THE PASSWORD BOOK

Internet Security & Passwords Made Easy

2018

JASON MCDONALD

The Password Book: Internet Security & Passwords Made Easy

Jason McDonald, Ph.D.

2018

MORE THAN A PASSWORD BOOK

Most **password books** are just that, mere places to write down websites and passwords. (*This book does that.*)

But that's not enough! In today's rough-and-tumble Internet – full of scammers, thieves, and scoundrels – you need more than just a "Password Book." You need:

> A book that provides **scam education** as to what scams are out there, how scams work, and how to be mentally savvy enough to avoid "being scammed."
>
> A book that helps you **inventory** and **upgrade** the **security** of each key Internet asset, especially the "big three" of your computer, your email, and your mobile phone.
>
> And, a book that gives you a "**password system**" so that you can easily construct hard-to-guess passwords and have a framework for three tiers of security.

That's what this book does, so let's get started!

For Mom & Dad

CONTENTS

DISCLAIMER

This book aims to help you to **protect yourself online** – that is, to protect your computer, tablet, email, bank account, and/or mobile phone, etc. – against Internet hacks and scams. However, no security efforts are perfect, and this book offers no guarantees. By reading this book, you agree that any actions you take (or fail to take) are at your own risk. Neither Jason McDonald, the JM Internet Group nor Excerpti Communications accepts any responsibility for the effects of your actions or lack of action vis-à-vis any potential scams, viruses, Trojan horses, or other software or apps or any unforeseen problems of any type.

All trademarks are the property of their respective owners; any use is for illustrative purposes only. This guide is independent and has neither received nor solicited any advice or financial support from any of the vendors mentioned herein.

RESOURCE LINKS
&
BOOK REGISTRATION

This book references numerous resources or websites on the Internet using "jump codes." To access a "jump code," visit the website **http://jmlinks.com/** in your Internet browser. Simply enter the "jump code" there and you will be automatically transferred to the referenced Internet website.

> For example, if you see **http://jmlinks.com/35w** then enter "**35w**" at **http://jmlinks.com/** to access the referenced website.

Register Your Book

If you register your book, you'll get a free PDF copy of the book which has easy, clickable links to all resources. To do so:

1) Visit **http://jmlinks.com/pwregister**
2) Enter the password: **2017pw**

1
ANATOMY OF A SCAM

Let me start with a story, the **anatomy of a scam** perpetrated against my Mom. My Mom is a very smart woman, very involved in the community with literally hundreds of key friends and contacts in my home town of Tulsa, Oklahoma. She's a prime target for scammers, however – she's older, she's affluent, and she has many friends, family, and colleagues who are also attractive "targets" in their own right. She also has an AOL email account, a dead give-away that someone is not a member of the technological cognoscenti!

On the morning of November 7, 2014, I received (as did everyone on my Mom's AOL email contact list), the following email, under subject: "Sad News":

I really hope you get this fast. I could not inform anyone about our trip, because it was impromptu. We had to be in Philippines for a Tour. The program was successful, but our journey has turned sour. We misplaced our wallets and cell phones on our way back to the hotel after we went for sight seeing. The wallet contains all the valuables we have. Now, our luggage is in custody of the hotel management pending when we make payment.

I am sorry if I am inconveniencing you, but I have only very few people to turn to now. I will be very grateful if I can get a short term loan of ($2,450) from you. This will enable me sort our hotel bills and get my sorry self back home. I will really appreciate whatever you can afford at this moment. I promise to refund it in full as soon as I return. Please let me know if you can be of any assistance.

Thanks

Since the scammers had seized control of my Mom's AOL email, if you replied to her email, you then received instructions on how to wire her and my Dad the money, or if you expressed doubt, some back-and-forth with the scammers about their "problems" to reassure you that it was really her. To make matters worse, the scammers not only had control of her AOL email account but had deleted her email contacts after exploiting her account, making it very difficult for us, after we regained control, to send out a legitimate email to friends and family to warn would-be victims of this heartless "vacation problem" scam.

Let's look at the **anatomy** of this **scam**, starting with the two steps:

1. My Mom had been "phished," meaning someone had tricked her into opening an email attachment or "reverifying" her AOL login and password so that the scammers could take control of her email.
2. My Mom's friends, family, and contacts were being "spearphished," meaning the scammers were using a person that they knew (*my Mom*) to attempt to get them to do something they wanted (*wire them money*).

And let's break this down further into the constituent

elements common to all scams:

The Spoof. Both, first to my Mom, and then to her contacts, the scammers were *pretending to be something or someone that they were not*. They were "spoofing" – first, a "trustworthy" email sender and "trustworthy" website or attachment to which my Mom would mistakenly give her login and password, and second, doing the same thing to her contacts, pretending to be my Mom, after they had gotten control of her email.

The Confidence Game. Throughout, the scammers strove to increase the *confidence* of their intended victims, by emailing back people who asked questions (and in other such similar scams, even going so far as to converse on the phone). First the scammers *spoof* and then they build *confidence*.

The Keys. Your car or house has a physical key, but your email account, your mobile phone, your bank account online, your Facebook, Twitter, or LinkedIn, have *virtual keys* – your *login*, your *password*, and sometimes your *two-step verification code*. Scammers want these keys as means to an end – usually, but not always, money. In my Mom's case, once they had the AOL login and password, they could use those Keys to work on their real targets, her friends and family.

The Ask. Scammers may start with getting your "keys" but their ultimately goal is to get money. To do this, they must *ask* for something. In my Mom's case, first they *asked* her to click on something in an email and then to "reverify" her AOL login and password, and later they *asked* her contacts to send money urgently to the Philippines.

At the anatomical level, all scams share these elements in

common: the **Spoof**, the **Confidence Game**, the **Keys**, and the **Ask**. There are simple scams and more complex scams (See Appendix A for a list of common scams), but they all share these elements in common.

Once you understand the "anatomy of a scam," you can be on the look out for its constituent elements and thereby make yourself harder to fool.

THE GOALS OF THIS BOOK

This book has two goals:

1. To *educate* you as to how scams work.
2. To provide practical *tips* so that you can protect yourself against scams.

First, we'll learn a little about what scams are, how they work, and what elements can tip you off that you may be facing a scam. And, second, we'll identify practical todos to decrease your vulnerability to scams and scammers. Along the way, we'll investigate tips to improve privacy on the Internet, plus steps you can take to harden your passwords, email accounts, bank accounts, and other key assets of your digital identity.

