2020 A New Decade of Cyber Challenges!

Plano East Rotary club, March 12, 2020

Copyright © David Mandala 2020

Overview

- Your Smart Phone
- Your Email
- IoT (your house/office is listening/watching you)
- Smart TV’s, Digital Assistants
- Never Trust your ISP
- WiFi (wpa2 is cracked)
- Cable Modem Exploit
- The Network (the flat network is dead)
- Business and Cyber Insurance
- Texas Law has changed!

Copyright © David Mandala 2020

Your Smart Phone

- Your cell / smart phone is not really a phone.
  - It’s a computer equal to your laptop.
  - It has the same areas that can be hacked:
    - WiFi access.
    - Bluetooth access.
    - USB plug access.

Copyright © David Mandala 2020

Your Smart Phone

- How to you fix it?
  - Make sure to install Anti-virus protection on the phone.
  - If you are not using it turn it off:
    - Turn off WiFi and Bluetooth when not actively using them.
  - Never plug your phone into the USB charging stations at malls, airports, trade shows, etc.
    - There are hacks out there that will take over your phone and steal all of your data.

Copyright © David Mandala 2020

Your Smart Phone

- Another way to be attacked on your smart phone is via Smishing. This uses your SMS as an attack point. You get an SMS from your bank, credit card company etc, saying you've been hacked and to click here to reset passwords or call a specific number to fix the problem.
  - This is an attack, if you do what it says you will be hacked and lose data and possibly money.
  - Call your bank, credit card company with your contact numbers (the ones on the back of the credit card, etc.), ask them if there is an issue. Likely there is not….

Copyright © David Mandala 2020

Email

- Email is an attack point.
  - Never ever blindly click on an attachment or a click point.
    - Ask yourself were you expecting the email?
    - Check the from and to addresses are they correct?
    - Hover over the click point and see if the URL makes sense to you.
    - Call the person and see if they sent the email.

Copyright © David Mandala 2020

Email

- Email is an attack point.
  - If you get an email purporting to be from your bank, credit card company, etc. Treat it like you would do with a fake SMS.
    - Call your bank, or credit card company with your contact numbers not the ones in the email and again NEVER click on a link.

Copyright © David Mandala 2020

Email

- Email is an attack point.
  - Some people are using the Coronavirus to scare people into clicking. This email appears to come from the CDCP and WHO.

Copyright © David Mandala 2020

Internet of Things

- The FBI say's you need to secure your Smart TV
  - They are called Smart TV's because they are connected to the Internet. You likely have one at home, in your office, etc.
  - Many have camera's and microphones built in! (Did you know that?)
  - Are the manufacturer and app developers watching you?
  - Worse the device can be a gateway into your home for hackers!
  - Are you a lawyer, real estate broker, financial adviser, CPA, etc. Could you be in additional legal trouble if information leaves your office?

Copyright © David Mandala 2020

Internet of Things

- The FBI say's you need to secure your Smart TV.
- Know exactly what features your TV has and how to control those features.
- DON'T depend on the manufactures default setting. Change passwords if possible. Find how to turn off mic and camera.
  - Can't turn off mic and camera? Do you really want that model?
  - If nothing else you can put black tape over the camera.
- Can the manufacturer reach in and update the firmware?
- Read and understand the privacy policy of the TV manufacturer and streaming services you use.

Copyright © David Mandala 2020

Internet of Things

- The rest of the IoT is as bad or worse then Smart TV's Digital assistants, fitness trackers, home security devices, thermostats, refrigerators, and even lights. That is not everything, how about interactive dolls, talking stuffed animals, the list goes on and on.
  - They all gather data from you and about you. How is the data collected how is it used?
  - Hackers can make use of an unsecured device and use it as a launching pad to attack your network and everything on your network.

