

Personal Cybersecurity

How to protect yourself at home

David J. Blezard

Senior Director, Enterprise IT Systems

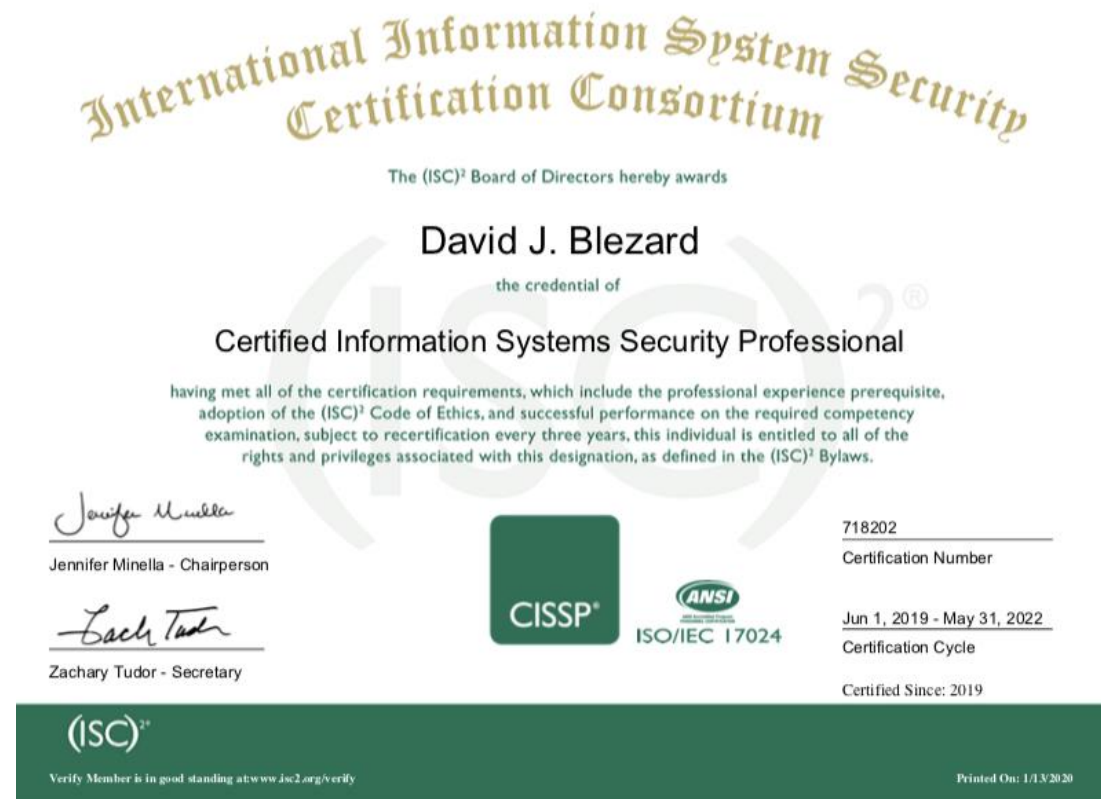
Trust is key to security

Why should you trust me?

28+ years managing and supporting networked computing systems

18 years teaching IT 609 - Network and System Administrator for the UNH CS department

Certified Information System Security Professional (CISSP) from ISC2 - since February 2019



Assess your Assets

- Financial
- Loss of photos or other data
- Loss of intellectual property
- Time and annoyance
- Reputational
- Ability to use your computer

The first part of defining a plan for security is knowing what you are protecting.

Assets – things you want to protect

Threats – what can damage your asset

Vulnerabilities – exposures you have to a threat

Risk = Threats x Vulnerabilities

The World's Safest Computer



CREATED BY VECTORPORTAL.COM

You cannot eliminate all risk.
You work to reduce risk to
an acceptable level.

Image: Science Museum Group Collection
<https://collection.sciencemuseumgroup.org.uk>

Threat #1 – Social Engineering



Mr. Robot episode 1.0 - hellofriend.mov

Email, text message, or phone calls can all be scams

- Don't trust – Verify!!!

Contact the company or person in question via another channel

- Go to the company's website directly not via the link you were sent
- Call the number you already know for your bank or credit card company
- Check if your friend really did mean to send you that attachment

Don't give out your passwords EVER

Don't give out by phone or email or anything other means a verification code that's texted to you other than in the normal login process

And no one will ever really want you to go buy a bunch of Amazon gift cards and then send them the numbers because they are sick/broken down on the highway/stuck in a foreign country

