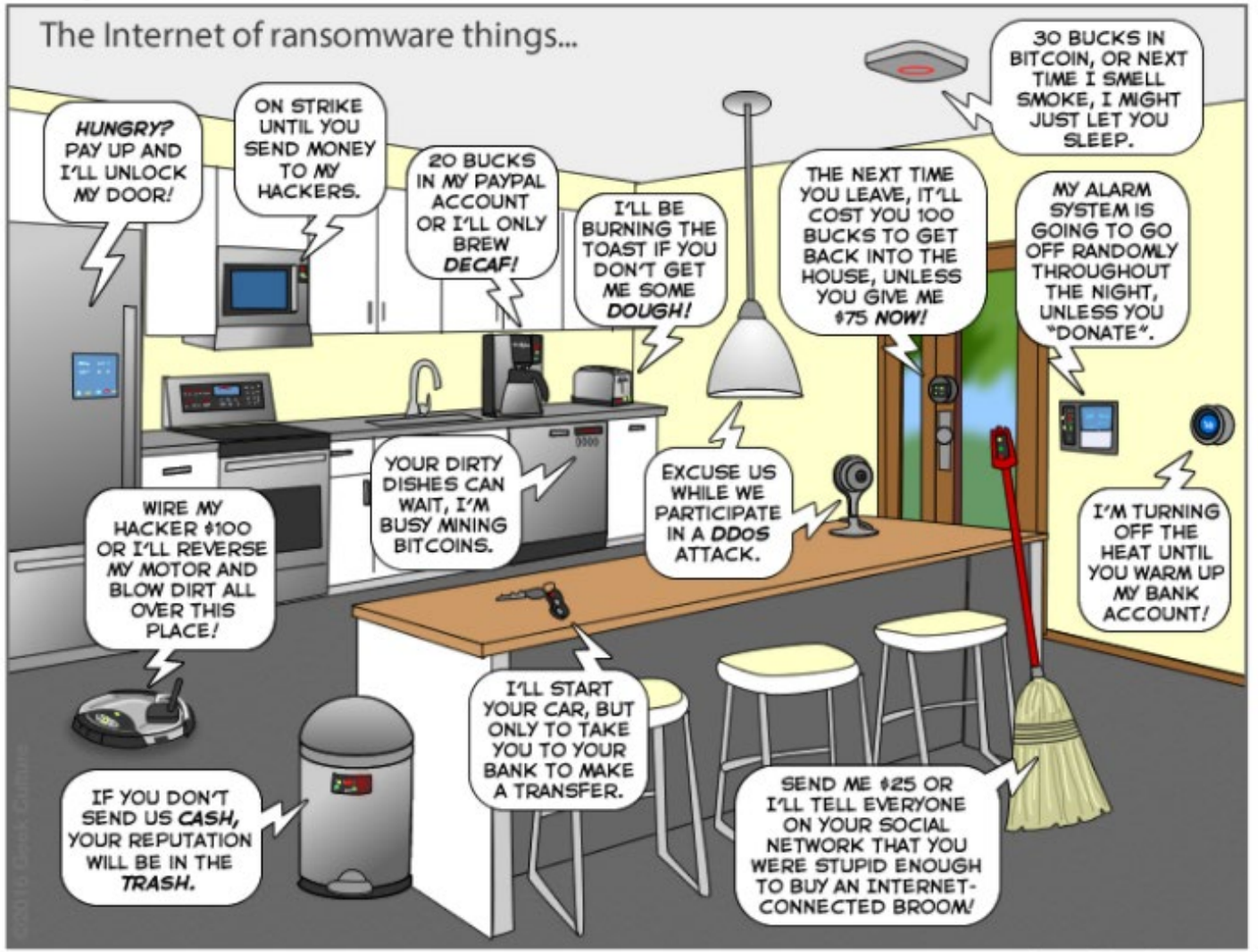
Home Automation Security

Bill James, APCUG Advisor, Region 8

Member, APCUG Speakers Bureau

Vice President, Computer Club of Oklahoma City

The Joy of Tech™ by Nitrozac & Snaggy



You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com

Agenda

- 1999 - 2020
- Home Networks
- Home Automation
- Hackers
- Privacy
- Smart TVs and Security
- Do Your Research
- Security and Your Router
- Home Automation Devices and Security
- Consumer Reports and Home Automation
- Resources

In 1999

- 4% of the world's population was online
- Kevin Ashton, British technology pioneer, coined the term Internet of Things
- Neil Gershenfeld of the MIT Media Lab wrote *When Things Start to Think*

In 1999

- Neil Gross, University of British Columbia professor, speaking to Business Week:

