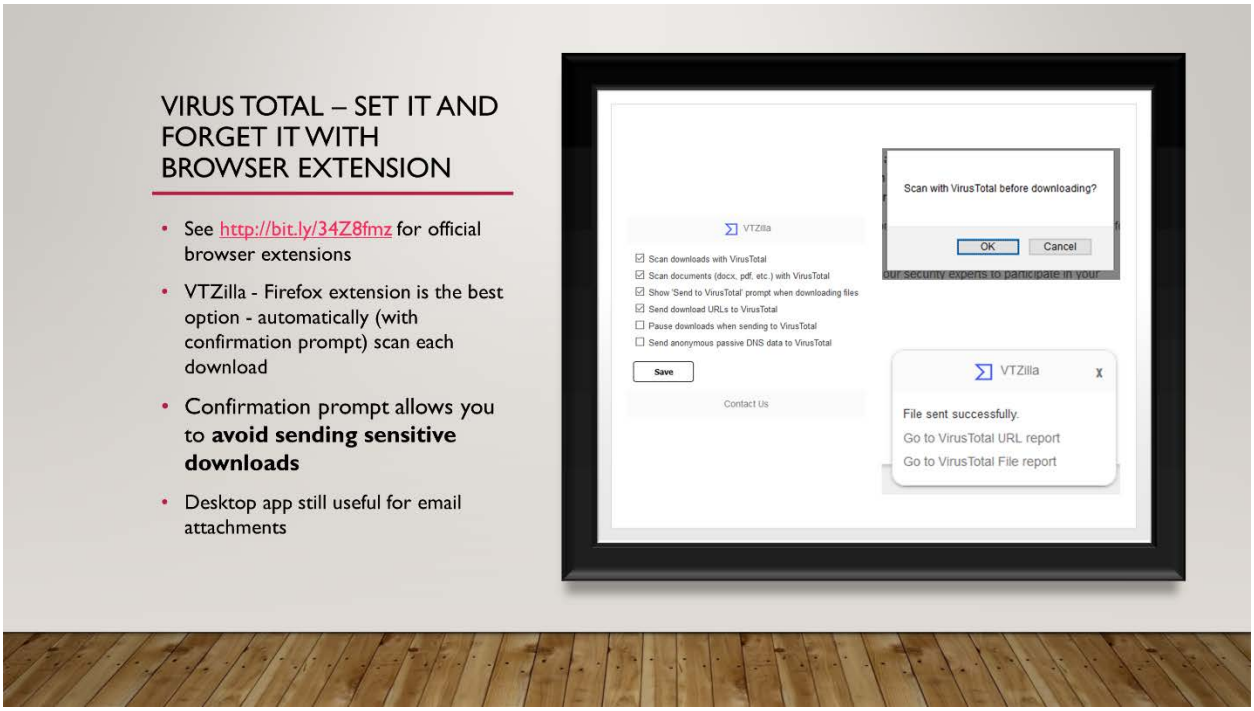
- AV-TEST | Antivirus & Security Software & AntiMalware Reviews — https://www.av-test.org/en/
- AV-Comparatives "…an independent organization offering systematic testing that checks whether security software, such as PC/Mac-based antivirus products and mobile security solutions, lives up to its promises." — https://www.av-comparatives.org/about-us/

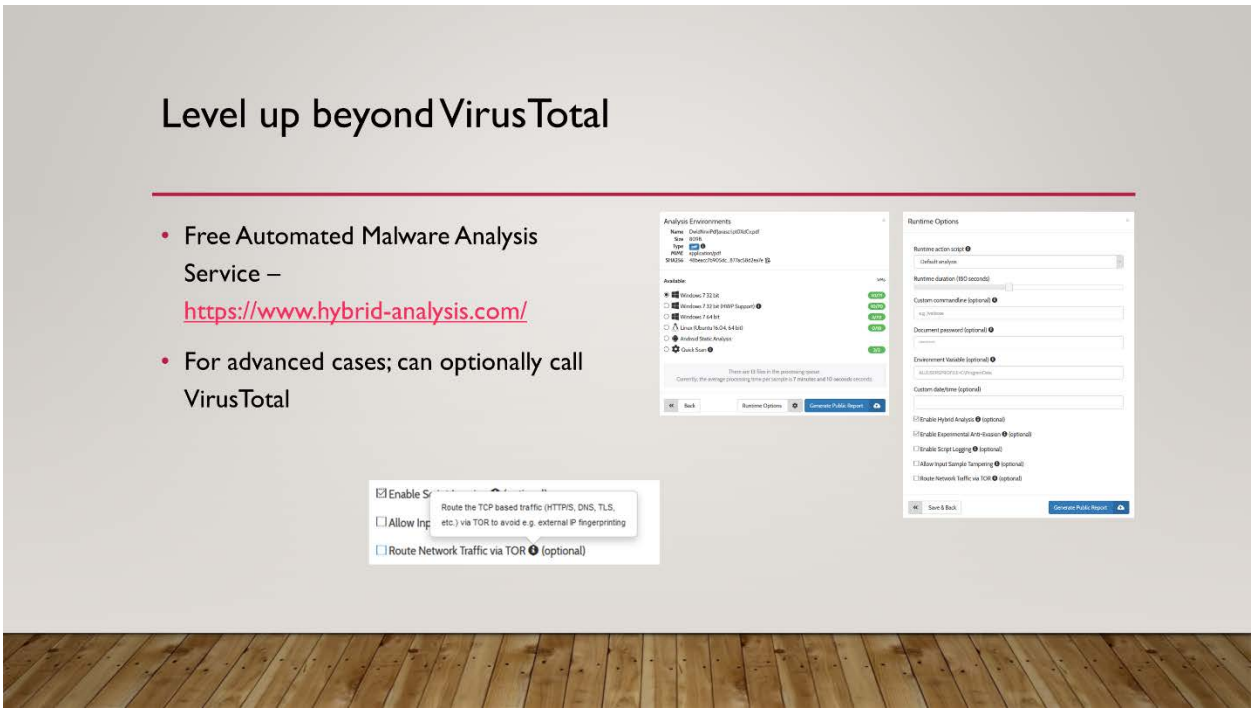
VirusTotal

- Which AV to use? All of the above!
- https://www.virustotal.com/
- I **highly recommend** the desktop install for Windows, Mac OS, or Linux.
  - Windows version adds **right-click** ease of use.
- There are 3rd party versions too.
- Tip: Use VirusTotal on **all** downloads and email attachments.
  - Well, **not** sensitive documents and proprietary stuff.



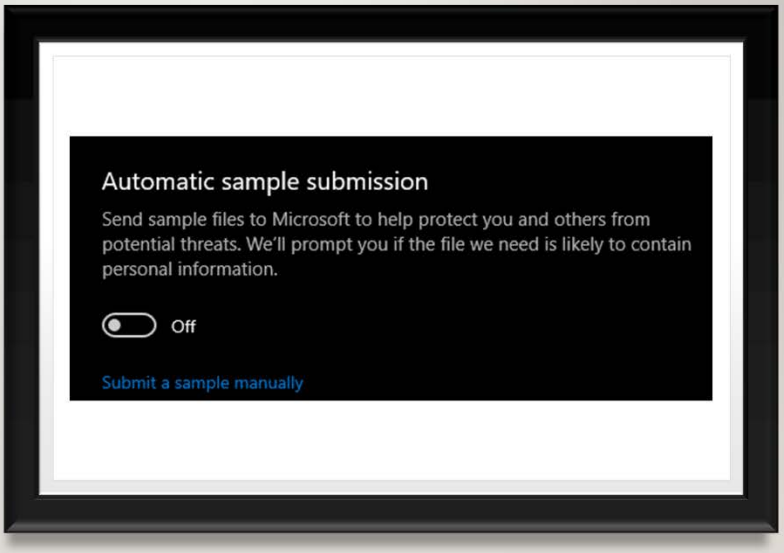
The desktop companion app is highly recommended because if it is not simple to send files to VirusTotal then you are not likely to use it. You want to get in the habit of sending all your downloads and email attachments. Your desktop AV is not as good as all of the industry's leading AVs.
You can find desktop companions for VirusTotal under the 9-dot logo in the upper-right corner of the site. Final URL is currently:
Desktop Apps – VirusTotal — https://support.virustotal.com/hc/en-us/articles/115002179065-Desktop-apps
As of Oct 2017 VirusTotal discontinued support for the official Windows uploader. However, it still works, and there is an open source alternative at https://github.com/SamuelTulach/VirusTotalUploader
One caveat about the official (but discontinued) version: it may say that your file is too large to upload. In that case surf to https://www.virustotal.com/ and try uploading it there, because the web interface handles larger files (500 MB) compared to the Windows app (128 MB).