A brief diversion about Passwords

Simple passwords are easy to guess or brute force

- So don't use them

Complex passwords are hard to remember

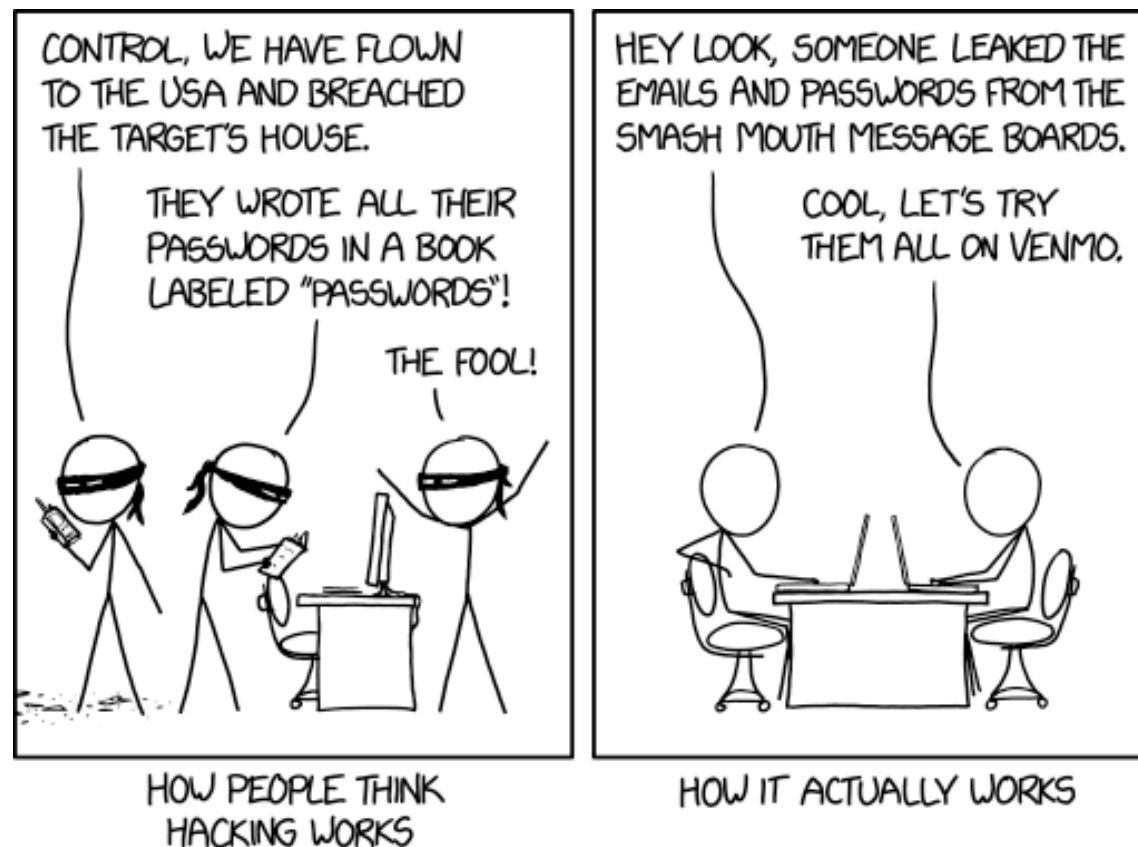
- But don't write them down!

