February 1, 2023

What if Chuck Norris taught Cybersecurity?

Steve Wujek

Senior Network & Cybersecurity Architect
TCDI, Inc.

- Been designing, building and securing networks and companies for over 25 years.
- Worked for Global Security Teams at AT&T, American Express and the DoD.
- Sr. Network Engineer for Polo, Ralph Lauren and Arthrex Medical Devices

Chuck Norris

Chuck Norris never needs an introduction!

ABSTRACT

The term ‘Cybersecurity’ has become an everyday part of our culture, news, politics, social lives and economy. Almost every day there is news of yet another business, government or social media website that have been hacked, spilling their secrets and your personal information. We are now seeing headlines about power plants being hit, hospitals being hit, in some cases, patients dying as a result. Countries attacking other countries using cyber weapons is now as commonplace as using a tank or an aircraft.

This presentation aims to teach you how to better understand the world of cybersecurity, and then, take it one step further, by teaching you how surf the web like a cyber pro. If Chuck Norris surfed the internet, then this is how he does it!

Disclaimer: Chuck Norris doesn’t surf the internet, it surfs to him…so I’ll be your cybersecurity guide to help you be safer online, not just at your business, but at home as well.

AGENDA

- Current state of cybersecurity and the internet; where's it headed?
- What are we seeing right now in the Cyber world?
- (Part 1) Now that I've scared you, what do you do for your Business?
- (Part 2) Now that I've scared you, what do you do at home?
  - What software/hardware should you use?
  - Tools of the Trade!
- What makes a Cyber Pros blood boil?
- Questions I get asked most often at presentations.

Current state of the Internet?

Let’s take a quick look at the old and the new.

Some Things Never Change…Carryovers from 2022

- Ransomware is still king…
- Crypto/Bitcoin is getting stolen faster than it can be mined…
- Users won't stop clicking on those free Amazon gift cards…
- Business Email Compromise (BEC): Definition - your corporate email getting hacked. Still rampant…
- Nation states (China, Russia, Iran, N Korea) still unchecked…
- Most Business Security/Cyber Training still sucks...
- Work from Home (WFH) was disastrous for businesses and has left most Cyber Pros totally burned out…
- **Wild, Wild West! After 25 years in this field, cybersecurity has gotten worse and there's no really no end in sight…**

What are we seeing right now in the Cyber world?

These are the scariest active threats and resulting problems that need a Chuck Norris roundhouse kick to the head!

Scariest Cyber Threats are…

Ransomware

- Still every hackers ‘dream come true’
- Email still the primary tool to deliver ransomware
- End-users becoming tone deaf to Ransomware
- Ransomware defense is out of scope for this presentation

Supply Chain Attacks

- Insert hidden code/hardware into a program or a device that activates and allows a hacker to infiltrate or take over.
- First SolarWinds, then Kaseya, then Mimecast, then GitHub…
- Hackers found a zero-day vulnerability in an open-source logging tool called Log4J, found in millions of worldwide apps/programs.
- 50% of the world’s networks using Log4J were attacked! Sleeping giants are being inserted everywhere!

Application Programming Interfaces (APIs)

- A way for two different applications to easily talk to each other
- Are you serious! “*Let’s write more code to help programs communicate easier over their already insecure code*?“

Scariest Cyber Threats are…

Work from Home (WFH)

- "*Everyone go home and work, IT will get everyone access by tomorrow … no pressure IT*"
- Corners cut everywhere, IT could not possibly keep up
- Extra work, burden of setting up WFH burnt out so many IT and Cyber staff
- Ramifications will be seen for years, attackers lying in wait in your network

Nation States – Russia/China/N. Korea/Iran

- **Russia** – Putin has turned Russian hackers loose!
  - I've seen a 3000% increase in Russian activity.
  - Good news: they bit off more they than can chew with the Ukrainians!
- **China** – They hack everything! Brazen! "Come and get me" attitude
- **North Korea** – Kim Jong-Un eats Bitcoin for breakfast.
- **Iran** – Busy for now with the Israelis. Make the best spam emails I've seen!

Scariest Cyber Threats are…still more

Social Media

- Spreads Disinformation faster than greased lightning!
- Polarizing the US to extremes, especially politically
- Algorithms are written by companies that are highly polarized themselves
- Abortion fear-mongering, Deepfakes – used as political tools
- Teenage girls + SocialMedia + Covid lockdowns = Scary (this one will be bad)

Crypto/Bitcoin meltdowns

- Kim Jong-Un says “Keep mining it, thank you, thank you”
- Sam Bankman-Fried…”You gave HIM how much??!!”
- Ronin Network (a gaming-based crypto network) lost $620 million (to Kim Jong-Un)
- Bitcoin – In my opinion, the Internet will never improve until it’s gone/fixed/outlawed

Application Programming Interfaces (APIs)

- A way for two different applications to easily talk to each other
- Are you serious! “*Let’s write more code to help programs communicate easier over their already insecure code*?“

Scariest Cyber Threats, bringing up the rear…

Snake-Oil Companies

- Cyber and IT Pros can't keep up with the onslaught of new companies popping up that are "Going to change the way you defend your networks!"
- As an regular attendee of Cisco Live, Black Hat and other IT/Cyber conferences, I am truly shocked at how many companies I've never even heard of, in the last 3-4 years!

Cyber Shortage

- IT/Cyber staff are burnt out!
- WFH crushed us!
- Push to get women into Cyber.
- Colleges haven't caught up in curriculums, still years away.

Cyber Insurance

- Lloyd's of London - Discouraging syndicates from providing cyber insurance. Published contractual language excluding coverage for cyber war and operation activities.
- Getting expensive extremely difficult for companies to qualify.

Credit Bureaus

- Hold every piece of credit info you've ever put on an application and their cyber hygiene is atrocious!
- Equifax and Experian are untouchable, they commit kindergarten-level mistakes for losing your info and then give you free 1 year credit monitoring.. for *their* service!

