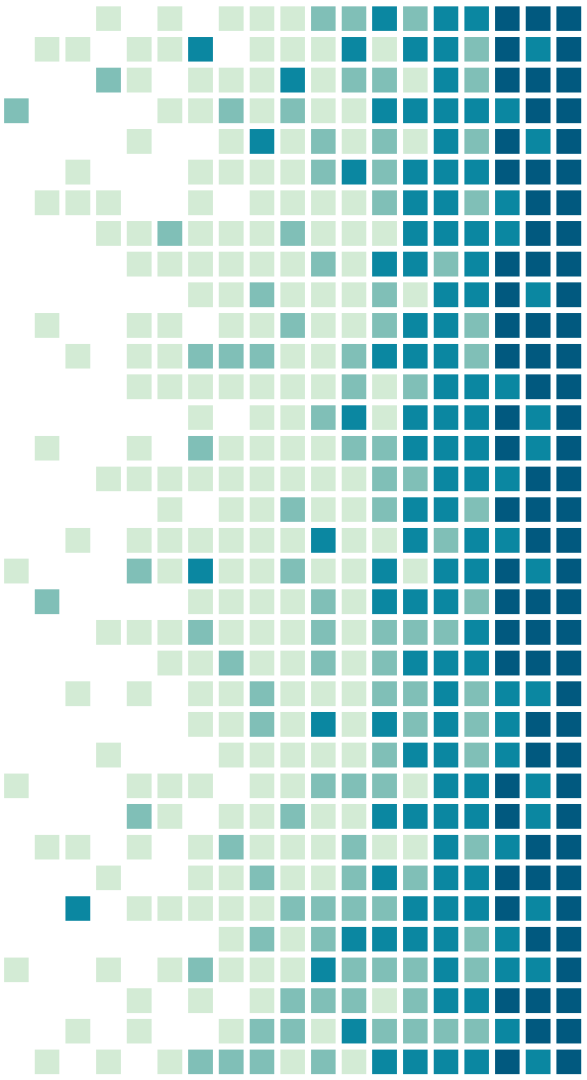
Protecting Personal Information on the Road

David Dixon

“I’m not doing anything illegal or immoral. I have nothing to really be worried about if my information is compromised.

1. PHYSICAL SECURITY

Let’s start with the easy stuff



LOSS/THEFT

- Computers, phones, tablets
- Identification documents, vehicle titles, registration, etc.
- Credit cards

Easiest to catch, not too hard to prevent, not so easy to mitigate afterwards

LOSS/THEFT

- Physical security
- Inventory
  - Make sure you know where all of these important things are frequently
  - Minimize what you carry
- Ability to render useless if lost/stolen

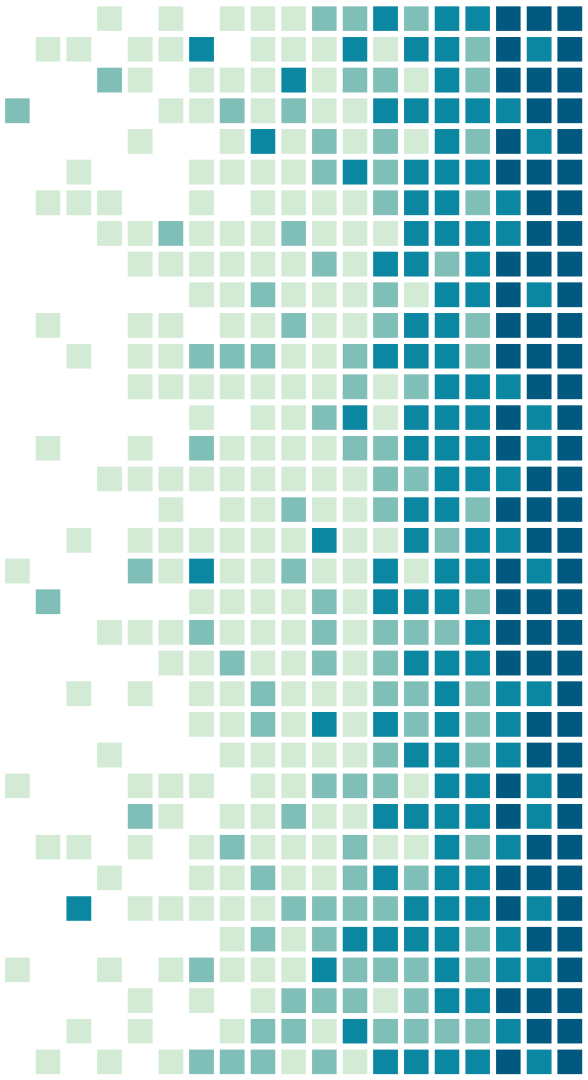
ABILITY TO RENDER USELESS

- Know how to contact all credit card issuing banks (keep a list of accounts and contact numbers)
  - Even if you think you've only temporarily misplaced a wallet, make the calls. You can have them temporarily disable the card, without having to issue a new one.
- Know how to protect/erase information on any electronic devices