Any password can be told to someone else who then effectively becomes you

- Don't do that

Reusing passwords increases risk of exposure and multiple breaches

- Use unique passwords



<https://xkcd.com/2176/>

Pass Phrases

- See xkcd

Maintain unique passwords especially for sensitive services like banking

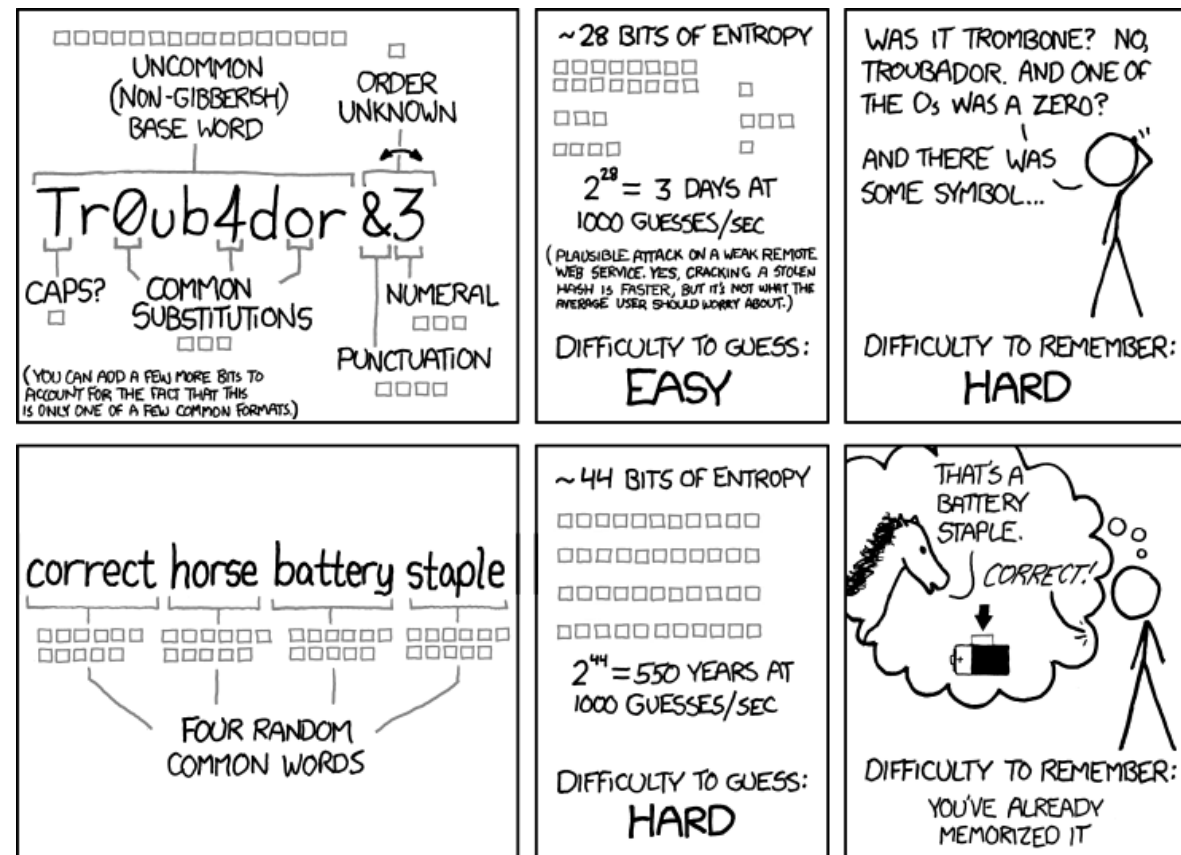
Use a password manager tool

- Dashpass, Lastpass, 1Password, et al.

Use Multi-Factor Authentication

- MFA combines something you have or something you are with something you know

Move to Passkeys (FIDO)



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

<https://xkcd.com/936/>

Threat #2 - Malware

Prevention >>> Cure

Borders

- Don't trust attachments or links to some random website
- Use the security features of your OS

Hygiene

- Keep your OS and applications up to date
- Don't install and run things you don't need
- Limit what your kids can do

Cleanup

- Malwarebytes



Threat #2a - Ransomware

Instead of malware just spreading or crashing things, ransomware will take your files and encrypt them.

You must pay to get the encryption key to get the files back.

Maybe.



Prevention >>> Cure

Borders

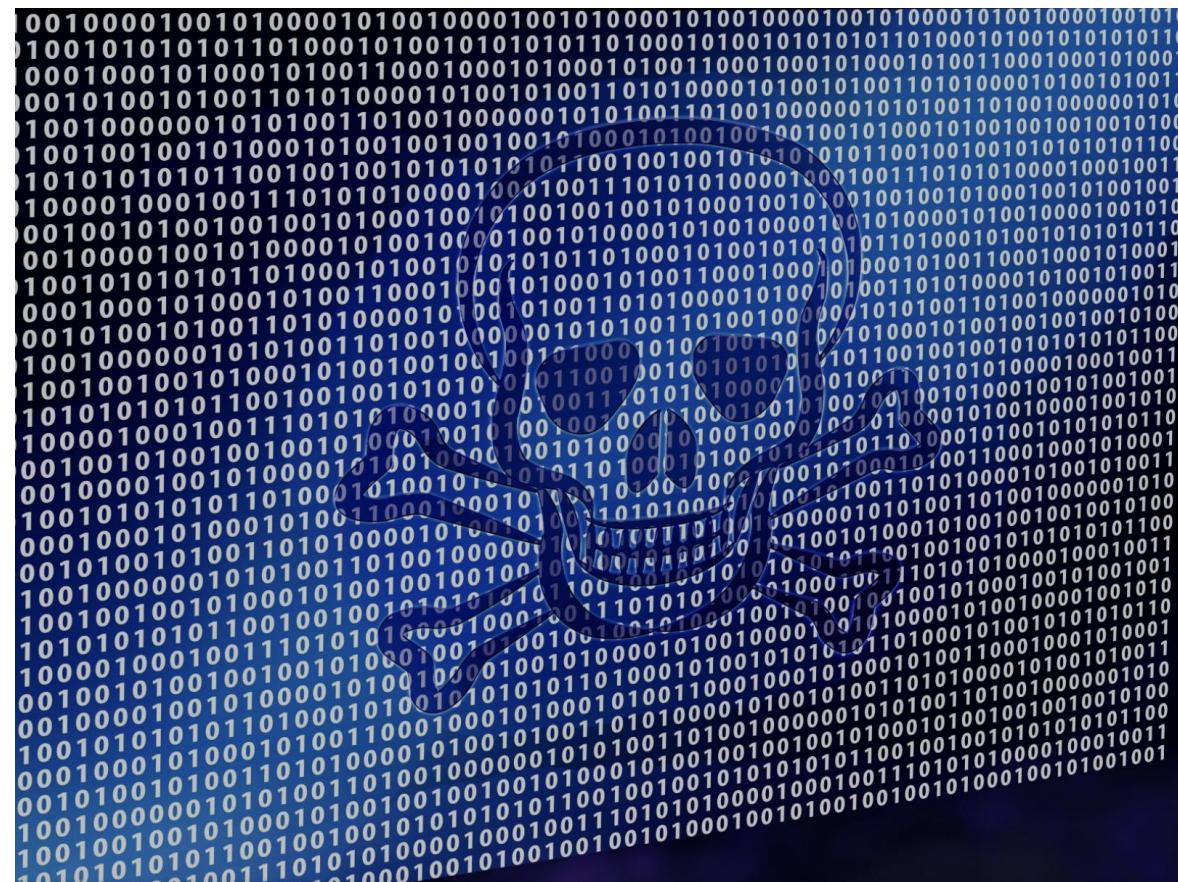
- Don't trust attachments or links to some random website
- Use the security features of your OS