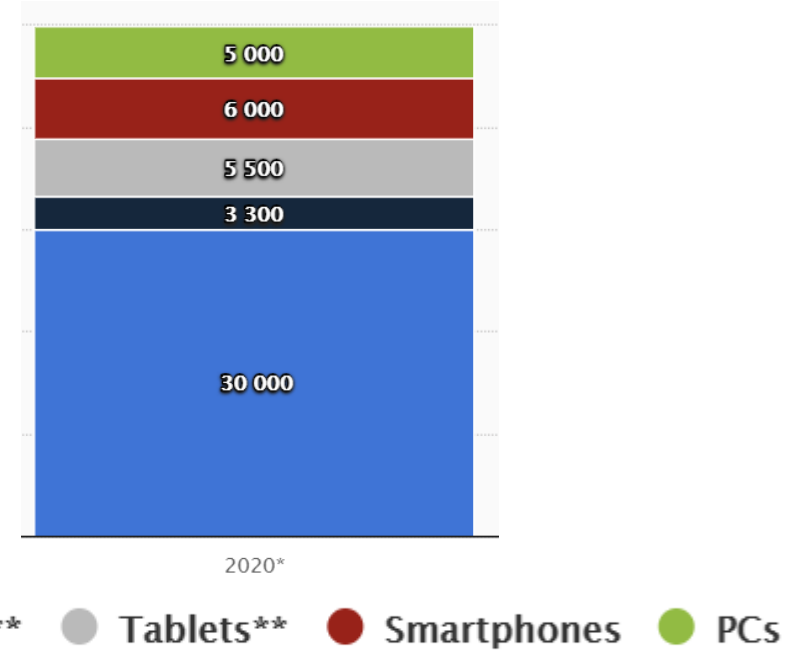
  "In the next century, planet Earth will don an electronic skin. It will use the internet as a scaffold to support and transmit its sensations."

- This skin is already being stitched together. It consists of millions of embedded electronic measuring devices: thermostats, pressure gauges, pollution detectors, cameras, microphones, glucose sensors, EKGs, electroencephalographs.
- These will probe and monitor cities and endangered species, the atmosphere, our ships, highways and fleets of trucks, our conversations, our bodies – even our dreams."

2020

- Neil Gross was correct.
- Almost 5 billion of the world's population is connected
- Estimated 50 million connected things are in use worldwide

WORLD INTERNET USAGE AND POPULATION STATISTICS 2020 Year-Q3 Estimates						
World Regions	Population (2020 Est.)	Population % of World	Internet Users 30 Sept 2020	Penetration Rate (% Pop.)	Growth 2000-2020	Internet World %
Africa	1,340,598,447	17.2 %	631,940,772	47.1 %	13,898 %	12.8 %
Asia	4,294,516,659	55.1 %	2,555,636,255	59.5 %	2,136 %	51.8 %
Europe	834,995,197	10.7 %	727,848,547	87.2 %	593 %	14.8 %
Latin America / Caribbean	654,287,232	8.4 %	467,817,332	71.5 %	2,489 %	9.5 %
Middle East	260,991,690	3.3 %	184,856,813	70.8 %	5,527 %	3.7 %
North America	368,869,647	4.7 %	332,908,868	90.3 %	208 %	6.8 %
Oceania / Australia	42,690,838	0.5 %	28,917,600	67.7 %	279 %	0.6 %
WORLD TOTAL	7,796,949,710	100.0 %	4,929,926,187	63.2 %	1,266 %	100.0 %



2020 - The 5 Biggest Cybersecurity Trends

- **Artificial intelligence (AI) will play an increasing role in both cyber-attack and defense**. AI is the new arms race, but unlike earlier arms races, anyone can get involved – there's no need for the sort of resources that were previously only available to governments.
- **Political and economic divisions between east and west lead to increased security threats.** In 2019, we also saw the US government effectively embargoing partnerships between US tech firms and the Chinese mobile giant Huawei, due to fears over the close links between Huawei and the Chinese state.

2020 - The 5 Biggest Cybersecurity Trends

- **Political interference increasingly common and increasingly sophisticated.** Targeted disinformation campaigns aimed at swaying public opinion have almost become an accepted feature of democracy today.

2020 - The 5 Biggest Cybersecurity Trends

- **The cybersecurity skills gap continues to grow.** During 2020, research suggests the number of unfilled cybersecurity jobs will increase from just 1 million in 2014 to 3.5 million.
- This deficit of skills is likely to become a growing matter of public concern during the early part of this new decade.
- The threats we face in cyberspace today, from thieves attempting to clone identities to carry out fraud, to political disinformation campaigns designed to alter the course of democracies, will only become more intense unless there are sufficient people with the skills to counter them coming through the pipeline.

2020 - The 5 Biggest Cybersecurity Trends

- **Vehicle hacking and data theft increases.** Even before we get into the subject of self-driving cars, vehicles today are basically moving data factories.
- Modern cars are fitted with an array of GPS devices, sensors, and in-car communication and entertainment platforms that make them an increasingly profitable target for hackers and data thieves.

Ransomware Targets the Internet of Things (IoT)

- Researchers have been detailing security flaws in IoT devices for years. In 2019, there were multiple product recalls on smart home devices due to critical security issues. While there was not a major security incident involving enterprise IoT, In 2020 the pendulum swung the other way.
- Last year, ransomware attacks targeted individual machines in hospitals and local governments, which led to whole cities being taken offline.

Ransomware Targets the Internet of Things (IoT)

- If these tactics expand beyond targeting specific machines to hold data for ransom, it's reasonable to assume that attackers will expand the ransomware model to target larger groups of IoT devices, such as medical devices – including pacemakers and insulin pumps – or focus on other systems like traffic control.
- Compromised machine identities make it entirely possible to use code signing certificates to "kidnap" IoT devices using malware or use TLS certificates to create zombies.
- It seems quite possible that we'll see an entire IoT network held for ransom in 2021.

What is a TLS certificate?

- A digital certificate comes in the form of server-side TLS certificate.
- TLS stands for transport layer security, and in common use it's a method of combining the advantages of public-key cryptography, external third-party (out-of-band) validation, and per-session encryption.
- TLS is the modern name for SSL, the preceding standard.