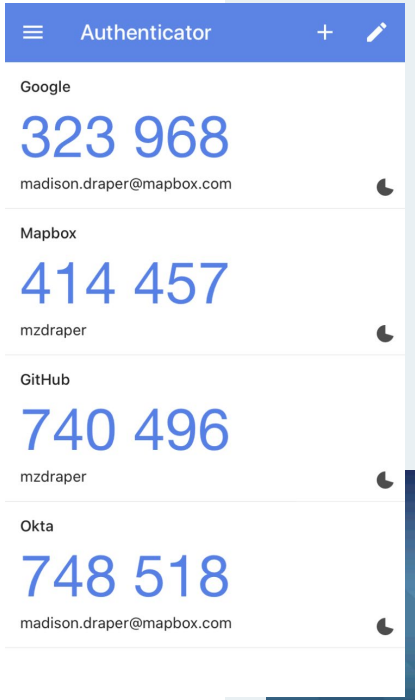
Now that we're all scared (except Chuck), what do we do now?

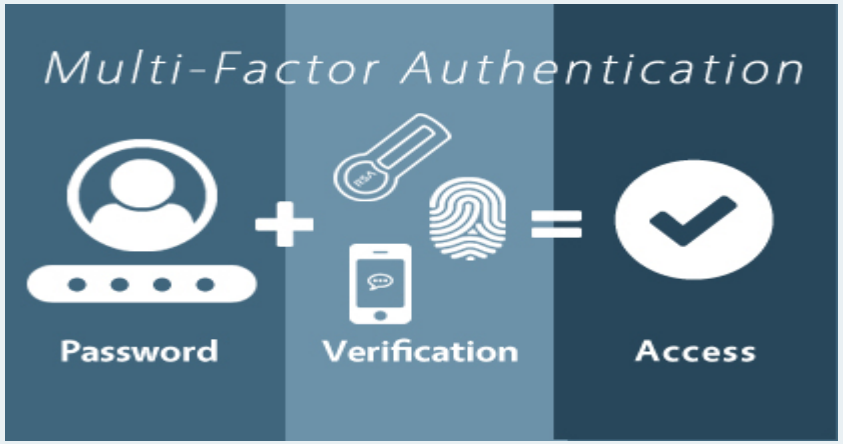
Part 1 – **Business** tips to help you understand what your own business IT/Cyber staff need to fix and what they're all talking about. Only going to hit the basics so we can get to Part 2.

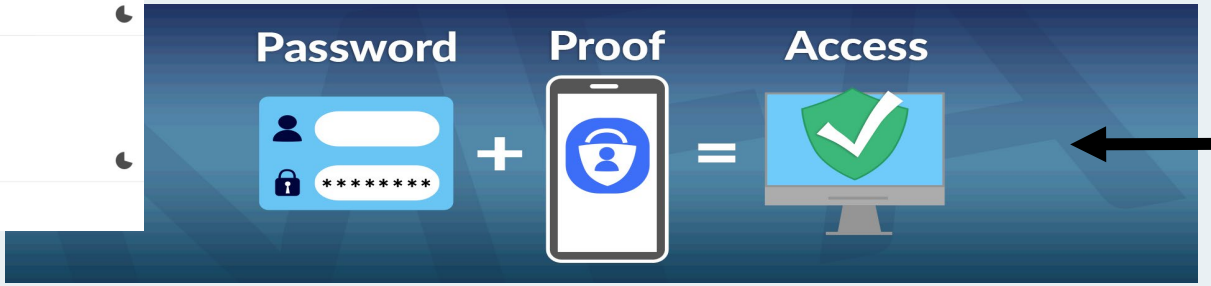
Disclaimer: Freddy Krueger has nightmares about Chuck Norris

MFA! MFA! MFA!

Multi-Factor Authentication: **If there is one factor that has stopped the majority of hacks better than any other I've seen in recent times, it is a good MFA solution!**
Vendors you may know: DUO, Yubikeys, Okta, PingID, DoubleOctopus, RSA, Google Authenticator, Microsoft Authenticator…







- This is that "phone-thingey" thing we have to say "Yes" to … the text message with that 'code' we put in.
- The "USB-lookin-thingey" we plug in to our laptops.

MFA is a security technology that requires multiple methods of authentication to provide an extra layer of protection on top of your user name and password.

Do this EVERYWHERE!
Banking, 401K, Investments

“The Basics”…AGAIN!

Stealing this slide from my 2022 TAF presentation because it’s still valid! Companies still failing to learn their ABC’s!

1. **Anti-Virus** – No Freeware! AV on EVERYTHING! Prefer AV with Artificial Intelligence built-in; XDR, EDR, Advanced Heuristics.
2. **Patching** – Patch everything, preferably ‘auto-update’. Mean time to patch a system has shrunk down to minutes for many areas of IT.
3. **Firewalls** – Software under a year old, buy the security add-ons!
4. **Backups** – Follow 3-2-1 rule; 3 copies on 2 different backup formats with at least 1 copy in the cloud or off-site.

Zero-Trust

You might as well get used to hearing about it and become familiar with what it is.

- Core tenant of Zero-Trust is to trust nothing, constantly check data along the way. Trust no one!
- Big push by the Federal Govt. mandating this on their networks.
- Has been a pipe-dream of IT for 10+ yrs now…
- Can be a concept, or a product, or a suite of products working in conjunction to provide security at every level.
- Depending on your business (I’m talking to you TAF), this could quickly become mandated by laws and regulations.

Speaking of Zero-Trust…

Is your network an Onion or an Apple or an Orange??

- Before Zero-Trust buzzword came out, I preached to businesses my “Onion Network Design” and how it keeps the hackers at bay.
- Orange or Apple - all you have to breach is the tough outer skin to get to the soft inner core.
- Onion - every layer stinks, every layer causes watery eyes, every layer burns your cuticles…
- Hackers give up peeling the onion-like layers of security!
- *Disclaimer: When Chuck Norris peels onions, the onions cry*

Now that we're all scared (except Chuck), what do we do now?