Hygiene

- Keep your OS and applications up to date
- Don't install and run things you don't need
- Limit what your kids can do

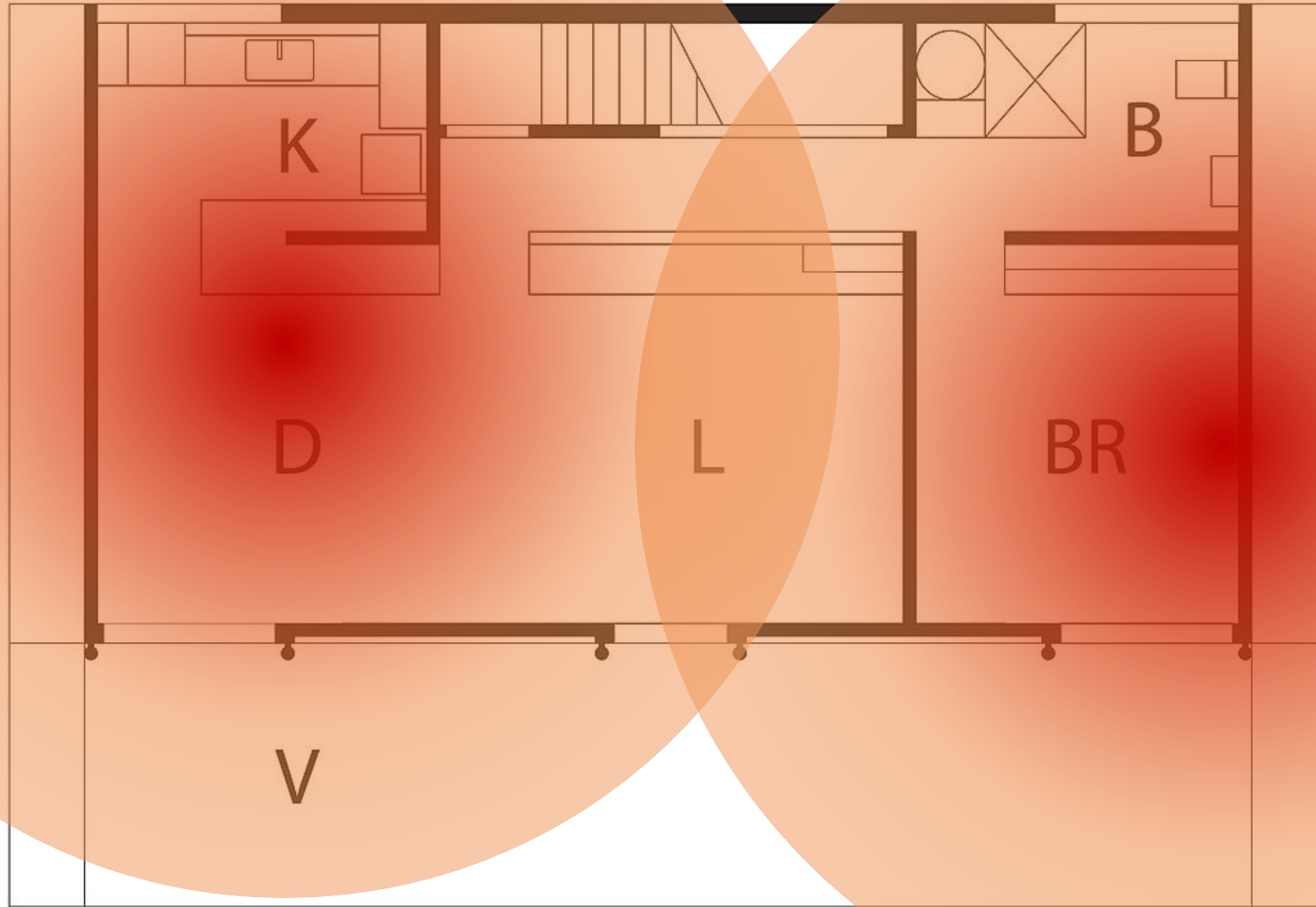
Backup

- Backup your files
- Keep your backup isolated
- Test the restoration of your backup



Threat #3 – Wireless at Home

This is your house on Wi-Fi



Two Home Wireless Threats

Unauthorized use

- Your neighbor surfing the net while you pay for the Internet service

Eavesdropping

- Your neighbor intercepting your passwords, credit card numbers, etc as you do your normal business

And this doesn't have to be your "neighbor" as good antennas can pickup Wi-Fi 1 KM or more away

Google search for "default wifi router password"

Default Router Username and Password List

Choose your router from the list below in order to see its default username and password. If you don't know your router's IP address you can [check it here](#)

2WIRE

Here are some popular router's credential information.

| Router Brand | Login IP | Username | Password |
|--------------|---|----------|--------------|
| 3Com | http://192.168.1.1 | admin | admin |
| Belkin | http://192.168.2.1 | admin | admin |
| BenQ | http://192.168.1.1 | admin | admin |
| D-Link | http://192.168.0.1 | admin | admin |
| Digicom | http://192.168.1.254 | admin | michelangelo |
| Digicom | http://192.168.1.254 | user | password |
| Linksys | http://192.168.1.1 | admin | admin |
| Netgear | http://192.168.0.1 | admin | password |
| Sitecom | http://192.168.0.1 | sitecom | admin |
| Thomson | http://192.168.1.254 | user | user |
| US Robotics | http://192.168.1.1 | admin | admin |

Display a menu

Encryption

- Prevents both unauthorized use and eavesdropping
- WEP is outdated and fundamentally flawed - Don't use it
- WPA3 is the latest and greatest, but use at least WPA2

Change the default password

- Prevents both unauthorized use and eavesdropping
- This is not necessarily about the password to join your network, but the password to manage the admin interface for the router!!

