Belfast CryptoParty
Online Privacy Tips

@pgmaynard

July 2015

“Privacy? I don’t have anything to hide.”

“Here’s my email address. What I want you to do when you get home is email me the passwords to all of your email accounts, not just the nice, respectable work one in your name, but all of them, because I want to be able to just troll through what it is you’re doing online, read what I want to read and publish whatever I find interesting.

Why privacy matters - TED Talk

Global Mass Surveillance

- **Five Eyes** United Kingdom, United States, Australia, Canada, and New Zealand
- **Nine Eyes** Denmark, France, Netherlands, Norway
- **Fourteen Eyes** Belgium, Germany, Italy, Spain, Sweden
- Cooperatively collect, analyze, and share intelligence
- Agreed to not spy on each other as adversaries
- **Members monitor each other's citizens and share intelligence to avoid breaking domestic laws**

Virtual Private Networks (VPN)

- Tunnel your traffic over a secured channel
- Prevents some people from monitoring you

Browser Fingerprint

- Your Browser sends information that makes you unique amongst millions of users and therefore easy to identify.
- Identifies based on available fonts, browser type, and add-ons.
- Test your browser now:
  - `https://panopticlick.eff.org/`
- Install NoScript, Privacy Badger, uBlock Origin and Disconnect.

WebRTC IP Leak

- WebRTC is a new communication protocol that relies on JavaScript
- WebRTC can leak your actual IP address even from behind your VPN
- Disable in Firefox's `about:config`:
  - `media.peerconnection.enabled = false`
- Disable in Chrome:
  - Addon 'WebRTC Block'
  - Easily circumvented. Firefox instead.
- Other browsers tend not to have implement WebRTC yet.

Firefox Privacy Addons

- Stop tracking with “Disconnect” and “Ghostery”
- Block Ads with “uBlock Origin”
- Hinder Browser Fingerprinting with “Random Agent Spoofer”
- Automatically Delete Cookies with “Self-Destructing Cookies”
- Encryption with “HTTPS Everywhere”

Technical knowledge required

- Be in total control with “NoScript Security Suite”
- Content control with “Policeman”

Firefox Hackz

- privacy.trackingprotection.enabled = true
  - This is Mozilla's new built in tracking protection.
- geo.enabled = false
  - Disables geolocation.
- browser.safebrowsing.enabled = false
  - Disable Google Safe Browsing and phishing protection. Security risk, but privacy improvement.
- browser.safebrowsing.malware.enabled = false
  - Disable Google Safe Browsing malware checks. Security risk, but privacy improvement.

Firefox Hackz cont. 1

- dom.event.clipboardevents.enabled = false
  - Disable that websites can get notifications if you copy, paste, or cut something from a web page, and it lets them know which part of the page had been selected.
- network.cookie.cookieBehavior = 1
  - Disable cookies
  - 0 = accept all cookies by default
  - 1 = only accept from the originating site (block third party cookies)
  - 2 = block all cookies by default

Firefox Hackz cont. 2

- network.cookie.lifetimePolicy = 2
    - cookies are deleted at the end of the session
    - 0 = Accept cookies normally
    - 1 = Prompt for each cookie
    - 2 = Accept for current session only
    - 3 = Accept for N days
- browser.cache.offline.enable = false
    - Disables offline cache.

Firefox Hackz cont. 3

- browser.send_pings = false
  - The attribute would be useful for letting websites track visitors' clicks.
- webgl.disabled = true
  - WebGL is a potential security risk. Source

Privacy-Conscious Email Providers

Never trust any company with your privacy, always encrypt.

These are not in the US and support SMTP-TLS, GPG?, Bitcoin and a free service

Email Clients

- Claws Mail
- Thunderbird
- Whiteout Mail
- K-9 Mail (Android)
- Mailpile (Web-mail + Beta)

Email Alternatives

- Bitmessage
  - P2P encrypted communications protocol one or many people.
  - Decentralized and trustless.
  - Strong authentication - sender of a message cannot be spoofed
- I2P-Bote (Beta)
  - Fully decentralized and distributed email system
  - Does not expose email headers; web application, IMAP and SMTP.
  - Bote-mails are transparently end-to-end encrypted; optionally signed

Email Alternatives Cont.

- Pond (Experimental)
  - Forward secure, asynchronous messaging
  - Messages expire automatically a week after they are received
  - Seeks to prevent leaking traffic information against everyone except a global passive attacker.

Encrypted Instant Messenger

Alternative to: WhatsApp, Viber, LINE or Threema.

- PGP + OTR + XMPP + Facebook + Google + Public XMPP servers
    - Conversations (Android)
    - Pidgin (Windows/Linux/Mac)
    - ChatSecure (iOS/Android)
- TextSecure / Signal
    - Mobile devices
    - Provide end-to-end encryption for your text messages

Encrypted Instant Messenger Cont.

