EDWARD SNOWDEN – PROTECT YOUR PRIVACY

WHO IS EDWARD SNOWDEN?

- Former CIA Employee
- Worked as an NSA subcontractor at a facility in Hawaii in 2013
- Came from a background of government officials
- Former Special Forces candidate
- Known for declassifying the global surveillance programs made by the NSA and the Five Eyes

2013 GLOBAL SURVEILLANCE LEAKS

- In 2013, Snowden was hired by an NSA contractor, Booz Allen Hamilton after previous employment with the CIA
- Snowden started to raise ethical concerns on what he was doing there

2013 GLOBAL SURVEILLANCE LEAKS

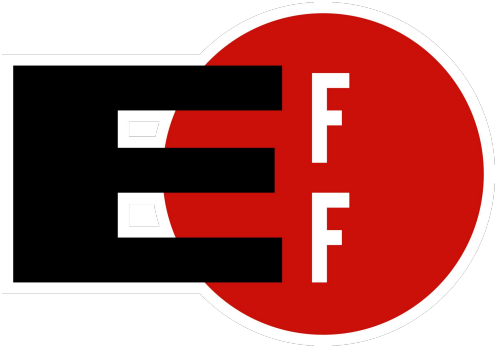
- May 20 2013 – Snowden leaves for Hong Kong
- Early June – reveals global surveillance programs to journalists of The Guardian and The Washington Post including Glenn Greenwald, Laura Poitras, and Ewen MacAskil
- Snowden fled to Russia and took asylum after revealing the programs and the USA assigning charges against him

CURRENT SITUATION AS OF TODAY

- Snowden is still in asylum in Russia , permit expires in 2020, might extend it until 2023
- His memoir “Permanent Record” was published in September 2019
- August 15 2020 – Trump might consider pardoning Edward Snowden

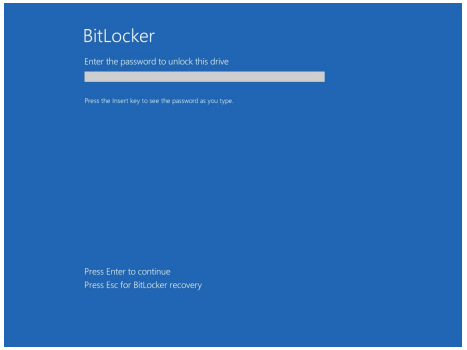
SNOWDEN – PRIVACY TIPS

- Current president of the Freedom of the Press Foundation (FPF), an organization that supports free speech and freedom of the press
- Affiliated with the Electronic Frontier Foundation (EFF) which seeks to promote internet civil liberties (ex. user privacy, FOSS software, freedom of expression etc.)
- Snowden gives numerous tips to improve your privacy and to escape from surveillance as much as possible



TIP #1 – ENCRYPT YOUR HARD DRIVE

- “You should encrypt your hard disk, so that if your computer is stolen the information isn’t obtainable to an adversary — pictures, where you live, where you work, where your kids are, where you go to school.”



LUKS
Linux Unified Key Setup

TIP #2 – ENCRYPT YOUR TEXT MESSAGES AND CALLS

- “The first step that anyone could take is to encrypt their phone calls and their text messages. You can do that through the smartphone app Signal, by Open Whisper Systems. It’s free, and you can just download it immediately. And anybody you’re talking to now, their communications, if it’s intercepted, can’t be read by adversaries.”

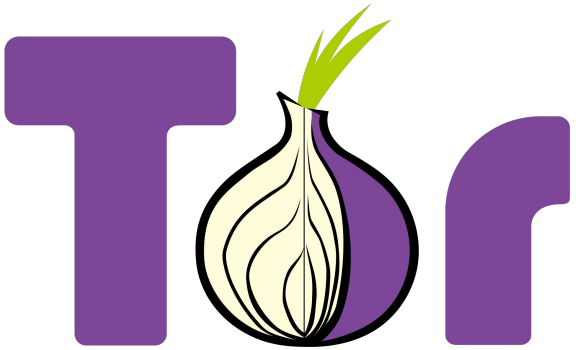
TIP #2 – ENCRYPT YOUR TEXT MESSAGES AND CALLS

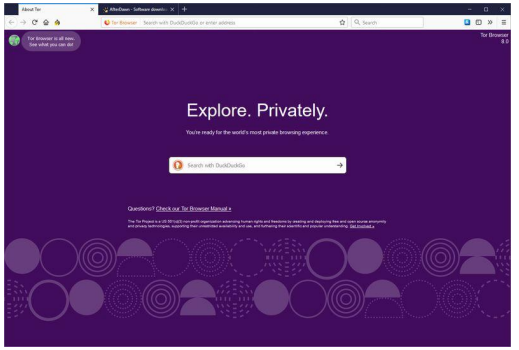
TIP #3 – AVOID ONLINE TRACKING WITH BROWSER PLUGINS

- “Everybody should be running adblock software, if only from a safety perspective”

- “If you use browser plugins like HTTPS Everywhere by EFF, you can try to enforce secure encrypted communications so your data is not being passed in transit electronically naked.”