Home Networks

- When we talk about home networks, we generally mean a system composed of at least two devices connected to each other.
- Usually, these devices also connect to the Internet.
- Technically, if you have only one device connected to the Internet, it's part of a larger network.
- But you wouldn't have a network of your own.

Home Networks

- Most home network designs have as their foundation a centerpiece device such as a router.

Example Only
D-Link DIR-842 Wi-Fi AC1200
Gigabit Router

Home Automation

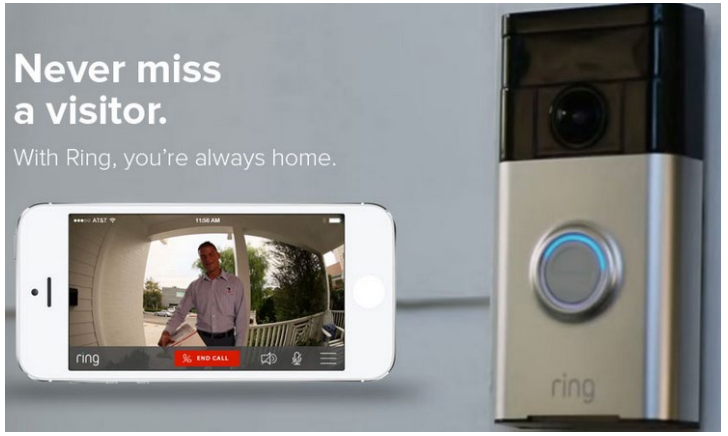
- Are you an early adopter?
  - Security features not fully implemented or non-existent
- Are you already using some type of Home Automation?
- Are you worried about home IoT (Internet of Things) devices listening in on your conversations?
- In 2016, Arkansas police demanded that Amazon turn over information collected from a murder suspect's Echo.

Home Automation

- Amazon's attorneys contend that the First Amendment's free speech protection applies to information gathered and sent by the device
- As a result, Amazon argues, the police should jump through several legal hoops before the company is required to release your data
- According to a March 2017 Gartner survey (10,000 people in the U.S., U.K., and Australia):
  - Nearly two-thirds of consumers are worried about their IoT devices listening to their conversations

Home Automation

- Are you concerned about your devices being compromised?
  - Security system
  - Smart doorbell / video camera
  - Refrigerator
  - Smart TV
  - Smart lightbulbs….



Home Automation

- Check out the Tech Specs

Nest Hello Doorbell

Overview | Tech Specs

Operating Temperature

5° to 104°F (–15° to 40°C)

Weather resistance

IPx4 rating

Security

128-bit AES with TLS/SSL

Wireless

802.11a/b/g/n/ac (2.4GHz/5GHz) 2x2 MI...

Hackers

What Can a Hacker Do With IoT Devices

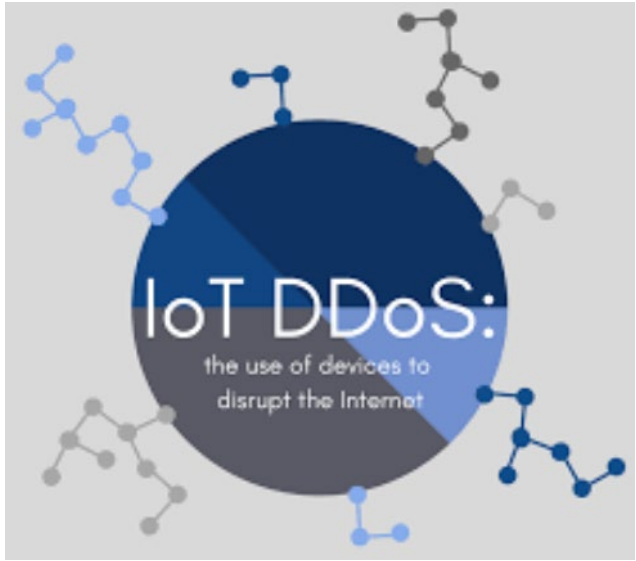
- Smart locks and Wi-Fi cameras
  - Allow them to easily break into your house
  - Allow them to see if anyone is home by looking at your video feed
- Smart Outlets / Thermostats
  - Gain temporary access to your Wi-Fi network where smart outlets are connected
  - Get remote access to the plug and your network

Hackers

- Routers, security cameras, health-and-fitness apps, cars are sold with vulnerabilities that leave them open to attack
- Most rely on an email username and password to access the app and a Wi-Fi network name and password for the setup process.
- Incidents illustrate need for consumers to be better educated and more vigilant when it comes to digital security
- Don’t come with a lot of security features

Hackers

- Cybercriminals are not always trying to steal our personal and banking information
- Sometimes they just want to create havoc
- They can use IoT gadgets to disrupt services or shut down websites
- DDoS (Distributed Denial of Services) attacks occur when servers are overwhelmed with more traffic than they can handle



Hackers

- 2014 - First cyber attack used 100,000 home routers, multi-media devices, televisions, and at least one refrigerator
  - 25% of the devices hacked were home appliances
  - 750,000 malicious e-mails sent
- 2016 - Dyn cyber attack believed to have been executed through a botnet consisting of a large number of Internet-connected devices

Hackers

- Affected services included:
- Amazon.com
- Ancestry.com
- BBC
- CNN
- Comcast
- DirecTV
- Fox News
- HBO
- Indiegogo
- PayPal
- Pinterest
- Spotify
- SquareSpace
- Starbucks
- Swedish Gov't
- Twitter
- Visa
- Verizon
- Walgreens
- Wall St. Journal
- Xbox Live