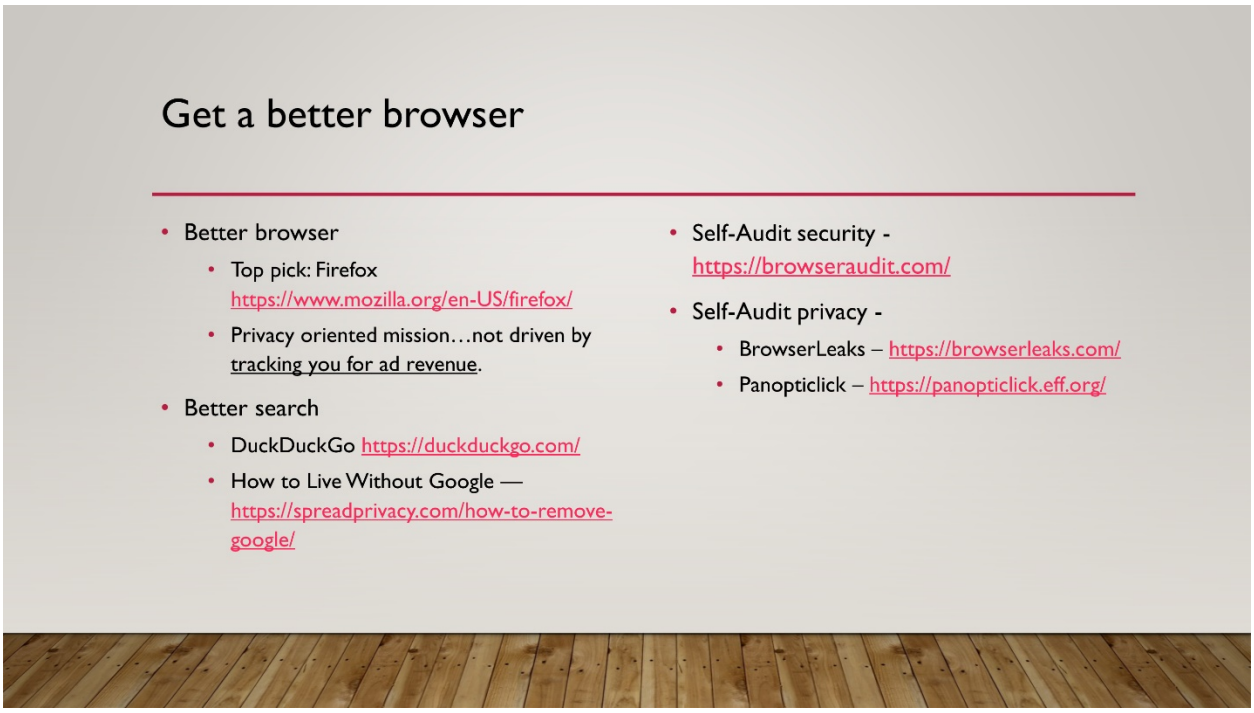


Sample at https://www.hybrid-analysis.com/sample/48beacc7b905dcbdcf992fef1d62a1ec1484c295db469adb2a7877ac58d2ea7e
Screenshot shows there was JavaScript running from PDF.
https://www.hybrid-analysis.com/sample/2818078484ec60ad7510106fdef02bf6b557a56c838132823251580b5bfde11b/5d840f8d028838d368ac17a6
Shows the PDF had web beacon in it making outbound connection to another site.

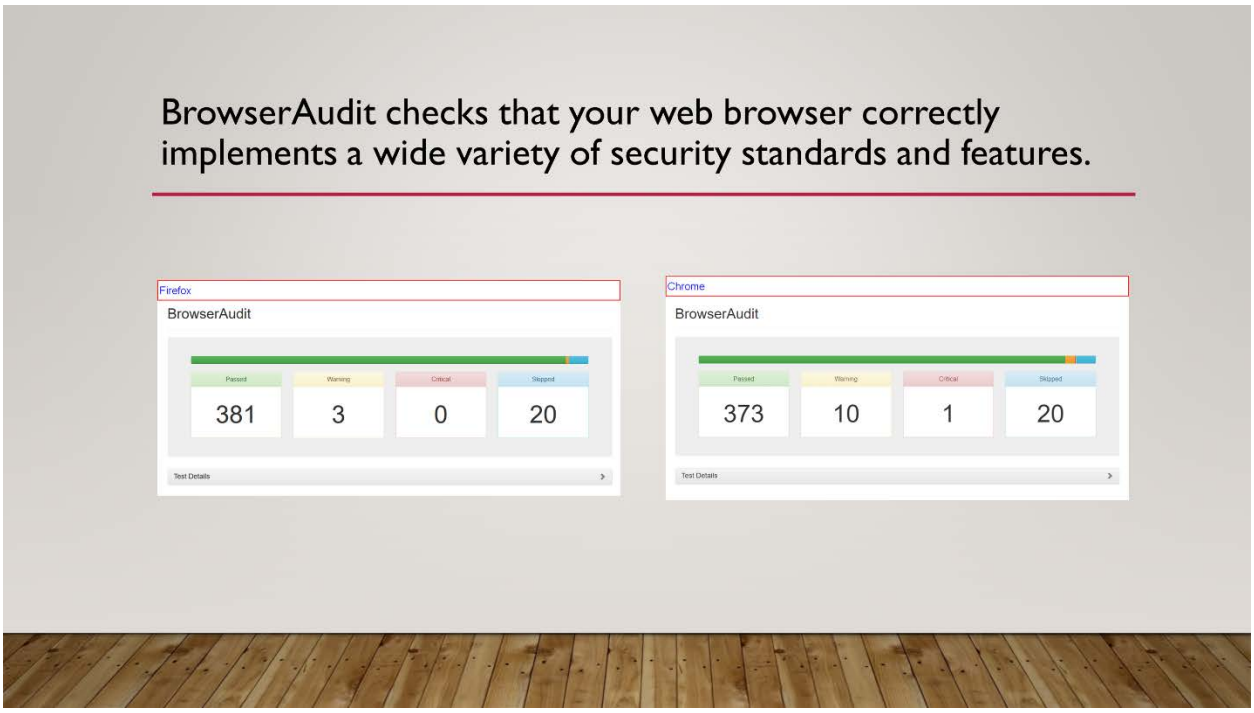
AV TIP: BE GREEDY - DON'T SHARE



Better browser



BrowserAudit checks that your web browser correctly implements a wide variety of security standards and features.
BrowserLeaks.com - Web Browser Security Checklist for Identity Theft Protection
* WebGL Fingerprinting
* HTML5 Canvas fingerprinting
* Font metric-based fingerprinting
* IP address / VPN detection

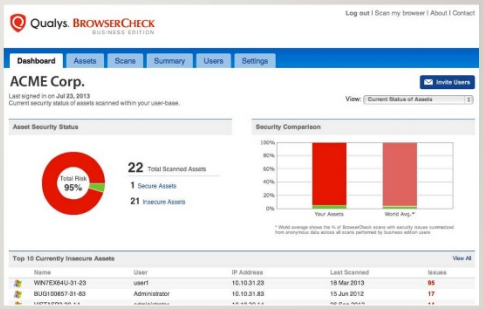


Quick test of Firefox vs. Chrome via BrowserAudit, which checks that your web browser correctly implements a wide variety of security standards and features.
BrowserAudit — https://browseraudit.com/

