INDIVIDUAL OPSEC & PERSONAL SECURITY

Michael Chesbro

Register Your Home and Cellular Telephones with the National Do Not Call Registry https://www.donotcall.gov

The National Do Not Call Registry gives you a choice about whether to receive telemarketing calls at home. Telemarketers should not call your number once it has been on the registry for 31 days. If you receive telemarketing calls after you have been listed in the registry for 31 days, you can file a complaint with the Federal Trade Commission. It is also important to note that legitimate telemarketing companies screen their call lists against the National Do Not Registry so any call you receive after registering your number is almost certainly a scam, attempt at identity theft, or some other type of criminal activity. Legitimate telemarketing companies don't call numbers listed in the National Do Not Call Registry.

Opt-Out of Prescreened Credit and Insurance Offers

Many companies that solicit new credit card accounts and insurance policies use prescreening to identify potential customers for the products they offer. Prescreened offers - sometimes called "preapproved" offers - are based on information in your credit report that indicates you meet criteria set by the offeror. Usually, prescreened solicitations come via mail, but you also may get them in a phone call or in an email. If you decide that you don't want to receive prescreened offers of credit and insurance, you have two choices: You can opt out of receiving them for five years or opt out of receiving them permanently.

To opt out for five years: Call toll-free 1-888-5-OPT-OUT (1-888-567-8688) or visit https://www.optoutprescreen.com. The phone number and website are operated by the major consumer reporting companies.

To opt out permanently: You may begin the permanent Opt-Out process online at www.optoutprescreen.com. To complete your request, you must return the signed Permanent Opt-Out Election form, which will be provided after you initiate your online request.

Opt-Out of Direct Marketing

Reducing the amount of junk mail (unwanted coupons, catalogs, etc.) delivered to your mailbox can be accomplished by signing up for mail preference services with Catalog Choice https://www.catalogchoice.org/ and with the Direct Marketing Association https://www.dmachoice.org/. By registering with these organizations your address will be added to the delete list used by advertisers to scrub their mailing lists.

You can opt-out of having the Yellow Pages Telephone Directory delivered to your home by registering at https://www.yellowpagesoptout.com/.

Other on-line sources to opt-out of direct marketing include:

AARP - http://www.aarp.org/about-aarp/aarp-privacy-policy-opt-out1/

Acxiom - https://isapps.acxiom.com/optout/optout.aspx

Comcast / Xfinity - http://customer.xfinity.com/help-and-support/account/do-not-call-do-not-mail-registry-requests

GEICO Marketing - https://www.geico.com/about/contactus/email/ (Select "Opt out of GEICO marketing communications" from the drop down menu.)

LexisNexis Direct Marketing Services - http://www.lexisnexis.com/privacy/directmarketingopt-out.aspx

Red Plum - https://www.redplum.com/tools/redplum-postal-addremove.html

ValPak - http://www.coxtarget.com/mailsuppression/s/DisplayMailSuppressionForm

Legitimate businesses will honor your opt-out requests. These businesses understand that not everyone wants to receive direct marketing and targeted offers for products and services; and that individuals who don't want to receive this type of advertising are unlikely to respond to it by making a purchase.

It is important to understand that there is also a disadvantage to opting out of direct and targeted marketing, and that disadvantage is that you will not receive offers for products and services that might not be generally available in the retail market. When you opt-out you are opting out of offers from legitimate businesses, some of which you might be interested in receiving.

Opting out of direct and targeted marketing is a choice each of us should make based on our own personal circumstances and preferences. We must each weight the value of our personal privacy and security against the convenience and advantage of receiving targeted advertising based on our shopping habits and interests identified in personal profiles built by marketing companies.

Remove Your Name from On-Line Directories and People Finders

On-line directories and people finders gather data from public records and other sources and then make the aggregation of that data available on-line. You can have your personal information removed from these directories by following the opt-out procedures provided by these companies. It is important to note that removing yourself from these directories does not remove your information from the original source where it was gathered. However, removing your personal information from these directories does help protect your privacy when someone is conducting on-line searches in an attempt to locate you. There are dozens of companies aggregating personal information from public records. Below are some of the most well-known of these companies and links to their opt-out pages.

