

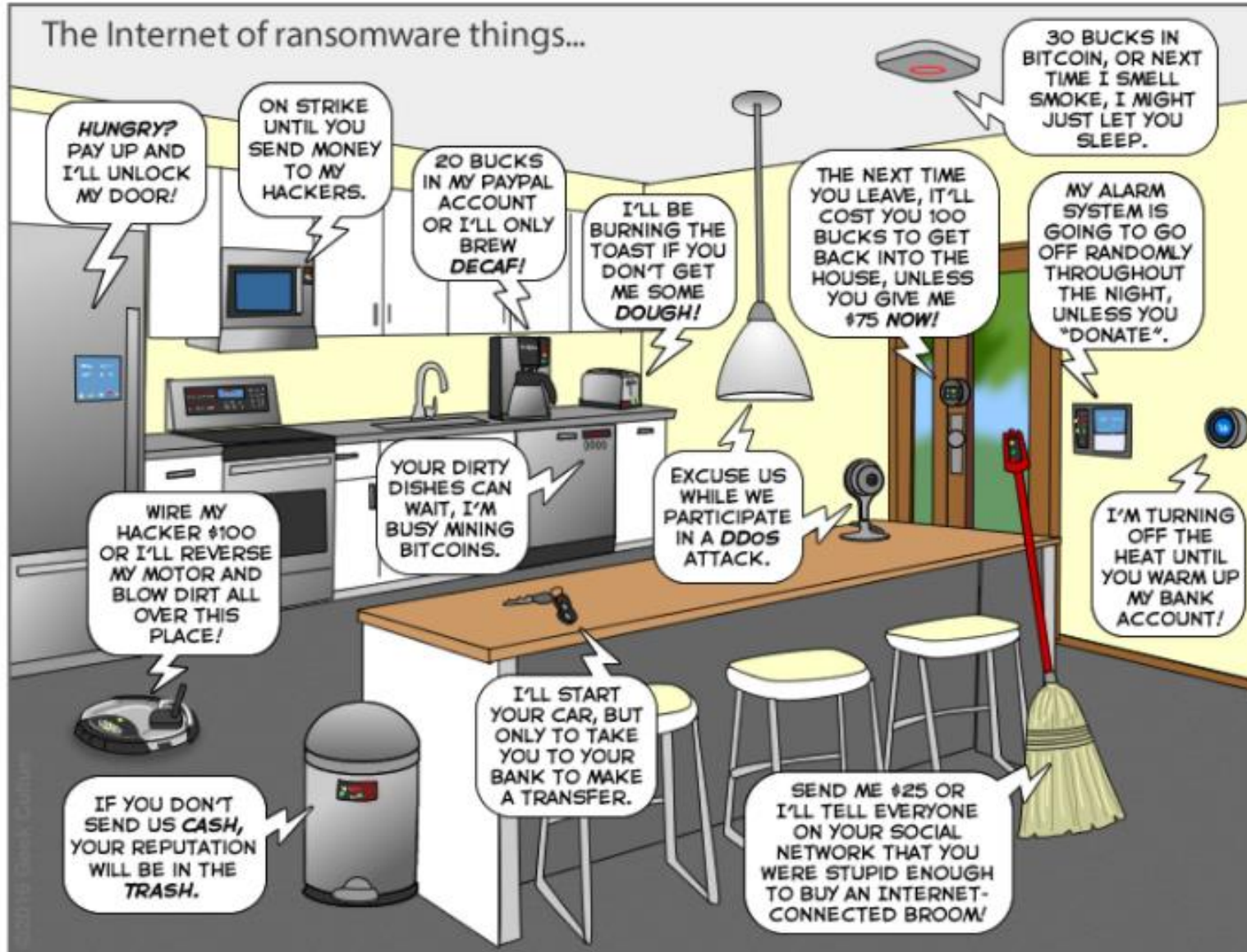


# Home Automation Security

Bill James, APCUG Advisor, Region 8

Vice President, Computer Club of Oklahoma City

## The Internet of ransomware things...



# Agenda

- 1999 - 2017
- Home Networks
- Home Automation
- Privacy
- Hackers
- Smart TVs and Security
- Do Your Research
- Security and Your Router
- Home Automation Devices and Security
- Consumer Reports and Home Automation
- Selling Your Home for More Money
- 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.”

