



# WIRELESS (IN)SECURITY, PRIVACY, AND DEFENDING BOTH

# AGENDA

- My goal is to inform you
  - Might entertain and scare you, too! 😊
- Audience participation welcome & encouraged
- Wireless encryption...what to use
- Wireless attack demos (live and recorded)
- Defending wireless
- Privacy: why people want to take it
- Privacy: ways to reclaim & defend it
- Many tips and tricks throughout
- Closing...questions/comments

## DISCLAIMER...PLEASE READ!!

- Please turn off your wi-fi, if you don't want to participate
- I won't be hacking your device, nor exposing it to attack, but will be collecting data that it broadcasts. This data will be purged from my system at the end of the talk.
- NO USERNAMES OR PASSWORDS WILL BE COLLECTED
- Please excuse any vulgar language in the passwords you may see. Password lists found on the internet almost always include nasty language.



# GOOD AND BAD WIRELESS ENCRYPTION

- Open: avoid this...really!
- WEP: it's broken and I'll demonstrate
- WPA/WPA2: either are fine; use a strong password and change it frequently
  - If you can choose, go with WPA2 and CCMP...as this is the stronger combination
- WPS (Wi-Fi Protected Setup)
  - Probably best to avoid...will demo why

# WIRELESS HACKING DEMOS





# WIRELESS DEFENSE





- Assume your traffic is being intercepted!
  - Wireless is just like radio...data goes everywhere
- Change your wireless network name (SSID) and password frequently
- Set your wireless network (SSID) to hidden
- Keep your router up to date (newer ones have auto-update features)
- Use WPA2 and CCMP encryption on your wireless router
- Don't be shy about contacting a techy person for assistance



Questions about wireless before moving on to privacy?



**CleanMemes.com**

**HEEEEEYY!!!**

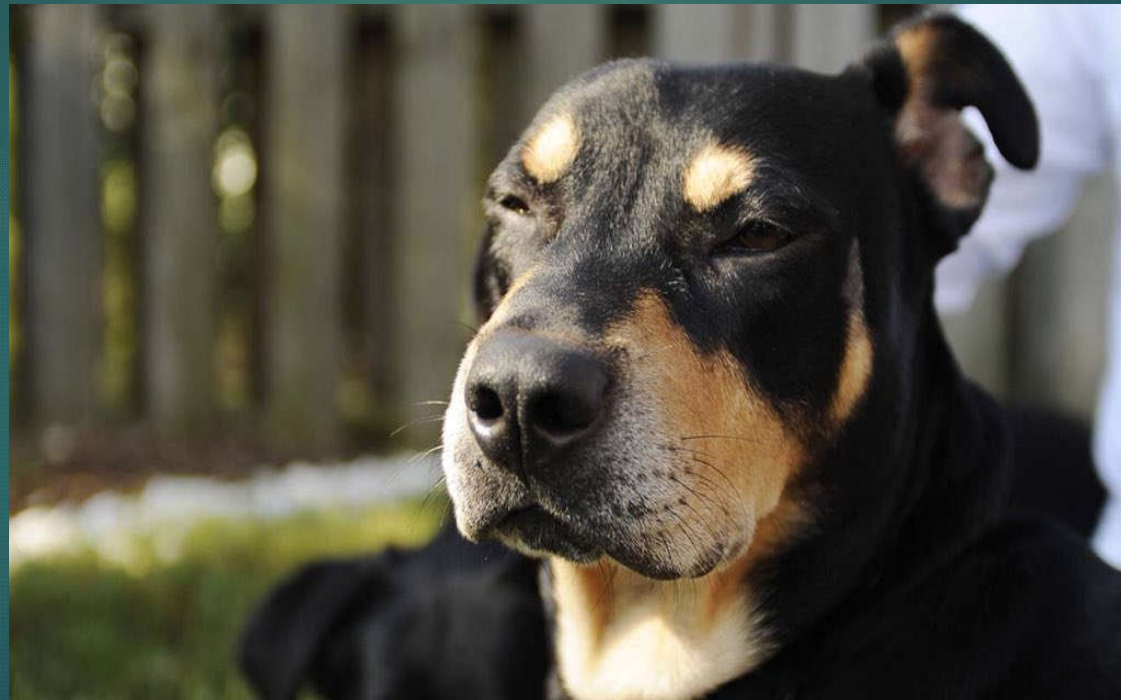


**A LITTLE PRIVACY PLEASE!**

# WHY TALK ABOUT PRIVACY?

- Everyone has something they want to hide, so hide if you like
- A right to privacy is enshrined in our laws & constitution
- Many businesses and the government have failed to keep our private data safe
  - Equifax breach, Target breach, 2015 Office of Personnel Management, etc
- Privacy isn't dead yet, but as technology advances, many argue that privacy is dying.
  - My parents said that privacy died because of the rise of credit.
  - Grandparents said the 1935 Social Security Act killed privacy.
- So, since it's hard to hide & maintain privacy, "drown out" real data with fake data