Hackers

- These types of attacks are performed with a botnet
- Instead of a couple of computers being taken over without our knowledge
- A botnet can be a number of Internet-connected devices
- Hackers can control our IoT gadgets to perform large-scale hacks or scams
- Your smart refrigerator, smart TV, thermostat, and webcams can be infected with malware to create a botnet

Hackers

- Many security researchers have discovered ways to hack into various Home Automation devices
  - SmartThings
  - Insteon
  - Philips
  - Ring

Hackers

- It's easy to talk about the IoT (Internet of Things) security issues in theory, but what actually happens when the IoT gets hacked?
- Understanding exactly what happens when IoT devices get hacked and how they get hacked is crucial in helping to protect your home. Knowledge, of course, isn't a cast iron guarantee you will avoid be hacked, but it certainly puts you in a much stronger position.
- Let's take a look at four real life examples of the IoT being hacked.

Hackers

Unsecured University IoT

- Verizon's Data Breach Digest 2017 report details the example of an unnamed university where the network was flooded with Domain Name Service (DNS) requests for seafood restaurants.
- While it sounds like a student prank, it was an outside attack by hackers that used 5,000 IoT devices such as vending machines and lighting systems.
- The hack was achieved through a brute force attack which took advantage of weak passwords so malware could be deployed and bring the university's network to a standstill.

Hackers

IoT Cameras Hacked

- The popular IoT security camera range – NeoCoolCam – has been found to contain a major security flaw which means that they can easily be hacked from outside the network they're on.
- Given the security nature of the devices, these cameras can easily be compromised for unauthorized surveillance or even as a steppingstone to get even deeper into a network.
- Researchers at Bitdefender have found that all it takes is for the easily accessible login screen to be manipulated in order to take control of any of the 100,000+ cameras currently in use.

Hackers

The Mirai Botnet

- Poor password management is one of the biggest flaws in data security and the Mirai botnet certainly takes advantage of this.
- A piece of malware which infects network devices running on Linux, Mirai instructs these devices to constantly search the internet for vulnerable IoT devices.
- The fatal flaw contained within these IoT devices is that their factory set default username and passwords have not been changed.

Hackers

The Mirai Botnet (Con't)

- As Mirai is loaded with a list of these default details, it's able to quickly take control of these devices and Mirai was also involved with an attack on Liberia's Internet infrastructure.

Hackers

Hacking a Jeep

- Perhaps the most disturbing and dangerous example of IoT devices being hacked is the case of a Jeep Cherokee 4×4 vehicle being compromised.
- Security researchers Charlie Miller and Chris Valasek were able to identify a zero-day exploit which allowed them to send instructions to the vehicle through its infotainment system.

Hackers

Hacking a Jeep (Con't)

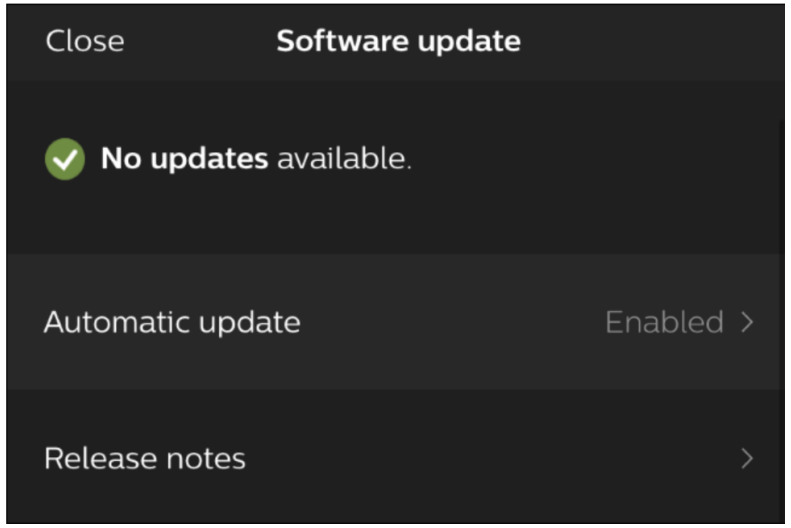
- Not only did this provide them with the opportunity to remotely change the in-car temperature, they could also influence the vehicle's steering and braking systems.
- All it required was knowledge of the individual vehicle's IP address to take control.

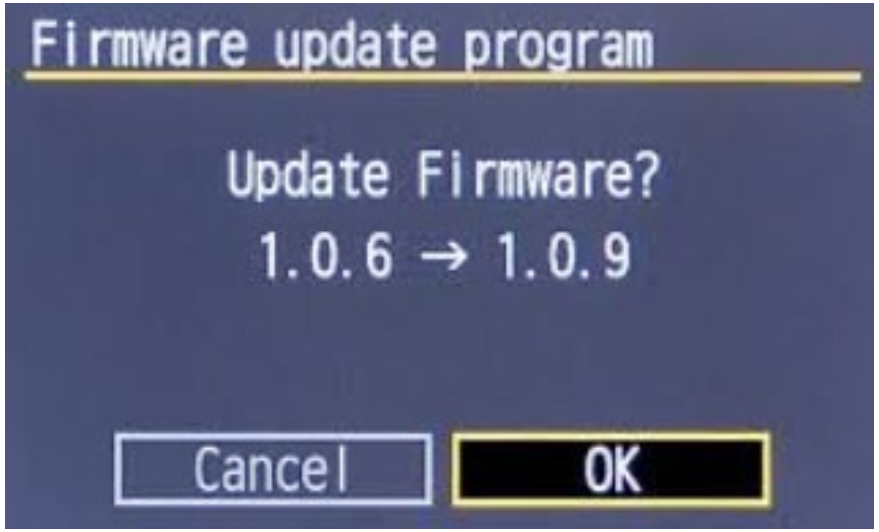
Hackers

- All four of these examples demonstrate just how far behind IoT device manufacturers are when it comes to the security of their devices.
- Naturally, the manufacturers have a lot to do to ensure their devices are safe from the moment they're installed, but the owners of these devices also need to be mindful of good password practices.