Copyright © David Mandala 2020

Internet of Things

- Had an interesting thing happen at my own house that shocked me and really made me think.
- My wife got an Alexa puck over the holidays, and asked me if she could use it in her home office.
  - I added it to our IoT guest network (yes I have one).
  - She was talking to the Alexa puck upstairs in her office (with the door open) telling it to play music, when I heard a voice in the living room respond and music started playing in the living room!!!!
  - Turns out her Amazon Fire tablet that she uses for reading got a software update that added Alexa and it heard her across the house and down stairs!!!!! (Funny part was the reader was “off”.)

Copyright © David Mandala 2020

Internet of Things

- Lessons learned:
  - NEVER EVER TRUST IoT Devices to be “OFF”, that Amazon fire heard her voice from over 30’ away and a floor below!
  - The microphone in these devices is much more sensitive then you think.
    - Anything that runs off wall power PULL THE PLUG when not being used.
    - If it uses a battery and the lid is shut It’s not “OFF”, Hold the power button down until it really powers down and is really “OFF”.

Copyright © David Mandala 2020

Internet of Things

- What does this mean for business:
  - Never leave any of these devices “on” if you are talking private business with a client. You could trigger it and create a data leak that could be expensive.
    - ***Unplug it!***
  - Understand what you have bought and know how to limit exposing your private business and conversations.
  - Make sure you keep all of your IoT devices firmware up to date to limit your security risks.

Copyright © David Mandala 2020

Internet Service Providers

- They are in business to make a profit not to make sure you are secure, if fact if you read your service agreement you will see how little liability they have.
- They provide a connection to the Internet, no more no less (well sometimes less when the connection goes down).

Copyright © David Mandala 2020

Internet Service Providers

- What happens when you order service from an ISP?
  - They send an installer to install your service, likely that person is a contractor and not an employee.
    - They connect the service, plug in the cable modem or router, turn it on and if the blinky lights blink in the correct pattern they are “done”. They never touch any of the internal firewall or quality of service settings.
    - In many cases the ISP has a back door into your business, they can come into your network unless you have your own firewall router blocking them!

Copyright © David Mandala 2020

Internet Service Providers

- ISP’s are not responsible for your security
- Many of the installers are not employees of the ISP but have access to the passwords to the Cable Modems and Routers they install.
- It is your responsibility to secure your own network. How do you do that? We will talk about that a little be later.

Copyright © David Mandala 2020

WiFi

- WiFi is dangerous in many ways:
  - WPA2 the wireless security method has been cracked for years. So really you have NO security on your entire network if you have WiFi on!
  - It is a radio, and you can’t control how far it reaches outside of your office. Radio’s can be snooped.
    - If you are in a multi-story building you can be snooped from above, below or to the side! Parking lots can be used for snooping.

Copyright © David Mandala 2020

WiFi

- WiFi is dangerous in many ways:
- WiFi is convenient in many ways too, but what is the price of convenience?
- Just leaving WiFi on when you are not using it is leaving a vector for attack. If you are not using WiFi TURN IT OFF.
- What can you do to secure WiFi, we will talk about it shortly.

Copyright © David Mandala 2020

Cable Modems

- Even your cable modem can’t be trusted!
  - New vulnerability announced called Cable Haunt
  - Hundreds of millions of cable modems are vulnerable to critical takeover attacks right now.
- What can you do about it? Well we will talk about that in a bit.

