

YOUR IDENTITY IS SHOWING

SECSIG



SecSIG provides Information Security related content to, for and by members of Mensa.

While our SIG membership is limited to members of Mensa, our content is freely available and usually published on our web site.

For any members of American or International Mensa who want to join us, come to our Facebook page or email us.

<https://facebook.com/groups/secsig>
info@secsig.org





WARNING

As with all of our content, we are not your lawyer. In fact, we are not lawyers and in no way is this sage advice.

You shouldn't do things that are illegal. We're not suggesting otherwise. For any reasonable purpose, you should assume that we don't know what we are talking about, and you should figure this stuff out on your own, or not at all.

Don't call us because your identity was stolen. Those bastards are crafty.

Enjoy.



THE AGENDA



Reduce Your Footprint



Secure Your Box



Hope Everyone Will Forget



FOOTPRINT

FOOTPRINT

Things you touch leave prints behind.
While you can't always control what people observe about you,
you can influence where you go and therefore what data you leave behind.

Our first goal is to understand common sources of data and how
Skip Tracing fills in the missing details.



OUR TARGET

STEP 1: Develop a Profile



What We Know

John Williams
12 Bent Branch Road
Bethesda, MD 20816
+1 571 204 3812
jwilliams@gmail.com

Search Engine Terms

"John Williams" "20816"
"John Williams" "12 Bend Branch Road"
"John Williams" "571" "204"
"jwilliams@gmail.com"

OPEN SOURCE INTELLIGENCE

STEP 2: Public Records Search

Traditional Sources

County Assessor Tax Records
Voter Roles
Professional Licenses
Government ID Search / Drivers License
Death Records
Bureau of Prisons

Online Places to Search

Google ([google.com](https://www.google.com))
Google Alerts ([google.com/alerts](https://www.google.com/alerts))
Duck Duck Go (duckduckgo.com)
PasteBin (pastebin.com)
Have I Been Pwned (haveibeenpwned.com)
Instant Checkmate (instantcheckmate.com)
IntelTechniques (inteltechniques.com/menu.html)
SpyTox (spytox.com)
That's Them (thatsthem.com)
Pipl (pipl.com)



THEY REALLY DO KNOW EVERYTHING

STEP 2: Extended Public Records Search

- Credit Reporting Bureaus
Free Credit Report (annualcreditreport.com)
Experian (experian.com)
Equifax (equifax.com)
TransUnion (transunion.com)
- Public Data Sources
LexisNexis (lexisnexis.com)
Westlaw (clear.thomsonreuters.com)
Acxiom (acxiom.com)
Sterling Infosystems (sterlinginfosystems.com)
Innovis (innovis.com)
Core Logic / SafeRent (corelogic.com)
- What have your neighbors said on social media?
EchoSec (app.echosec.net) Commercial Product
- What data are you leaking?
Reward & Loyalty Programs
Google / Facebook



YOU'RE THE PRODUCT

The More You Know

Amazon

Order History: amzn.to/2Q7I4nm

Dialog History: [amzn.to/ 2NQ8TKn](https://amzn.to/2NQ8TKn)

Apple

privacy.apple.com

Facebook

www.facebook.com/ads/preferences

www.facebook.com/dyi

Google

takeout.google.com/settings/takeout

LinkedIn

GDPR Compliance: bit.ly/2M3IfvX

Twitter

Download Archive: bit.ly/2M3luXI





SECURING YOUR BOX





YOU'RE VULNERABLE

STEP 1: Remove Insecure Software

- Remove all unused or outdated software
- Operating System Updates
- Search Out Vulnerabilities
Saner Personal (bit.ly/2MPWSbh)
- AntiVirus / Personal Firewall
Glasswire

STEP 2: Protect Your Identity

- Password Manager
LastPass / KeePass
Automatically Changed Passwords
- Multifactor Authentication
YubiKey / Google Authenticator

STEP 3: Encrypt Your Data

- Encrypt your Hard Drive
Apple Filevault
Microsoft Bitlocker
- Encrypt your Files
Veracrypt
- Evaluate Where Your Data is Stored
Dropbox / Google Drive / One Drive



YOUR NETWORK SUCKS

STEP 1: Basic Home Internet

- Use your own cable modem
(e.g. ARRIS SURFboard – check with your provider)
- Use a SOHO firewall
Ubiquiti EdgeRouter X / Internet Security Gateway
- Use a SOHO wireless solution
Ubiquiti AmpliFi Wi-Fi
Implement WPA2 PSK