Part 2 – Home and Home Office software/hardware that gets the 'Chuck Norris Stamp of Approval'.

Rarely have I seen businesses teach any of this to their employees.

Think of this as asking your Dentist "*Which toothbrush and toothpaste do you use*".

What Internet Browsers do I use?

Google Chrome

Favorite browser for most sites

Under ‘Settings’ > Privacy & Security > Security > Enhanced Protection

Mozilla FireFox

Sometimes can ‘break’ a website due to their own twist on security.

Also a favorite of mine.

Microsoft Edge

DO NOT USE IT!

Apple Safari

My fave on an iPhone (tell you why on next slide).

Only available on Apple products

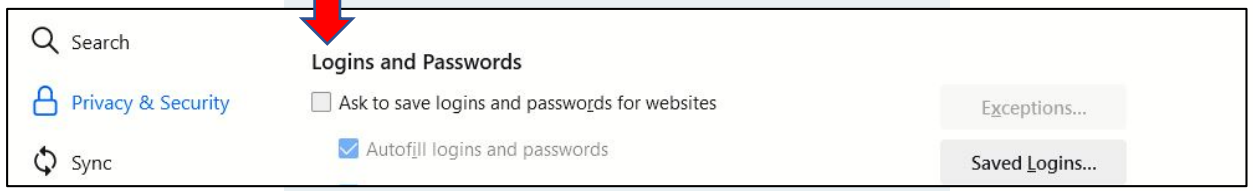
Tips for all browsers

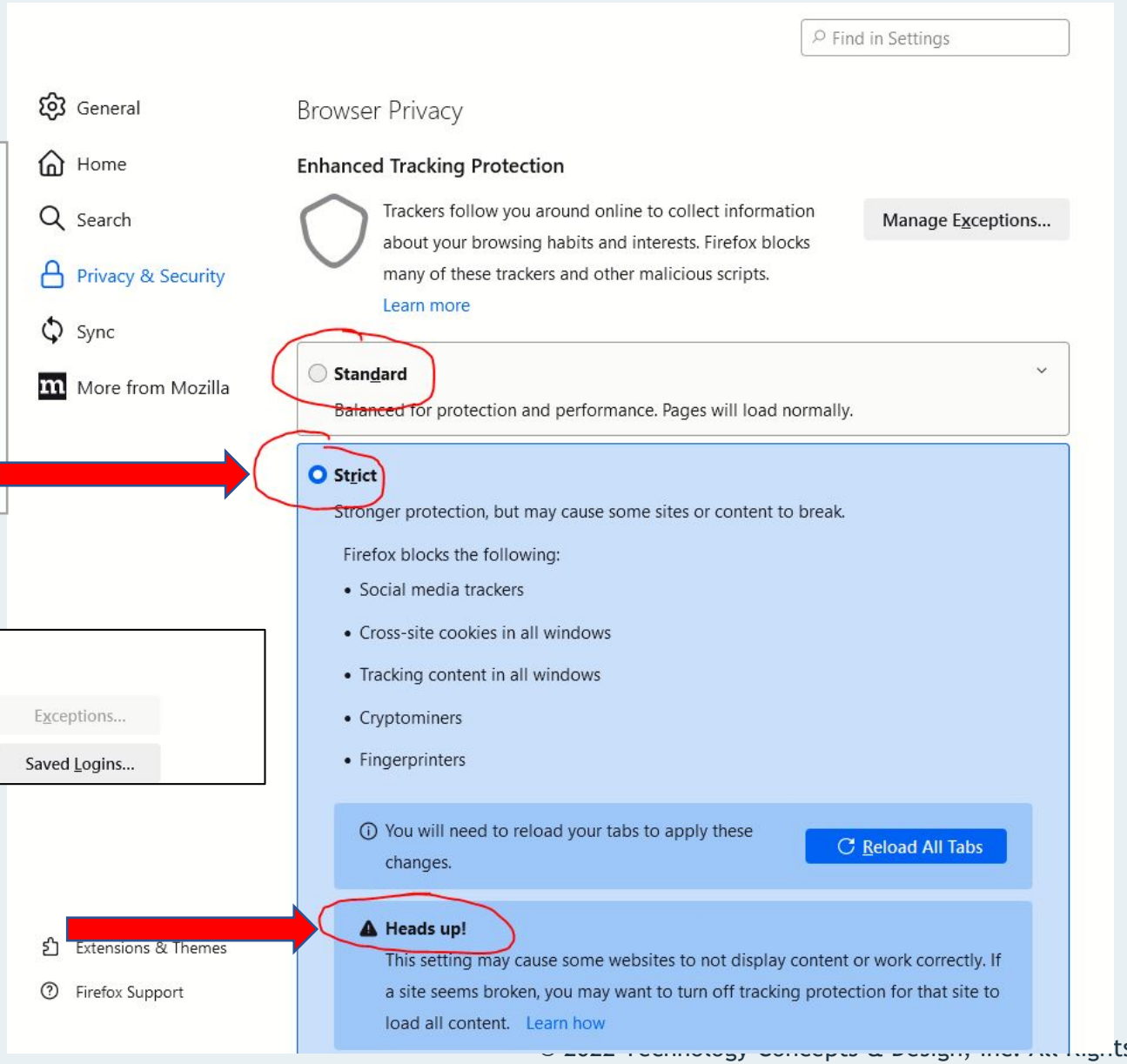
- Set all to auto-update!
- Do not recommend using their built-in password auto-fill (more later)
- Check ‘**Privacy Settings**’ or ‘**Privacy & Security**’ and turn off ‘**Data Collections**’, ‘**Studies**’, ‘**Suggestions**’
- Be careful in their ‘Store’ or ‘Extensions’ store.

What Internet Browsers do I use?

Mozilla FireFox

- Sometimes can ‘break’ a website due to their own twist on security.
- I run ‘Strict’ mode
- Logins and Passwords set to off





AdBlockers: The best kept secret in IT!