Security Test your Browser

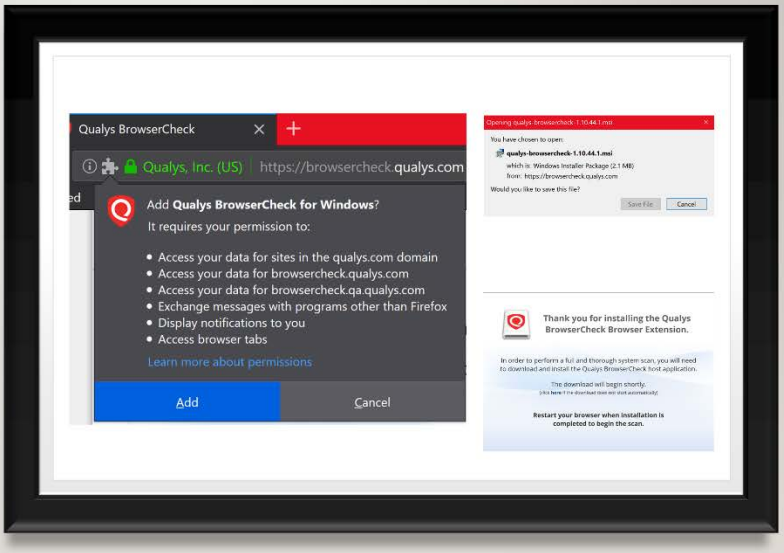
- https://browsercheck.qualys.com/
- Quick check without plugin
- More thorough with the plugin

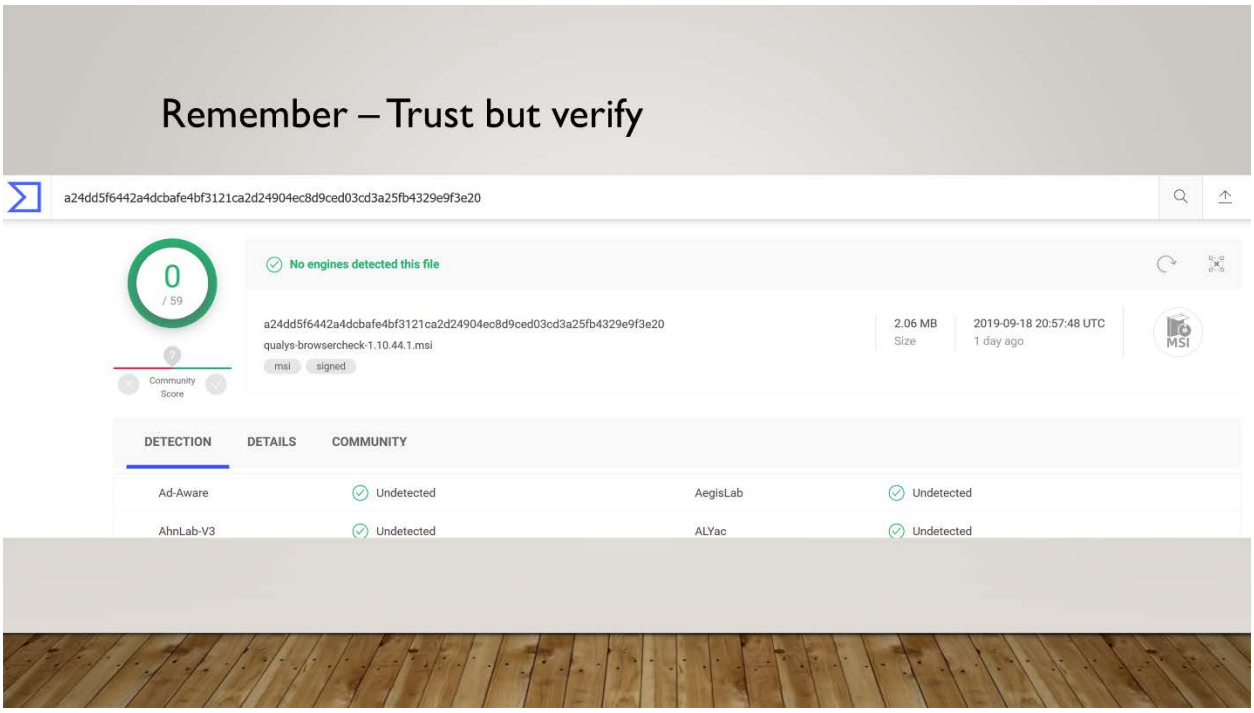
- https://www.qualys.com/free-tools-trials/browsercheck/
  - Personal (above)
  - Business (dashboard of all browsers)



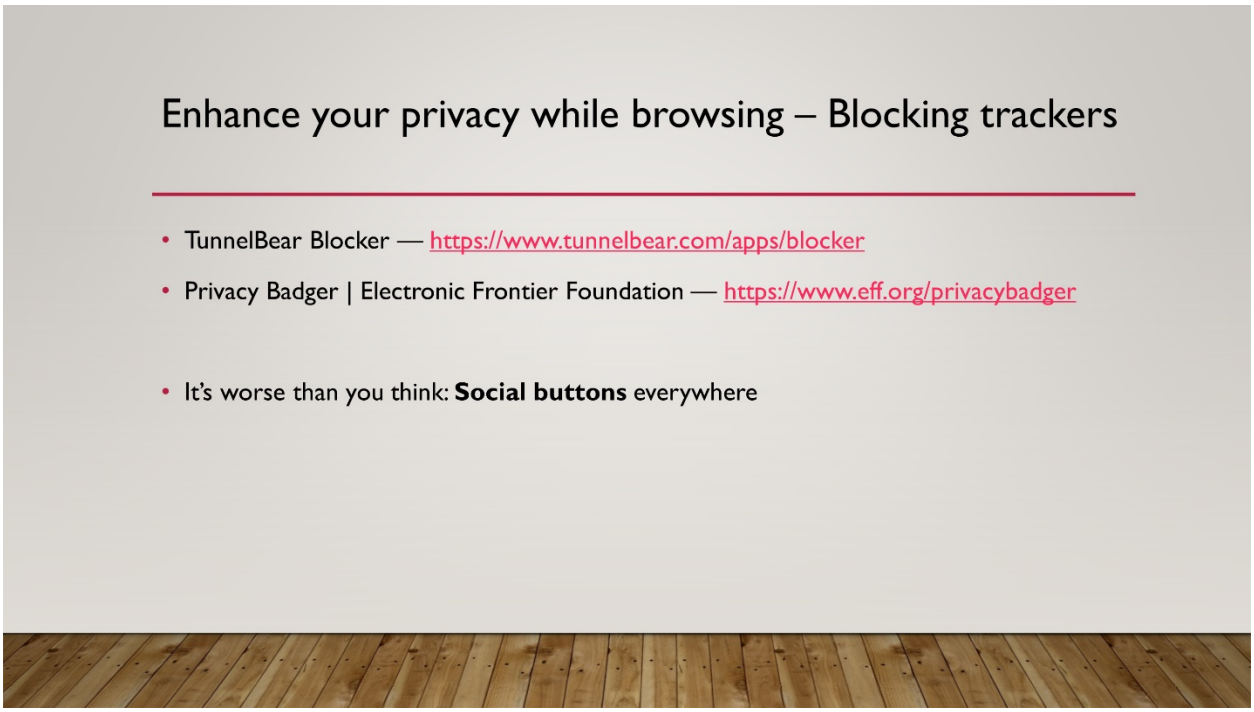
BROWSERCHECK PLUGIN

- But wait, there's more…
- Remember – every piece of software increases your attack surface.
  - Cost vs. Benefit