# WHY BUSINESS & GOVERNMENT WANT YOUR PRIVACY





# DATA IS VALUABLE

- The average person doesn't realize how valuable...until it gets lost in a breach!
- Data aggregators make TONS of money: Facebook, Google, credit bureaus, etc.
- Governments use data to keep track of citizens, especially criminals
- Bad guys like personal data for identity theft, medical fraud, credit card fraud, etc
- People like me use personal data for more targeted attacks...only with permission, of course

# KNOWLEDGE + DATA = POWER

- Businesses use targeted ads to entice repeat customers
  - Notice how you tend to see things you like in Kroger mailings when you have a Kroger card?
- Laws mandate that a lot of your data is public record (i.e. house & land buys)
  - I got all kinds of crap about mortgage insurance, title searching, etc. when I bought my house
- A lot of criminal history is public, like national & local sex offender registries
- People put tons of data about themselves online via social media (e.g. Twitter, Facebook, LinkedIn, etc)

# WAYS TO RETAIN/RECLAIM/DEFEND YOUR PRIVACY





# FIRST THINGS FIRST...

- Don't give up any data on yourself without a good reason!
  - Does your mechanic really need your correct address?
- If you get a paycheck from your employer, it's almost impossible to hide. Be careful when telling strangers where you work.
- Don't get arrested...criminal history never really goes away
- Securely destroy any data (physical or otherwise) you don't need
- Turn off Wi-Fi on your mobile devices when not using it.
- When using an ATM, cover the PIN pad with your other hand before typing the number.
- Freeze your credit at all 4 credit agencies: Equifax, Trans Union, Experian, and Innovis
  - Costs between \$8 and \$20 at each agency



## DID YOU KNOW?

- When answering an unfamiliar number, wait 3-4 seconds before speaking. Robo-dialers typically hang up before then.
- Social security numbers can be guessed by criminals who have your birth date, place of birth, and the last 4 digits. SSNs weren't randomized until 2011.
- Take a look at the back of your work computer now & then. Do you see devices plugged in you don't recognize? If so, don't remove the device & don't use your computer; contact your IT person.
- USB charging stations for phones & mobile devices...DON'T USE THEM
- Avoid free wireless internet...refer to my previous examples as to why ☺
- Attackers frequently target people via social media (Twitter, LinkedIn, Facebook).
- When changing passwords, be sure to vary the pattern you use. For example, if your current password is Hello!76, change it to something like yeLP40C@t.
  - Size matters. HimynameisDavidRMoore is a better password than Ch0c0l@te55!



# HELPFUL LINKS

- Opt out of pre-approved offers of credit or insurance at [www.optoutprescreen.com](http://www.optoutprescreen.com)
- Reduce junk phone calls by registering at the national do not call list at [www.donotcall.gov](http://www.donotcall.gov)
  - Some organizations are exempt; see the website for more info.
- Remove your house from Google street view: [sileo.com/google-street-map-remove-house/](http://sileo.com/google-street-map-remove-house/)
- Credit freezing: [krebsonsecurity.com/2015/06/how-i-learned-to-stop-worrying-and-embrace-the-security-freeze/](http://krebsonsecurity.com/2015/06/how-i-learned-to-stop-worrying-and-embrace-the-security-freeze/)
- Block electronic access to Social Security benefits at [secure.ssa.gov/acu/IPS\\_INTR/blockaccess](http://secure.ssa.gov/acu/IPS_INTR/blockaccess)
- Data breach info at [haveibeenpwned.com](http://haveibeenpwned.com)
  - Can search email addresses, usernames, passwords
- Do you use [informedelivery.usps.com](http://informedelivery.usps.com)? Has someone signed up for you?
  - A stalker's dream: allows you to "digitally preview your mail & manage your packages"
- Take advantage of [www.annualcreditreport.com](http://www.annualcreditreport.com) to request your credit report from the credit reporting bureaus yearly, for free. Spread it out through the year.
- Go to your cell provider store, and establish a password so that someone can't change your carrier. See [krebsonsecurity.com/2018/02/how-to-fight-mobile-number-port-out-scams/](http://krebsonsecurity.com/2018/02/how-to-fight-mobile-number-port-out-scams/)



## NOW FOR DECEPTION

- Lie when needed...truth and privacy can be mutually exclusive.
- Post wrong stuff on your social media accounts (e.g. on vacation when you aren't, wrong birthdate, etc)
- Bumper stickers on your car which have nothing to do with your life or political views. For example, you're not a football fan, use a Dallas Cowboys sticker.
- Occasionally answer a telemarketing call, and tell them you died. This often gets you removed from a call list.
- I sometimes give strangers a fake name by which to address me
- Put a sticker with a fake PIN number on your debit card. If you lose the card, and someone tries to use it more than 3 times, the ATM will eat the card.
- Change your cell provider now and then.