# 2017

- Gross was correct
- Almost 4 billion of the world's population is connected
- Estimated 8.4 billion connected things are in use worldwide

WORLD INTERNET USAGE AND POPULATION STATISTICS MARCH 31, 2017 - Update						
World Regions	Population ( 2017 Est.)	Population % of World	Internet Users 31 Mar 2017	Penetration Rate (% Pop.)	Growth 2000-2017	Internet Users %
<a href="#">Africa</a>	1,246,504,865	16.6 %	353,121,578	28.3 %	7,722.1%	9.4 %
<a href="#">Asia</a>	4,148,177,672	55.2 %	1,874,136,654	45.2 %	1,539.6%	50.1 %
<a href="#">Europe</a>	822,710,362	10.9 %	636,971,824	77.4 %	506.1%	17.0 %
<a href="#">Latin America / Caribbean</a>	647,604,645	8.6 %	385,919,382	59.6 %	2,035.8%	10.3 %
<a href="#">Middle East</a>	250,327,574	3.3 %	141,931,765	56.7 %	4,220.9%	3.8 %
<a href="#">North America</a>	363,224,006	4.8 %	320,068,243	88.1 %	196.1%	8.6 %
<a href="#">Oceania / Australia</a>	40,479,846	0.5 %	27,549,054	68.1 %	261.5%	0.7 %
<a href="#">WORLD TOTAL</a>	7,519,028,970	100.0 %	3,739,698,500	49.7 %	936.0%	100.0 %

# Home Automation

- Are you an early adopter?
- Are you already using some type of Home Automation?
- Are you worried about home IoT (Internet of Things) devices listening in on your conversations?
- Arkansas police recently demanded that Amazon turn over information collected from a murder suspect's Echo.



# Home Automation

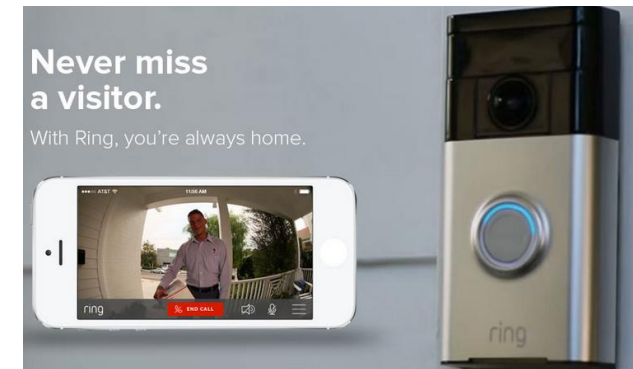
- Amazon's attorneys contend that the First Amendment's free speech protection applies to information gathered and sent by the device
- As a result, Amazon argues, the police should jump through several legal hoops before the company is required to release your data

# Home Automation

- 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

- Do you think your devices can be compromised?
  - Security system
  - Smart door bell / video camera
  - Refrigerator
  - Smart TV
  - Smart lightbulbs....



# Home Automation

- Routers, security cameras, health-and-fitness apps, cars are sold with vulnerabilities that leave them open to attack
- Some setup processes do not require users to change default username and password
- 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

# 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 offering remotely monitored food consumption of an elderly relative
- Different individuals will be able to use the same things and services differently from those around them

# 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   | HBO         | Swedish Gov't    |
| • Ancestry.com | Indiegogo   | Twitter          |
| • BBC          | PayPal      | Visa             |
| • CNN          | Pinterest   | Verizon          |
| • Comcast      | Spotify     | Walgreens        |
| • DirecTV      | SquareSpace | Wall St. Journal |
| • Fox News     | Starbucks   | 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

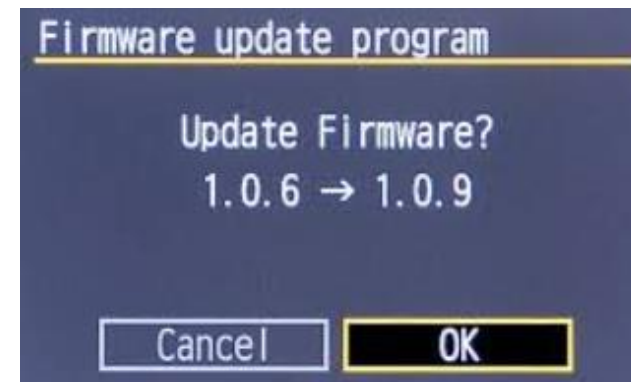
- Many security researchers have discovered ways to hack into various Home Automation devices

- SmartThings
- Insteon
- Philips
- Ring



# Hackers

- Companies released new firmware to patch these holes
- Always need to update devices with new patches
- Think Windows updates
- Updates may be manual, check your settings



# 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

# Smart TVs and Security

- Does your TV have a built-in microphone & web cam?
- TV stores personal information – user names & passwords for all services subscribed to
- 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 compatibilities
  - Learn the various protocols (Wi-Fi, IFTTT, ZigBee, Z-Wave)
  - 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.

# 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 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.

# 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:

# Security and Your Router

- 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 D-Link routers vary depending on the model
- Most of them can be accessed using a combination of what's in this table

