Cypurr Sessions

October 22nd, 2017

WELCOME!

Outline

- Introduction
- Rules n’ Such
- Current Events
- Breakout Groups
- Thank You/Resources

Who are we? Who are you?

- We are the…
  - The Cypurr Collective: A group of folks that organize cybersecurity workshops and socials, looking to spread knowledge and talk about privacy rights!
- ...and you are?
  - Name
  - Pronouns (i.e. he/him, she/her, they/them, ze/zer, etc)
  - In a few words, what brings you here today?

A few rules for this workshop …

- Share the space!
  - Step Up Step Back: Ask a question, give a comment, leave room for others to speak
- Stack!
  - Raise your hand and we will put you on the speaking queue
- Saf(er) Space
  - We DO NOT tolerate language or behavior purposefully meant to demean or harm folks based on their identities
- Bonus Rule: Try not to invalidate experiences!

Current Events!

(spooky edition)

Matteo Retweeted

Robert Webb @arobertwebb · Oct 20

Anyone who expects to feel safe in a driverless car has never owned a printer.

312 6.3K 18K

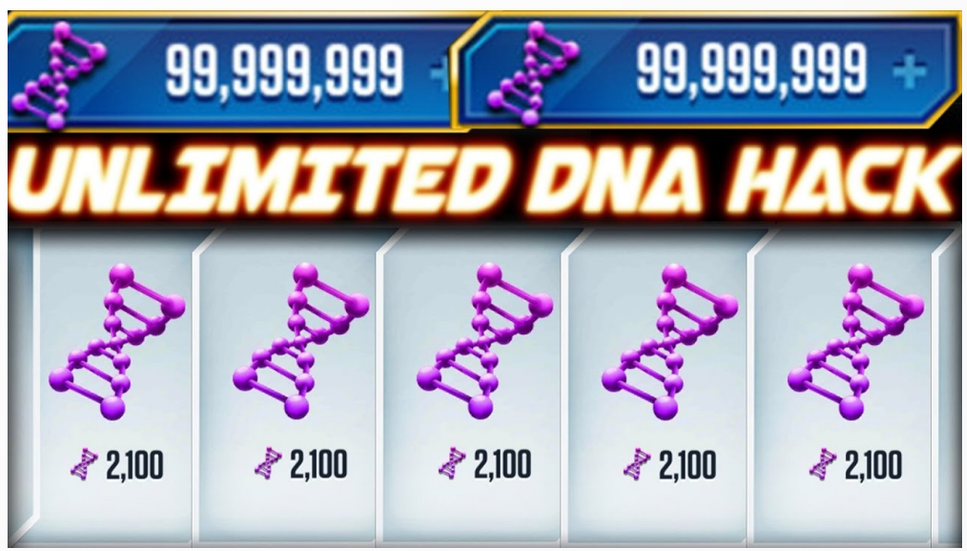
Story #1:D.N.AHHHH!!

- What DNA Testing Companies' Terrifying Privacy Policies Actually Mean
- Gizmodo, October 18th

The Story?

- “When it comes to DNA tests, don’t assume you have any rights.”

- Ancestry, 23and me, don’t own your DNA, but can do what they want with the samples



The Threat?

- You don’t know who is handling your info
- Could effect your insurance
- Information can be stolen
- 23andMe: If you sue us and lose, you will pay
- You get no $$ for medical breakthroughs

What To Do?

- “There’s really no very good reason to do a consumer DNA test,” said Winston. “But people at least need to know what they are signing up for. These companies need to say outright, ‘You’re giving us your information and we can do with it whatever we want.’”
- “...companies disclose the name of every other organization that touches consumer’s genetic information, and better disclose the measures put in place to make sure those third parties are keeping data secure.”

Story #2: Those Links are following me...

- LinkNYC Improves Privacy Policy, Yet Problems Remain
- EFF, October 4th

The Story?

- LinkNYC (a project of CityBridge, owned by Google), installing a bunch of WiFi kiosks around NYC, has edited its Privacy Policy, including tidbits such as:
  - Limit of time on retention of data
  - Will not track browser history when folks use their own devices around kiosk
- Privacy Policy still leaves a lot of gaps that don't protect consumers