But, for now, let's return to my Mom and her friends, and identify specific actions that could have (and did) help her resist being successfully scammed:

- **Be suspicious**. Whether it's a text message, an email, a message via Facebook or some app on your phone, or even an unsolicited inbound call, be suspicious. *Is this really who or what it pretends to be?*
- **When in doubt, don't click, and don't enter**. If

an email (app, text message, website), asks you to click on something and you're not sure, don't click. And if you do click, don't enter your login, password, or other identity information without *independently* verifying that the website / person / app is what it purports to be.

- **Be on high alert if money, identity information, or any "software downloads" or "app installs" are involved**! Anything that involves money or the Keys to your online identity (e.g., logins, passwords, social security numbers, phone, address, answers to secret questions, and/or two-step verification codes), should be approached with **extreme caution**.
- **Verify identities (independently)**. When in doubt, pick up your phone. *Call* your bank, or pro-actively *call* your Mom. Open up a new browser and manually type in the website of address of your bank. But don't rely on clicking on any link embedded in an email, or the CallerID that pops up on your phone (which is easily falsified). **Independent verification** is a must!

There are other steps we'll identify in the Chapters that follow that can help safeguard you against scammers. As for my Mom's "trip to the Philippines," fortunately no one fell for the scam, but her phone rang off the hook that day with concerned calls from friends and family. Tulsa is still a small enough town where no one believed that my Mom and Dad would *secretly* visit the Philippines.

SHARE THIS BOOK!

As a digital marketer, concerned citizen, and frustrated son of two loving but somewhat naïve parents, I am so passionate about scam education that I am publishing this

book at the lowest possible price on the Amazon Kindle platform, as well as allowing folks to "gift" others a free copy of the book in digital format. To do so, visit **http://jmlinks.com/pw**. Enter your information and we'll generate a "coupon code" for Amazon for the PDF, Kindle, or paperback version.

Get a $5.00 Rebate

At that web page, you can also get a $5.00 rebate by taking a quick scam survey about the book. (*Supplies are limited, and limitations and restrictions apply, so please see the website for details. Offer is limited to the first 100 persons*).

In addition, check out The Password Book's Facebook page at **https://facebook.com/thepasswordbook**. If you have any password or security tips as well as examples of new scams making their rounds on the Internet, please email those via **http://jmlinks.com/contact** or call 800-298-4065.

ABOUT THE AUTHOR

Jason McDonald earned his Ph.D. from the University of California, Berkeley, in 1992. He resides in the San Francisco Bay Area, where he teaches courses in Internet Marketing (SEO and Social Media Marketing) online and in person at Stanford Continuing Studies. He has several popular books on Internet marketing for small business, including the *SEO Fitness Workbook*, the *Social Media Marketing Workbook*, and the *AdWords Workbook*. Learn more about Jason at **https://jasonmcdonald.org/** or just Google "Jason McDonald."

1
COMMON SCAMFOOLERY

"You never know what a fool you can be
till life gives you the chance."
~ Eden Phillpotts (Author)

Your **online security** can be broken at the weakest link, and guess what? The weakest link is **you**.

No virus software, no "strong password," no two step verification, no encryption, no password manager, and no malware removal tool – *no matter how advanced* – can protect you from your own *carelessness* or *stupidity*!

It's not, however, really that most of us are that *stupid*.

It's that most of us are too *trusting*, and relatively *easy to fool*. With a little distraction and a little scamfoolery to make "A" look like "B," it's not that difficult for the scammers of the Internet to trick innocent folk into giving up their login or password, social security number or answer to

their "secret" questions, or any other item of information with which they can hack online identities and begin their mischievous mischief.

We've already looked at the **conceptual elements** of every scam – the Spoof, the Confidence Game, the Keys, and the Ask. Now, let's look at a few of the most common **scams** on the Internet in **template format**. All scams, after all, follow certain patterns, and if you know to look for them you will be less easy to scam.

TEMPLATE #1: PHISHING

One of the most common ways to be scammed online is to fall victim to a "**phishing email**." (See **http://jmlinks.com/36h** for a definition). You are sent an email that purports to be from a friend or relative, your bank or credit card company, PayPal, Google, or Facebook, or perhaps one that claims you've won a sweepstakes or even a large sum in the lottery. All you have to do is click on an attachment, which may look like a harmless Microsoft Word document or even a common Adobe PDF. Another variant is to trick you into "reverifying" your login and password at a "spoofed website," a website that looks like Amazon, Gmail, Facebook, etc., but really isn't.

By clicking on the email attachment, however, you install a virus or malware program to your computer that surreptitiously gives the thieves full control of your device. Or, if you reverify on the phony website, you've given the thieves access to your account. If you fall for it, in other words, you've been "phished."

And if you think you're too smart to be "phished" by phone or by email, yet another variant of phishing is

spearphishing, in which first they "phish" a friend of yours, and then they impersonate that friend via email or Facebook to trick you into clicking on an attachment or providing key information. In this template, you don't get an email that pretends to be your bank, Amazon, Facebook, Gmail, AOL, etc., but rather you get an email that pretends to be a friend or colleague, and that email tricks you into giving out required information. The spearphishing request can come by email but scammers can also use Facebook messenger or posts, or any other communication technology. (*This is how John Podesta, Chairman of Hillary Clinton's 2016 Presidential Campaign was tricked into giving access to his emails, and – as they say – the rest is history*).

TEMPLATE #2: SPOOFING

If **phishing** is the most common online scam template, a closely related template is **spoofing**. In a "spoof," the scammers create an app or website that looks exactly like a real one in the so-called **reverification scam**.

Here's how it works. Thieves send out "helpful" emails pretending to be your bank, Amazon, Google, Facebook, etc., and "alerting" you that you may have been "hacked," so they ask you to please "reverify" your password and login credentials via a web link. The web link sends you not to the real, legitimate website but a website that is a spoofed copy. Pretending to be who they're not (*Amazon, Google, Facebook, your bank, etc.*), and pretending to be what they're not (*on your side, just here to help*), they "phish" you into giving them key identity information by **reverifying** your identity into a **spoofed website**.