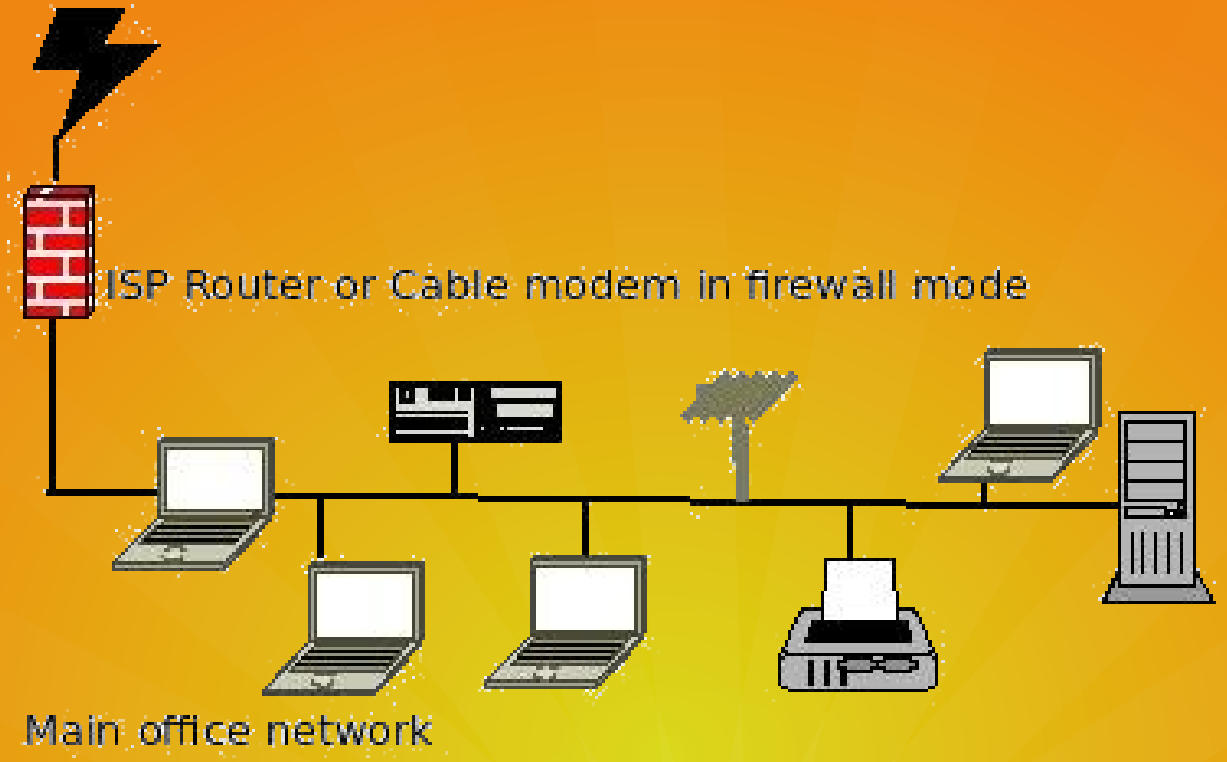
Copyright © David Mandala 2020

Your NETWORK

- In all likelihood your network is a flat network.
  - What is a flat network?
    - It’s a network that has a single entry point, a cable modem or router owned by the ISP.
    - All other devices are behind that entry point. All devices can reach all other devices within the network.
    - Most flat networks also have WiFi turned on. This means anyone that comes in via WiFi has access to EVERYTHING on your network.