AnyWho - http://www.anywho.com/help/privacy

Been Verified - https://www.beenverified.com/faq/opt-out/

Intelius - https://www.intelius.com/optout.php

Instant Checkmate - https://www.instantcheckmate.com/optout/

LexisNexis - http://www.lexisnexis.com/privacy/

PeekYou - http://www.peekyou.com/about/contact/optout/

People Finder - http://www.peoplefinder.com/optout.php

People Smart - https://www.peoplesmart.com/optout-go

Phone Detective - https://www.phonedetective.com/PD.aspx?_act=OptOutPolicy

Pipl - https://pipl.com/directory/remove/

Private Eye - https://secure.privateeye.com/optout-form.pdf

Spokeo - http://www.spokeo.com/opt_out/new

US Search - http://www.ussearch.com/privacylock

USA People Search - http://www.usa-people-search.com/manage/

Veromi - http://www.veromi.net/Help#26

White Pages - https://support.whitepages.com/hc/en-us/articles/203263794-Remove-my-listing-from-Whitepages-

ZabaSearch - http://www.zabasearch.com/block_records/

Review a Copy of Your Credit Report

AnnualCreditReport.com is the official site to get your free annual credit reports. This right is guaranteed by Federal law.

Federal law allows you to:

- Get a free copy of your credit report every 12 months from each credit reporting company.
- Ensure that the information on all of your credit reports is correct and up to date.

Visit https://www.annualcreditreport.com/ to get a free copy of your credit report.

Add A Credit Freeze to Your Credit File If You Believe You Are at Risk

A credit freeze (sometimes called a security freeze) is designed to prevent the information in your credit file from being reported to others. Because most creditors will check your credit

report before opening a new account a credit freeze is an effective means of protecting yourself against identity thieves who open accounts in your name.

There are some inconveniences associated with having a credit freeze / security freeze on your credit file when you try to establish new credit yourself, but for some people the additional protection provided by a credit freeze may be worth the associated inconvenience.

The Federal Trade Commission provides more information on credit freezes here:

http://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes

If you choose to place a credit freeze on your credit file, you will have to contact each of the major credit reporting agencies to complete the process.

Experian - http://www.experian.com/consumer/security_freeze.html

Equifax - https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

TransUnion - http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page

Experian 1-888-397-3742 | Equifax 1-800-525-6285 | TransUnion 1-800-680-7289

Consider Single Use Credit Card Numbers When Shopping On-line

When you shop on-line or over the telephone it is necessary to provide a credit card number to complete your purchase. But what happens to your credit card data after the transaction is complete? Does the merchant keep your credit card information on file? Will you be charged for a re-occurring transaction when you only authorized an on-time charge?

To help protect you against identity theft and loss of your credit card data, both Bank America and Citibank allow you to generate single use credit card numbers for a specific merchant or transaction.

- Bank of America ShopSafe - https://www.bankofamerica.com/privacy/accounts-cards/shopsafe.go
- Citibank Virtual Account Numbers - https://www.cardbenefits.citi.com/products/virtual-account-numbers.aspx

The single use credit card number works just like the number, expiration date, and security code printed on your credit card, and of course these charges appear on your monthly bills as usual. However, single use credit card numbers are limited to a single merchant, a single transaction, or for a limited period of time sent by you. Once the transaction is complete or the expiration date you assigned to the single use credit card number is reached, that number is canceled and can't be used if stolen or later accessed by an unscrupulous merchant.

If you don't have a credit card issued by either Bank of America or Citibank, you can still take advantage of the security offered by single use credit card numbers by subscribing to services like "Blur" from Abine, Inc. https://www.abine.com/index.html

Avoid Showing ID When Making a Credit Card Purchase

Some merchants may ask that you present ID when making a purchase with a credit card. In most cases the cashier ringing up your purchases just matches the name on the credit card to the name on the ID you present. These merchants wrongly believe that this somehow makes you safer by ensuring that you only use a credit card in your own name. However, there is nothing illegal about using someone else's credit card as long as you have their permission to do so. Furthermore, the major credit card companies know that presenting ID really does very little if anything to stop credit card fraud. Because of this the major credit card companies prohibit merchants from requiring that customers present ID as a condition of making a purchase with a properly signed credit card. The credit card companies ask that cardholders report merchants that are in violation of their policies. Here is Mastercard's on-line reporting form https://www.mastercard.us/en-us/consumers/get-support/report-problem-shopping.html. Note that one of the specific violations listed is "The merchant/retailer required identification."