Variations of a spoofing scam can be conducted via Google. For example, there's the fake **anti-virus scam** or

tech support scam. In it, you do a Google search for "Why is my PC so slow?," click over to a website that purports to be a tech support company, and a "helpful popup" on that website "warns" you that you "may have a virus." You follow the instructions to download their free "antivirus software," or perhaps you call the website's 800 number and speak with a "helpful" representative who asks you to download an applet to allow him to "inspect" your computer and, before you know it, they've installed and signed you up for a "ransomware" program requiring you to pay a monthly fee to remove "computer viruses" that don't even exist!

Another variant is to send you an email that looks like it came from Amazon alerting you of an impending delivery for an expensive item such as a flat screen TV for $775. In this Amazon **delivery scam** (**http://jmlinks.com/36j**), the email has a link that says something such as "Didn't order this?" or just "Reconfirm shipping," and when you angrily login to "Amazon" by clicking the link to dispute the shipment, you have provided the thieves with your Amazon login and password at the phony Amazon website. You think you've blocked a fraudulent shipment, when in fact, you've just provided the scammers with your Amazon login and password by logging into a fake Amazon lookalike website yet providing your real Amazon login and email to the scam team.

TEMPLATE #3: UNSOLICITED CALLS

Email is the vehicle of choice for scams these days, but scammers can also use Facebook, messenger apps, or even text messages to your mobile phone. In fact, one of the growing types of scams uses robocalls and even calls by real people.

With the ease of spoofing the US CallerID system and the cheapness of robocall programs, scammers now spoof local area codes and phone numbers, and can even spoof a CallerID to make it look like it's a bank, Amazon, Google, or even the IRS. (See **http://jmlinks.com/35y** for more information.)

In fact, one of the most common **unsolicited call** phishing/ spoofing scams to make the rounds is the **Internal Revenue Service (IRS) scam**. (See **http://jmlinks.com/36e**.) Someone (a person or a robocaller) calls you out of the blue to "warn" you that the IRS will be filing a lawsuit against you, or that the IRS is literally coming to arrest you in just a few hours. You're instructed to wire money immediately to avoid imprisonment. Your caller ID may show an official IRS number or even say "Internal Revenue Service," but the scammers can be physically located anywhere in the world, from Pakistan to India, Mongolia to Russia, and anywhere in between. Even the call back number may look like it's in the USA, while you are actually speaking to someone halfway around the world who pretends to be an IRS employee! (You can watch a hilarious YouTube video on this scam at **http://jmlinks.com/35x**. in which the YouTuber scams the scammers)

Another type of unsolicited call scams is the **grandchild scam** (**http://jmlinks.com/36c**). In this spearphishing scam, the scammer pretends to be your grandson or granddaughter or perhaps some other family member who has been "arrested" in some foreign country, and is now desperate to have bail money wired to them immediately. And still others are the fake **tech support scams** (**http://jmlinks.com/36f**) whereupon they call you with a spoofed number that pretends to be Microsoft or Apple to alert you that your computer has been hacked. If you fall for it, you're instructed to visit a website, and

download some inspection software, which is then used to take control of your computer, sign you up for fake virus protection, or bill you for fake tech support.

TEMPLATE #4: CONFIDENCE SCAMS

The next scam template is the confidence scam. Someone or something is used to build up confidence that they are trustworthy. A famous example is the **Cashier's Check scam** (**http://jmlinks.com/36g**). You post an item such as a car or boat for sale on eBay or Craigslist, and you are contacted by a scammer. They offer to overpay for the item, work with you on the details of the deal to build up confidence, and then send you an official-looking check. Or, they get the item via PayPal, pay you, and then dispute the charge. If it's a Cashier's check, it's a forgery and if you ship the item, you're out the item, but even if not, you're out the funds you wired them as a "kick back" for the overpayment.

The Nigerian Prince scam in which a person pretends to be a famous Nigerian person or even royalty but needs help claiming his inheritance and asking you to participate is another type of confidence scam. The "prince" needs you to wire him some money, and he promises to pay out of his "proceeds." Learn more at **http://jmlinks.com/36b**.

Another confidence scams is the **online dating scam**, in which a (usually young) lover approaches you online, "falls in love with you," builds confidence and then, sooner or later, falls upon hard times and needs access to your credit cards or cash to help them out. An even more dramatic type of confidence scam is when you're contacted by a "hitman" who has been hired to kill you, or someone who knows someone has been hired to kill you, and you are

then extorted out of money to avoid the hit. Learn more at **http://jmlinks.com/36d**.

TEMPLATE #5: TROJAN HORSE SCAMS

By exploiting vulnerabilities in the operating system of your PC or Mac, iPhone or Android device, or tablet computer, scammers can install software that can do nearly anything – from logging your keys to steal your logins and passwords, to deploying your device in a "bot army" to attack other computers on the Internet, to even remotely monitoring your camera. Up-to-date anti-virus programs are pretty decent as nullifying security vulnerabilities (if you keep these up-to-date), so the more common attack scenario these days is what's called a **Trojan Horse**.

The Trojan Horse, of course, was used by the Greeks to enter the city of Troy. Unable to defeat the Trojans and enter their city, the Greeks built a beautiful wooden horse and hid themselves inside. When they awoke, the Trojans saw the horse (but no Greeks), and pulled the horse inside their city walls, only to be terrified the next day when the Greeks climbed out of their hiding place to slaughter the Trojans and take the city. This, by the way, is where we get the saying, "Beware of Greeks bearing gifts."

In computing, a Trojan Horse is thus a trick in which the scammer tricks you into installing a seemingly innocent piece of software or app and yet this software or app allows him to log your keystrokes, steal your passwords, or otherwise compromise your system. In this way, they get around your anti-virus program by tricking you into installing the malicious software.

Ransomware is a variant of this template, as once installed, the thieves lock you out of your device or files

and then demand ransom from you in order for you to regain access. But the first step in ransomware is usually some type of phishing and software installation hijack. Learn more about ransomware at **http://jmlinks.com/35z**.

SUMMING UP

This short survey of scams has indicated five basic templates:

Phishing / spearphishing, in which unsolicited emails tricks you to opening an attachment.
Spoofing / spoofed websites, in which you are directed to a fake website that tricks you into giving away your login details.
Unsolicited calls, in which you are cajoled or threatened into doing something, usually involving money.
Confidence scams, in which your confidence is built up until you comply with some demand.
Hijack scams (viruses, trojan horses, ransomware), in which malicious software is installed on your computer, tablet, or phone.

Armed with this knowledge, as well as the concepts of the **Spoof**, the **Confidence Game**, the **Keys**, and the **Ask**, it's now time to take the "Pledge of Paranoia."