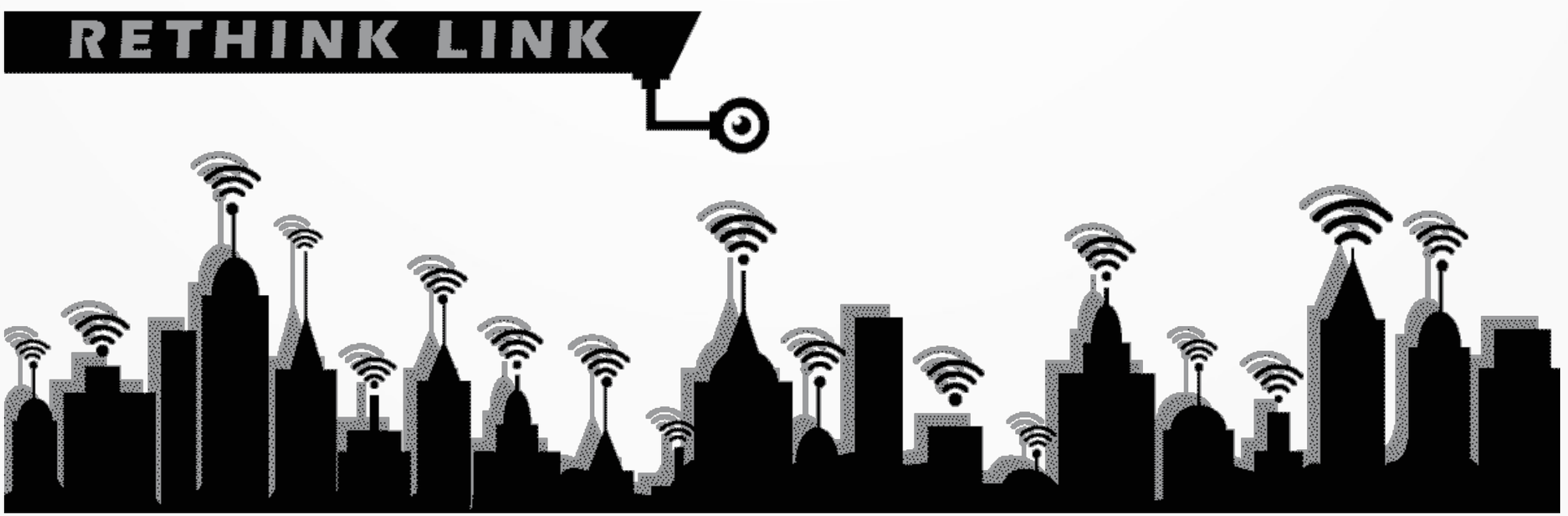
The Threat?

- “LinkNYC still collects what it describes as “Technical Information,” including information such as IP addresses, anonymized MAC addresses, device type, device identifiers, and more, for up to 60 days.”
- “Additionally, the LinkNYC kiosks have cameras that store footage for up to 7 days.”
- “Despite the positive privacy-minded revisions, the policy still fails to provide a pathway for public participation and includes no reference to remedies for potential violations” (data breach)

What to do?

- Be aware of the risks of using corporatly-funded WiFi

- Check out local efforts to curb the privildeges of this project



Story #3: (don't) ABANDON ALL HOPE YE WHO USE WIFI!

- WPA2, KRACK, WTF? A Basic, basic summary
- RoseRegina.Wordpress, October 18th

The Story?

- “In July, Mathy Vanhoef, an academic security researcher in Belgium, discovered a problem with the most common way to set up a password protected wifi network (WPA2).”
- “What Vanhoef found was that if someone pretends to be the wifi router you want to connect to...the device will resend the requested information and the imposter router will be able to to figure out the shared secret key between the router and the device, allowing the attacker continuing impersonating the router and to decrypt the data sent between the router and the device.”

The Threat?

- “We rely on WPA2 for.. all sorts of sensitive data over wifi, like passwords, financial data, and health information...we need to be able to trust this important infrastructure with not only more traditional kinds of sensitive information, but also our most personal communications and private questions.”
- “Unlike a lot of security issues, anyone attacking you would have to be within wifi distance (generally 90 meters or less)
  - Higher-risk individuals affected

What To Do?

- Install updates on your wifi router firmware and all of the devices that you use to connect to wifi.
- Install the HTTPS Everywhere extension on your web browser!
- “Wifi Routers aren’t magic. They are tiny computers with radios attached. In the current state of consumer electronics, we don’t necessarily know if the devices we are using are getting security updates and it can be very hard to tell. That means it is really hard to push for better options as an end user.

Breakout Groups!

- Diceware/Hidden Writing
- Threat Modeling!

Thank You and Resources

- CyPurr Collective on Facebook for Future events!
  - Sign up to our email list too, we won't spam ya!
- Current Events Resources
  - Gizmodo, What DNA Testing Companies' Terrifying Privacy Policies Actually Mean
  - ReThink Link- http://rethinklink.nyc/
  - RoseRegina.Wordpress.com- KRACK and Other Great Resources!

Thank You and Resources

- Further Resources
  - NYC CryptoParty Meetup
  - CryptoParty Harlem
  - Tactical Tech Collective- *Holistic Security*, *MyShadow*
  - EFF- *Surveillance Self Defense*

(Boo!)

See you next time!