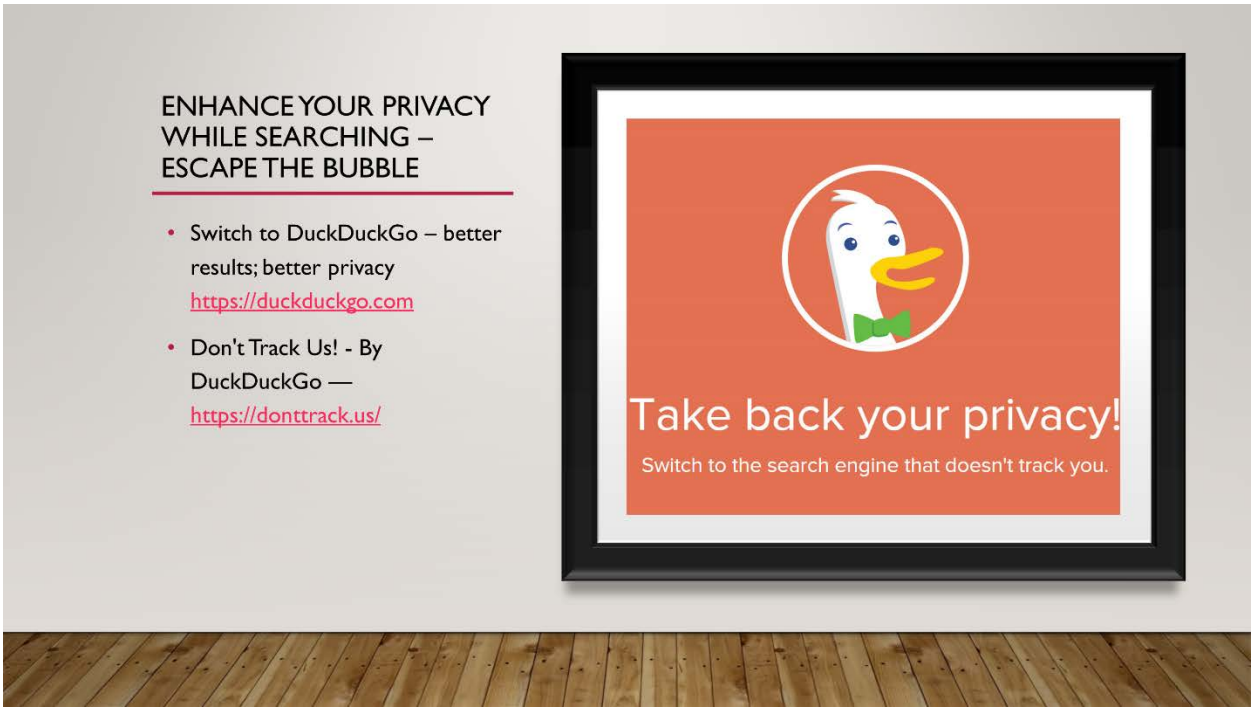




Remember to test all your downloads with VirusTotal.

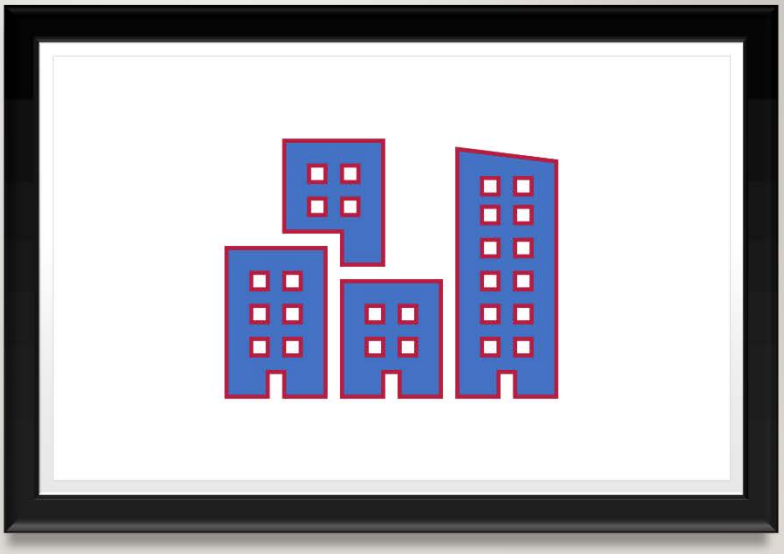


“What are social buttons?
Social buttons are widgets embedded within websites that allow users on web pages to “Like”, “Tweet”, and share those pages via social media. Whether or not you press these buttons or are a member of these services, they relay your browsing patterns back to those organizations. Many people would prefer if social media companies and advertisers did not have a profile of their website browsing.
What’s an example?
A user planning a surprise trip for his partner is browsing vacation resort websites, most of which feature social buttons. Despite not clicking on any of these buttons, targeted ads for these resorts and flight deals appear on future third-party web pages visited by his browser, and also start popping up on his Facebook timeline for the next week. This kind of tracking can feel pretty invasive, hard to evade, and stressful concerning the risk of the user’s partner finding out about his plans. “
Source: https://www.tunnelbear.com/blocker/info



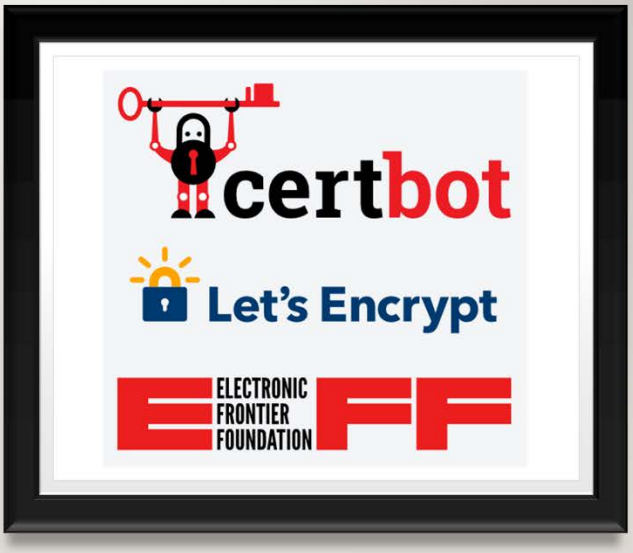
Filter bubble - Wikipedia — https://en.wikipedia.org/wiki/Filter_bubble
Filter bubble – a state of intellectual isolation

Small business



Small Business websites - HTTPS

- Non-HTTPs is a bad look (at best)
- Confidentiality – Eavesdropping, even on encrypted Wi-Fi is easy.
- Integrity - MITM attacker can inject malicious content
- Free - https://certbot.eff.org/