SURVEY REBATE

Earn $5.00 via a quick survey. Visit **http://jmlinks.com/pw**, take a quick survey, and earn $5.00. You can even gift a friend a free Kindle copy of the book! Expires 12/1/2017 or without notice.

2
THE PLEDGE OF PARANOIA

"A paranoid is someone who knows
a little of what's going on."
~ William S. Burroughs (Author)

Take the following **Pledge of Paranoia**, and refer to this anytime your gut instinct gives you the slightest tinge that you may be facing a scam.

"Whereas I recognize that the **Internet**, even more so than real life, **is full of thieves, scammers, and scoundrels**…

"Whereas I recognize that companies such as AOL, Google, banks, credit card companies, the government, Facebook, Amazon, etc., can (and will) only do so much to protect the innocent…

"Whereas I recognize that password managers, anti-virus and anti-malware software, and regular updates of the operating systems of my computer, tablet, and mobile

phone can also only do so much to protect me…

"Whereas, although I shall rely on companies and organizations as indicated above to help in my protection as well the capabilities of regular software updates, anti-virus and anti-malware programs…

"I commit to taking pro-active steps to safeguard my online logins, passwords, verification codes and other forms of identity, such as the following:

- **I shall be suspicious** of any unsolicited emails, text messages, phone calls, pop up messages or other forms of Internet communications from *unknown* persons or entities.
- **I shall be suspicious** as well of any emails, text messages, phone calls, pop up messages or other forms of Internet communications from seemingly *known* persons or entities that seem a little strange, and especially those that ask me to click on a link, open an attachment, or – heaven forbid – provide logins, passwords, and/or verification codes.
- **I shall be suspicious** of any software or app downloads / installs to my computer, tablet, and/or cell phone. I will only install software or apps from reputable vendors, and conduct "due diligence" on any vendor BEFORE I download software or an app from said vendor.

When I have any feeling that something may be amiss in any type of communication – email, text, or phone, especially any communication that asks me to *click on a link*, *open an attachment*, *download or install an app or software*, *verify or reverify my login credentials* or *otherwise reveal login, passwords, or identity information*, *not to mention money*, I shall immediately –

- **Verify** the identity of the incoming person or entity through an **independent** means ideally by the act of a direct voice call to that entity or person; and/or
- **Verify** the identity of the incoming person or entity through an **independent** means such closing the email or text and **pro-actively** calling, emailing or texting the person or organization in question; and/or
- **Verify** the identity of the incoming person or entity through opening up a **new browser window** and **manually** typing in the website address of the entity in question.

"If I am unable to independently verify the identity of said person or entity, I shall – *under no circumstances* – click on any web link, open any attachment, download or install any software or app, or provide my identity information such as login, password, secret questions, etc., nor transfer money to any such individual

Pledged this day ___ of _____, 201_.

Name: _____

3
HOW TO GENERATE STRONG PASSWORDS

"I changed my password everywhere to 'incorrect.' That way when I forget it, it always reminds me, 'Your password is incorrect.'" ~ Anonymous

Passwords are important. No one denies this, and it's very clear that thieves want to steal one (or all) of three things:

Your **login**.
Your **password**.
Your two-step **verification code** (if in use)

Generally speaking, you don't change your logins, and your two-step verification codes are generated on the fly. So that leaves your **passwords** as the most important item to steal.

In this Chapter, we'll leave aside the problem of being

"tricked" into giving out your login, password, and/or verification code. We'll assume you've taken the *Pledge of Paranoia*, and are suspicious of things like unsolicited emails, texts, or even phone calls. So we'll focus on how to generate hard-to-crack passwords. There are two systems that you can use:

System #1.

Use a professional **password manager**. You can literally just Google "password manager," and you'll see a number of competitive products that you can purchase to manager your passwords across devices – your PC, tablet, and phone. Even better, to read overviews on password managers, visit **http://jmlinks.com/34q** or **http://jmlinks.com/34r**. And better still, some of the password managers such as Dashlane, LastPass, Zoho, or TrueKey have free offerings. Most require that you pay for features such as cross-device access, however, so that you can use the app on your phone, table, and PC.

The downsides to password managers are as follows. First, your master password can be hacked, either indirectly by tricking you into revealing it, or directly by the provider itself being hacked (which has, unfortunately, happened). Second, you may not be comfortable trusting a large corporation with sensitive access to your key accounts (their promises of security and trustworthiness to the contrary). In this age of post-9/11, post-Enron, and post-financial crisis, I – for one – take every corporate claim of responsibility with a huge grain of salt. And, third, a password manager may be overkill when you don't have that many accounts to keep track of, and you don't want the hassle of having yet another piece of software to install and manage. They also cost a small sum of money.

And, finally, don't fall into the trap of thinking a password

manager can protect you from your own gullibility. The weakest link remains you, in the sense that if scammers can trick you into giving them your password or trick you into installing a key logger or some type of nefarious system they can open your password management software and have one universal key to everything. A password manager creates a single point of failure.

System #2.

A cheaper system that is easier for most people is to use a **three-tier password system**. This is my preferred recommendation for most individuals who want primarily to manage their key online assets – especially their bank / financial institution(s), their mobile phone, their email, and their important social accounts like Facebook. Here's how you can set up a three-tier system.

SET UP A PASSWORD GENERATION SYSTEM

First, choose a "pattern generation system" to generate your passwords. Instead of using common words and numbers as passwords (which are easy for thieves to guess), create a pattern that goes from something you can easily remember to creating a password that's hard to guess.

Here are two ways to do that:

1) Choose an object and a related number sequence. For example, you could choose "States in the United States" and the "date that they entered the Union." So for *Oklahoma* you would have, "Oklahoma," and "November 16, 1907." Or, you could choose something like famous scientists and their birthdays, so you'd have "Einstein" and

March 14, 1879, or you could choose "Elements" and their "Atomic Weight," so you'd have "Gold" and "196.96". (One of the beautiful things of this system is you just have to remember the item and the pattern, so you can Google, "When did Oklahoma enter the Union?" or "What is Einstein's birthday" if you forget). Choose something that you like and that's easy to remember at this core level.

a. Next, choose a way to scramble the two elements, again a pattern that you can easily remember. For example, say, "Take the first two numbers of the month expressed as digits, the first six letters of the word, and the last two numbers of the year." So for Oklahoma, you'd have *11, Oklaho, 07 (*because Oklahoma entered the Union on 11/07). Or, for Einstein, you'd have *03, Einste, 79* (because Einstein was born on 03/79).
b. Many sites require a non-alphanumeric character, so choose one such as **, !, @* or *%* and part of your system. So "place the non-alphanumeric character" at the end, for example.
c. Many sites also require at least one capital letter, so make sure that your word pattern has that. For example, capitalize the first letter of the state name or person's name as in **O**klahoma or **E**instein.