FULL-DISK ENCRYPTION

- Whether laptop or mobile device, make sure you prevent access to the data stored on it.
- This is different than a pin/password/fingerprint to log in.
  - If the device storage itself is unencrypted, another device can be used to access it without needing to guess/circumvent your password
  -

2. DIRECT FINANCIAL RISKS



CREDIT CARDS

- Physical cards still have magnetic stripe with plain-text data
  - Don’t let cards leave your sight
- EMV (chip) only enhances the security of data stored by merchants
  - Standard online payments are no more secure than the magnetic stripe.
- Use Google Pay/Apple Pay/Stripe/PayPal
  - Merchants never get access to your card information
  - Faster than EMV payments
  - Easier recordkeeping for you

BANK ACCOUNTS

- Every check (even blank) has everything someone needs to withdraw money from your bank account.
  - Fraud can be reversed, but can leave you stranded in the process
- Use your bank’s bill paying service for things where a real check is still necessary.

CRYPTOCURRENCY WALLETS

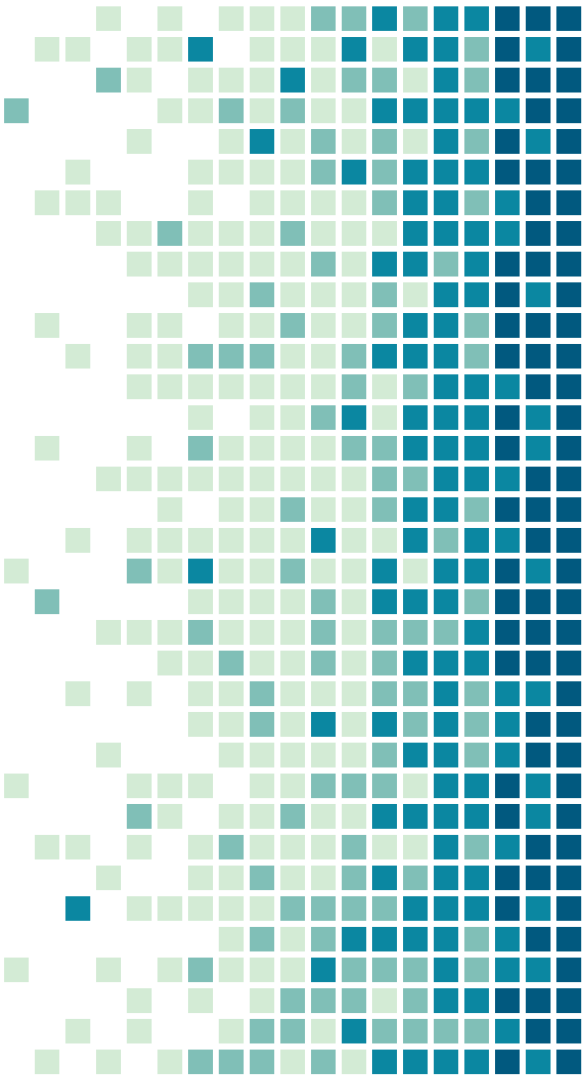
- Generally, far more secure than any conventional wallet or bank account.
- But once it’s gone, it’s gone.
  - Whether by theft or simple loss of keys
- There’s no middleman to reverse a transaction.

YOU HAVE SOCIAL MEDIA PROFILES

Even if you've never created an account on any social media site

3. WHAT'S IN A PROFILE?

We're not talking about the bad guy knowing what's for dinner.



IT MAY NOT BE OBVIOUS

Direct Sharing

Things you post, places you visit, apps you use, browsing habits

Indirect/Inadvertent Sharing

Contacts in your phone, location history, relationship info, cross-site tracking, services that automatically do stuff based on e-mails, social media/Google logins