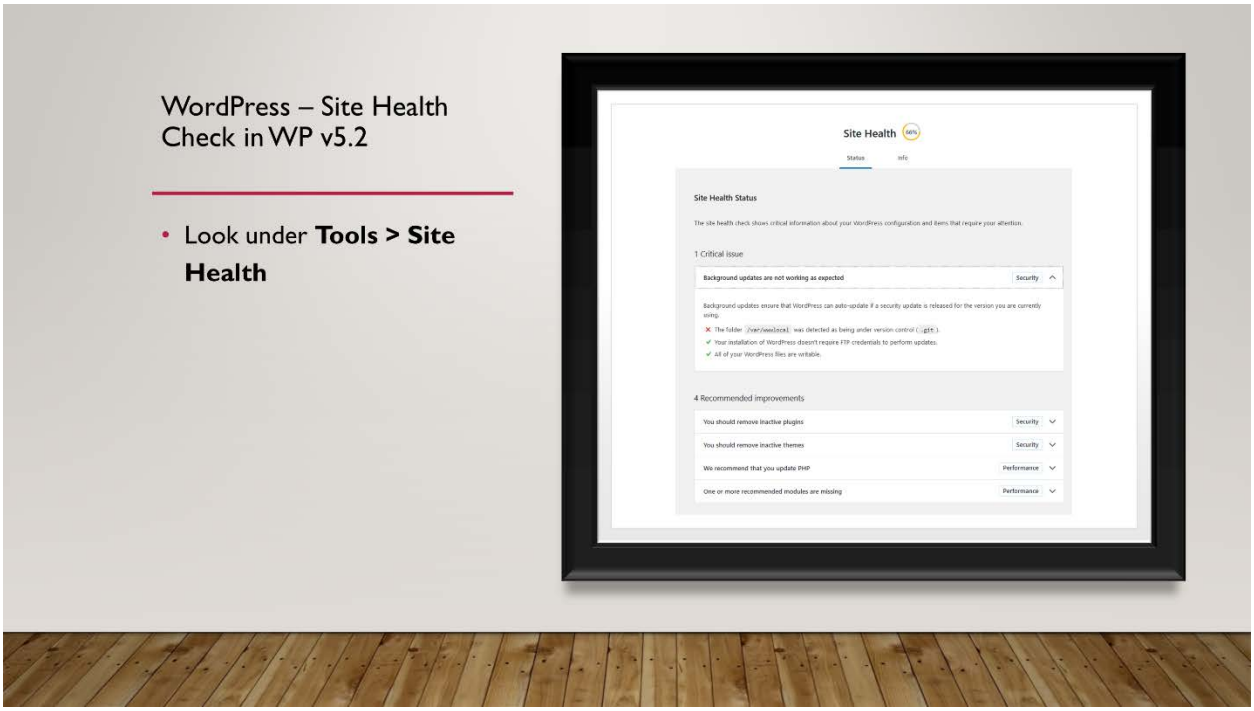


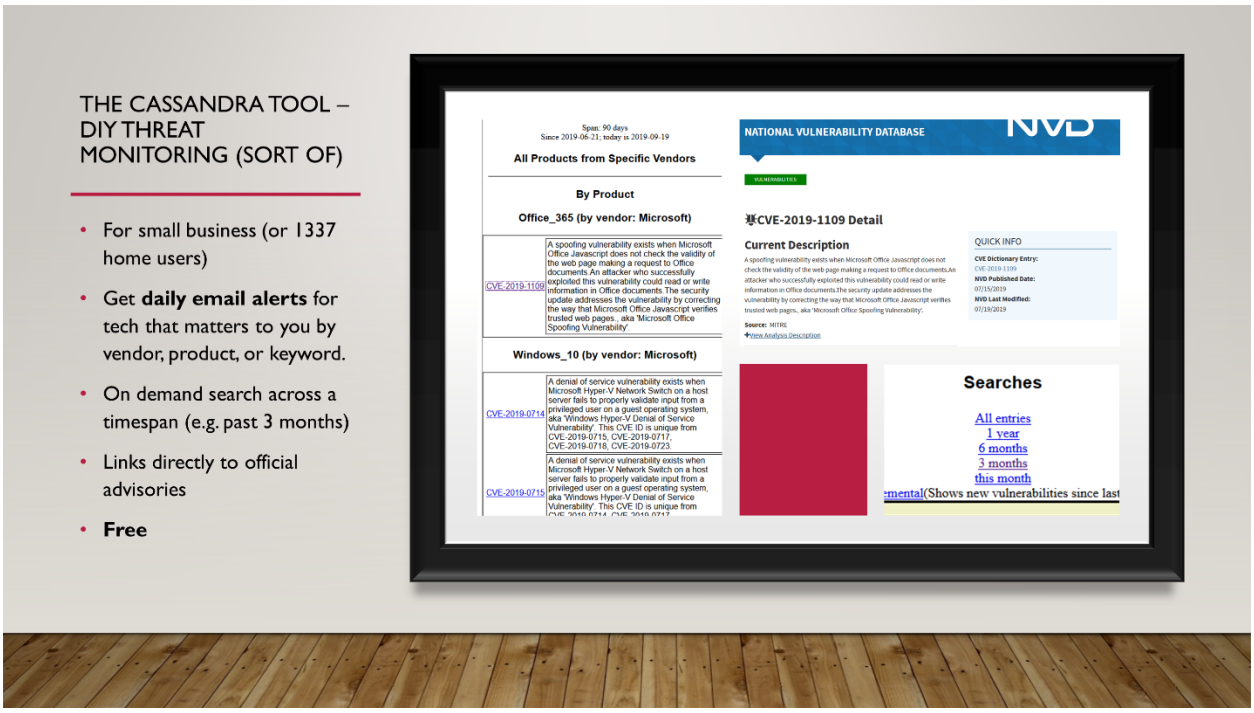
Certbot is a free, open source software tool for automatically using Let's Encrypt certificates on manually-administrated websites to enable HTTPS.
Certbot is made by the Electronic Frontier Foundation (EFF), a 501(c)3 nonprofit based in San Francisco, CA, that defends digital privacy, free speech, and innovation.

DKIM is a method to validate the authenticity of email messages. When each email is sent, it is signed using a private key and then validated on the receiving mail server (or ISP) using a public key that is in DNS. This process verifies that the message was not altered during transit.
SPF is a way for ISPs (like Gmail, Yahoo, etc) to verify that a mail server is authorized to send email for a domain. It is a whitelist for the services who are allowed to send email on your behalf. Like DKIM, SPF also works via DNS.
DMARC (Domain-based Message Authentication, Reporting & Conformance) is a standard that prevents spammers from using your domain to send email without your permission — also known as spoofing.
DMARC lets you tell ISPs how you want them to behave if SPF and DKIM fail or are not present.
Source — https://postmarkapp.com/guides/dmarc

A free tool to monitor & implement DMARC
DMARC is a standard that prevents spammers from using your domain to send email without your permission — also known as spoofing.

They will process reports from major ISPs about your domain's DMARC alignment and turn them into human-readable weekly email digests, absolutely free. — https://dmarc.postmarkapp.com/





The Cassandra Tool

This tool simplifies keeping up-to-date with vulnerabilities in the National Vulnerability Database (NVD, formerly ICAT) or Secunia databases. Instead of going to these sites every day and repeating your searches, Cassandra does the work for you (even twice a day for Secunia). It works by saving lists of products, vendors and keywords into "profiles". Whenever new information is available, Cassandra can notify you by email. You can create as many profiles as you want, for networks, typical installs, important hosts, or simply areas of interest to you. The important thing is that you should get emails only for things that are relevant to you, so you don't have to scan every message on various mailing lists. — https://cassandra.cerias.purdue.edu/main/index.html

PHISHING

- Free Phishing Security IQ Test by PhishingBox — https://www.phishingbox.com/phishing-test
- PhishMe Free | Simulated Phishing Training — https://cofense.com/free/
  - Includes training and testing
- Top 9 Phishing Simulators [Updated 2019] — https://resources.infosecinstitute.com/top-9-free-phishing-simulators/
  - A bit more **DIY** if you have IT staff (or simply someone that has a penchant for wearing hoodies)

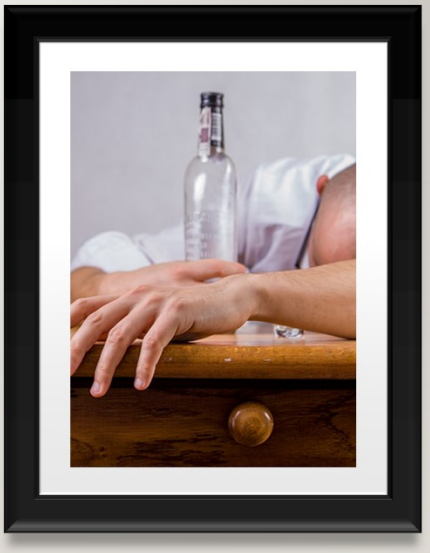
Training Resources

#GetWoke

A good collection of various resources, and a decent primer for parents.
Security Awareness for Kids: Tips for Safe Internet Use — https://resources.infosecinstitute.com/security-awareness-kids-tips-safe-internet-use/