Hackers

- Companies release new firmware to patch these holes
- Always update devices with new patches
- Turn on Automatic updates





Privacy

- If there's a depressing slogan for the early era of the commercial internet, it's this: "Privacy is dead – get over it."
- If privacy isn't dead yet, then billions-upon billions of chips, sensors, and wearables will seal the deal
- Most IoT devices require location services turned on and to be functional are in listening mode 24/7

Privacy

- Be forewarned, IoT is about more than just Internet-connected refrigerators
- It also represents a move to have even more objects networked and embedded
- Sensor-embedded kitchen devices might support precision-control cooking in one home, while in another offers remotely monitored food consumption of an elderly relative

Smart TVs and Security

- Does your TV have a built-in microphone & web cam?
- TV's store personal information – usernames & passwords for all services you subscribe.
- How about the password for your Amazon account….
- "Red button" attack (on / off remote button) could allow a hacker to intercept the sound, picture, and data sent by a broadcast
- Can send content he/she wants to your TV

Smart TVs and Security

- Smart TV needs to be as secure as your computer system
- Hacker can get control of web cam and spy on whatever you are doing in your living room or bedroom
- Voyeuristic or just when you are out of the house = potential burglary
- Old school - put a Post-it over your web cam

Do Your Research

- Before purchasing, research
  - Device capabilities
  - Do they work together
  - Security Features
  - Do you need a hub to connect your devices
  - Does company provide firmware updates
  - Think USA

How Secure Are You?

- Each device should have a secure way of accessing the network
  - Disable unrequired features and services
- Malware is infesting a growing number of IoT devices, but their owners may be completely unaware of it.
- Poor security on many IoT devices makes them soft targets.

Security and Your Router

- Most IoT devices connect to the Internet through ‘Wi-Fi’ or ‘wired’ connection via a router
- A router determines where to send information from one device to another
- A router has three separate, but related jobs:
  - Ensures information doesn’t go where it’s not needed
  - Makes sure information securely makes it to the intended destination
  - Wraps data in a secure envelope (encryption) for outbound traffic

Setting Up Your Router

- Find best position for it
- Fastest Internet provider and up-to-date hardware, etc. doesn't help if router isn't in the correct place
- Place it near center of your home
  - Not on the floor – desk, table, shelf preferable
  - Not next to a wall – will absorb signal
  - Not next to other Wi-Fi devices

Setting Up Your Router

- Adjust the antennas
  - Make sure pointing in right direction to optimize range and performance
  - Try positioning them perpendicular to each other
  - One facing up and another facing out
- Update firmware – no telling how long its been in the box

Security and Your Router

- Change SSID (name of the router network) and Admin log-in / password
- Can find default information on the Internet
- Default login for routers vary depending on the model and Manufacturer
- Most of them can be accessed using a combination of what's in this table

D-Link Model	Default Username	Default Password
DI-514, DI-524, DI-604, DI-704, DI-804	admin	(none)
DGL-4100, DGL-4300, DI-701	(none)	(none)
Others	admin	admin

Security and Your Router

- Change router name
  - Don’t use anything that identifies you
- Set up a ‘Guest’ network with it own SSID and password
  - Change password frequently
- No access to shared files or networked devices
- Activate encryption
  - WPA3 Personal for better security, or WPA2/WPA3 Transitional for compatibility with older devices

Security and Your Router

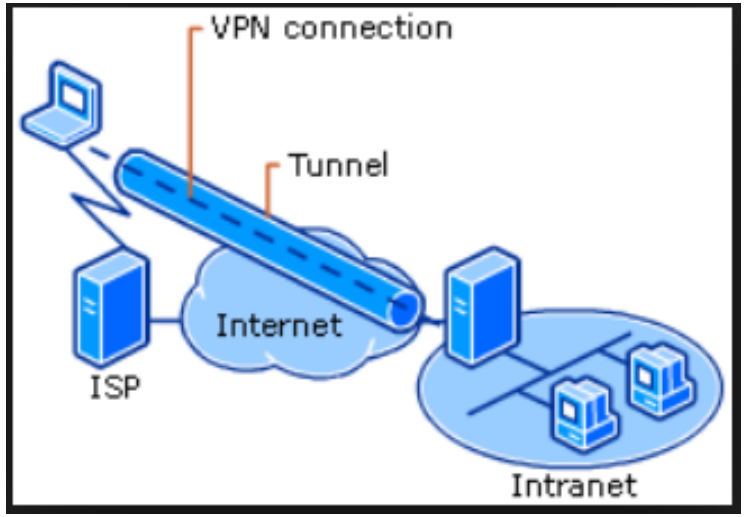
- WPA2 Personal (AES) is appropriate when you can't use one of the more secure modes. In that case, also choose AES as the encryption or cipher type, if available
- Activate router firewall = double protection
- Settings that turn off security, such as None, Open, or Unsecured, are strongly discouraged
- Turning off security disables authentication and encryption and allows anyone to join your network, access its shared resources (including printers, computers, and smart devices), use your internet connection, and monitor data transmitted over your network or internet connection (including the websites you visit)