Bonus: Guest network

- An unsecure guest network lets your friends use your network easily without having to give them the password to get to the secure stuff
- But, it also allows anyone to use the guest network

Threat #4 – Wireless not at Home

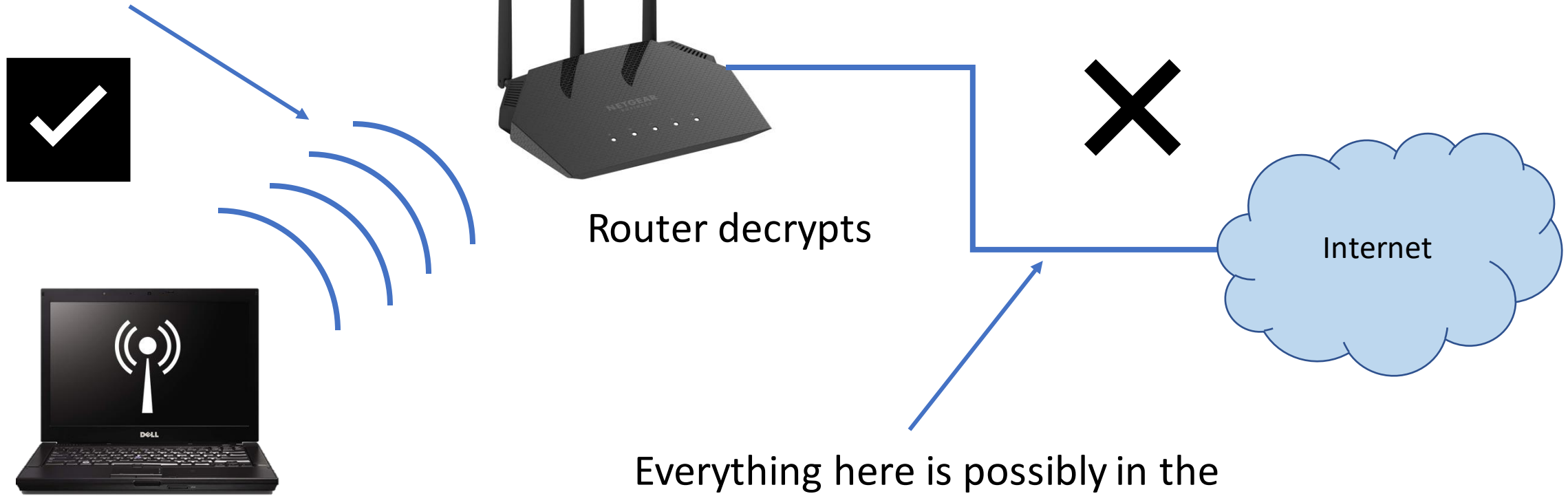
Isn't it great that you can get on Wi-Fi so many places????

Maybe not

- Communications on open wireless networks can be intercepted by anyone else in the space or the person running the network
- Even if the network requires logins and the Wi-Fi is encrypted, that ends at the base station