Copyright © David Mandala 2020

Flat Network



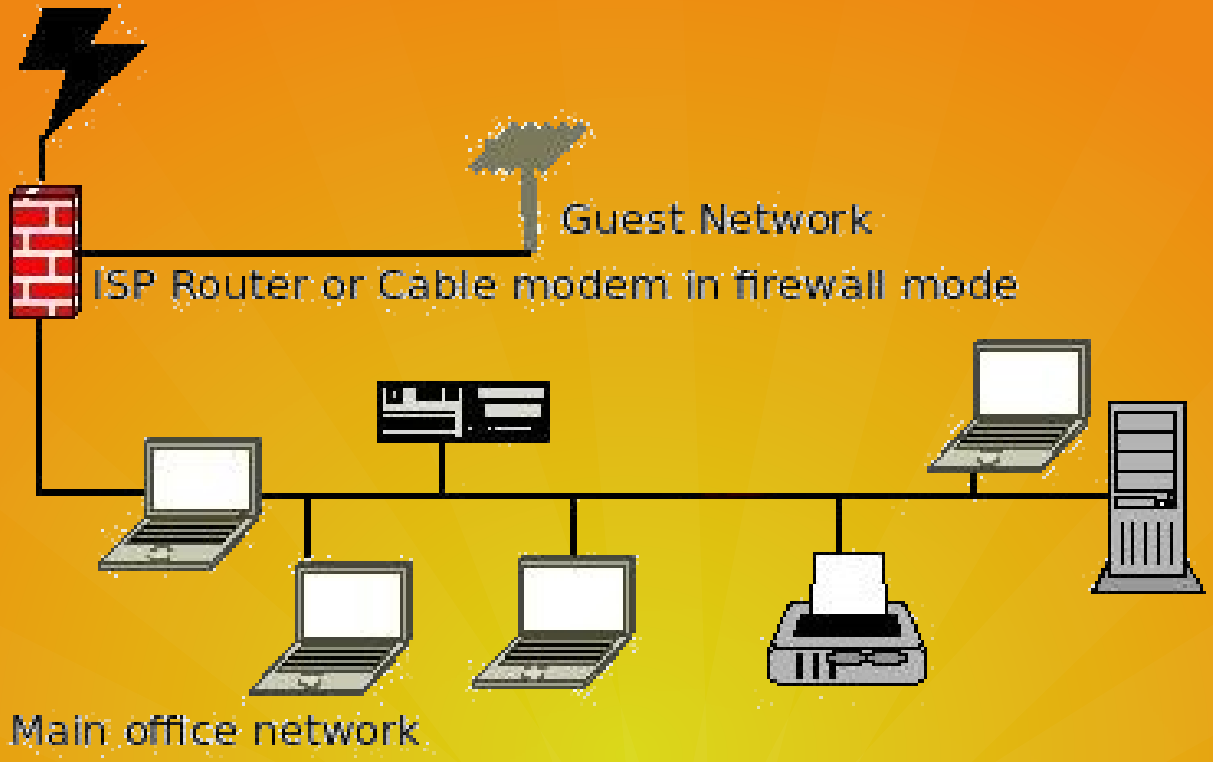
Copyright © David Mandala 2020

Segmented Network

- The day of the flat network is dead. The FBI has finally recommended that owners of IoT devices isolate them from their primary network. This creates a segmented network. This is exactly the same advice I and other security experts have been giving for years.
  - What is a segmented network?
    - It’s a network that splits into separate segments, devices in one segment can’t reach devices in other segments.