AdblockPlus

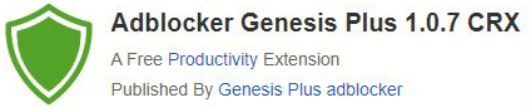
Adblock Plus

https://adblockplus[.]org

AdBlock

AdBlock

https://getadblock[.]com/en



Adblocker Genesis Plus

Search for '*adblocker genesis plus download*' and go to crx4chrome[.]com link directly.

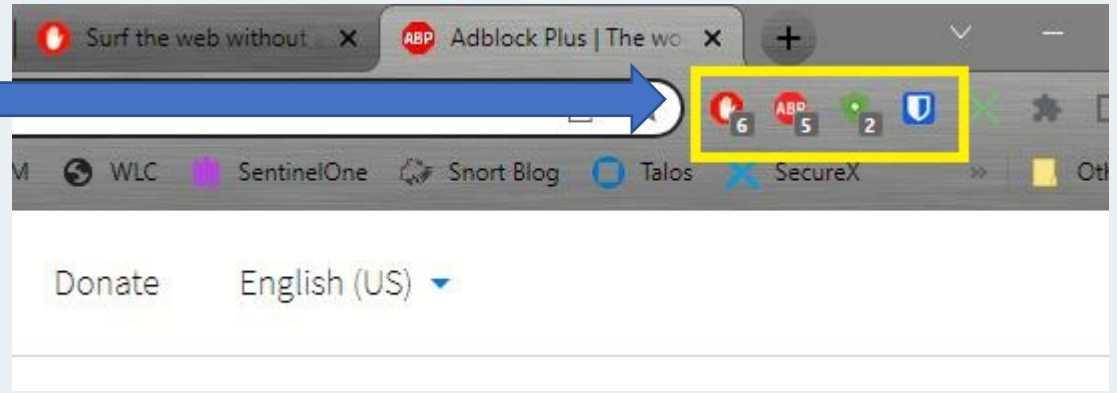
Google hates this one, LOL!

All Adblockers…

- **BE CAREFUL!** Only use the ones on this page or research carefully!
- Lots of fake adblockers!
- Can sometimes break a website, can be frustrating.
- Can also be added through the browser's Extension store. Look for the exact one and match the icon! Lots of imitators.
- Google can make finding these difficult.
- Some websites require you to turn off adblockers to see their content. I stop visiting them!

AdBlockers: Will change how you surf the net!

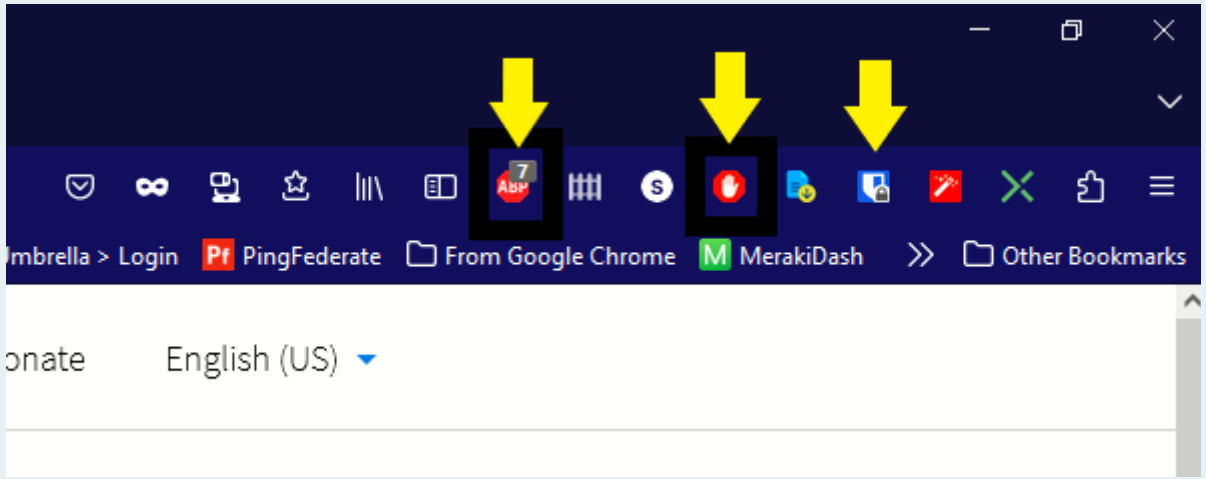
Match the icon to the name!



AdblockPlus

AdBlock

Adblocker Genesis Plus 1.0.7 CRX
A Free Productivity Extension
Published By Genesis Plus adblocker



Personal Email that I use?

Google Gmail

- Good security
- Great free plan
- Use it for orders, more important emails
- Works great with Adblockers

Yahoo Mail

- Use it only for junk mail, catalogs, sites that require you to sign up with an email
- Security sucks!
- Does a terrible job at stopping malicious spam!
- Adblockers work to clean it up visually

Outlook (OWA) MS365

- Only use it for business when absolutely necessary.
- I do not use it for personal email

ProtonMail

- Proton[.]me
- High security, end-to-end encryption
- When you need to send secure email!
- You may have to pay for a plan depending on your needs.

Hotmail

Still around…
Not used so can't comment…

What Password Managers (PM) do I use?