STEP 2: Isolate your Internet of Insecurity

- Isolate your IoT Devices
Create an IoT Wireless Network

STEP 3: Upgrade to Professional Security

- Use a prosumer firewall like pfSense
- Use a VLAN capable network switch

Come See the SecSIG Network



WALK SILENTLY

STEP 1: Everyday Protections

- Mozilla Firefox
uBlock Origin
EFF Privacy Badger
Cookie AutoDelete
Blank Start / Home Page
- CCleaner Pro
Monitoring > Auto Delete
- Spybot Anti-Beacon (Windows)

STEP 2: Starbucks Model

- Privoxy Non-Caching Web Proxy
- Private Internet Access VPN

STEP 3: Partially Anonymous

- The Onion Router (TOR)
- Tor Browser
- Tails Operating System





BEING REMEMBERED OR TRYING TO FORGET



ESTABLISHING YOUR BRAND

(BEFORE SOMEONE ELSE DOES)

STEP 1: Proactively protect your name / brand

- Establish your name across multiple sites
Knowem (knowem.com)
- Common Email Addresses
AOL (aol.com)
Gmail (gmail.com)
Inbox (inbox.com)
Mail (mail.com)
Microsoft (outlook.com / hotmail.com)
Yahoo (yahoo.com)
- Common Domain Names
Knowem (knowem.com)
Network Solutions (netsol.com)
Domain History (domainhistory.net)
Domain Tools (research.domaintools.com)
Security Trails (securitytrails.com)
- Search for Existing Instances
SpyTox (spytox.com)
That's Them (thatsthem.com)
Pipl (pipl.com)



ROBOTS ARE NOT YOUR FRIENDS

STEP 2: Drop the Bots

Estimates vary widely, but it is generally believed that up to 25% of social media accounts are bots.

Or more generally, are not the people they appear to be.

ACTION: Review your Social Media Accounts

1. List all of the sites you visit. Classify them into 'get and give information', 'give information' and 'get information'.
2. For the 'give' sites, review all of your 'friends and followers'. Remove any accounts that you don't personally know to be authentic.
3. For the 'get' sites, consider if the information you are being provided is likely to be true.

WE'RE HERE FROM THE GOVERNMENT

STEP 3: Know the Law

General Data Protection Regulation

UK ISO: bit.ly/2NWGKRC

Wikipedia: bit.ly/2wJX55K

Does **GDPR** affect **US** companies? **Yes!**

Forbes: bit.ly/2oKSI5S

Are the **US** States catching up? **Yes!**

Martech: bit.ly/2NO9fRy

- Privacy, TOS and EULAs are all being updated to reflect new requirements
- Right to know what is being collected
- Right to be forgotten
- Opt-In defaults



LIMITING USE

STEP 4: Monitor and Protect Your Credit

Consumer Credit Freeze

FTC Credit Freeze Info: bit.ly/2oJlFhL

Free Annual Credit Report: bit.ly/2wUQExI

Opt-Out Prescreened Credit: bit.ly/2MMGCI5

Equifax: bit.ly/2NoLkeq

Experian: bit.ly/2M0YB8w

TransUnion: bit.ly/2Q8nwdt

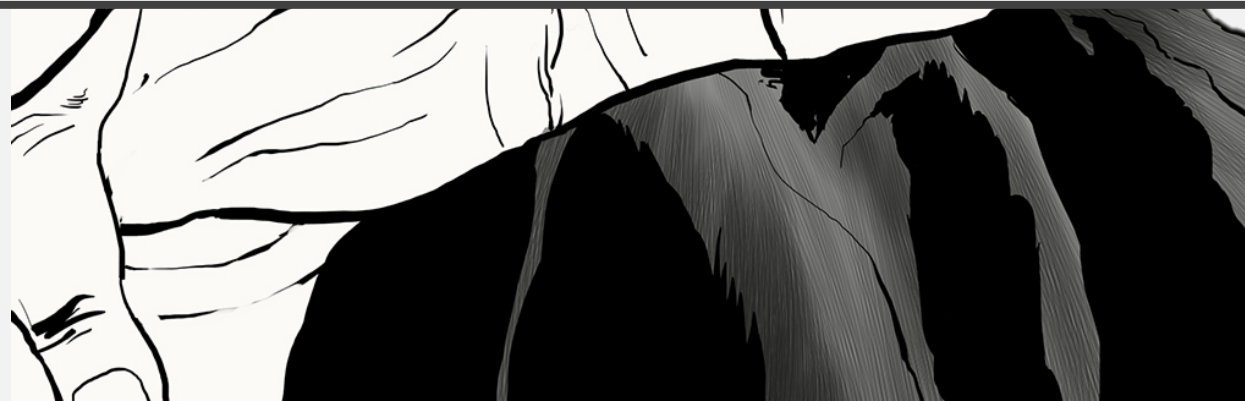
The More You Know

There are numerous private databases that maintain data on you. The OSINT book referenced at the end of the presentation has large sections dedicated to managing this risk.





