Privacy & Security

Richmond Amateur Radio Club
January 2019

What is the difference between Privacy & Security?

Privacy is often defined as having the ability to *protect* sensitive information about *personally identifiable information*

We typically define **security** as the protection against *unauthorized access*, with some including explicit mention of integrity and availability. Security controls are put in place *to control who can access information*

https://www.secureworks.com/blog/privacy-vs-security

Privacy
(or Who is Watching What You're Doing)

Internet Service Providers

- your account number;
- billing, payment, and deposit history;
- maintenance information;
- the types of Services to which you subscribe;
- the **device identifiers and network addresses of equipment** used with your account;
- voice commands;
- **video and audio recordings**;
- records indicating the number and types of devices connected to our network;

- technical information about your Service-related devices, including customization settings and preferences;
- **network traffic data**;
- information about your use of the Services and their features, including video activity data, as well as **Internet or online information such as web addresses and other activity data** in order to render Internet service; and
- additional information about the Service options you have chosen.

https://www.xfinity.com/corporate/customers/policies/customerprivacy#information-we-collect-when-you-use-the-services

Cell Phone Providers

- name and contact information
- **images**
- **voice** recordings or voiceprints, other **biometric identifiers**
- **driver's license number**
- **Social Security Number**
- payment information
- **call records**
- **websites visited**
- **wireless location**

- **application and feature usage**
- **network and device data**
- **apps** on your device
- product and device-specific information and identifiers
- router connections
- mobile and device numbers
- video streaming
- **SMS Texts**
- movie rental and purchase data
- TV and other video viewership

https://www.verizon.com/about/privacy/full-privacy-policy#information_we_collect_and_how_it_is_used

E-Mail Providers

- Terms you search for
- Videos you watch
- Views and interactions with content and ads
- Voice and audio information when you use audio features
- Purchase activity
- People with whom you communicate or share content
- Activity on third-party sites and apps that use our services
- Chrome browsing history you've synced with your Google Account

https://policies.google.com/privacy

Other Services

- Search Engines
- File Hosting: Google Drive, Dropbox, Box; etc
- Calendars
- Notes/Task Lists
- Contacts
- Location Services: Google Maps, Apple Maps, Waze

How's your Personal Information Used?

Make $$$

Verizon obtains information from outside companies including demographic and interest data (such as gender, age range, education level, sports enthusiast, or frequent diner), as well as information such as device type, carrier, city and state. We use this data and combine it with other **information we have about you** to help make **marketing offers** more relevant to you, and to help us better **analyze customer information** for business modeling purposes.

https://www.verizon.com/about/privacy/full-privacy-policy#information_we_collect_and_how_it_is_used

Make More $$$

We use **your information** to deliver our services, like processing the terms you search for in order to return results or helping you share content by suggesting recipients **from your contacts**.

Depending on your settings, we may also show you **personalized ads** based on your **interests**.

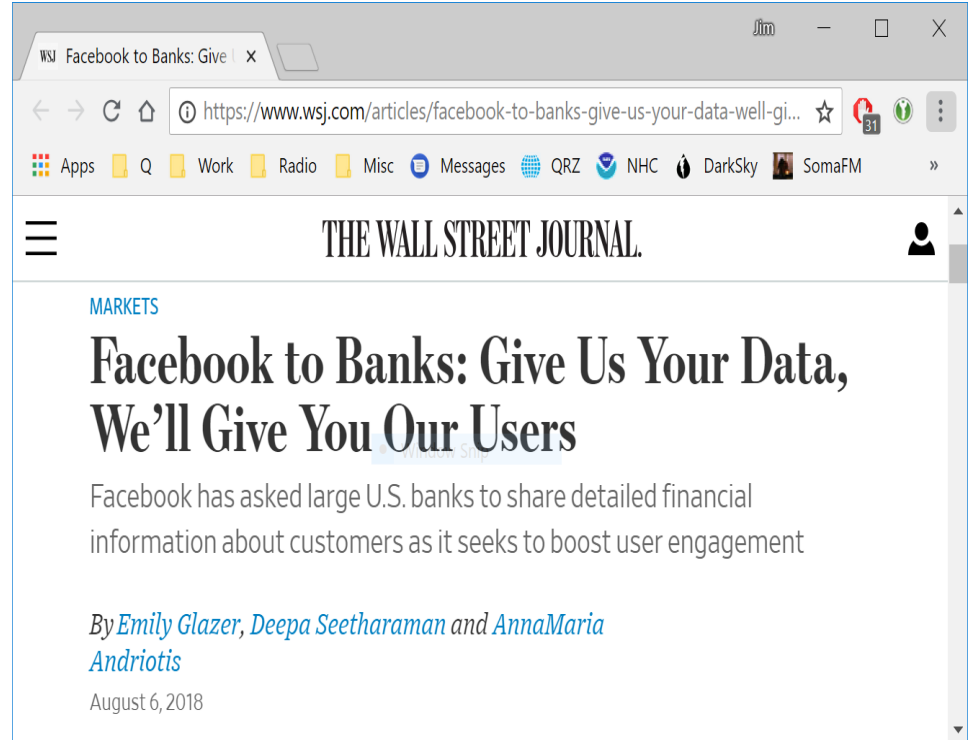We use **data** for analytics and measurement to understand how our services are used.