YOU MAY NOT HAVE CONTROL

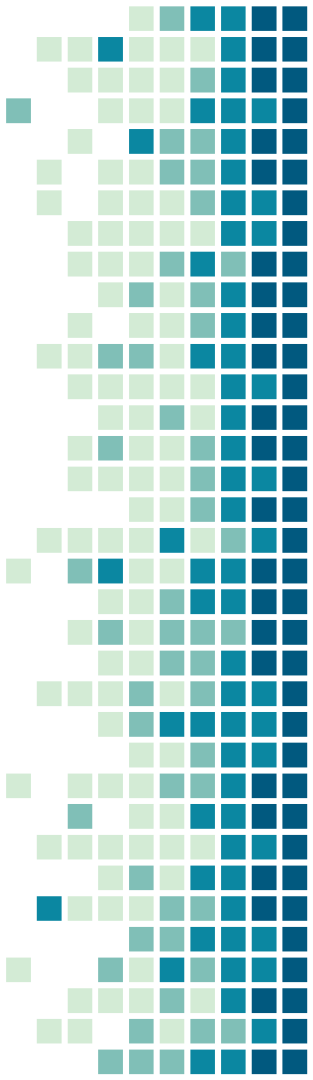
Friends/Family, Business Interactions

Things they post, sharing of contact lists, their granting app access to emails, etc.

Companies who share information with merchant banks, social media, etc.

Analysis of Seemingly Benign Bits of Data

Your profiles can be used to determine things like voting habits, selection for IRS audits, targeted advertising, phishing, spearfishing



THOSE BITS OF INFORMATION HAVE POWER

Authentication

Mother’s maiden name, first car, favorite ice cream flavor, birthdate, first house you lived in, mascot at your last high school

Monetization

Targeted advertising, criminal/civil prosecution, tax audits, class identification, setting prices you see

LEARNING TOO MUCH?

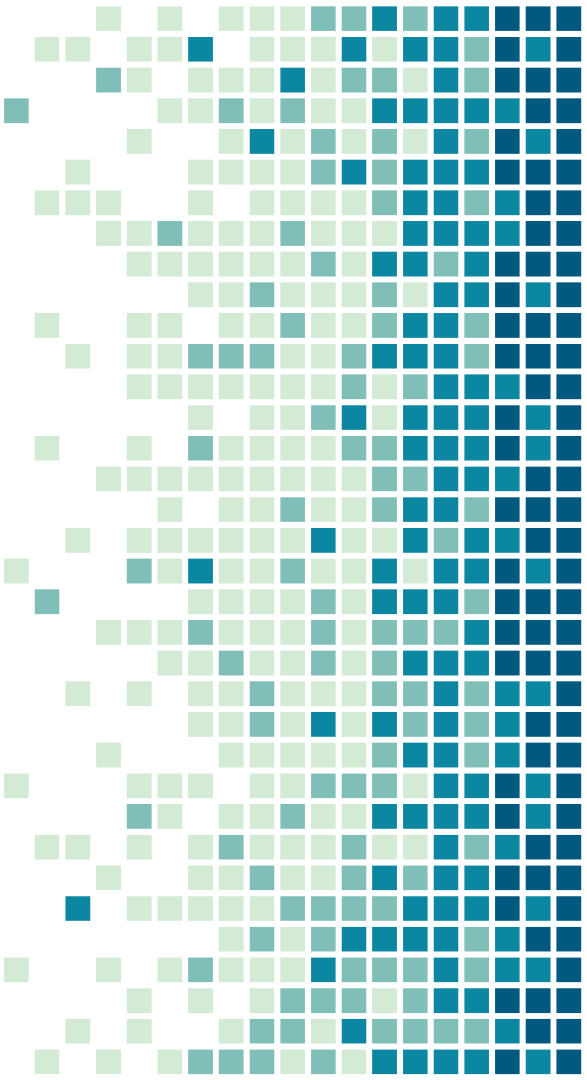
- A man who years ago donated sperm to a couple, secretly, so they could have a child—only to have Facebook recommend the child as a person he should know.
- A social worker whose client called her by her nickname on their second visit, because she'd shown up in his People You May Know, despite their not having exchanged contact information.
- A woman whose father left her family when she was six years old—and saw his then-mistress suggested to her as a Facebook friend 40 years later.
- An in-person conversation, about wanting a baby, is followed by ads for fertility clinics, adoption services, etc., despite a desire keep it to themselves.
- Your spouse getting an ad for a divorce lawyer based on your confidential visit to a counselor.

SHADOW PROFILES

- Third-party tracking
- Logging calls and texts
- Facebook also buys data about its users’ mortgages, car ownership and shopping habits
- Sharing information across platforms (e.g. WhatsApp, Instagram, Facebook; Gmail, Maps, Drive, other Google services, Microsoft, Skype, LinkedIn, Office 360)
- Audio recording, even when not in an app with permission
- Google Home, Amazon Echo (wiretapping!!)
- Other people’s data sharing
-

4. REDUCING EXPOSURE

Controlling who’s listening



PRIVATE, IN-PERSON CONVERSATION

- Batteries removed from all electronic devices with cameras/microphones
- Anything else should be considered insecure.