In this way, you'd go from "My password system is to choose a state in the USA and their date of entry into the union" to a password that is:

11Oklaho07@

Or from "My password system it to choose famous scientists and their birthday" to a password that is:

03Einste79@

A Quote Pattern. An alternative pattern map can also be used. For example, you could identify famous quotes on love, and then take the first letters of the first five words plus the birthday of the author. Take the first two digits of the birth month, and place them at the beginning, then the first letter of the first five words in the middle, and then the last two digits of the birth year at the end. So you'd have:

"Shall I compare thee to a summer's day? Thou art more lovely and more temperate." ~ William Shakespeare, born April 23, 1564.

Which then becomes:

04sictt64

And then add a capital to the first letter, and an alphanumeric character to the end, so you'd get:

04Sictt64#

In your Password Book, you can safely write down your "pattern generation system." So you'd write:

My password generation system is to take a famous quote on love, take the first letters of the first five words plus the birthday of the author. Then take the first two digits of the birth month, and place them at the beginning, take the five letters from the quote (capitalizing the first letter), and the last two digits of the birthyear at the end. Finally, add the non-alphanumeric

character # at the end.

Or, if you use a state, you'd write that system down as well. *My password generation system is to take a United States State and the date that it entered the Union. Then I take the two digits of the month, then the first six letters of the state name with the first letter capitalized, and then the last two digits of the year. Finally, I add the symbol @ at the end.*

You now have a way to generate pretty strong passwords. Not as strong as from a password generator, but far, far stronger than most passwords used by most people. If you're curious, you can visit a website called "How Secure is My Password?" to check passwords you're generating at **http://jmlinks.com/34u**. If you enter *04Sictt64#* into this site, you'll see it estimates it will take six years (!) for a computer to guess this password. Or you can visit the Password Meter (**http://jmlinks.com/34v**) which estimates this password at a score of 97% or "Very Strong."

Note: Just to be on the safe side, I wouldn't use your *actual* passwords in the tools above; just use a password generated by your pattern, and then throw that one away.

Once you decide on a password generation system stick with it, as you can "generate" as many passwords as you need yet make them pretty easy to remember.

IDENTIFY YOUR TIERS

Now that you have a pattern generator, it's time to identify your **password tiers**. Most people should use tiers such as the following:

Tier #1: Super Secret Password. Use this tier for your

email account and your mobile phone access as well as your bank account(s), financial account(s), and credit card accounts. Each one should get a *unique password* that is not shared with any other entities. So, let's say you're using the US state system to generate your passwords. You might then have:

Email password: *03Nebras67@*
Mobile phone password: *09Califo50@*
Bank of America password: *03Vermon91@*
Chase credit card password: *12Pennsy87@*.
etc…

Do not share these passwords with any other entity! So your email account password is *unique* to Gmail (or AOL, or Microsoft Live, etc.) your Schwab Financial password is *unique* to Schwab, etc. You'd write down your logins and passwords in your Password Book (or, even better, knowing your password generation system, you could just write Bank of America, login: Jasonm27, password: "Nebraska." "Nebraska" would tell you enough to generate your password using your password generation system in case you forgot it).

Too Much?

If this sounds like too much, you can also use the same password across all your Tier #1 sites, for example, using *03Nebras67@* as your password for your email, your mobile phone, and your bank accounts. It's less secure than a unique password, but you still have a barrier between Tier #1 passwords and the tiers below.

Just remember that if you're compromised, you'll have to quickly reset your passwords across all Tier #1 sites.

Tier #2: Secret Password. Use this tier for less important sites like the Apple App Store / Google Play, Facebook, Twitter, Instagram, LinkedIn, etc. or other shopping or social media sites.

Here, you can share the password across sites (easier), or create unique ones for each one (more difficult, but more secure). So you might have one password for all these second-tier sites such as:

2nd Tier Sites, password: *03Florid45@*

You just have to remember if any site in the tier gets hacked or has an issue, you have to change the password for all sites in the tier. There's a trade off in ease-of-use and security of course. It's better for every site to have a unique password, but that might not be practical without a password manager. So just use one password across your entire range of Tier #2 sites, but be aware that if one site is compromised you have to reset the password across all sites.

Tier #3: General Password. This tier might be third party website such as blogs, apps, newspaper websites like the *New York Times*, etc. These are generally sites that do not involve money, and/or are not social media sites. You can use this password across these 3rd tier sites. So you might use the state, Virginia, and generate a 3rd Tier password of *06Virgin88@* for all your 3rd tier sites.

Note: if this seems too complicated, it's OK to have a much easier-to-remember password for your Tier #3 websites. For example, if you're using the State theme, you might use *Oklahoma1907* or *19Oklahoma07!*, or if you're using the Genius them, you might use *Einstein1879* or *18Einstein79!*. Since your Tier #3 are sites like the *New York Times* or perhaps the password to your local

newspaper, or an online game, it's not a big deal if these get hacked. And, since your Tier #3 password is totally different from Tier #2 and Tier #1, it means that thieves can't use the one to get to the other.

DON'T MIX TIERS

Hackers are unlikely to penetrate the Tier #1 sites such as your bank or email providers as those companies tend to have the best security. And, even if they do, you only have to deal with the password being hacked at that one particular site. Similarly, hackers are less likely to penetrate the Tier #2 sites like Google Play or Facebook to hack passwords than they are some third-rate blog or media site. And, if they do, then you only have to change your passwords across Tier #2. As for your Tier #3 passwords, you avoid the problem that hackers set up a fun or interesting fake blog or app to *phish* passwords, because even if they do, they are only getting your 3rd tier password with which they will be unable to get into your tier-one assets such as your email or bank account. Big deal if they hack into your password for online spades or even the local newspaper!

Don't Mix Tiers! But to be perfectly clear: never share the login / password details of your Tier #1 or Tier #2 sites with sites that are in the Tier #3. This is important because the most common way that hackers get logins and passwords is not by "brute force" attacks but by phishing password for folks who use the same login / password across many websites. With separate tiers, you avoid the problem that if they know your login / password on one site, they can use it on other sites.