BitWarden

- Great security
- Great free plan
- Works across all your devices
- Has a paid Family Plan
- My personal favorite

1Password

- Great security
- User friendly
- Allowed on iPhones
- May require a paid plan

Keeper

- Great security
- Allowed on iPhones

DashLane

- Great security
- IT and Cyber pros use it and recommend it
- Allowed on iPhones
- Has a paid Family Plan

~~Lastpass~~

- Cannot recommend anymore!
- Has been severely hacked twice in the last year, Supply Chain Attacks

KeePass

- **NOT** user-friendly
- Rock-solid security!
- Time tested and vetted
- Not an ‘online tool’ per-se
- I use it as my backup for online PMs

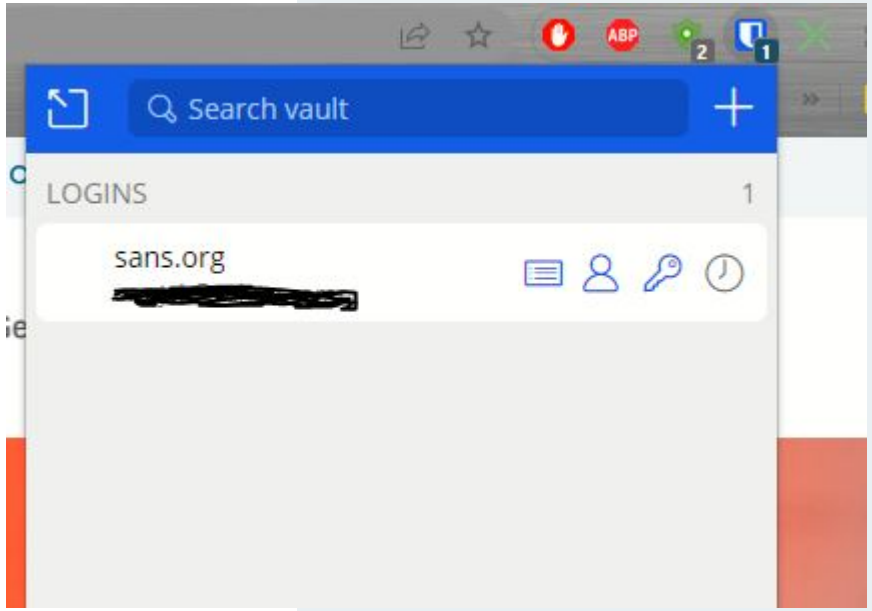
Password Managers continued…

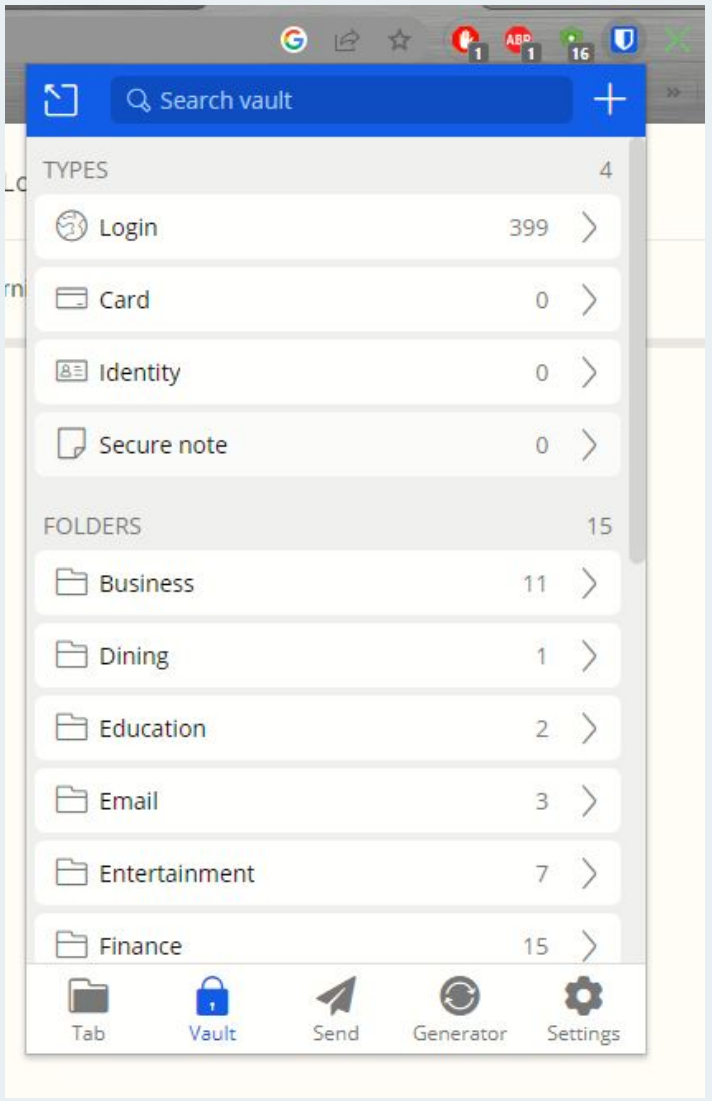
Password Managers…Tips

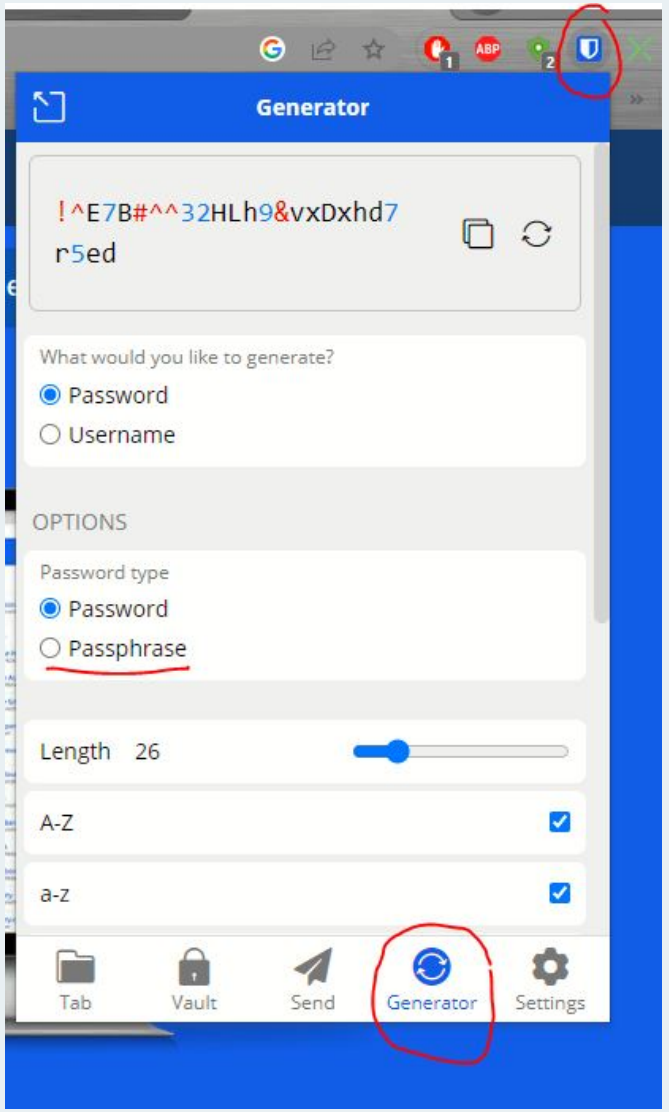
- Securely saves your username/password for all your websites
- Click on the icon when you visit a saved website, click on the dropdown box and Voila!, it pastes your username/password
- Allows you to use unique and crazy long passwords for every website.
- Do not lose your ‘Master’ password! Memorize it!
- All work on a zero-knowledge principle (except LastPass); meaning they do not have your ‘Master’ password
- Think of them like a Bank Vault; you enter your Master password to open your Vault
- Most work across all browsers, phones and computers
- All have a fantastic built-in Password Generator
- They install to your Browser on a computer; you install the App on a phone/iPad
- Some cannot remember and then store a new website on a phone
- iPhones only their use on Safari, hence my choice of browser for Apple products
- LEARN ONE OF THESE!