Security and Your Router

- This is a risk even if security is turned off temporarily or for a guest network
- Don't create or join networks that use older, deprecated security protocols like WPA/WPA2 Mixed Mode, WPA Personal, TKIP, Dynamic WEP (WEP with 802.1X), WEP Transitional Security Network, WEP Open, or WEP Shared
- The above are no longer secure, and they reduce network reliability and performance. Apple devices show a security warning when joining such networks

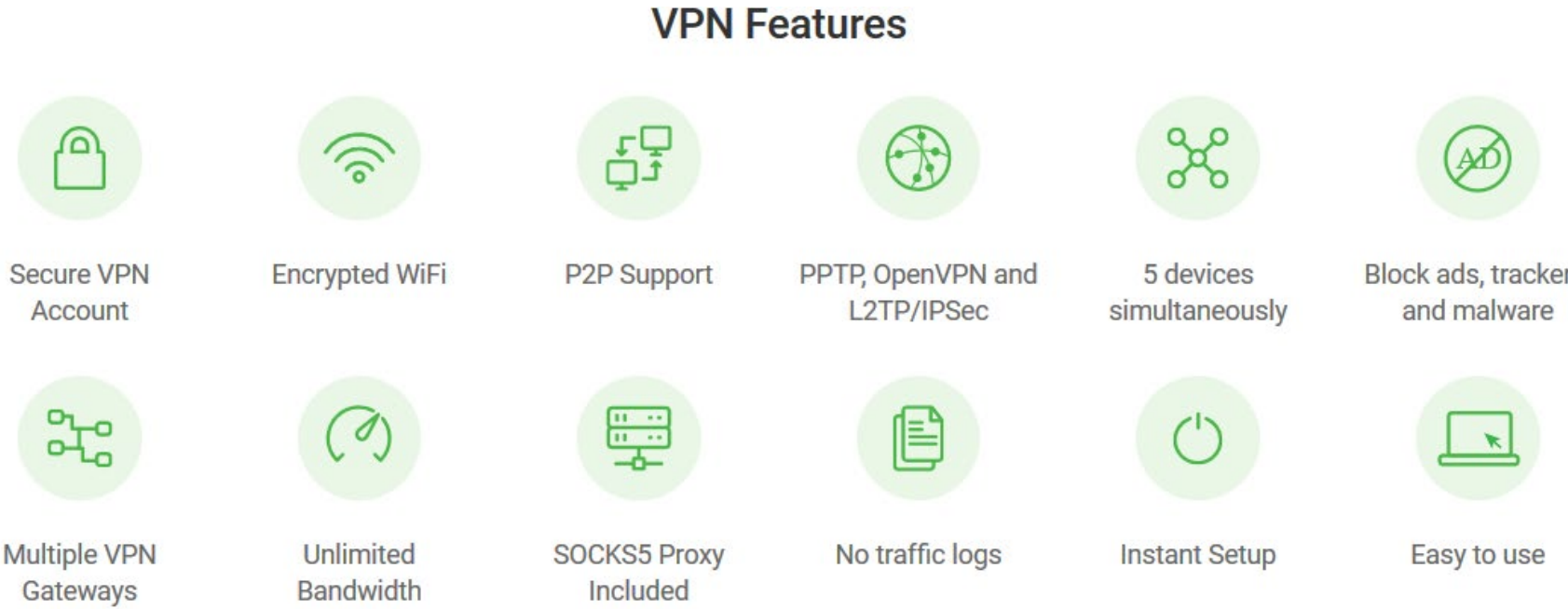
Security and Your Router

- Use a VPN
  - Makes a tunnel between your device and the Internet through a third-party server
  - Helps mask your identity or makes it look like you're in another country
  - Prevents snoops from seeing your Internet traffic
    - Like putting a postcard in an envelope



Security and Your Router

- Groovy Post recommends Private Internet Access (PIA), Denver, Colorado - $40/year
  - **Information is FYI/not recommended by APCUG or presenter*