Events

List of All Cybersecurity Conferences to Attend in 2021 — https://securitytrails.com/blog/cybersecurity-conferences



EVENT: BSIDES DELAWARE

- What: Talks, workshops, CTF, lockpicking village, Wi-Fi CTF, Spawn Camp (for kids)
- Where: Newark, DE 19713
- When: November
- Cost: $12
- Notable: Kid-friendly hacker con. ☺
- http://www.bsidesdelaware.com/

Cyber Security Events in Delaware

- What: cyber security training for Delaware's citizens, business employees, students, and government employees.
- When: Typically Oct & Nov; TBD for 2021
- Where: Wilmington, DE 19801
- Cost: Free

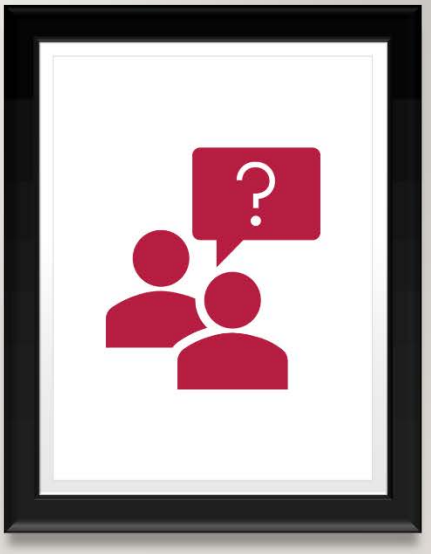
- https://digiknow.dti.delaware.gov/pages/cybersecurityevents.shtml
- Various events throughout the year for seniors, kids, small businesses…

Orgs with Cyber Security Events:

- Delaware Infragard https://deinfragard.org/infra/
- Information Systems Security Association (ISSA) Delaware Valley Chapter — http://www.issa-dv.org/meetings/
  - Holiday CISO Panel discussion – Dec 18, 2020 – 10 am - 2 pm

InfraGard is a partnership between the FBI and the private sector. It is an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S.
ISSA is the community of choice for international cybersecurity professionals dedicated to advancing individual growth, managing technology risk and protecting critical information and infrastructure.
The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

Pop quiz: Why do you think "USB" devices are dangerous?



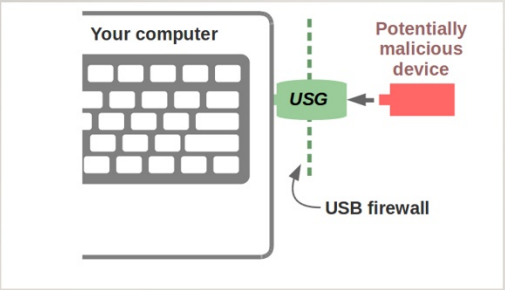
Reasons to fear USB devices – Malware

- Malware
  - Stuxnet delivered to Iranian nuclear plant on thumb drive - CNET — https://cnet.co/2M1zleZ
  - Ploutus-D Malware turns ATMs into IoT Devices — http://bit.ly/2LYpHiA
  - IBM warns of malware on USB drives shipped to customers | ZDNet — https://zd.net/2M1zpkl
- Physical Damage
- But wait, there more… in two slides.

Stuxnet delivered to Iranian nuclear plant on thumb drive - CNET — https://www.cnet.com/news/stuxnet-delivered-to-iranian-nuclear-plant-on-thumb-drive/
Ploutus-D Malware turns ATMs into IoT Devices — https://www.zingbox.com/blog/ploutus-d-malware-turns-atms-into-iot-devices/
IBM warns of malware on USB drives shipped to customers | ZDNet — https://www.zdnet.com/article/ibm-warns-of-malware-on-usb-drives-shipped-to-customers/

VOLTAGE DEFENSE – USB "FIREWALL"?

- robertfisk/USG Wiki — https://github.com/robertfisk/USG/wiki

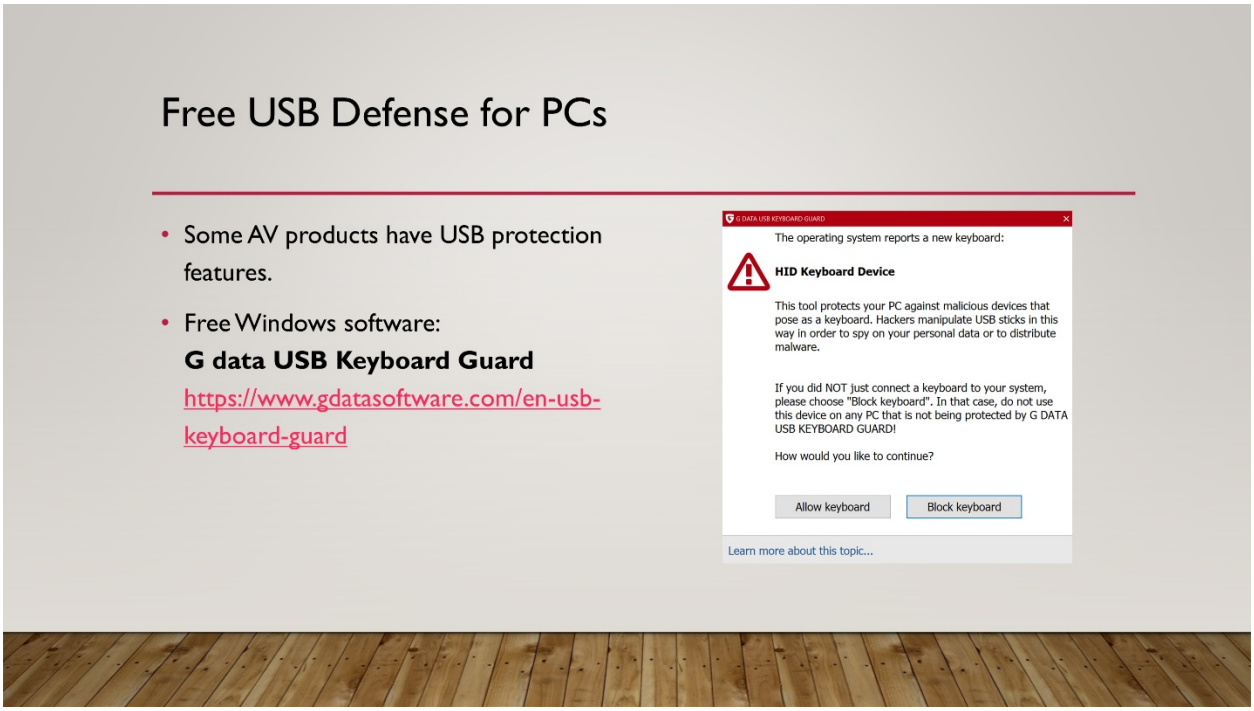


This defense is only for the most sensitive systems, such as ones that are typically air-gapped maybe.