# SOME WAYS TO HIDE...

- Politely (or impolitely) ask people not to take your picture or video you
- Change your name, if you're really paranoid
  - Pick a name similar to a famous person, or a common name...helps you hide on Google.
  - My full name is common...very useful!
- When moving, get copies of your medical records from doctors, and ask they destroy any copies. I'm not a lawyer, but as I understand HIPPA, they must comply with your request.
- Use cash...credit is easily trackable. Don't use the same credit card (or credit card provider) more than 1 year.
- Ask your friends to keep your privacy private (i.e. don't post about me on Facebook)
- When you move, do you really need to notify everyone of your new address? Maintain a P.O. box for privacy, or a personal mailbox at a UPS store
- Get a new social security number
  - [www.consumer.ftc.gov/articles/0248-do-you-need-new-social-security-number](http://www.consumer.ftc.gov/articles/0248-do-you-need-new-social-security-number)

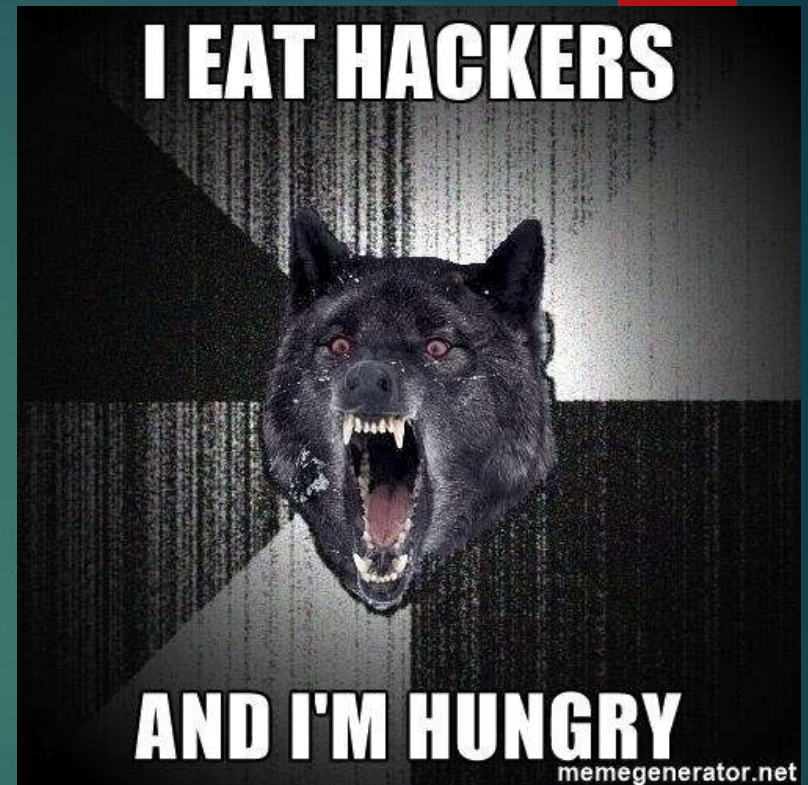
## MISCELLANEOUS TIPS

- Take regular backups of your important data, and save them on external storage
  - Don't forget to backup your mobile devices, too
- Remove un-needed/obsolete applications from your computer & mobile devices
- Always install software updates when prompted (on all computing devices)
  - Most devices have an auto-update feature
- Install an anti-virus software (just one) and keep it updated
  - Microsoft Security Essentials is free & works well
- Be suspicious of all requests for your personal information
- Password-protect your computing devices
- When available, use 2-factor authentication for your online accounts
  - Sometimes called "enhanced login" or "2-step verification"
- Change your passwords regularly, and usernames, too, if possible



## CLOSING

- Turn off wi-fi on your devices when not in use
- Change your wireless network name & password frequently
- Make friends with a techy person 😊
- Your personal data & privacy are valuable; guard them appropriately!
- If a product/service is free, then the objective of the provider is to harvest YOUR data!
- When you put anything on the internet, assume someone will try to hack or steal it.



QUESTIONS OR COMMENTS?