TWO STEP VERIFICATION

Finally, wherever possible and especially at Tier #1, enable "two step verification." (This may also be called "Two Factor Verification" or "Multifactor Verification" or "Identification"). This is when you need to know not only your login and password, but also a verification code that is sent to your mobile phone. All the major banks offer this, as do the major email providers such as Gmail or Yahoo mail. Even Amazon and other big retailers offer it. For anything in Tier #1 or Tier #2, I strongly recommend that you enable two-step verification. To do so, visit their website and search for "Two Step Verification" or just Google "Two Step Verification" and their name. For example, if you Google "Amazon Two Step Verification" (**http://jmlinks.com/34w**), you'll quickly get to Amazon's page on how to enable two-step verification.

Once you've enabled two-step verification, remember as well that your bank, Gmail, Yahoo, Amazon, or whatever entity will never text or call you with a secondary message asking what the verification code is. The process is always:

1) Visit the organization's website (e.g., BankofAmerica.com).
2) Enter your login.
3) Enter your password.
4) Get texted a "verification code" to your mobile phone.
5) Enter that "verification code" on the website.

You can also then choose to "trust" your device, so that you don't have to continually reenter verification codes on your computer, tablet, or phone.

Beware The Two-Step Verification Scam

Thieves have figured out a way around two-step verification. It works like this. First, they obtain your username and password (e.g., for your Bank of America account), perhaps by means of a key logger or other type of massive data breach. But you have two-step verification turned on. So, they attempt to login putting in the correct username and correct password and Bank of America asks for the "verification code" (which has been automatically texted to your cell phone). The thieves then text your cell phone directly pretending to be Bank of America and asking you to text them back the verification code "as if" they were Bank of America asking for you to text it.

At this point, they now have tricked you into texting them the verification code, and they can use that code to take control of your Bank of America account, resetting your verification device to their cell phone. They're off and running.

If for some reason, you get a) a text from your bank, financial institution, or email provider like Google's Gmail of a verification code, and then b) an immediate second text asking for you to text back that code, then you've been scammed.

IMMEDIATELY contact your bank, financial institution, or email provider and have them reset your login, password, and verification settings. You should also scan your phone, computer, or tablet for keylogging software.

You can read more about this "2FA" (Two Factor Authentication) scam at **http://jmlinks.com/35q**.

WRITING PASSWORDS DOWN

Should you write your passwords down? In a perfect world, no, you'd never write them down. But who could possibly remember all their passwords? You either have to write them down, or use a password manager.

Consider which is more likely. That someone breaks into your home, finds your password book, comprehends your password generation system, goes to your computer, visits your bank website, logs in, and steals your money… or that someone hacks a website that has the same passwords as your bank, and then uses that treasure trove of hacked or phished passwords to login to a bank, financial institution, or credit card website? The problem is more hacking and phishing on the Internet than crooks breaking into people's homes and stealing their password books. (Vulnerability to hacking is one of the problems with all the online password managers; they are also obviously big targets for hackers!).

So I recommend that you do write your passwords down in your Password Book.

Fear of Coworkers, Family Members, or Others

Let's face it, however. You might not want to leave your Password Book out at work, or even at home for fear not of prowlers but of coworkers or less-than-honest family members, gardeners, maids, etc. If that's the case, for more security, however, you can choose to split the location of where you write your "Password Generator" down from where you write your passwords down.

For example, you can write down your password generator theme, tear that page out of the book, and place that in

one place (e.g., hidden in a dresser drawer), and then write in your Password Book only the corresponding US State or Scientist. So your Password Book entry for Bank of America might just say only:

Bank of America: Password: Oklahoma.

Which tells a thief nothing, but tells you to use Oklahoma to generate the corresponding password based on the Password generator of US states as explained above.

SUMMING UP

At the end of this Chapter, you should have:

a) Identified a **password generator system** that will be easy for you to remember.
    a. Identified which entities such as your bank, financial institutions, or email providers like Gmail that allow two-step verification.
b) Identified which entities are in which of your three **tiers** (Tier #1, the most secure level; Tier #2, secure level; and Tier #3, general level).
c) **Created** and **written down the passwords** for each entity in each of your three Tiers.


https:
search

5
YOUR COMPUTER

""If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."
~ Bruce Schneier (American Cryptographer)

First among the keys to your kingdom is your **computer** (or your **tablet** if you don't use a laptop or desktop computer). Cyberthieves would love to install a virus, malware, and/or spyware on your computer. Why? Well, generally for one of three purposes:

#1 to install a **keylogger**, a secret type of spyware that sends every keystroke (including your logins and passwords) to them; and/or
#2 to install **remote access** so that they can literally take control of your computer remotely and in combination with a keylogger "hijack" your computer to take control of your bank accounts and other financial assets; and/or

#3 to use your computer as a "**bot**" in a bot army so that they can use it for nefarious purposes such as sending out spam emails, engaging in denial of service attacks, etc.

Your best defenses are as follows.

Keep Your Operating System Up-to-date

Both Apple and Microsoft allow free upgrades to your operating system. Be sure to continually update your operating system to the latest and greatest version of Apple iOS or Windows. I recommend checking this monthly, and here's how:

For Apple iOS

- Open the App Store app on your Mac, then click Updates in the toolbar. If updates are available, click the Update buttons to download and install them.

For Windows

- Click the "Start" button in the left corner of the screen
- Then go to Settings > Update & Security > Windows Update and select "Check for updates." If updates are available follow the prompts to update your software.

I recommend that you enable automatic updates for either iOS or Windows, and periodically check to make sure that the automatic updates are indeed being installed.

Keep Your Browser Up-to-date

Your browser is what you use to browse the Internet, and accordingly any vulnerabilities in the browser can be used by hackers to exploit your computer and even possibly install malicious software. Most of us browse the Web using one of the major browsers, i.e. Google's Chrome, Mozilla's Firefox, Apple's Safari, or Microsoft's Edge. Be sure to update whatever browser you're using.

Here's how:

> **Chrome**. Open Chrome, at the top right, click on the three dots (Menu), then click Help > About Google Chrome. *If you need to update, it will automatically update Chrome.*
>
> **Firefox**. Open Firefox, at the top right, click on the three bars (Menu), then click the Question Mark > About Firefox. *If you need to update, it will automatically update Firefox.*
>
> **Safari**. Open the Mac App Store and click on Updates. If there is an update for Safari, it will show up there.
>
> **Microsoft Edge**. If you use Microsoft Edge, just be sure to update Windows and that will automatically update the Edge browser as well.