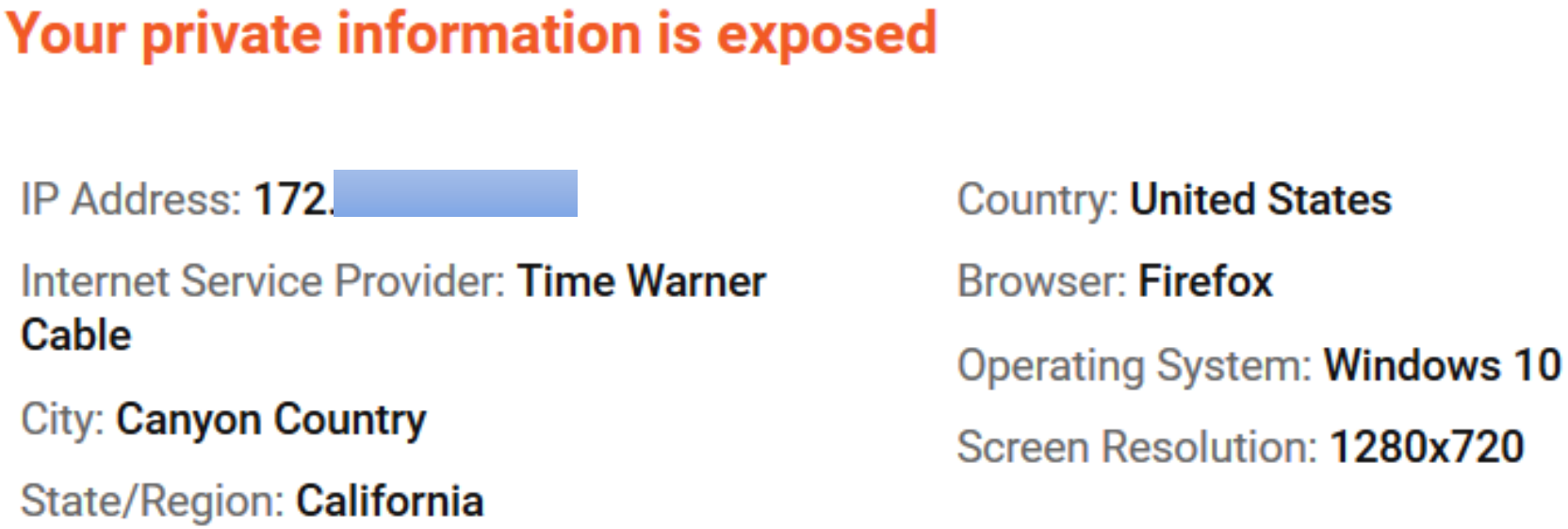


Security and Your Router

- “While the client software is quite spartan, the minimalist design makes it easy for non-technical people to use, while still allowing technophiles access to the inner workings under the “advanced” tab. This makes PIA a great choice for grandmas and system admins alike.” Cloudwards
- Lifehacker surveyed its readers in April, asking for an opinion on the best VPN provider and PIA was the winner

Security and Your Router

- PCMag – Excellent
- PCWorld – “Private Internet Access doesn't have a pretty interface, but this no-frills VPN gets the job done at a good price.”



Home Automation Devices & Security

- Passwords
  - Bill Burr wrote the password 'bible' in 2003
  - Worked for the U.S. Government
  - Now admits he was WRONG
- Guidelines about using numbers, symbols and capital letters have made computers easier to hack

Home Automation Devices & Security

- Experts now believe long passwords that contain minimum of four words are much harder to break than shorter ones with a mix of letters, characters and numbers
- 550 years to crack 'correcthorsebatterystaple’
- Three days to crack 'Tr0ub4dor&3’
- Infamous Edward Snowdon of WikiLeaks agrees
- Recommends using passphrases to be more secure

Home Automation Devices & Security

- Have a different password for each device
- Need to give your password to a technician?
  - In-person or via the phone
  - Change it after the repair
- Getting a new cable modem?
  - Change the password

Home Automation Devices & Security

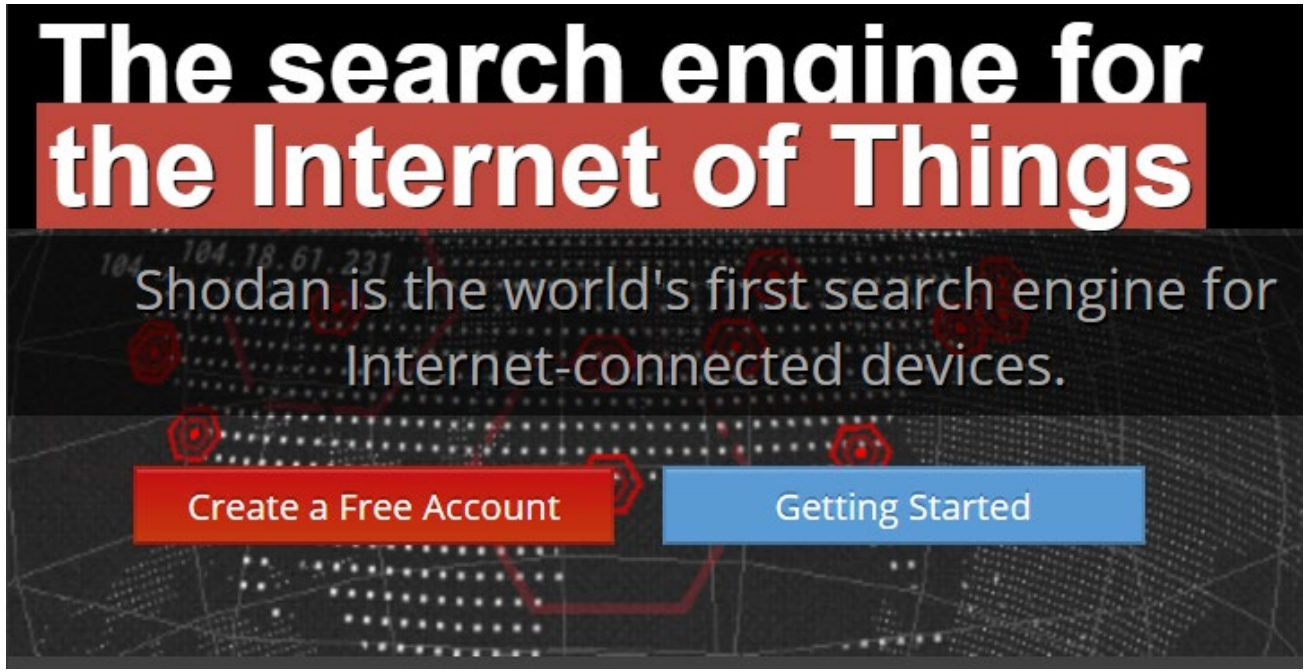
- What can you do to stay safe with your IoT devices?
- Use the Shodan Internet of Things Scanner*
  - World's first search engine for Internet-connected devices
  - It's FREE
- Shodan shows which of your devices are connected to the Internet

https://www.shodan.io/

**FYI / Not recommended by APCUG or presenter*

Home Automation Devices & Security

- Shodan shows which of your devices are connected to the Internet
- Where they are located
- Who is using them
- Plugin for Chrome and Firefox
- (Info from How-to-Geek)