WPA Encryption is HERE



Router decrypts

Everything here is possibly in the clear and trivial to intercept

Internet

Encryption

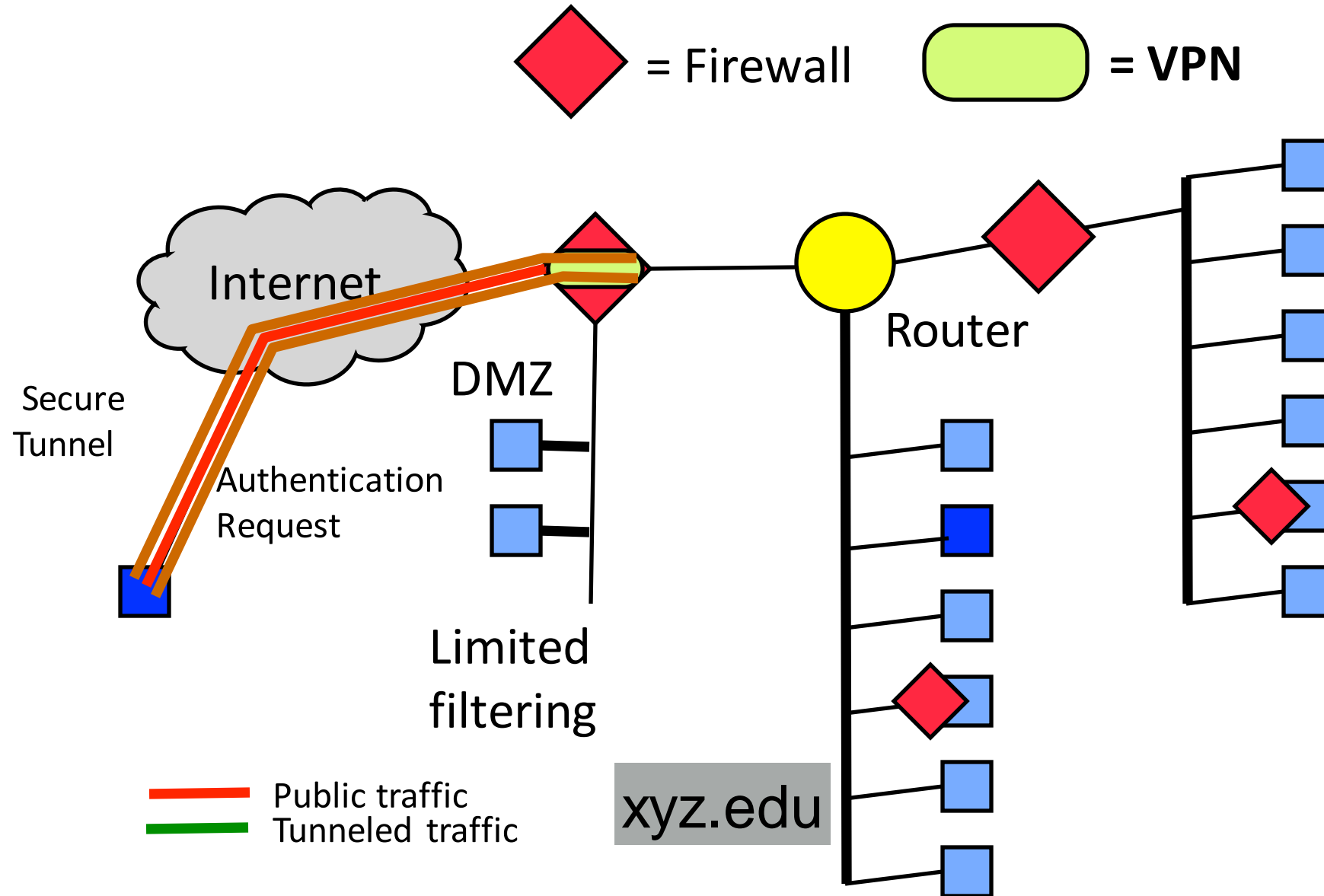
- Bring your own in the form of a VPN
- Make sure the website or other service is encrypted
 - Look for HTTPS or the lock icon in your web browser
 - SSH not Telnet
 - SFTP not FTP
 - Modern authentication for email services

Use your own mobile service

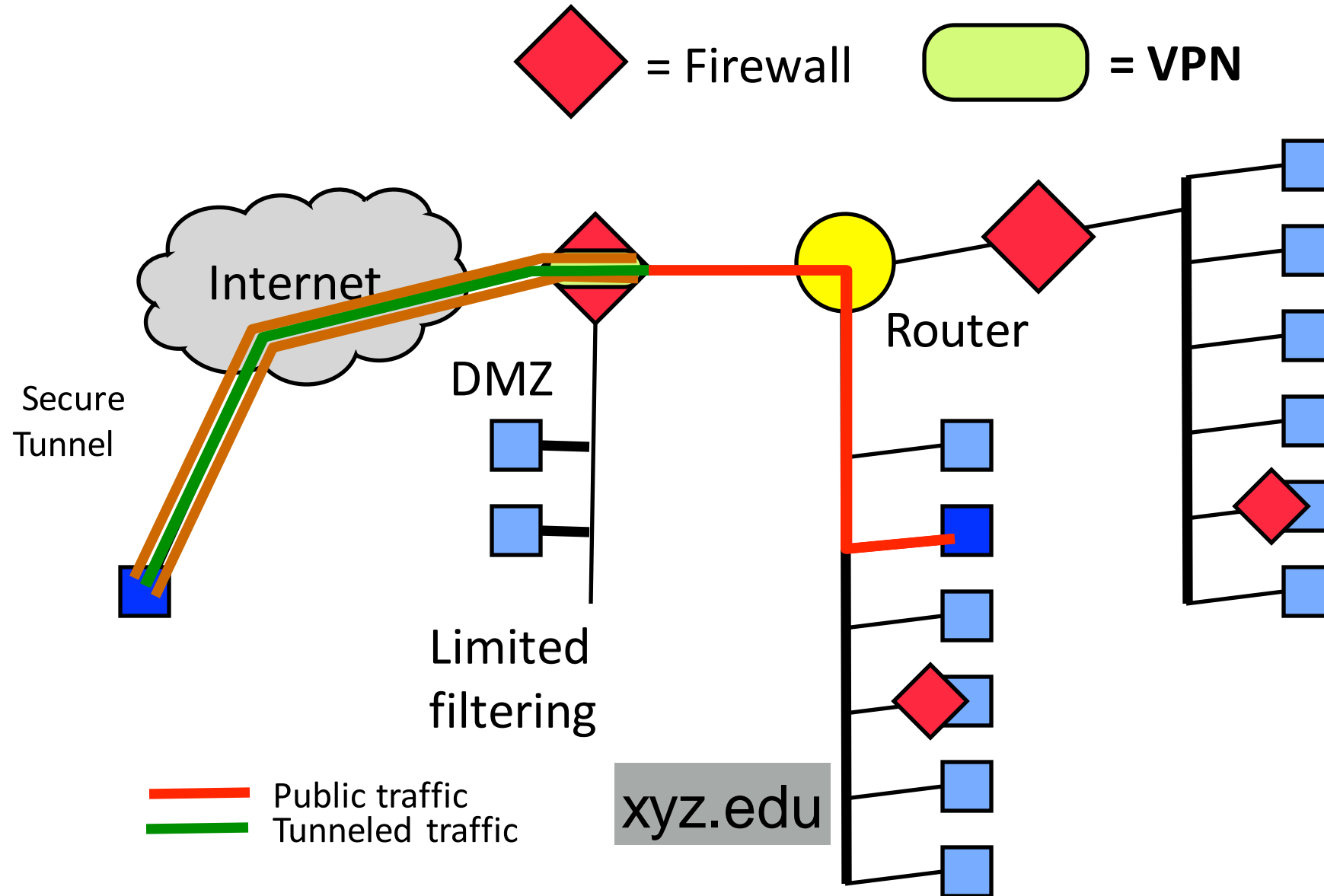
- 5G cellular networking services are encrypted
- Older standards are also encrypted, but not as strongly