Unfortunately, most browsers don't auto-update, so I recommend checking at least once a month to make sure that they are up-to-date.

Install and Use an Anti-virus Program

Computer viruses are programs that "infect" your

computer. Once you're infected, they can literally ruin your computer and make it inoperable, do other malicious things like slow it down, and do really malicious things like install key loggers, allow remote control, or even deploy your computer as a "bot" in an Internet "bot" army. For this reason, you must use an anti-virus program.

Nowadays both Windows and Mac iOS come with pre-installed anti-virus software. Be sure it's installed and running. Here's how.

Windows / Windows 10

If you're running Windows 10, it's called *Windows Defender*. If you keep Windows up-to-date then it runs in the background, and you'll be notified if there's a problem. You can check it by going to the "Windows Defender Security Center" which is accessed by hitting the "Start" window at the lower left, and then typing "Defender" and selecting "Windows Defender Security Center.

You should also make sure that **Windows Firewall** is enabled. To do so, go to the Start Menu on the lower left, then type "Control Panel," and then click on System and Security, and then Windows Firewall. Follow the instructions to enable it. (Note: if you are running a proprietary anti-virus program it may have its own firewall).

If you're running previous versions of Windows, it's called *Microsoft Security Essentials*. Be sure to install and run it, though you'd be better off upgrading to Windows 10.

Mac iOS

Mac has built-in firewall, anti-virus and other security software like Windows. Just be sure to keep your iOS up-to-date.

Paid Anti-virus Programs

If you think you need to go to the next level of security, you might consider upgrading to a paid anti-virus platform. You can find a nice article on the best anti-virus software programs at **http://jmlinks.com/35j**. Both Windows 10 and iOS have other security features, which you can read about here (**http://jmlinks.com/35k** for Windows) and here (**http://jmlinks.com/35m** for Mac iOS).

Stay Up-to-Date

In summary, here are your monthly todos:

1. Check to see if your operating system needs an update.
2. Check to see if your Web browser like Google Chrome needs an update.
3. Check to see if your anti-virus program has been running and, if not, run it manually.

In summary, keep your operating system up-to-date, make sure to update your browser on a regular basis, and use some type of anti-virus program. Your computer is a key asset and thieves definitely are on the prowl looking for vulnerable computers.

The Human Element: a Recap

After all this technical mumbo-jumbo, don't forget the **human element**. The weakest link isn't your software; it's you.

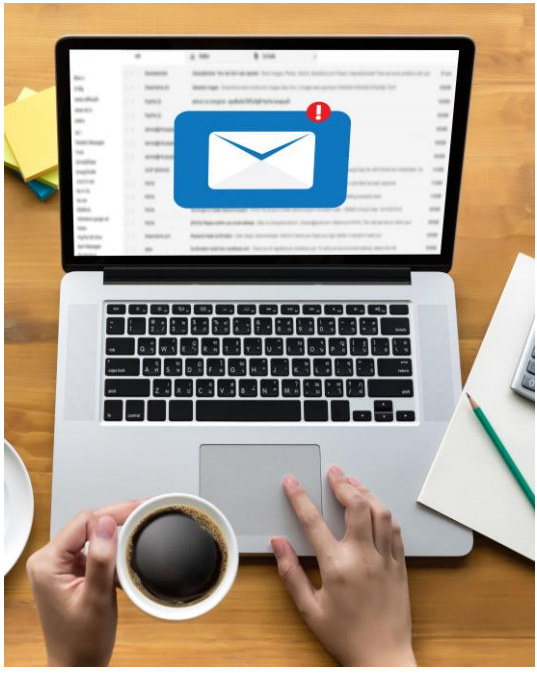
To recap what we learned in Chapter 2, by far the easiest way for a hacker to compromise your computer it to get you to install a malicious program. These "Trojan Horses" appear to be nice, useful, or benevolent software programs but in reality are designed to install hacker software in the background.

The usual paths to trick you are:

- Getting you to click on an **email attachment** from an unknown sender or a "spoofed" sender that appears to be a friend or family member. Always remember to be highly skeptical BEFORE opening and installing any email attachment.
- A **website popup** that deceivingly lies to you and says "you're infected" with a virus, and then prompts you to download a "virus check." Don't do it! Close your browser, open your real anti-virus program and scan your computer manually.
- A **human trickster** that calls on the phone or send you an unsolicited email as a fake tech support call from Microsoft or Apple. These calls or emails pretend to be official tech support and ask you to visit a website and install an analysis program. Neither Microsoft nor Apple ever pro-actively call customers and "warns them" that they are infected, so don't fall for this scam!
- A **Google search** that lands you on a website and then that website has some "fun" or "useful" software that also includes a Trojan Horse program. (A common ploy is a Google search for

something like "Is my computer infected" and you land on a malicious site that a) confirms you are infected, and b) offers to scan your computer after you install its "free" software). Be very, very careful before installing any "free" software from any site on the Internet. Buy and install software only from reputable vendors!

These sorts of "Trojan Horses" programs are also called **malware** or **ransomware**. A good program to install if you're concerned about malware or ransomware is called Malwarebytes and you can learn more at **http://jmlinks.com/35n**. You can also use a cloud-based backup program such as Carbonite backup (**http://jmlinks.com/35p**) if you have valuable files on your computer; by backing them up to the cloud, if your computer is hacked or penetrated by malware, you can still retrieve your valuable files from the cloud even though your physical computer has been compromised.



6
YOUR EMAIL

"Email is the greatest thing.'"
~ Wally Amos (American Entrepreneur)

Forgot your login? Forgot your password? Click here to reset your password. We've all seen those links across the Internet, and they all rely on one system: **email**. A chain is only as strong as its weakest link, and for that reason, scammers really want to seize control of your email account. Once they control your email, they can often reset your passwords for everything else, including your bank or financial institutions.

Your email security is one of the "crown jewels" of your Internet security and privacy. You want to protect it, very very carefully.

Here are the basics for any and all email providers:

Use a Tier #1 Super Secret Password that is unique to your email. Do not share that password with any other website, app, etc.!

Turn on "**Two Step Verification**" which most email providers now offer. If your email provider does not have "Two Step Verification," I strongly recommend that you switch providers!