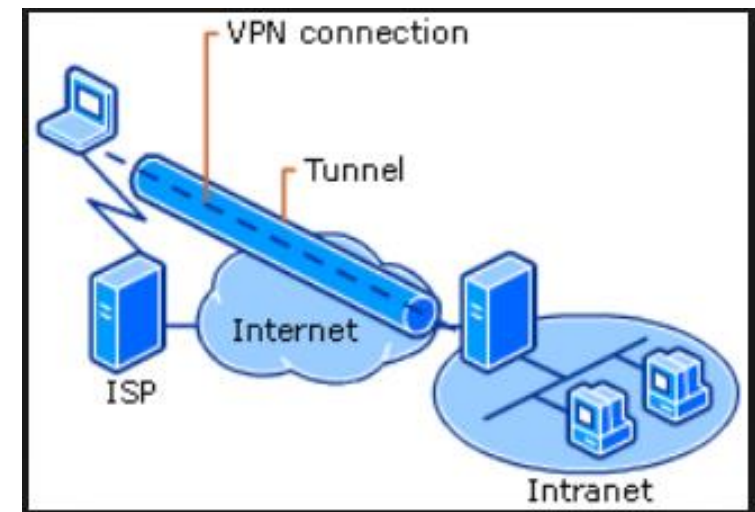
D-Link Model	Default Username	Default Password
DI-514, DI-524, DI-604, DI-704, DI-804	admin	(none)
DGL-4100, DGL-4300, DI-701	(none)	(none)
Others	admin	admin

# Security and Your Router

- Change router name
  - Don't use anything that identifies you
- If possible, set up a 'Guest' network with it own SSID and password
  - Change password frequently
- No access to shared files or networked devices
- Activate encryption
  - WPA2 Personal (it may show as WPA2-PSK)
- Activate router firewall = double protection

# 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 - \$3.00 / month
  - *\*Information is FYI/not recommended by APCUG or presenter*

## VPN Features



Secure VPN  
Account



Encrypted Wi-Fi



P2P Support



PPTP, OpenVPN and  
L2TP/IPSec



5 devices  
simultaneously



Block ads, trackers,  
and malware



Multiple VPN  
Gateways



Unlimited  
Bandwidth



SOCKS5 Proxy  
Included



No traffic logs



Instant Setup



Easy to use

# 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.”
- **Your private information is exposed**
  - IP Address: [REDACTED]
  - Internet Service Provider: Cox Communications
  - City: Oklahoma City
  - State/Region: Oklahoma
  - Country: United States
  - Browser: Edge
  - Operating System: Windows 10
  - Screen Resolution: 1920x1080

# 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

***BURR'S PASSWORD ADVICE  
PUSHED USERS TOWARD LAZY  
AND EASY-TO-PREDICT  
PRACTICES***

# 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 Snowden 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

*\*FYI / Not recommended by APCUG or presenter*

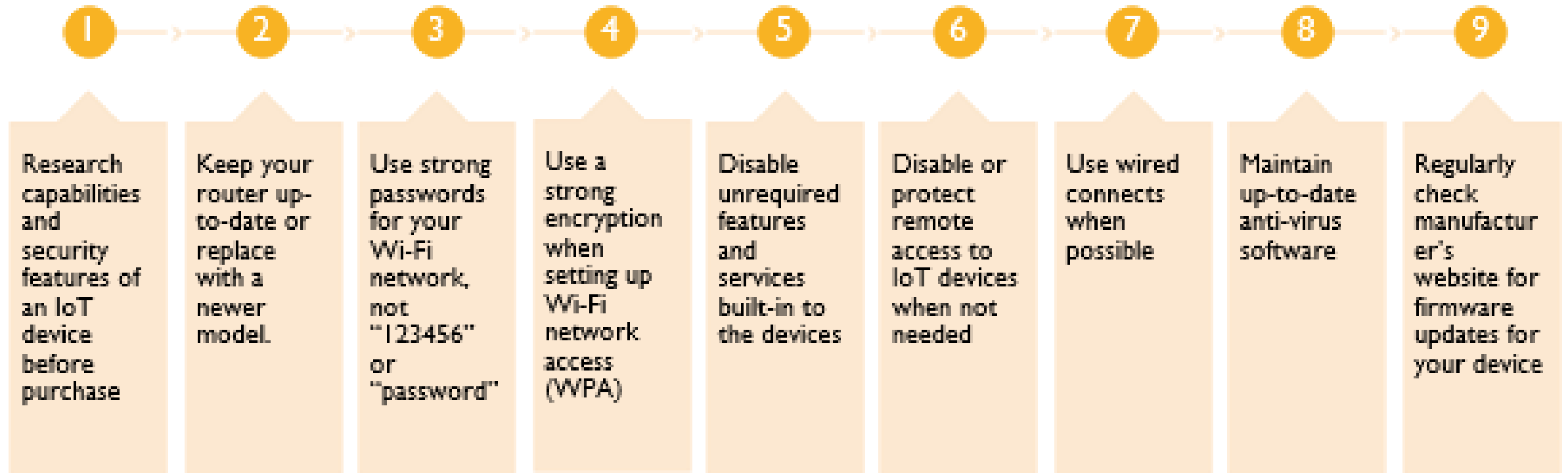
# Home Automation Devices & Security

- 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



# 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”



# 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

# Selling Your House for More Money

- 2/3 Coldwell Banker Real Estate agents find homebuyers are more interested in homes with smart technology than 2-5 years ago
- Nest Learning Thermostat (most favorite)
- Smart doorbell / camera
- Smart security
- Appliances

# 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!

# Questions

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

wjames (at) apcug.org



An International  
Association of Technology  
& Computer User Groups

# 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](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 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>