According to consumer reporter Susan Hogan, WPRI News (September 9, 2015) Businesses cannot require credit card users to show ID - According to the report "Security experts say the information on your driver's license could be enough to steal your identity, which is why the Federal Trade Commission is cracking down on retailers who ask consumers to show theirs... Both MasterCard and Visa actually prohibit merchants from requiring identification as a condition for accepting their credit cards, provided the card is signed." http://wpri.com/2015/09/09/businesses-cannot-require-credit-card-users-to-show-id/.

Get a Paper Shredder for Your Home

To help protect yourself against identity theft, stalking, and similar crimes it is important that you never place intact documents containing your personal, private, or financial information in the trash. A paper shredder is the best way of destroying sensitive documents before disposing of them in your trash or recycle bin. Paper shredders for home use range in price from around $50 to several hundred dollars. For home use a cross-cut shredder costing less than $100 will more than meet the needs of most users. An example of a good paper shredder for home use is the Amazon Basics 8-Sheet Micro-Cut Paper/CD/Credit Card Shredder http://goo.gl/UHYxUK.

If you can't afford to purchase a personal shredder for your home; check with your local sheriff, police department, crime stoppers organization, or bank for information about upcoming community shred events. Many times these organizations will hire industrial mobile shredders to allow community members to destroy personally sensitive documents for free.

Secure Your Browser and On-line Activities

Install Mozilla Firefox - https://www.mozilla.org/en-US/firefox/new/ - and set it as your default browser. We choose Firefox because it allows for the best security configuration in the Windows operating environment.

Install the following add-ons to Firefox…

HTTPS Everywhere - https://www.eff.org/https-everywhere
Privacy Badger - https://www.eff.org/privacybadger
Adblock Plus - https://addons.mozilla.org/en-US/firefox/addon/adblock-plus/

HTTPS Everywhere attempts to encrypt your connections to the web-sites that you visit on-line, while Adblock Plus and Privacy Badger keep those sites from downloading adware or other unwanted programs to your computer.

Further enhance the security of your system and home network by installing a firewall. A basic firewall has been built into Windows since the introduction of Windows XP in 2001. At a minimum make sure that the Windows firewall is turned on. You can check the status of the Windows firewall from the control panel 'System and Security' area. The Windows firewall protects your system from outside attacks, but more robust protection can be obtained by running an advanced firewall. Install either the Comodo Firewall - https://www.comodo.com/home/internet-security/firewall.php or the Zone Alarm Firewall - http://www.zonealarm.com/software/free-firewall/. Both of these firewalls are free.

Adjust the privacy settings on your social media accounts to ensure good privacy and security of your personal information. Information on enhancing security of your social media accounts can be found on 'Social Media Smartcards' (developed by Novetta in consultation with the FBI) or you may choose to use a service such as AVG PrivacyFix - http://www.avg.com/ww-en/privacyfix.

- Facebook - http://security.arizona.edu/sites/securitysiab/files/facebook_smartcard.pdf
- Google+ - http://security.arizona.edu/sites/securitysiab/files/google_smartcard.pdf
- LinkedIn - http://security.arizona.edu/sites/securitysiab/files/linkedin_smartcard.pdf
- Smartphone - http://security.arizona.edu/sites/securitysiab/files/smartphone_smartcard.pdf
- Smartphone EXIF Removal - http://www.novetta.com/wp-content/uploads/2014/12/Smartphone_EXIF_Removal_Smart_Card_073014_COM.pdf
- Traveling Safely with Smartphones - http://security.arizona.edu/sites/securitysiab/files/traveling_safely_with_smartphones_smartcard.pdf
- Twitter - http://security.arizona.edu/sites/securitysiab/files/twitter_smartcard.pdf

Encrypt Your E-mail

If you access your e-mail using MS Outlook or Mozilla Thunderbird https://www.mozilla.org/en-US/thunderbird/ you will be able to install a digital certificate that allows you to digitally sign and encrypt your e-mail. You can obtain a free digital certificate from Comodo https://www.comodo.com/home/email-security/free-email-certificate.php. Once

you have your digital certificate installed you can digitally sign all for your e-mail and encrypt e-mail sent to other people who also have their own digital certificate installed.

