Table of Contents

Who am I?

I'm Jason Chambers. I've been a software engineer all my life. For the past ten years my work has focused on data and network security. I'm proud to work for Cisco working where I develop Cisco Stealthwatch. I put together this guide to help my friends and family stay safe on-line.

What's at risk?

Your money
Your credit score
Your reputation (fake social media posts)
Your digital photos, videos, files
Your identity

Protect all the things

This will give your defenses an immediate huge boost.

Do this	Why	How
Use a Password Manager	Makes it convenient to follow password best practices. I use 1password, but LastPass is a good option too. You no longer need to remember/or write down all those passwords.	(1password) (LastPass)
Use strong passwords (generated using your new Password Manager)	Strong passwords make it very difficult for your password to be guessed and/or cracked using brute-force techniques.	

Use different passwords for each on-line account (using your new Password Manager)	Using different passwords protects you from Credential Stuffing where attackers automatically attempt to use your stolen credentials harvested from one breach (e.g. Marriot) to gain access to other on-line services (e.g. Your bank).	
Turn on 2FA for your e-mail	Even if the attacker has your login/password – with 2FA they will need your phone to access your account. Your e-mail account is the most valuable account to an attacker. Once they have compromised your e-mail, it's easy to gain access to every other account you might have. According to FBI 2018 Internet Crime Report, Email Account Compromise (EAC) is the #1 crime type by victim loss. I use Google Mail but check with your email service provider.	(Google Apps)
Audit and clean up your email inbox and sent folders	Imagine if someone did gain unauthorized access to your e-mail – what would they find? Sensitive documents to your CPA? Passport images to your Travel Agent? Consider deleting this from your email.	
Find out if you have been compromised and change passwords (using your new Password Manager)	Now that you have changed your passwords so that they are strong and unique, you should have little to worry about.	(Have I been pwned?)
Be careful sending sensitive information over e-mail (and SMS too)	If you wouldn't write it on a postcard, don't write it in an e-mail/SMS. They are not confidential and like real mail, there are multiple stops on its journey to the recipient. Create an encrypted PDF and send as an attachment.	(Mac How-to) (Office How-to)

Don't fall victim to Phishing attacks	91% of hacking attacks start with phishing e-mails. 30% of phishing emails get opened. 97% cannot identify a sophisticated phishing attack. Phishing scams cost US businesses $500 million a year.	(Tips to identify)
Consider using Cisco OpenDNS	Just in case you click on that link – OpenDNS provides another line of defense by checking the reputation of the web-site and blocking it.	(Open DNS)
Buy "Cyber Smart" book, Bart R. McDonough	To learn more about how to protect yourself. Strongly recommended.	(Wiley)

Protect your money

Follow these steps to reduce your exposure to identity theft and fraud.

Do this	Why	How
Freeze your credit with all major bureaus	Equifax 2017 data breach exposed the sensitive personal information of 143 million Americans. You are likely at risk from identity theft/fraud.	(Clark Howard)
Monitor your credit score continuously	Provides early detection of identity theft/fraud plus good practice anyway. I use CreditKarma. It’s free and works well for me – but check the Privacy Policy to see if it works for you too.	(Credit Karma)
Turn on 2FA for your on-line banking.	Passwords alone are too easy to crack. (If they’ve cracked your e-mail, they don’t even need to crack your banking password – they can simply reset it). If your bank doesn’t support 2FA, find another bank that does.	(twofactorauth.org)
Turn on on-line banking + credit card notifications	So that you instantly know when fraudulent charges occur you can minimize the damage.	
Stop using your debit card	In the event of fraudulent charges, it’s better to dispute charges than to have to recover stolen money.	
Confirm wiring instructions over the phone AND lookup the routing number and IBAN – NEVER trust e-mail messages by default	The person you may be e-mailing back-and-forth may not be the person you think it is – their e-mail may have been compromised.	(IBAN checker)

		(ABA number checker)
Be wary of on-line dating scam artists	Federal Trade Commission estimates that Americans lost $143 million in online romance scams last year.	(FTC Report)
Don’t fall victim to “IRS” tax scams – even if caller ID looks authentic	It is very easy to spoof caller ID. The IRS doesn't initiate contact with taxpayers by email, text messages or social media channels to request personal or financial information. These impersonators are after your personal information and your money.	(IRS Scams)
Use a dedicated e-mail address just for banking – nothing else	Reduces your exposure to financial risk in the event of your regular e-mail account take-over.	

Protect your files

Do this	Why	How
Invest in a cloud-based backup solution	Enables you to recover your files from Ransomware attacks, if your computer’s hard-drive crashes, if your computer is stolen, or if you accidentally erase your files. DropBox is a sync-solution not a backup solution. I use Backblaze. Do your research.	(Backblaze review)
Turn on hard-drive encryption	In case your laptop is stolen, prevent the thief from accessing your files.	(Mac guide)

		(Windows guide)
Wipe clean your old Mac/PC before selling or donating it	Your files are potentially more valuable than the device. You don’t want to disclose them inadvertently to the person you are selling it to.	(Mac guide) (Windows guide)

Free Public Wifi usage tips

Do this	Why	How
Consider using your Mobile data plan instead	It’s probably safer because you are less likely to be intercepted by an attacker.	
If you have no choice, use a VPN service	This ensure the communications are encrypted – so if you are intercepted, the attacker cannot do much damage.	With a work laptop, you should be equipped VPN anyway. I run my own VPN but recognize that is not everybody ☺ For personal devices, you may want to look at services such as TunnelBear or similar (as a bonus, you can unlock Netflix while travelling overseas).
Verify the WiFi hotspot details	You may be connecting to an attacker’s bogus Wifi hotspot that just relays to the real hotspot. Even if you do connect to the official hotspot – you are still exposed.	Look for official signs at the airport. Check with the Coffee Shop employee.
Consider limiting types of transactions e.g. no on-line banking over public Wi-Fi	If your communications do get intercepted, they are of limited value to the attacker.	