Home Automation Devices & Security

1. Research capabilities and security features of an IoT device before purchase
2. Keep your router up-to-date or replace with a newer model.
3. Use strong passwords for your Wi-Fi network, not "123456" or "password"
4. Use a strong encryption when setting up Wi-Fi network access (WPA)
5. Disable unrequired features and services built-in to the devices
6. Disable or protect remote access to IoT devices when not needed
7. Use wired connects when possible
8. Maintain up-to-date anti-virus software
9. Regularly check manufacturer's website for firmware updates for your device

Consumer Reports & Home Automation

- CR partnering with cyber experts to:
  - Create a new open-source industry standard to make connected devices safer
  - With a baby monitor, parents can talk to their baby or caregiver when away from home
  - 2015 – Song playing through baby monitor – the Police's "Every Breath You Take"

CR Consumer Reports

Consumer Reports & Home Automation

- Lyrics were particularly ominous
  - “Every game you play, every night you stay, I’ll be watching you.”
- Consumers shouldn’t have to constantly play defense when the products aren’t engineered with basic privacy and security protections built in.

Consumer Reports & Home Automation

- CR launching first phase of collaborative effort to create new standard that safeguards consumers' security and privacy
- CR hopes industry will use the standard when building and designing digital connected device products
- Standard can also eventually be used by CR and others in developing test protocols to evaluate and rate products
- Consumers will make more informed purchasing decisions

Final Thoughts

- Always use unique, strong passwords or passphrases for each account. This will limit the impact if one of your passwords gets compromised. Recent data breaches have shown the importance of using unique passwords for each account.
- Cybercriminals will attempt to use passwords obtained from one site to breach others. When setting up a new account, be sure the password you select is strong and different from others you have used in the past.
- Wherever possible, set up multi-factor authentication on your accounts. Enabling MFA will require a second method to verify a user's identity after the password has been entered, making it more difficult for criminals to access your account if your password gets compromised. MFA can work via text message, hardware token, or through an authenticator app on a mobile device.

Final Thoughts

- Don’t click on links or open attachments in unexpected emails. Sender information on emails can be falsified, so it’s important to confirm with the sender in person or via a trusted phone number.
- Be careful when sharing personal information online. Cybercriminals will use whatever information they can find to try to impersonate you or compromise your accounts.
- Avoid doing online banking or working with sensitive information when on public wireless networks. By using a VPN, you can protect your network traffic when you’re connected to public Wi-Fi.
- Make sure your devices are updated regularly. Most systems can be configured to install updates automatically. Ensuring your devices have the latest security patches can help prevent attackers from compromising your systems.

Final Thoughts

- Clap your hands; lamp turns on. Clap them again; lamp turns off. Magic… that was 1986
- Home automation has come a long way since the humble days of the Clapper. There is a lot more choice of different home automation technologies and products, all claiming to be the best home automation system
- Make your choices wisely!

Resources

- 10 Things You Must Do With a New Router – Makeuseof.com
- http://bit.ly/2vFU4nS
- 12 Ways to Secure Your Wi-Fi Network – PC Magazine
- https://www.pcmag.com/article2/0,2817,2409751,00.asp
- Are My Smarthome Devices Secure? – How-to Geek
- http://bit.ly/2vGjCkO

Resources

- Consumer Reports
- http://bit.ly/2vPveS7
- Consumers are wary of smart homes that know too much – TechHive from IDG
- http://bit.ly/2vPyqgv
- Default Router Passwords - Lifewire
- http://bit.ly/2uqEmgv

Resources

- Dyn Cyber Attack - Wikipedia
- https://en.wikipedia.org/wiki/2016_Dyn_cyberattack
- Hackers are outsmarting IoT gadgets - Act now to protect yourself – Kim Komando
- http://bit.ly/2ftVGun

Resources

- Internet World Stats
- http://www.internetworldstats.com/stats.htm
- John Oliver interviews Snowden re passphrases
- http://bit.ly/1GPve2D
- Private Internet Access
- https://www.privateinternetaccess.com/
- Shodan
  - https://www.shodan.io/

Resources

- The 5 Biggest Cybersecurity Trends In 2020, Everyone Should Know About. https://www.forbes.com/sites/bernardmarr/2020/01/10/the-5-biggest-cybersecurity-trends-in-2020-everyone-should-know-about/?sh=51eb10487ecc
- The Internet of Things Connectivity Binge: What Are the Implications? (PEW Research Institute)
- http://pewrsr.ch/2vFTq9D
- Use a sentence instead of complicated passwords – Daily Mail
- http://dailym.ai/2uqtwHn

Questions

Home Automation Security
Bill James, APCUG Advisor, Region 8
Member, APCUG Speakers Bureau
Vice President, ccOKC

wjames (at) apcug.org

An International
Association of Technology
& Computer User Groups