Open PGP is an unofficial Internet standard for e-mail encryption, and anyone seriously interested in personal privacy and security should have and maintain a PGP key pair. GNU Privacy Guard for Windows (GPG) https://www.gpg4win.org/ is one of the easiest ways to set up Open PGP on your Windows computer. If you have not used a PGP type product in the past, you may find that there is a slight learning curve when you start using GPG. That being said, GPG is not particularly difficult to learn and the documentation available with the software provides clear instructions for setting up and using the program.

A similar program for conducting public key encryption in web-based e-mail programs is Mailvelope https://www.mailvelope.com/ which can be downloaded as either a Google Chrome Extension or a Firefox add-on. Install Mailvelope as an add-on to your Firefox browser. Once installed open Mailvelope, choose options and generate a key pair. You can now exchange encrypted messages with other Mailvelope and Open PGP users.

Another useful tool for using Open PGP encryption is GPG4USB http://www.gpg4usb.org/. GPG4USB combines a text editor and an Open PGP key manager into a small file. You can generate key sets, import external keys (such as the keys you generated in Mailvelope), and encrypt / decrypt messages in the text editor.

Protect Your On-line Chats with OTR Encryption

Use encrypted chat programs to protect your on-line conversations from being intercepted and monitored. Pidgin Instant Messenger https://www.pidgin.im/ is a universal chat client that consolidates all of your chat programs in one place. Using OTR Encryption https://otr.cypherpunks.ca/ , a plug-in for Pidgin, you can encrypt your chats to protect your personal privacy. The Electronic Frontier Foundation has detailed instructions on how to use Pidgin and OTR https://ssd.eff.org/en/module/how-use-otr-windows.

Other secure chat programs include Cryptocat https://crypto.cat/ and Ricochet IM https://ricochet.im/ which runs over the TOR Network https://www.torproject.org/.

Encrypt Sensitive Information on Your Home Computer

It is important to safeguard sensitive information stored on your computer. An effective way of doing this is to use an encrypted drive or encrypted container to secure your files when they are not in use. For a long time TrueCrypt https://www.grc.com/misc/truecrypt/truecrypt.htm was favored as the open source standard for disk encryption. In September 2014, the TrueCrypt developers claimed that the program was no longer secure and stopped all further support and development of the program. The TrueCrypt developers offered no detailed explanation for why the program was suddenly being declared unsecure. An independent review of the code, completed in April 2015, found no significant cryptographic weaknesses, and many people still

use TrueCrypt for their disk encryption. If you currently use TrueCrypt it is probably safe to continue using it.

For individuals with doubts about the current security of TrueCrypt there is a replacement called VeraCrypt https://veracrypt.codeplex.com/ that functions in much the same way as TrueCrypt, and is in fact just a continued development (a fork) for the TrueCrypt program. Another similar open source program is DiskCryptor https://diskcryptor.net/wiki/Main_Page, a program that supports full-disk encryption.

If you do not currently use disk encryption, download either VeraCrypt or DiskCryptor and create an encrypted container on your hard-drive in which you will store your sensitive files and documents.

If you want to encrypt just single files and folders, AxCrypt http://www.axantum.com/axcrypt/ integrates seamlessly with Windows and provides an easy-to-use, secure option. The US Air Force Software Protection Institute provides a free program, Encryption Wizard http://www.spi.dod.mil/ewizard.htm, that you can run from your computer desktop that will provide strong encryption to protect your personal information.

Use Anonymous E-mail Forwarding & Temporary E-mail Addresses

Anytime you provide your personal e-mail address to someone you open yourself up to potentially being flooded with SPAM, Phishing attempts, and all sorts of other unwanted e-mail. Using anonymous e-mail forwarding and temporary e-mail addresses protects your personal e-mail account from a flood of unwanted mail, while still allowing you to receive and reply to validation e-mail when you sign-up for a web-site or service on-line.