TIP #4 – ONLINE ANONYMITY





- "I think Tor is the most important privacy-enhancing technology project being used today. I use Tor personally all the time.[...]What Tor does is it provides a measure of security and allows you to disassociate your physical location."

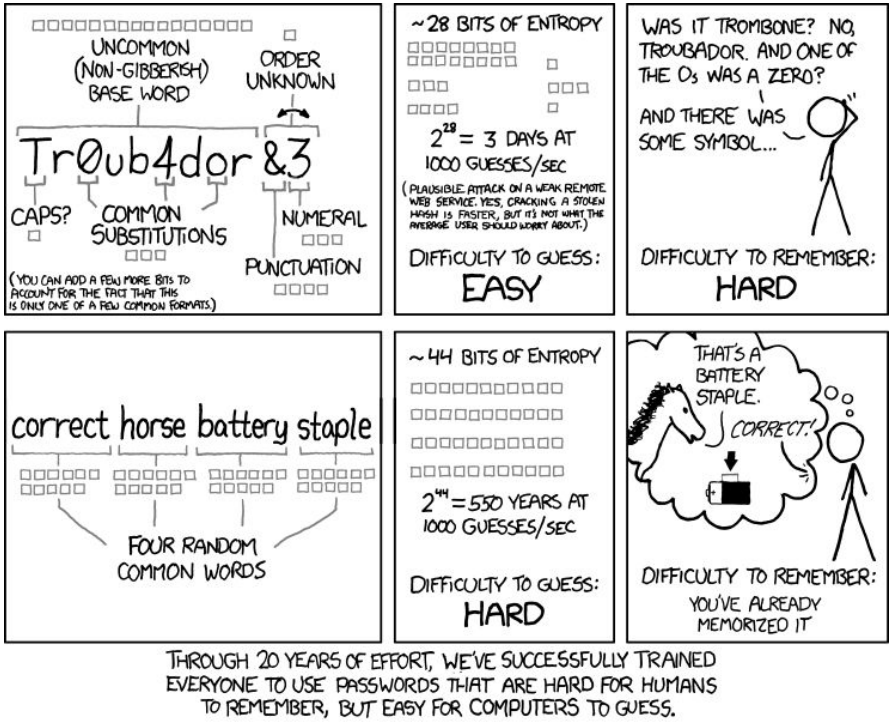
- "But the basic idea, the concept of Tor that is so valuable, is that it's run by volunteers. Anyone can create a new node on the network, whether it's an entry node, a middle router, or an exit point, on the basis of their willingness to accept some risk. The voluntary nature of this network means that it is survivable, it's resistant, it's flexible.

TIP #5 – AVOID ONLINE CONSUMER SERVICES LIKE GOOGLE, FACEBOOK AND DROPBOX

- “Facebook’s internal purpose, whether they state it publicly or not, is to compile perfect records of private lives to the maximum extent of their capability, and then exploit that for their own corporate enrichment.[...]Google ... has a very similar model.”

- "Dropbox is a targeted you know wannabe PRISM partner[...],so they're very hostile to privacy."

TIP #6 – CREATE STRONGER PASSWORDS (OR PASSPHRASES)



- "Bad passwords are one of the easiest ways to compromise a system. For somebody who has a very common 8 character password, it can literally take less than a second for a computer to go through the possibilities and pull that password out"

TIP #7 – USE A PASSWORD MANAGER

- “Use a password manager. One of the main things that gets people’s private information exposed, not necessarily to the most powerful adversaries, but to the most common ones, are data dumps. Your credentials may be revealed because some service you stopped using in 2007 gets hacked, and your password that you were using for that one site also works for your Gmail account. A password manager allows you to create unique passwords for every site that are unbreakable, but you don’t have the burden of memorizing them.”

TIP #8 – USE TWO-FACTOR AUTHENTICATION

- “The other thing there is two-factor authentication. The value of this is if someone does steal your password, or it’s left or exposed somewhere … [two-factor authentication] allows the provider to send you a secondary means of authentication — a text message or something like that.”

CONCLUSION

- Take all the privacy tips into consideration
- Be careful to who you give your data
- Protect yourself from malicious threats
- Don’t trust anyone. Research them first.

INTERVIEWS WHERE HE MENTIONED THE TIPS

- Edward Snowden explains how to reclaim your privacy
  https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/
- The Virtual Interview: Edward Snowden - The New Yorker Festival

  https://www.youtube.com/watch?v=fidq3jow8bc
- Edward Snowden and ACLU at SXSW
  https://www.youtube.com/watch?v=UIhS9aB-qgU
- Edward Snowden on Passwords
  https://www.youtube.com/watch?v=yzGzB-yYKcc
- Edward Snowden says Facebook is just as untrustworthy as the NSA
  https://www.vox.com/recode/2019/10/31/20940532/edward-snowden-facebook-nsa-whistleblower
- Edward Snowden on Dropbox:
  https://www.theguardian.com/technology/2014/jul/17/edward-snowden-dropbox-privacy-spideroak