USB devices – it's worse than you think

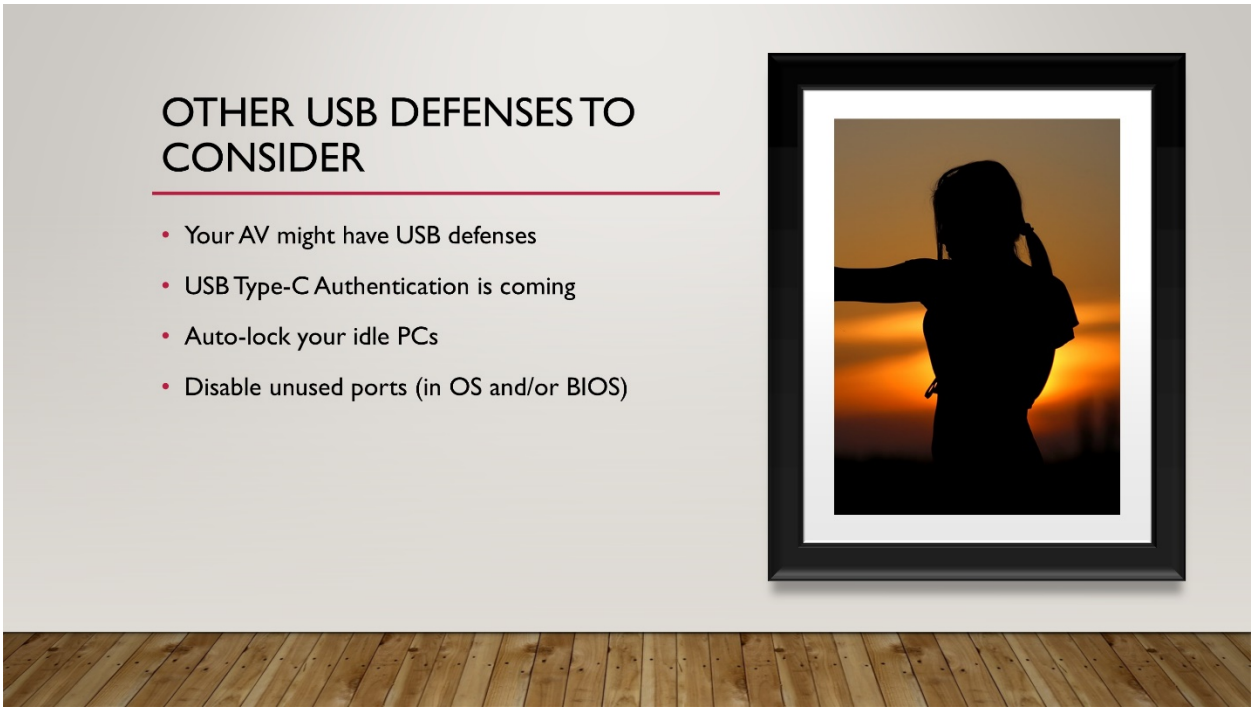
- Threat: USB thumb "drive" is also a remote keyboard (or network card)
  - Opens command prompt
  - Starts hacking your system;
  - Enables remote access
- Attack hardware for sale: https://shop.hak5.org/

I'm not sure if it is obvious why USB devices are so dangerous. If you think it's because it might have malware you'd be seriously underestimating the danger. What if the "storage" device suddenly changes configuration and acts like a keyboard? Allowing a storage device to act like a keyboards is a serious threat that is not typically considered. Most people are worried about malware, but you likely have AV protection against that. However, a rogue USB device (like a Rubber Ducky https://shop.hak5.org/products/usb-rubber-ducky-deluxe) can suddenly act like a keyboard, open a command prompt, and start entering the commands needed to download and install whatever it wants. Complete, remote, automated PC take over. Just plug it in and walk away. Talk about a ghost in the machine.

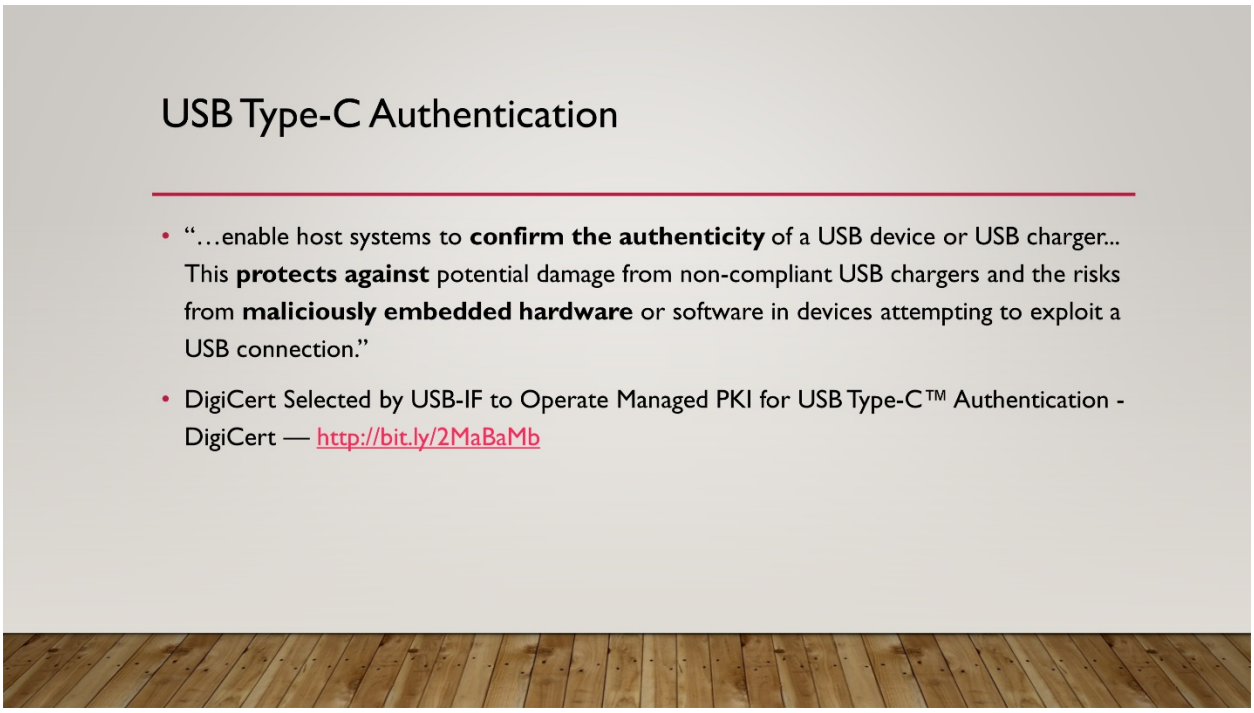


Here's a free app I use that effectively acts like a USB firewall, prompting the user if a USB device suddenly wants to be a keyboard (rather than simply storage):https://www.gdatasoftware.com/en-usb-keyboard-guard
The app is called "G Data USB Keyboard Guard". So, the next time you're giving a presentation, and someone hands you the USB dongle for the wireless presentation remote, this app will ensure the "mouse" stays a mouse.
BTW most presentation remotes include a wireless USB dongle that includes drivers for both a mouse and a keyboard, so don't freak out when this app pops up a warning. It's not Logitech

trying to hack you :-) it's just cheaper to build these USB dongles with multiple drivers installed. With this app you can block the keyboard part and use it as a mouse.

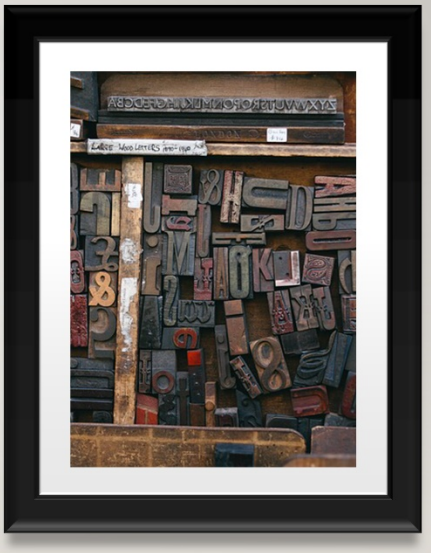


Don't forget to auto-lock your idle PCs, and disable ports on computers that don't need them. Otherwise, someone might use a USB drive to exfiltrate data out of your network via sneaker net. Or worse, use a Bash Bunny (https://shop.hak5.org/products/bash-bunny) to plugin in the next gen of rouge USB, emulate a network card, and perform attacks on the PC that was **supposed** to be air-gapped off the network.