Anonymous e-mail forwarding lets you create multiple e-mail addresses that forward to your primary e-mail account. If one of the e-mail forwarding addresses you create starts receiving lots of SPAM or other unwanted e-mail, you can turn it off without having to disrupt your primary e-mail address. Sites that let you create permanent anonymous e-mail addresses include: Not Sharing My Info http://notsharingmy.info/ and 33Mail https://www.33mail.com/

Temporary e-mail addresses are designed to let you sign up for on-line services and reply to a validation e-mail, but usually last no more than a few minutes to a few days. Incognito Mail http://www.incognitomail.com/, Guerrilla Mail https://www.guerrillamail.com/, YopMail http://www.yopmail.com/en/, and Mailinator https://mailinator.com/ are all sites that let you create a temporary e-mail address.

Use A Password Manager

Password managers allow you to create and manage strong passwords across multiple sites. Password managers allow you to use long, complex passwords, without the need to remember more than a single master password for the password manager of your choice. Some of the most

popular (and secure) password managers include: LastPass https://lastpass.com/, Keepass http://keepass.info/, KeepassX https://www.keepassx.org/, Password Safe https://pwsafe.org/, Dashlane https://www.dashlane.com/passwordmanager, , Norton Identity Safe https://identitysafe.norton.com/, and RoboForm http://www.roboform.com/password-manager.

Use TOR and TAILS

"The Tor software protects https://www.torproject.org/ you by bouncing your communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching your Internet connection from learning what sites you visit, it prevents the sites you visit from learning your physical location, and it lets you access sites that are blocked. The Tor Browser lets you use Tor on Windows, Mac OS X, or Linux without needing to install any software. It can run off a USB flash drive, comes with a pre-configured web browser to protect your anonymity, and is self-contained (portable)."

Tails https://tails.boum.org/ is a live operating system, that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your privacy and anonymity, and helps you to:

- use the Internet anonymously and circumvent censorship;
- all connections to the Internet are forced to go through the Tor network;
- leave no trace on the computer you are using unless you ask it explicitly;
- use state-of-the-art cryptographic tools to encrypt your files, emails and instant messaging.

Improve Your Home Security with Crime Prevention & Neighborhood Watch Programs

Use Checklists and Guides from the National Crime Prevention Council
http://www.ncpc.org/resources/files/pdf/neighborhood-safety/

Consider starting or participating in a Neighborhood Watch Program
https://www.bja.gov/Publications/NSA_NW_Manual.pdf

Review the State Department Guidance on Personal Security
At Home, On the Street, While Traveling
http://www.state.gov/m/ds/rls/rpt/19773.htm

You can also develop a general crime profile of your neighborhood by using on-line databases such as: Spotcrime - http://spotcrime.com/, Neighborhood Scout - http://www.neighborhoodscout.com/, Crime reports - https://www.crimereports.com/, and Family Watchdog - http://www.familywatchdog.us/.

Install a Burglar Alarm and Other Home Security Devices

A study conducted by the University of North Carolina at Charlotte: "Understanding Decisions to Burglarize from the Offenders Perspective" (2012) http://airef.org/wp-content/uploads/2014/06/BurglarSurveyStudyFinalReport.pdf found that: "Indicators of increased security (alarm signs, alarms, dogs inside, and outdoor cameras or other surveillance equipment) was considered by most burglars when selecting a target." and "About 60% of the burglars indicated that the presence of an alarm would cause them to seek an alternative target altogether." Even fairly inexpensive alarm systems such as the Simplisafe2 Wireless Home Security System - http://goo.gl/0klTLL or the Fortress Security Wireless Home Security Alarm System with Auto Dial - http://goo.gl/yTbxEX can enhance the security of your home. The security of your home increases even more by adding security cameras such as the Vimtag Wireless Security Camera with Two-Way Audio and Night Vision - http://goo.gl/Mr5xUM. Additional security devices such as 24-Hour Digital Timers - http://goo.gl/7njaSP, FakeTV Burglar Deterrent- http://goo.gl/hLRp86, and Heavy Duty Motion Sensor Security Lights - http://goo.gl/uwM9BG all add even more security to your home.

After having high-quality dead-bolt locks installed throughout your home, some may wish to consider the addition of Door Armor - http://goo.gl/feO5Ul, Window Security Film - http://goo.gl/9x2yPe, and using Master Lock Dual-Function Security Bars - http://goo.gl/lgX6l0 to increase security.