Password Managers continued…

BitWarden screenshots







How do I come up with passwords?

Use your Password Manager

- Great security
- I use 26 characters!
- Allows you to use different password for every website!
- All have a built-in Password Generator

Tips

- Use a passphrase over password
- **The Blue dog jumped over 3!** …is 114 bits long! Easy to type too! Try it…
- Base them off of a group of like objects:
  - Cars
  - Planes
  - Movies

Personal Banking?

- Use your Password manager
- Go 21 characters minimum, I go 26!
- Change them at least twice a year
- **Turn on MFA!!! Credit Cards, 401Ks, Banking, Mortgage Loan**

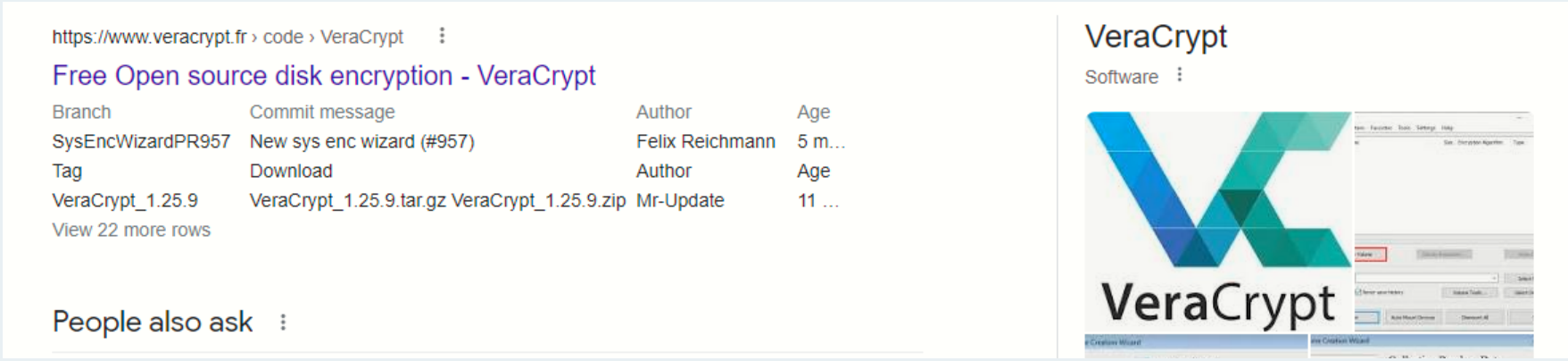
What program do I use to encrypt files?

Veracrypt

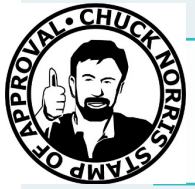
- Bulletproof security
- Probably most user-friendly program out there
- Has a learning curve
- Free for personal use
- Became the gold standard after TrueCrypt retired
- If you're familiar with TrueCrypt, VeraCrypt is easier

Used for?

- Tax Files, Banking Files
- Encrypting whole folders to keep hidden from hackers
- Encrypt files in case of laptop theft



What Anti-Virus (AV) do I use?



BitDefender

Favorite AV, what I use

Other AV Vendors

- Sophos
- TrendMicro
- WebRoot
- ESET

Norton or McAfee

Ehhh...

All Anti-Virus…

- Set all to auto-update!
- Pay for a well known brand!
- Quality can change year to year, next year I may recommend a different vendor
- You don't need all their add-on junk. Basic plan is all most users ever need
- You don't need their VPN Network, only for advanced users
- Some have built-in adblockers that are part of basic plans
- Turn off their 'marketing' notifications
- Also called XDR or EDR or XDR w/ AI

What Online Storage do I use?

Google Drive

- What I use…
- Good security
- Great free plan

DropBox

- Great security
- Most affordable paid plans
- Great functionality to send files
- User friendly

Microsoft OneDrive

- Great security
- Confuses even me! Not user-friendly on purpose

Apple iCloud

- Great security
- Can get pricey if you have lots of photos/videos/music
- Confuses even me sometimes

All Online Storage…Tips

- If the files are important, encrypt them (VeraCrypt)
- **Beware: Most, by default, store your pictures at a lower resolution**
- Any on this page can be accessed anywhere in the world if you have a computer and internet connection
- **BEWARE: Hackers can still encrypt your encrypted files but they cannot open them.**

What Physical Storage do I use?