- Ricochet
  - A peer-to-peer instant messaging system built on Tor hidden services. Your login is your hidden service address, and contacts connect to you through Tor.

Encrypted Video & Voice Messenger

- Jitsi
  - Jitsi is a free and open source multiplatform voice (VoIP), videoconferencing and instant messaging application. It supports several popular instant-messaging and telephony protocols, including open recognised encryption protocols for chat (OTR).
  - OS: Windows, Mac, Linux.
- RedPhone / Signal for Mobile
- Tox
  - A free and open-source, peer-to-peer, encrypted instant messaging and video calling software.

Encrypted Cloud Storage Services

Alternative to: Dropbox, Google Drive, Microsoft OneDrive or Apple iCloud.

- Seafile *1GB Free Storage*
  - Your data is stored in Germany or with Amazon Web Service in the US for the cloud version.
  - **Encrypt files with your own password.**
  - Host on your own server.
  - Client OS: Windows, Mac, Linux, iOS, Android. Server: Linux, Raspberry Pi, Windows.

Encrypted Cloud Storage Services Cont.

- disk42 *10GB Free Storage* (Open Beta/German)
  - online storage with sync and sharing.
  - all code is open source
  - All your files are encrypted on your own device.
  - OS: Windows, Mac, Linux.

Secure File Sync Software

- Sparkle Share
- Syncany
- Syncthing

Password Managers

- KeePass / KeePassX
- Encryptr (Cloud Based)

Dark Nets / Deep Web / Self Contained Networks

- I2P Anonymous Network
  - OS: Windows, Mac, Linux, Android, F-Droid.
- GNUnet Framework
  - OS: GNU/Linux, FreeBSD, NetBSD, OpenBSD, Mac, Windows.
- The Freenet Project
  - OS: Windows, Mac, Linux.
- Tor Project

Decentralized Social Networks

Alternative to Facebook, Twitter or Google+

- diaspora*
  - Key philosophies: Decentralization, freedom and privacy
  - Host your own
- Friendica
  - Emphasis on extensive privacy settings
  - It aims to federate with as many other social networks as possible.
    - Facebook, Twitter, Diaspora, GNU social, App.net and Pump.io

Decentralized Social Networks Cont.

- GNU social
    - Provide the potential for open, inter-service and distributed communications between microblogging communities.
    - Similar to Twitter; Host your own

Productivity Tools

- ProtectedText
  - open source web application.
  - It encrypts and decrypts text in the browser, and password (or it's hash) is never sent to the server
  - No cookies, no sessions, no registration, no users tracking.
- Turtl
  - Remember ideas, track research, share documents, or bookmark your favorite sites.
  - Turtl makes it easy to organize your life and uses solid encryption to keep it all safe.

PC Operating Systems

Alternative to: Microsoft Windows or Apple Mac OS X

- GNU/Linux
  - Debain
  - Ubuntu
  - Fedora, etc
- Trisquel
  - The project aims for a fully free software system without proprietary software or firmware
  - Linux-libre, a version of the Linux kernel with the non-free code (binary blobs) removed.

PC Operating Systems Cont.

- Qubes OS
  - Qubes is an open-source operating system designed to provide strong security for desktop computing.
  - Separate each application via virtual machines
- Whonix
  - Debian based security-focused distribution; privacy, security and anonymity on the internet.
  - Contains two virtual machines a “Workstation” and a Tor “Gateway”. All communication are forced through the Tor network to accomplish this.

Live CD Operating Systems

- Tails
  - Aims to preserve privacy, anonymity and circumvent censorship
- KNOPPIX
  - Runs applications from removable drive and in memory
- JonDo Live-CD
  - Proxy clients for JonDonym, Tor Onion Router and Mixmaster remailer.

Mobile Operating Systems

- CyanogenMod
- Firefox OS
- Ubuntu Touch
- Replicant
  - A free and open source operating system based on the Android, which aims to replace all proprietary Android components with their free software counterparts.

Recommended Privacy Resources

ipleak.net - IP/DNS Detect - What is your IP, what is your DNS, what informations you send to websites.
Surveillance Self-Defense by EFF - Guide to defending yourself from surveillance by using secure technology and developing careful practices.
PRISM Break - We all have a right to privacy, which you can exercise today by encrypting your communications and ending your reliance on proprietary services.
Security in-a-Box - A guide to digital security for activists and human rights defenders throughout the world.

Recommended Privacy Resources Cont.

The Ultimate Privacy Guide - Excellent privacy guide written by the creators of the bestVPN.com website.

IVPN Privacy Guides - These privacy guides explain how to obtain vastly greater freedom, privacy and anonymity through compartmentalization and isolation.

AlternativeTo.net - Great collection of open source online and self-hosted software sorted by likes.

Keybase.io - Get a public key, safely, starting just with someone's social media username.

Security Now! - Weekly Internet Security Podcast by Steve Gibson and Leo Laporte.

Slides based on

https://www.privacytools.io