YOU MUST BE FUN AT PARTIES





CHOOSE YOUR ADVENTURE

You're not going to be able to remediate all risk.

Secure What Can Be Secured

Review and Reduce Your Footprint

Look For Evidence of Abuse

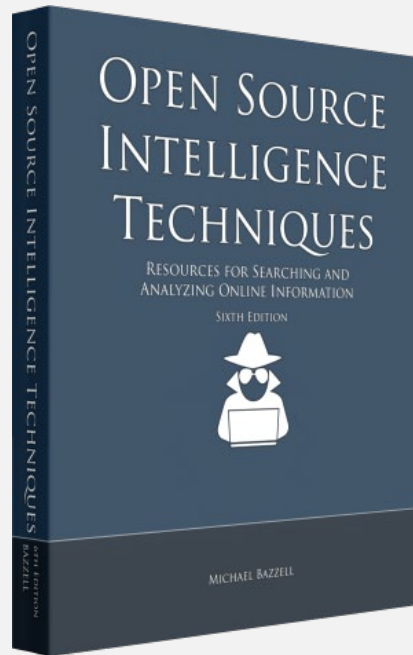
Consider Privacy and Reputation as an Agreement Criteria



EXTRA CREDIT



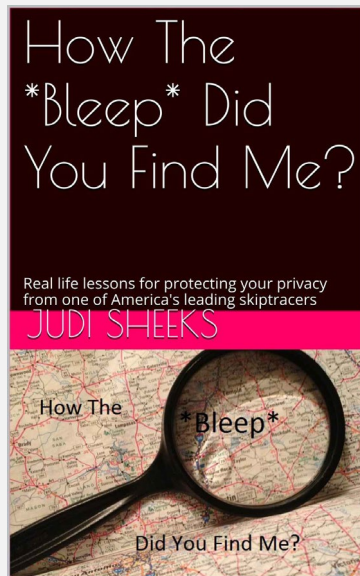
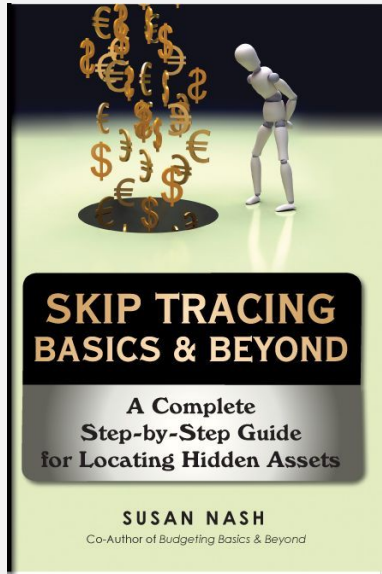
OSINT FOUNDATION



Open Source Intelligence Techniques
Michael Bazzell

inteltechniques.com





SKIP TRACING

Skip Tracing Basics & Beyond: A Complete Step-by-Step Guide for Locating Hidden Assets
Susan Nash

How The *Bleep* Did You Find Me?: Real life lessons for protecting your privacy from one of America's leading skiptracers
Judi Sheeks



QUESTIONS

Visit us and download this presentation at SecSIG.org
Turn In An Evaluation and Get A Free Handout of Today's Presentation



US Mensa Security Special Interest Group Presentation

Title: Your Identity is Showing
Version: 2018.11.18
Time: 45 Minutes + QA
Audience: General Interest

Abstract

The audience will learn about general tools that can be used to gather information about a person online. Personal information is collected, aggregated, sold and used to profile us in such quantity that it is not practical to try to stop it. However, consumers can be aware of when and how they interact with these services and have a more prescriptive way of releasing their information online.

Our first goal is awareness. This presentation provides a sample of some sites that demonstrate the problem. In this and other SecSIG offerings, we discuss how to remediate and reduce risk.

Speaker Biography

Bill Weber is the Director of Cybersecurity at MIT University's Lincoln Labs and a frequent speaker on personal and information security as well as cryptocurrency and blockchain technology.

With over 30 years in the field, Bill has worked with organizations like Microsoft, Electronic Data Systems, Hewlett-Packard and now MIT to provide leadership in cybersecurity to defense, financial and healthcare clients globally.

Contact Info

Email: info@secsig.org

Web: secsig.org