Copyright © David Mandala 2020

Segmented Network



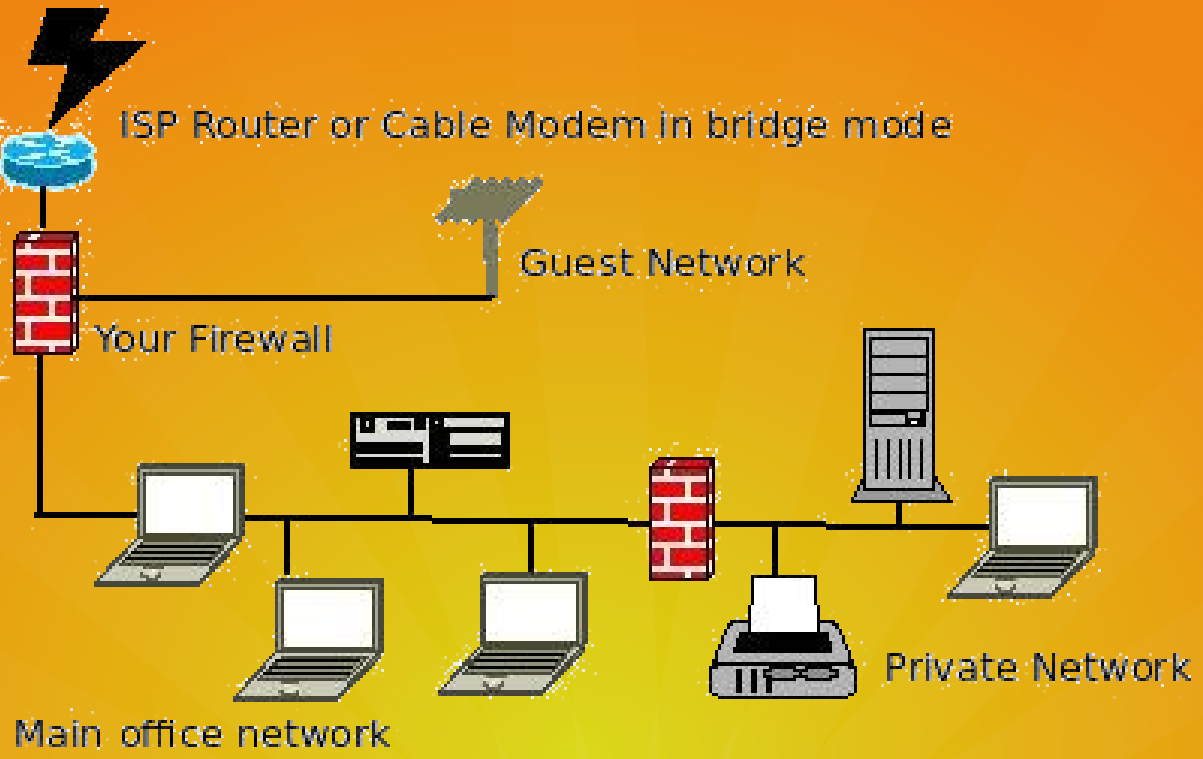
Copyright © David Mandala 2020

Secure Segmented Network

- So the FBI has finally recommended using segmented networks.
- As you saw from the prior slide this does help to keep you safer but is it truly secure as it could be. What else could you do to be more secure?
- Create a Secure Segmented Network, add your own firewall that the ISP has no control over. Put the ISP's device into bridge mode and put your own firewall between the ISP's device and your network. Turn off WiFi in your network. Add as many segment subnetworks as you need.

Copyright © David Mandala 2020

Secure Segmented Network



Copyright © David Mandala 2020

Secure Segmented Network

- Segment subnetworks can be VLAN’s (virtual LAN), if you control the FIREWALL and your switches you can add as many VLAN’s as you need for security.
  - You need a firewall and managed switches that understand VLAN’s.
  - A VLAN can contain a single machine.
  - VLAN’s allow access to the Internet but not other VLAN’s.
  - VLAN’s can protect you from internal attacks.

Copyright © David Mandala 2020

Business and Cyber Insurance

- Business insurance will not protect you from Cyber losses especially if you don’t keep all security patches up to date.
- Cyber insurance will not protect you from cyber losses if you are in any way at fault.
  - If you don’t keep your machines up to date with security patches and have a large loss you are going to find that the insurance company will bow out of covering you. Ask your insurance agent.

Copyright © David Mandala 2020

Texas Law

- Texas Businesses Must Report Data Breaches Under New Law Effective Jan. 1, 2020
- Under HB 4390, which was approved by the Texas Legislature in 2019, businesses operating in Texas are now required to provide notice within 60 days if they experience an online data breach or other unauthorized access of customer's personal information.

Copyright © David Mandala 2020

Texas Law

- Under the revised statute, notifications to affected customers must include the following information:
  - A detailed description of the nature and circumstances of the breach, or the use of sensitive personal information acquired as a result of the breach;
    - The number of residents of this state affected by the breach at the time of notification;
    - The measures taken by the person regarding the breach;
      - Any measures the person intends to take regarding the breach after the notification under this subsection; and
      - Information regarding whether law enforcement is engaged in investigating the breach.
- Furthermore, if more than 250 Texans are impacted by a data breach, Texas businesses are required to report the breach to the state's attorney general.

Copyright © David Mandala 2020

Summary

- IoT devices are a high risk to privacy and to network security.
- The FBI and security experts recommend putting all IoT devices on their own network segment.
- Don’t trust your ISP to provide anything except a connection to the Internet.
- WiFi is fundamentally broken, if you don’t absolutely need it, turn it off.
- Over 200 million Cable Modems are at risk currently.

