

# NEbraskaCERT Staying Safer while WFH

By Matt Payne, Ron Woerner  
& Aaron Grothe

August 19. 2020



# Introduction

Welcome to the first virtual NEbraskaCERT CSF.  
Please be patient if we have any technical issues.

# Staying Safe While Working From Home

Couple of things we'll mention tonight

- Segregating your home/work network - wifi
- Managed switches - ethernet
- DD-WRT/OpenWRT, etc...
- PfSense/Fortigate, etc...

# Segregating Your Home Network - Wifi

Goal: Separate your work machines from your home network

How: Use the guest network option to prevent work machines from talking to home network.

Most modern routers have an option for a guest network.

# Segregating Your Home Network - Wifi

---

## Wireless Network (2.4GHz b/g/n) - Profile

Enable Guest Network

Enable SSID Broadcast

Allow guests to see each other and access my local network

Guest Wireless Network Name (SSID):

---

## Security Options - Profile

None

WPA2-PSK [AES]

WPA-PSK [TKIP] + WPA2-PSK [AES]

---

## Security Options (WPA-PSK + WPA2-PSK)

Password (Network Key):

(8-63 characters or 64 hex digits)

---

# Segregating Your Home Network - Wifi

## Tips:

- Make sure to uncheck the box "Allow guests to see each other and access my local network"
- Set Encryption options - ideally to WPA2-PSK [AES], wep is still bad
- Set a long network key - suggest stringing multiple APG generated passwords together

```
mattgpayne 2.4 py ~ apg
Ten0BakIbPyft: (Ten-ZERO-Bak-Ib-Pyft-COLON)
6$QuervEv{ (SIX-DOLLAR_SIGN-Querv-Ev-LEFT_BRACE)
>Fig8Sligann (GREATER_THAN-Fig-EIGHT-Slig-ann)
Rin9gram- (Rin-NINE-gram-HYPHEN)
1odlidaypIj0d* (ONE-od-lid-ayp-Ij-0d-ASTERISK)
Rov:kivaj5 (Rov-COLON-kiv-aj-FIVE)
mattgpayne 2.4 py ~
```

# Segregating Your Home Network - Wifi

## Limits:

- Each machine connected to your guest network cannot see the other machines
- Trusting the firmware of your router to separate your networks
- Limited to the speed of your wifi

# Segregating your Network - Ethernet

Goal: Separate your work machines from your home network at the port level

How: Use a managed switch to allow you to separate ports into VLANs and apply policies to them.

The options from switch to switch vary.



# Managed Switches - Ethernet

## VLAN Support for Traffic Segmentation

Enhance network security and simplify administration



## ZYXEL GS1200-5 - Fanless 5 Port GbE L2 Web Managed Switch

[Visit the ZyXEL Store](#)

★★★★☆ 25 ratings

| 3 answered questions

Price: **\$24.99** ✓prime & FREE Returns

Pay ~~\$24.99~~ \$0.00 after using available Amazon Rewards Visa Card Points.

- **SIMPLE SETUP.** Initial setup is just plug and play. Advanced features can be configured via WebGUI from any desktop web browser.
- **ADVANCED FEATURES.** Use VLANs to segment your traffic, QoS to prioritize voice or video services, IGMP for IPTV, and more.

# Segregating your Network - Ethernet

## Tips:

- Make sure to buy a managed switch
- Look for GbE or else you might end up with 10/100
- VLAN/QoS are usually good things to make sure are included
- Read the reviews

# Segregating your Network - Ethernet

## Limits:

- Interfaces and capabilities vary wildly from manufacturer to manufacturer
- Vlan can slow performance of switch dramatically
- Check to see if it still listed on manufacturer's website and has updated firmware available

# Upgrading your Router's Firmware

Goal: Unleash the Linux computer in your router

How: Switch from using your stock firmware to a more robust firmware

Two of the most popular are DD-WRT and OpenWRT

# Upgrading your Router's Firmware

DD-WRT - Google Chrome

DD-WRT

dd-wrt.com

HOME | DOW

**Professional**

- Customization Services  
Get Your Own DD-WRT version
- DD-WRT Shop  
Professional Soft- & Hardware
- Activation Center  
Access & Manage Your Licenses