Keep an Inventory of Your High-Value Items
Participate in Operation Identification

1. Mark property or valuables with an identifying mark, preferably your driver's license with state abbreviation followed by number: Example: CA-B1234567

2. Inventory your marked property on a form with descriptions including brand, model number, and serial number. Keep it in a safe place.

3. Display the Operation ID decal on windows to show your participation in the program and to discourage burglary.

The Insurance Information Institute offers a free program "Know Your Stuff" https://www.knowyourstuff.org/iii/login.html to keep an inventory of your personal items.

Take A Firearms Safety Course

The Washington, DC Metropolitan Police Department offers an on-line firearms safety course - https://dcfst.mpdconline.com/. There is no cost for taking this course and it should take approximately 30 minutes to complete. Even if you don't own a firearm, understanding how firearms function and how to safely handle them is important.

According to U.S. Bureau of Justice Statistics data, having a gun and being able to use it in a defensive situation is the most effective means of avoiding injury (more so even than offering no resistance) and thwarting completion of a robbery or assault. In general, resisting violent crime is far more likely to help than to hurt, and this is especially true if your attacker attempts to take you hostage, such as sometimes happens in a carjacking situation. Most often with gun defenses, criminals can be frightened away or deterred without a shot being fired. Estimates of these types of defensive uses of firearms are wide ranging, from a low of 65,000 to 82,000 annual defensive gun uses (DGUs) reported to the U.S. Department of Justice's National Crime Victimization Survey (NCVS), to a high end of some 2.1-2.5 million annual DGUs, but they seem to occur at least as often (if not far more often) each year as misuses of firearms by violent criminals. (http://www.bjs.gov/content/pub/pdf/fv9311.pdf)

If you choose to carry a firearm for personal protection, get training from an NRA Certified Instructor http://www.nrainstructors.org/search.aspx. Obtain legal guidance on the proper use of a firearm for personal protection from an attorney specializing in this area of law, i.e. Alex Kincaid Law http://www.alexkincaid.com/

Enhance Your Security Awareness with Free On-line Courses

JS-US007 - Level I Antiterrorism Awareness Training - http://jko.jten.mil/courses/atl1/launch.html

Cybersecurity Awareness Version 2.0 - http://cdsetrain.dtic.mil/cybersecurity/index.htm

Counterintelligence Awareness and Security Brief - http://cdsetrain.dtic.mil/ci-security-brief/index.htm

Insider Threat Awareness - http://cdsetrain.dtic.mil/itawareness/index.htm

IS-915: Protecting Critical Infrastructure Against Insider Threats - https://training.fema.gov/is/courseoverview.aspx?code=IS-915

New Face of Threats - http://www.lewis-mcchord.army.mil/des/OPSEC%20Training/New%20Face%20of%20Threats/module-0/0_1.html

Thwarting the Enemy - Counterintelligence and Threat Awareness Information to the Defense Industrial Base - http://cdsetrain.dtic.mil/thwarting/index.htm

IS-106.16 - Workplace Violence Awareness Training 2016 - https://training.fema.gov/is/courseoverview.aspx?code=IS-106.16

IS-906: Workplace Security Awareness - https://training.fema.gov/is/courseoverview.aspx?code=IS-906

IS-907 - Active Shooter: What You Can Do - https://training.fema.gov/is/courseoverview.aspx?code=IS-907

Active Shooter Prevention Training with OSHA Message (Video) - https://www.youtube.com/watch?v=nKA_l8iI7nc

IS-912: Retail Security Awareness: Understanding the Hidden Hazards - https://training.fema.gov/is/courseoverview.aspx?code=IS-912

IS-914: Surveillance Awareness: What You Can Do - https://training.fema.gov/is/courseoverview.aspx?code=IS-914

IS-916: Critical Infrastructure Security: Theft and Diversion - What You Can Do - https://training.fema.gov/is/courseoverview.aspx?code=IS-916

Smartphones and Tablets - http://iatraining.disa.mil/eta/smartphone_tablet_v2/launchpage.htm

Social Networking - http://iaseapp.disa.mil/eta/sns_v1/sn/launchPage.htm

Phishing Awareness - http://iatraining.disa.mil/eta/phishing_v2/launchpage.htm

Michael Chesbro

January 25, 2016

http://www.chesbro.tech