A brief diversion about VPNs

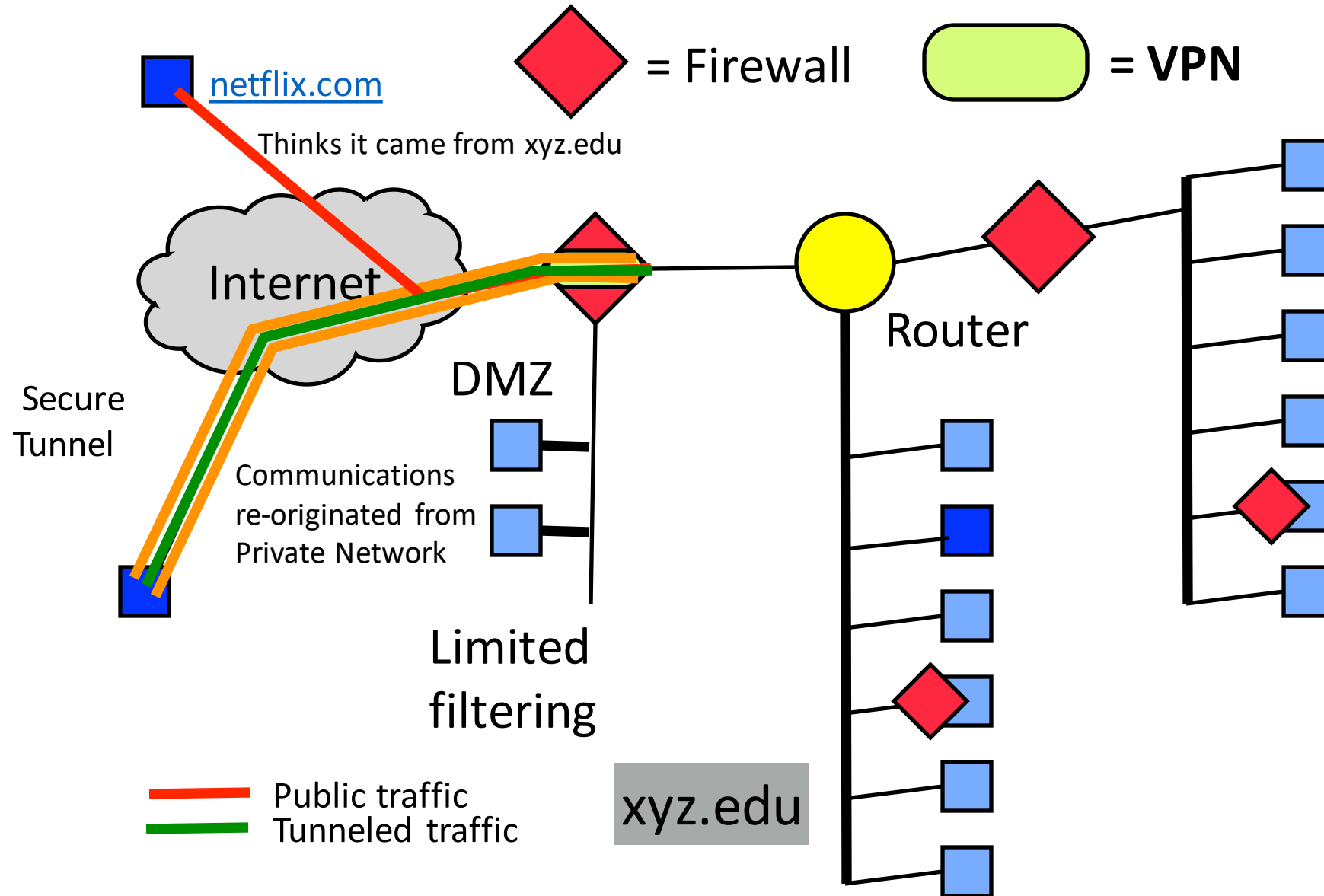
VPN - Topological Diagram



VPN - Topological Diagram

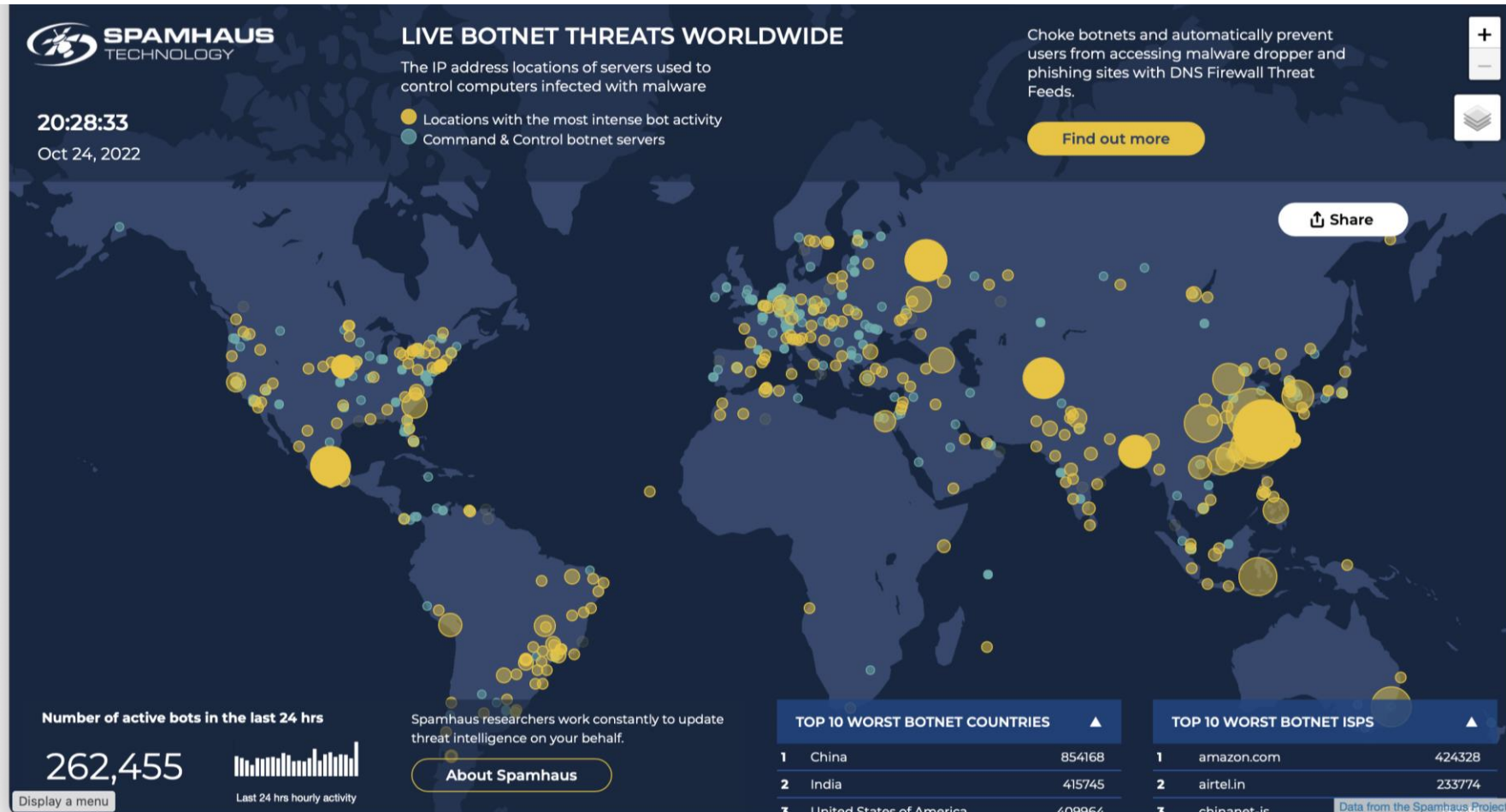


VPN - Topological Diagram



Threat #5 – Zombot Apocalypse

<https://www.spamhaus.com/threat-map/>



If your computer becomes a bot, your computer is not your own

Bad for you

- Your computer will be functioning poorly
- It's running up your electricity bill
- You could get blamed for the actions of the attacker

Bad for the rest of the world

- Your computer could take part in distributed attacks (DDOS) on other targets
- Your computer could transmit malware to other computers

And botnets can be made up from Internet of Things (IoT) devices, too – cameras, routers, storage devices, et al.

Updates

- Update your operating system
- Update your applications
- Update your IoT devices

Change default passwords

Don't install untrusted software or visit untrusted websites

Any of this sounding familiar???

Congratulations!

You are now more aware of some cybersecurity concerns that you were an hour ago.

And hopefully you might change a behavior or two to reduce your risk to make yourself safer and also help make USNH and the rest of the world a bit safer.



**CYBERSECURITY
AWARENESS
MONTH**