PRIVATE, ELECTRONIC MESSAGING

- Telegram or Signal
- Off-the-Record from EFF
- Enigmail plugin for Thunderbird (e-mail)
  - Keep track of who shares your address, as it may indicate how they handle your privacy more generally
- Do NOT use ordinary text messages (SMS/MMS)

WHO SHARES YOUR E-MAIL ADDRESS?

- When you use the same e-mail address for every service, it can be almost impossible to tell.
- Separate e-mail accounts for every service would be a pain to administer
- Gmail allows the use of “+” to add suffixes
  - e.g. dave+autozone@gmail.com, dave+amazon@gmail.com
  - Allows you to see who shares info, but also allows easier sorting/filtering

SHARING ON SOCIAL MEDIA

- Make sure you understand privacy settings
  - Assume that no matter the settings, the social media site/app has access (and will access) every post, message, video chat, etc.
- Generally, don’t post anything with a “world” audience
- Always be aware that any posting on a group or someone else’s page/wall/timeline is under their control, not yours
- Always be mindful that anything someone else can see can be saved, copied, and shared
- Think about what the little tidbit you share might contribute to someone learning about you.

Public Key Cryptography

- Messages are encrypted with a key that's "publicly" available
  - Both sender and recipient have access to public key, which is often also published for certain purposes
- Messages can only be decrypted with a private key
- Underpins almost all cryptography in electronic communications today

TRANSPORT LAYER ENCRYPTION (SSL/TLS)

- This is the most common, and most widely used.
- It can protect against the compromise of data between it's origin and destination
  - Note that in most cases, the origin/destination are you and a server (Facebook, Google, etc.) not the person you intend to read your message.
  - End-to-end encryption means nothing if those services hold the keys to decrypt
- Most relevant in protecting against interception of data over public WiFi networks, and from other men-in-the-middle.

MANAGING PASSWORDS

- I won’t ask for a show of hands, but odds are most of you have a handful of passwords recycled over all of the sites you use.
- THIS IS BAD.
- Compromise of a single site could reveal your password, and grant access to other stuff you’d like to protect
- Compromise of multiple sites likely reveals a pattern in your passwords, aiding in further invasion
- Use a multi-platform, open-source password manager like KeePassXC
  - Use it to to manage passwords, but especially use it to auto-generate random passwords

TWO-FACTOR AUTHENTICATION

- Making use of two things, i.e. something you know (password) and something you have (token generator)
- Most common form is SMS-based one-time use codes
  - Extremely vulnerable
  - But still better than just a password
- Use Google Authenticator and other similar tools for offline password generation
  - A legitimate tool needs no permissions, internet access, etc. to function on your mobile device
- Make sure to securely store backup codes away from device, but where you can retrieve them

SIM HIJACKING THREAT

- Probably one of the biggest vulnerabilities for Rvers
- Involves someone contacting your provider, and convincing them to issue a new SIM card for you. Usually takes minimal information, often things you've shared at some point online or with friends/family
- Once SIM is issued and activated, your phone no longer works.
- While your phone no longer works, thieves are able to access virtually any account you have, getting text messages and e-mails to confirm they're really you
- Can empty a HUGE amount of your data and dollars in a short period of time
- Make sure you keep your personal data secure, and make sure you have a PIN, used nowhere else, on your account with your cell phone carrier

BROWSER FIRST, NOT APP

- It’s hard to circumvent tracking links when launched from an app. Using browser (regardless of device type) gives you more control
- It’s easier to close a browser window/tab, use containers, etc., than it is to prevent an app from logging data in the background when you’re not using it.

TOOLS TO PROTECT YOUR ONLINE ACTIVITIES

HTTPS Everywhere

Rewrites HTTP requests to HTTP**S** automatically.

Privacy Badger

Addresses third-party trackers, link shimming, and a long list of other privacy concerns.

Firefox Multi-Account Containers

Allows organization of tabs in separate, isolated containers.

Firefox’s Tracking Protection

First level of built-in protection

NoScript

Does lots of things, but most useful is the ability to block cross-site scripting (XSS).

Red

Is the color of blood, and because of this it has historically been associated with sacrifice, danger and courage.

SUMMARY

Web Browser

Firefox, not Chrome or Edge

E-Mail Client

Thunderbird with Enigmail plugin

Phone Account

Have PIN set up.

KeePassXC

Use auto-generated passwords

Two-Factor Authenticator Apps

Google Authenticator, Authy, etc. NOT SMS

Payments

Google Pay, PayPal, Credit Card, Cash

*Cryptocurrency if acceptance was broader

THANKS!

Any questions?