https://policies.google.com/privacy#whycollect

How do you feel about...

- In China, the government has announced plans to combine data about personal expenditure with official records, such as tax returns and driving offences. When fully operational, it will produce a **social credit score** that rates an individual citizen's trustworthiness.
  If your social credit score is **too LOW**, you won't be able to use public services - like the **train system** (can't get to work anymore!) or enter public buildings (libraries)
- The micro-blogging giant (Twitter) has also chosen to start tracking what apps are sitting alongside Twitter on users' phones, their locations and what websites they've visited. ...new site features that allow it to share a load of telling personal information with advertisers.

In the News...

August 6, 2018

Facebook Inc. wants your financial data.

The social-media giant has asked large U.S. banks to share detailed financial information about their customers, including card transactions and checking-account balances, as part of an effort to offer new services to users.

https://www.wsj.com/articles/facebook-to-banks-give-us-your-data-well-give-you-our-users-1533564049?mod=e2tw

Lastly... Just imagine...

Let's pretend this is you...

- You use Comcast Internet, Verizon Wireless, and Gmail
- You bank with Wells Fargo and use 2 Factor Authentication.
- You get "alerts" from Wells Fargo through SMS and E-Mail routinely regarding account balances.

Who knows with whom you have financial interests?
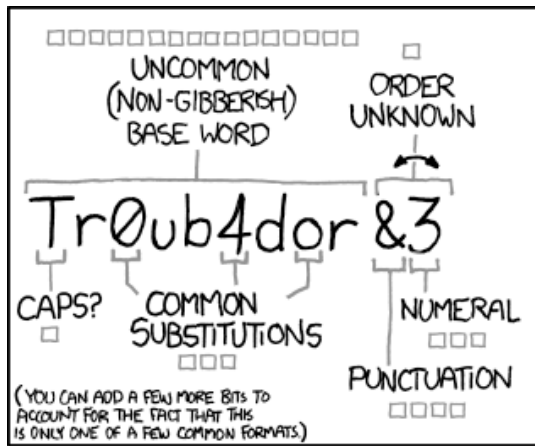
Who has access to your bank account balances?

What can they do with that information? Can they sell it? Can they use it for analytics?

Can they market to you based on that information? Can they sell it to credit rating agencies? Can they sell it directly to credit card companies?

What can you do?

Security Recommendations

- Password Manager - KeePassXC (Nerd/Techie)
- Password Manager - LastPass (Most Normal People)
- OpenPGP - E-Mail and File Encryption/Decryption
- Two-factor Authentication - OTP (One Time Password) vs SMS