Portable Hard Drives/Solid State Drives

- Always back up your important photos/videos/taxes to a portable HDD/SSD.
- Solid State Drives (SSD) have no moving parts, very durable, but pricey.
- HDDs are economically priced compared to SSDs and offer huge storage limits
- My favorite are Apricorn HDD/SSD with a keypad built-in. Cost more but offer extra security if it were to be lost or stolen.
- Not a fan of the Home NAS boxes anymore. If you use one, don't allow it to connect to the internet! Tend to have terrible security.
- Get those photos off your phone and laptop.
- They do have a shelf-life and lose 'bits' over time. When you can hear the drive crackling, replace it! I replace mine about every 6 years.

What Wi-Fi and OS do I run at home?

Google Nest Mesh for Wi-Fi

- What I use currently…
- Great/Good security
- Only has one Ethernet port on main router

Linksys

- Great security for Home use
- Great functionality for gamers in your house
- User friendly
- Great gear for Apartments

Honorable Mentions

- TP-Link
- Netgear – Great Mesh Wi-Fi
- Belkin

What OS…

- Windows 10 & 11
- Apple iMac/Macbook, not as user friendly as they used to be…
- Run an Ethernet cable for speed/reliability!
- Run anti-virus on your iMac/Macbook!
- Set all to auto-update, no matter the OS!

About Wi-Fi…

- ‘Mesh’ is the newest Wi-Fi tech but can be pricey
- Go with Mesh tech if you have over 2500sq ft
- Always use WPA3 security on your Wi-Fi

Eero Mesh Wi-Fi

- Ehhhh…
- Some people love it

What makes Cyber Pros (and Chuck's) blood boil!

Rated on a scale of 1-4 Chuck Norris 'smackdowns'!

What gets the Chuck smackdown, rated!

Digital Transformation – Prove to me you're doing 'The Basics' first, then, maybe…

"But we're in the Cloud" – "the Cloud isn't auto-magical with Unicorn tears and Sasquatch poop?"

"Anti-Virus slows down our servers so we removed it"… Kim Jong-Un loves you too!

"But I use a Mac/Apple" – Macs may not be vulnerable to malware but they store and spread it to everything else on the network. See this a lot at SMBs!

"Did you figure it out yet"… "Can I get an update?!" … "How much longer will this take?"

Ancient Hardware or Software – "If I show up and see you're running Windows 3.1…"

Microsoft RDP (Remote Desktop Protocol) allowed from the outside …Kim loves you!

Questions most often asked after every presentation I give…

- The only dumb question is the one you didn’t ask!
- The world of IT is the fastest changing technology on the planet!

What are…? What is…? How do I…?

Virtual Machines (VMs)

- Can also be called a “VDI” (Virtual Desktop Interface) … because no one wants to say “VD”
- One big computer carved up into hundreds of tiny computers
- Think of a big house with rented out rooms
- Can be spun up by IT very quickly!

Quantum Computing?

- The technology is coming…
- Has the potential to dangerously alter everything connected to the internet
- Passwords instantly made obsolete
- Think SkyNet
- Think Nuclear Weapons calculations taking seconds to complete vs years
- If the bad guys get it first….not good!

Crypto/Bitcoin?

- SBF and FTX
- Original intent has been lost due to FOMO

Careers/Employment in Cyber?

- Join the US military for training
- Job openings are opening like wildfire!
- Recession proof career
- Huge push for Women in the field
- TCDI has some positions open for over a year now

What are…? What is…? How do I…?

VPNs … Oh boy!

- **Endpoint VPN** – program that securely connects your computer to a business
- **Point to Point VPN** – Also called IPSec VPN, PtP VPN. How businesses securely connect sites or locations together

- **VPN Service** – usually the one that I get asked about most…How do they work?
  - You connect to their network with a VPN. They then feed you the website you are browsing to…they go get it and bring it back to you like a Labrador Retriever
  - Think ***NordVPN*** on TV
  - I do not use them
  - Break many websites
  - Can be slow
  - BEWARE: Lots of Marketing fluff

How to stop spam calls?

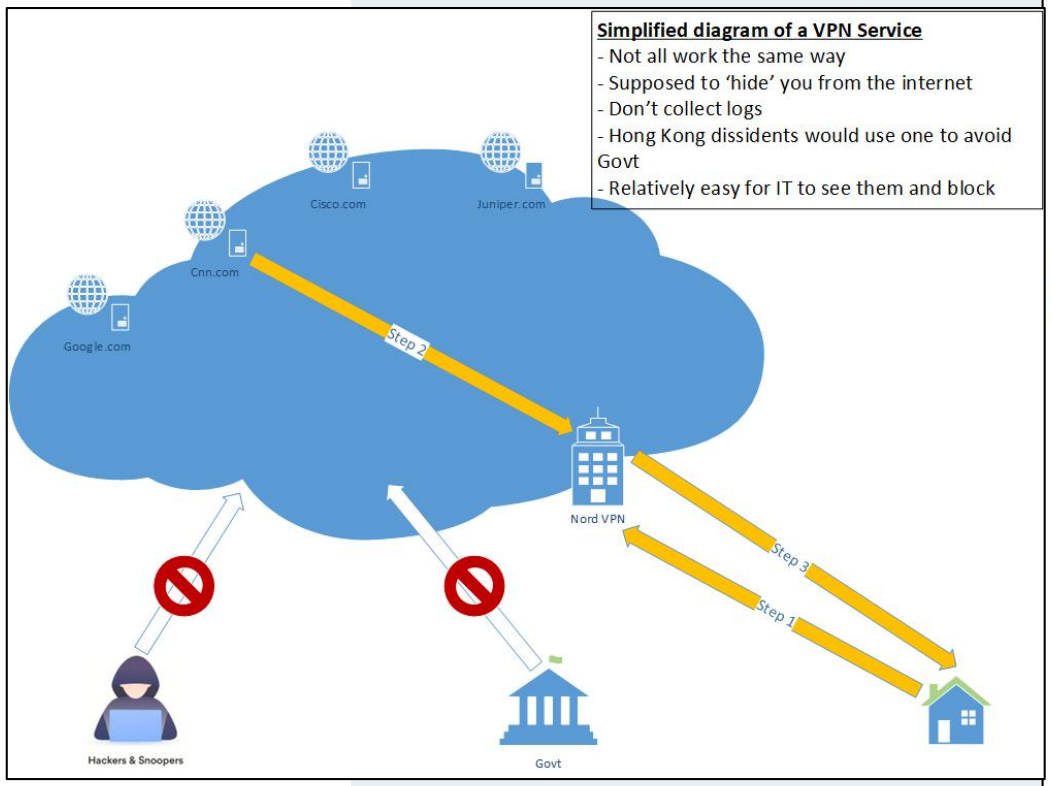
- **DoNotCallRegistry[.]gov;** check it 3x a yr
- If you answer one, put the phone down and walk away.
- Spammers are paid by ‘touches’, a touch is a conversation
- Most Cell providers have an ‘Anti-Spam Call’ feature, but has to be turned ‘On’.