Copyright © David Mandala 2020

Summary

- The days of flat networks are gone, for security you need a segmented network, and the more segments the better in some cases.
- Provide your own “Firewall”, do not rely on your ISP’s devices, they could be used to gain access to your network and they are likely not configured beyond the default settings.
- Business and Cyber Insurance are of limited help if you don’t keep your security updates current on all devices.
- And finally Texas Law has changed, effective January 1, 2020, you must notify your customers of any data loss of their data with some interesting requirements.

Copyright © David Mandala 2020

Bonus Question

- On the next slide is a common device, can anyone tell me what it is?

Copyright © David Mandala 2020

What is this?

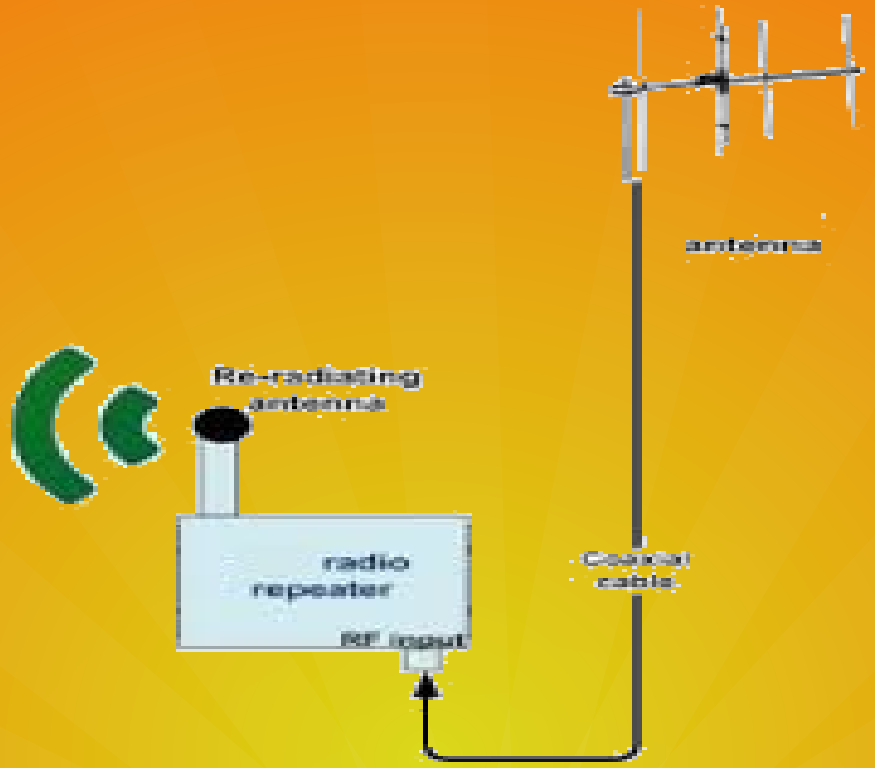
Copyright © David Mandala 2020

Bonus Question

- It’s a radio controller that happens to control access to a car. It’s NOT just a car key.
- Using a common tool (from amateur (HAM) radio) called a repeater I can use your “key” in your house to start your car and take it away! How?

Copyright © David Mandala 2020

Bonus Question



Copyright © David Mandala 2020

Bonus Question

- All you have to do is stand next to the car, sweep the antenna toward your house until you see a radio signal, then press the unlock button on the door, if the car lets you in step on the brake and press the start button! And away we go!!!!!
- How to avoid that, the “key” needs to go into a RFID blocking box or sleeve when not in use so it can’t be seen by a repeater.

Copyright © David Mandala 2020

Bonus Question

Copyright © David Mandala 2020

References

- https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesday-internet-of-things-iot
- https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/tech-tuesdaysmart-tvs
- https://www.zdnet.com/article/fbi-recommends-that-you-keep-your-iot-devices-on-a-separate-network/
- https://www.routersecurity.org/vlan.php
- https://capitol.texas.gov/tlodocs/86R/billtext/pdf/HB04390F.pdf#navpanes=0

Copyright © David Mandala 2020

Thank you for your time.

Copyright © David Mandala 2020