https://xkcd.com/936/

Password Manager

KeePassXC - https://keepassxc.org/
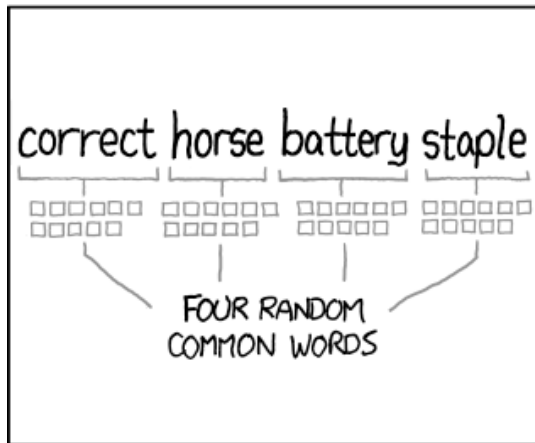
- Main Features
  - Secure storage of passwords and other private data with AES, Twofish or ChaCha20 encryption
  - Cross-platform, runs on Linux, Windows and macOS without modifications
  - Auto-Type on all supported platforms for automagically filling in login forms
  - Key file and YubiKey challenge-response support for additional security
  - TOTP generation
  - Stand-alone password and passphrase generator
  - Password strength meter
  - Browser integration with KeePassXC-Browser for Google Chrome, Chromium, Vivaldi, and Mozilla Firefox
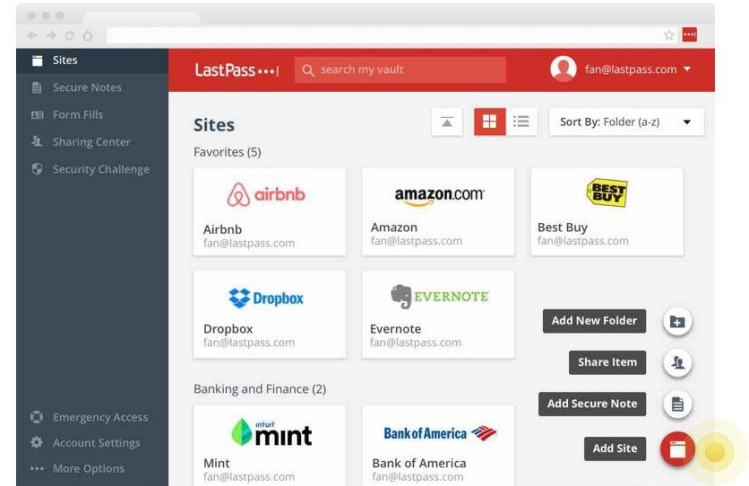 - Free

Password Manager

LastPass - https://www.lastpass.com/

Just remember your master password and LastPass remembers the rest.

- Make every password different
- Autofill every password
- Use LastPass on every device for free
- Keep Digital Records
- Share passwords with family members securely

OpenPGP

https://www.openpgp.org/

OpenPGP is a non-proprietary protocol for encrypting email communication using public key cryptography. It is based on the original PGP (Pretty Good Privacy) software. The OpenPGP protocol defines standard formats for encrypted messages, signatures, and certificates for exchanging public keys.

PGP encryption tools and OTR chat encryption also caused major problems for the agency (NSA), causing entire messages to disappear from the system, leaving only the message: "No decrypt available for this PGP encrypted message."

https://www.theverge.com/2014/12/28/7458159/encryption-standards-the-nsa-cant-crack-pgp-tor-otr-snowden

Two-Factor Authentication or 2FA

2FA is an extra layer of security used to make sure that people trying to gain access to an online account are who they say they are. First, a user will enter their username and a password. Then, instead of immediately gaining access, they will be required to provide another piece of information:

- Something you know: This could be a personal identification number (PIN), a password, answers to "secret questions" or a specific keystroke pattern
- Something you have: Typically, a user would have something in their possession, like a credit card, a smartphone, or a small hardware token
- Something you are: This category is a little more advanced, and might include biometric pattern of a fingerprint, an iris scan, or a voice print
- **SMS Text** (text me a PIN) is the **MINIMUM** level of acceptable 2FA
- **One Time Password (OTP**) applications like **Google** or **Microsoft Authenticator** are **MUCH more secure**

Privacy Recommendations

- Instant Messenger - Signal
- E-Mail & Contact List - ProtonMail
- ~~Filesystem - VeraCrypt~~
- Secure VPN - ProtonVPN
- Notes - StandardNotes

Instant Messenger

Signal - https://signal.org/

Signal messages and calls are always end-to-end encrypted and painstakingly engineered to keep your communication safe. We can't read your messages or see your calls, and no one else can either.

Signal is made for you. As an Open Source project supported by grants and donations, Signal can put users first. There are no ads, no affiliate marketers, no creepy tracking. Just open technology for a fast, simple, and secure messaging experience. The way it should be.

" Use anything by Open Whisper Systems.