**Support**

- Router Database  
Check Router Support & Downloads
- Documentation  
Learn How To Setup & Configure
- FAQ  
Get Answers For Common Issues

**Community**

- Forum  
Meet Other DD-WRT Users
- Wiki  
Get More Information About DD-WRT
- Donations  
Ways To Support The Project

# Upgrading your Router's Firmware

## Tips

- It is [dd-wrt.com](http://dd-wrt.com) - not [dd-wrt.org](http://dd-wrt.org)
- Keep in mind this can potentially brick your router.  
Please read the documentation....
- 30-30-30 - the hard reset
  - With the unit on hold the reset button for 30 seconds
  - Unplug the router while continuing to hold the reset button for 30 seconds
  - Plug back in continue to hold reset button for 30 more seconds
- Read the Forum posts for your router
- Some like netgear have semi-official ports of DD-WRT

# Upgrading your Router's Firmware

## Limits

- Keep in mind this can potentially brick your router.  
Please read the documentation in mind
- Isn't necessarily stable on all routers - my netgear for example :-)
- The interface may not be as user-friendly as the stock firmware

# PfSense/Fortigate, etc...

Goal: More powerful options, some of which can be sent to remote users

How: Buy/Install or use a system with optional commercial support

PfSense is a firewall/router running on top FreeBSD. You can supply your own hardware, run a VM or buy an appliance with it already installed. Very full featured, SG-1100 runs about \$200.00.

Fortinet Fortigates are commercial systems. Your company may be running on one of these. 40F starts at around \$350.00. Support



Hack yourself before someone else  
does...

Audit your network? Inside out...

SANS White Paper "Wireless Network Audits using Open  
Source tools" looks interesting.

TODO(MGP): Try out some of that

[https://www.sans.org/reading-room/whitepapers/auditing/wireless-net  
work-audits-open-source-tools-1235](https://www.sans.org/reading-room/whitepapers/auditing/wireless-network-audits-open-source-tools-1235)

# Audit your network? Outside In...

<https://www.grc.com/shieldsup>

**ShieldsUP!!**<sup>tm</sup>

**Port Authority Edition – Internet Vulnerability Profiling**

by Steve Gibson, Gibson Research Corporation.

THE EQUIPMENT AT THE TARGET IP ADDRESS  
**DID NOT RESPOND TO OUR UPnP PROBES!**

*(That's good news!)*

And what else?

# VPNs

What VPN do you use? (answer in chat)

When do you use a VPN?

Does your organization provide you with a VPN?

What about Split-Tunneling?

# Nebraska Security Community Slack

Intent: Share information, resources, announcements, etc. relevant to the Nebraska Cybersecurity, IT Audit, Compliance, Privacy, etc. community.

Extends our community beyond monthly meetings.

Open to all in that space.

Please read the Code of Conduct pinned on #welcome  
Share ideas on how to make it better.

[https://join.slack.com/t/ne-cyber-security/shared\\_invite/zt-gps88s2c-CRsPSICUTKdbXjyO4tQVNg](https://join.slack.com/t/ne-cyber-security/shared_invite/zt-gps88s2c-CRsPSICUTKdbXjyO4tQVNg)

# Security News

SANS Breach - Phishing still works :-)

Haveibeenpwned Going Open Source - <https://haveibeenpwned.com/>

Security 2020 Elections - Volunteer at  
<https://www.eac.gov/help-america-vote>

Other news?

# Going for help

If you have an incident, please reach-out for help  
(according your your IR Plan)

- BBB Scam Tracker: <https://www.bbb.org/scamtracker>
- AARP, <https://www.aarp.org/FraudWatchNetwork>
- FBI, Internet Crimes Complaint Center (IC3):  
<https://www.ic3.gov/>
- StaySafeOnline (NCSA): <http://staysafeonline.org/>
- NICCS: <https://niccs.us-cert.gov/>