DigiCert Selected by USB-IF to Operate Managed PKI for USB Type-C™ Authentication - DigiCert — https://www.digicert.com/news/digicert-selected-to-operate-managed-pki-for-usb-type-ctm-authentication/

Misc. Tips



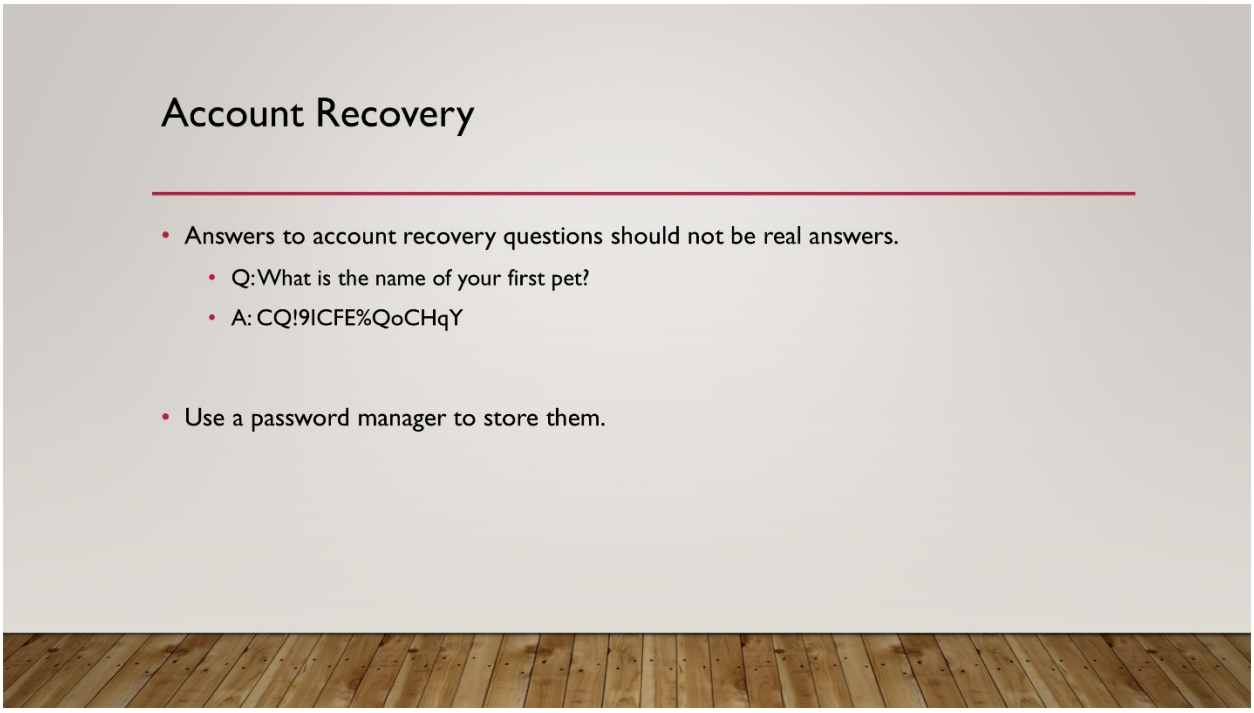
Authentication

- For **critical** accounts insist on MFA/2FA that is not SMS.
- Do not use the same (or similar) password for multiple sites
  - Use a password manager to keep track of a long random **unique** password for every site.
- Leverage browser password manager on **trusted** system.
- Poll: What types of accounts are most critical to you?
  - Banking, social media, …

SMS 2FA gave us sweet FA security, says Reddit: Hackers stole database backup of user account info, posts, messages • The Register — https://www.theregister.co.uk/2018/08/01/reddit_hacked_sms_2fa/
Twitter Suspends SMS-Based Tweeting After High-Profile Account Hacks — https://www.bleepingcomputer.com/news/security/twitter-suspends-sms-based-tweeting-after-high-profile-account-hacks/
I would say the most critical accounts I have are:

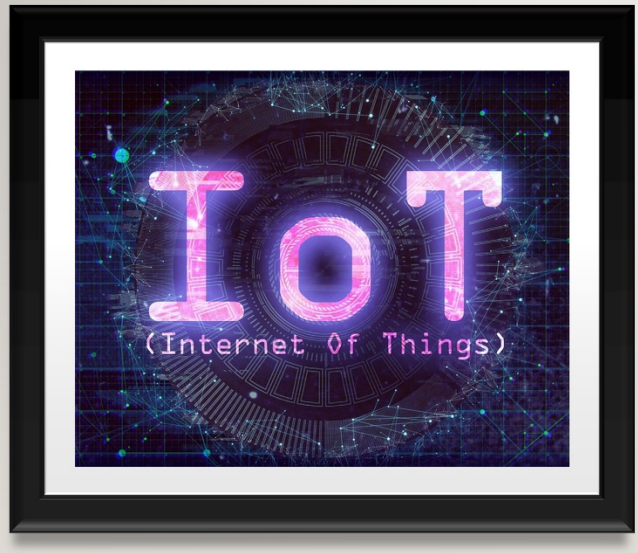
- Business and personal banking accounts
- Domain name registrar
- Email (#1 concern because it is the key to getting access to so many other accounts via "account reset" procedures).

It's Time to Stop Using SMS and 2FA Apps for Two-Factor Authentication — https://www.makeuseof.com/tag/two-factor-authentication-sms-apps/
Types of two-factor authentication, pros and cons: SMS, authenticator apps, YubiKey | Kaspersky official blog — https://www.kaspersky.com/blog/2fa-practical-guide/24219/



Money, Money, Money

- On-demand, single-vendor use credit cards
  - Privacy - A better way to pay. — https://privacy.com/
    - [Author note – I've not used this but was told about it.]
    - Extension puts a convenient button in the card field at checkout, so all you have to do is click.
- Tip: Enable transaction notification (push or SMS) for **credit card** purchases and **bank** transactions.



IOT

- If possible use network segmentation
- Research the vendor's track record for posting firmware updates.
- Look for independent security testing/research:
  - Internet of Things | AV-TEST — https://www.av-test.org/en/internet-of-things/

Test: Parental Control Software for Desktops with Windows 10 & MacOS | AV-TEST — https://www.av-test.org/en/news/test-parental-control-software-for-desktops-with-windows-10-macos/

Further Resources

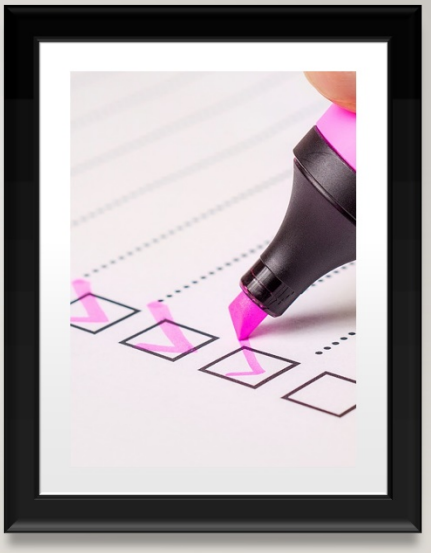
- Krebs on Security — https://krebsonsecurity.com/
  - Great news storied and some original investigative work

Bonus – Let's rant about school issued IT devices

- **CTRL + H** in browser to see history…each day ☹
- But you need physical access ☹ because G Suite for Education does not include online access to all the browsing history…that's a paid feature not in Education version. ☹
- You can see some history for G Suite accounts **online**; but only Google properties (includes YouTube)

Closing Summary

But first, let's take some questions



Summary of Next Steps

- Understand your specific risks
- Segment your wireless network via "guest network"
- Make everyone use a "Standard" user on Windows
- VPN when using public Wi-Fi
- USB protection
- Switch to Firefox and DuckDuckGo for better privacy; with tracking blocker
- Do not re-use a password; Use a password manager
- Add 2FA/MFA to critical accounts
  - Avoid SMS 2FA where possible

Author Contact Information

I hope you found this useful.
Remember, with great power comes great responsibility.
Please submit feedback via the event, or send it directly to me.
We can be reached at +1-877-MAVEN-HQ (1-877-628-3647)

Non-attributed images are from one of these sources:

https://pixabay.com/service/license/

https://www.pexels.com/photo-license/

Licensed but attribution in this context not required.