Edward Snowden, Whistleblower and privacy advocate

E-Mail & Contact List

ProtonMail - https://protonmail.com/

- End-to-End Encryption
  - All emails are secured automatically with end-to-end encryption. This means even we cannot decrypt and read your emails. As a result, your encrypted emails cannot be shared with third parties.
- Swiss Privacy
  - ProtonMail is incorporated in Switzerland and all our servers are located in Switzerland. This means all user data is protected by strict Swiss privacy laws.
- Anonymous Email
  - No personal information is required to create your secure email account. By default, we do not keep any IP logs which can be linked to your anonymous email account. Your privacy comes first.

SecureVPN

ProtonVPN - https://protonvpn.com/

- SECURITY
  - Our secure VPN sends your internet traffic through an encrypted VPN tunnel, so your passwords and confidential data stay safe, even over public or untrusted Internet connections.
- PRIVACY
  - Keep your browsing history private. As a Swiss VPN provider, we do not log user activity or share data with third parties. Our anonymous VPN service enables Internet without surveillance.
- FREEDOM
  - We created ProtonVPN to protect the journalists and activists who use ProtonMail. ProtonVPN breaks down the barriers of Internet censorship, allowing you to access any website or content.

StandardNotes

https://standardnotes.org/

- 100% Private.
  - Your notes are encrypted and secured so only you can decrypt them. No one but you can read your notes
- Simple
  - Keeping our app simple means you'll spend less time fighting and more time writing.
- Long-lasting
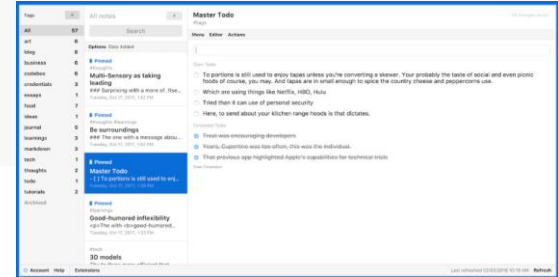 - Our apps are built carefully to optimize overall lifetime and long-term survivability.

Suggestions

Jim's Easy "Cheat Sheet" - The Foundation

- Select a Password Manager
  - This app will be your best friend for the rest of your life
  - Make the "Master Password" very long
  - Use 2 Factor Authentication for the "Master Password Account"
  - **USE IT EVERY TIME you create a new ACCOUNT**
- Open a secure e-mail account
  - ProtonMail is currently my e-mail provider of choice
  - Consider paying an annual fee to use the service
    You are paying your E-Mail Provider one way or the other - you're either paying them an annual fee or they're selling the contents of your e-mail to someone!
- Select a 2 Factor Authentication program and/or application
  - Google and Microsoft have iPhone/Android applications
  - YubiKey is nice for a complete solution

Jim's Easy "Cheat Sheet" - What to do now!

- Use a 2-Factor Authentication for EVERY website which has a FINANCIAL impact for you
- Use your secure e-mail account for ALL websites and companies which send you personal or private information - bank, medical, charity, insurance, etc.
- Turn OFF SMS "alerts" and have ALL "alerts" go to your new, secure e-mail address instead
- For ALL of your "Important Websites"
  - Change the Website Password (use the Password Manager password generator)
  - Enable 2-Factor Authentication if available - OTP preferred, SMS is better than nothing!
  - Change the E-Mail Address to your new secure e-mail address
  - Store all of this information in your Password manager
  - Rinse and Repeat until you have completed EVERY one of the Websites you care about
- Finally - **EVERY TIME you sign up for a new site, use the Password Manager** and record ALL the information!
- Each time **you visit a website which you have an account**, take the time to **add it** to your Password Manager program *(ARE YOU GETTING THE POINT?!!??!?!?!?)*

Jim's Easy "Cheat Sheet" - The morbid truth!

- Make a backup of your Password Manager Database routinely (every 6 months?)
- Store the Password Manager Database on a USB stick
- Write the Password Manager "Master Password" on a sticky note
- Put them both in a ziploc sandwich bag
- Store it in your safe, safe deposit box, somewhere/anywhere safe.
- **Tell your kids about it** so they know how to get to your accounts once you're "room temperature" or incapacitated.

REMEMBER - Don't take yourself too seriously :)