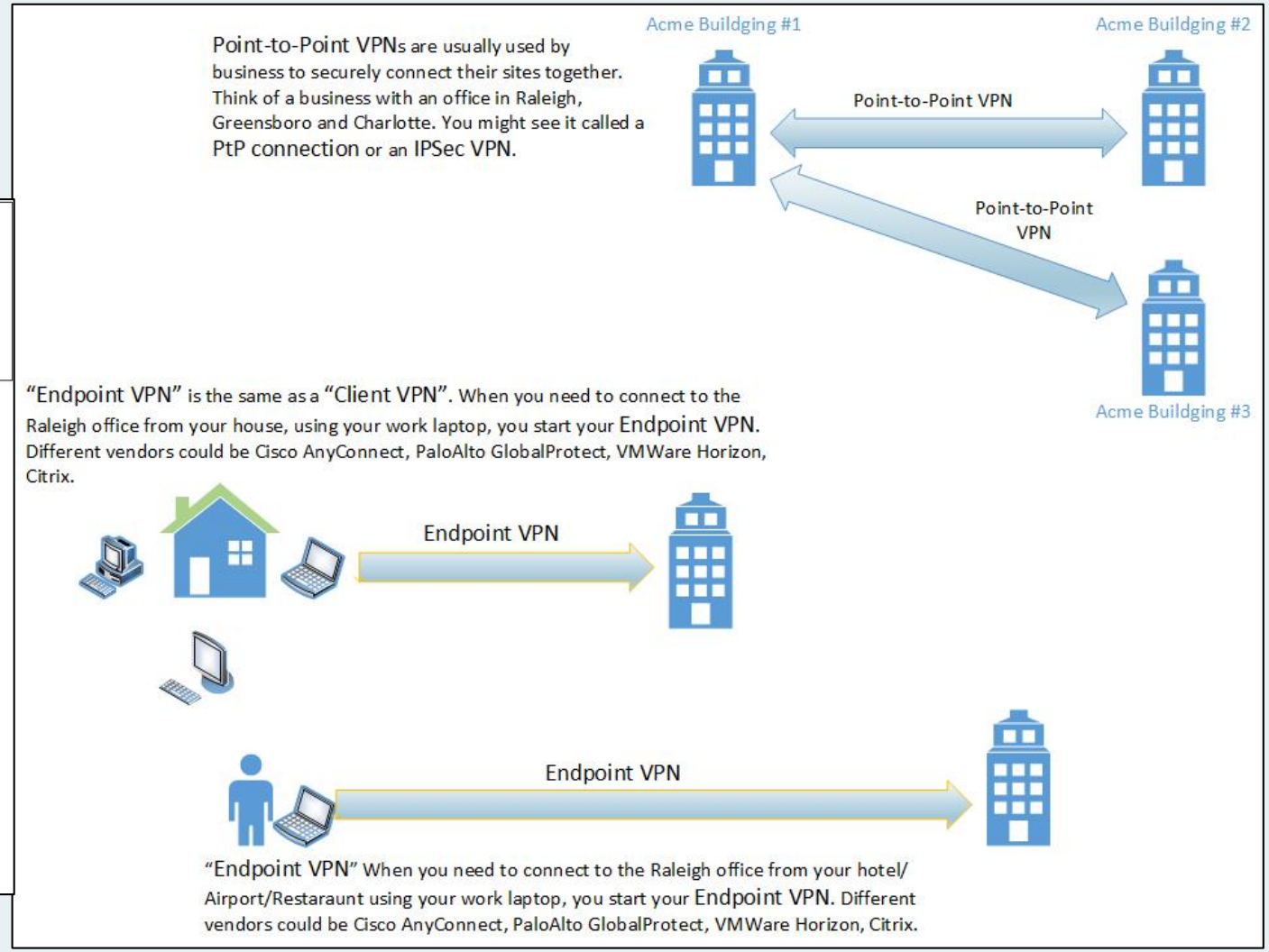
“Who do we call for Cybersecurity help?”

- Your Cyber Insurer may dictate from their list, ask them first!
- Fidelis - $$$ (800)-652-4020
- Cisco Talos - $$$$ (844)-831-7715
- Mandiant - $$$$ (866)962-6342
- GuidePoint Security - $$ (877)889-0132
- One Source - $$ (877) 651-1650

What are…? What is…? How do I…?

VPNs … Oh boy!





What are...? What is...? How do I...?

How do I stop my kids from…?

- Opendns[.]com/home-internet-security
- Blocks websites that you select
- Keep the password away from kids, LOL!
- Can block categories or individual websites
- Free plans works great for your Home!
- Paid plans for laptops if you travel
- Adds another layer to your security

Questions?

Greg Michalek
Senior Director, Business Development, TCDI
1-888-823-2880
g_michalek@tcdi.com

Steve Wujek
Senior Network & Cybersecurity Architect, TCDI
s_wujek@tcdi.com

All photos used courtesy of US DoD, Creative Commons Attribution 3.0/4.0, Alan Light, the Kremlin Creative Common License, Creative Common License, Kim Jong-Un