Anytime you ever suspect your email account may have been compromised, immediately login and reset your password *manually* by visiting the provider's website *directly*.

While there are many email systems, in this Chapter, we'll examine a few of the most common – Gmail, Yahoo, Microsoft's Live mail, and AOL.

Choose your email provider from the list below:

Gmail (**https://www.gmail.com**). One you're logged in, click on your name / photo in the top right of the screen, and then click **My Account** in blue. Next, click **Signing in to Google** in blue. At this point, you can take the following steps:

1. **Change Your Password.** Upgrade to a **Tier #1 super secret password** for Gmail.
2. Enable **two-step verification** for your Google / Gmail account at **http://jmlinks.com/34e**.
3. **Account recovery options.** Add a recovery email, recovery phone, and robust security question.

Google also has a nice feature called "Security Checkup" which will lead you step-by-step into checking your security settings and options. You can access it at **http://jmlinks.com/34f**.

There is also Google's "Privacy Checkup" at **http://jmlinks.com/34g**. Don't miss Google's "Personal info and privacy page" about you at **http://jmlinks.com/34h** especially the "My Activity" link which will show you all the information Google is tracking about you online. For example, at "Activity controls" you can see and manage all the information Google is collecting about you across devices, such as your Google Maps and Navigation information and recordings of your voice and audio interactions with Google at **http://jmlinks.com/34j**.

Yahoo (**https://www.yahoo.com**)

Login to Yahoo, then under your name / photo click "Account Info" and then click "Account security." Optimize the following features:

1. **Change Your Password**. Use a **Tier #1 super secret password** for Yahoo mail.
2. Click on **Two-step verification** to enable two-step verification to your mobile phone.
3. **Email addresses**. Add a backup email to recover account access in case of a problem.

You can also check security features on Yahoo mail by first going to the Yahoo main page, clicking on the mail icon on the top right, and then click on the gear icon at the very top right of the email manager. Next, click on *Settings* > *Security*. There's not much here, other than whether or not to embed images in received emails. The real controls are on Yahoo's main page as indicated above.

Microsoft Outlook / Live Mail

Go to Microsoft's main page at **https://www.live.com/**. Login to your account, and then click on your name and then "View Account." Here you can optimize the following:

1. Password. Click on "Change password" to update it to a **Tier #1 Super Secret Password**.
2. Go to Microsoft Security at **http://jmlinks.com/34k**. Click on "Update your security info" to check your security settings such as an alternate email, mobile phone, and voice phone contact information.

To enable Two-step verification on Microsoft Outlook / Live, go to the Security Settings Page (**http://jmlinks.com/34m**).

While you're there, you can click on the "Privacy Tab" to review your privacy information (**http://jmlinks.com/34n**).

AOL (**https://www.aol.com**)

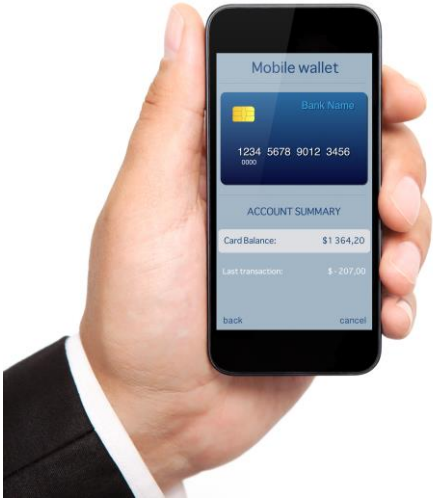
Login to your AOL account, and then in the top right click on "Account Info." Once there, you can update your password as well as turn on 2-Step verification. Unfortunately, to use 2-Step verification on AOL, you must download their very clunky desktop software, but if you are a heavy AOL user that may still be a good idea. You can (and should) update your mobile phone, alternate email, and security question here. Access this at **http://jmlinks.com/34p**.

Other Email Providers

If you're using another email provider, check with your email provider. The two main items are:

1. Use your "Tier #1 Super Secret Password."
2. Enable two-step verification, if available.

If they do not allow two-step verification, I strongly recommend you switch to another email provider. In addition, where possible, also enable alerts on suspicious logins, and be sure to enter your phone number, alternate email address, and security questions so that you are able to regain access in case you are locked out, maliciously or otherwise.


Mobile wallet
Bank Name
1234 5678 9012 3456
0000
ACCOUNT SUMMARY
Card Balance:
$1 364,20
Last transaction:
$-207,00
back
cancel

7
YOUR PHONE

"My cell phone is my best friend.
It's my lifeline to the outside world."
~ Carrie Underwood (Singer)

Guess what? Thieves don't have to *physically* steal your cell phone to steal your cell phone. Because mobile phone numbers are portable, all they have to do is convince your provider (Verizon, AT&T, T-Mobile, Sprint, etc.) to "port" your number to a new device, and "presto!" they've *virtually* stolen your cell phone and are now in control of it. If you're using two-step verification, they now control that second step and in combination with your username and password, they're home free.

Your mobile phone is a very key part of your Internet security, and so you must secure it.

Step #1: Secure Your Account at Your Phone Provider's Website

The first step is to login on your computer to the website of your mobile phone provider (such as T-mobile.com, ATT.com, Verizon.com), etc., and make sure that you:

- Know your login (usually your mobile number)
- Set your password (use a Tier #1 Super Secret Password). Write your password down in your password book.
- Set any security questions or other security features.

Some providers also have two-step verification for access to their websites; be sure to enable it. The problem is that the thieves will call into the call center, claiming to have "lost" your phone and then use that call to reset your phone to their device. So in this case two-step doesn't really help you. You can read more about mobile phone hijacking and how it works at **http://jmlinks.com/35r**.

You should also login and update your password (including turning on two-step verification) at both Apple ID and Google Play, as these allow app installations and contain important payment information. For Apple ID (iPhones and iOS devices), visit **https://appleid.apple.com/**. For Google Play (Android phones and devices), visit **https://myaccount.google.com/**.

Step #2: Secure Your Account at the Call-in Center

Since thieves may call into the "Call Center" of your mobile phone provider such as Verizon, AT&T, or T-Mobile, you should, therefore, call in and ask the provider to set a "**call in password**" or "**account password**." This is a password that you (or anyone else) will be required to know before they are allowed to make changes to the

account, such as porting your mobile phone number to a new device. Many people use their mother's maiden name for this, but (*as I am paranoid*) I don't use my mother's real maiden name, but rather a fake maiden name that only I know. You can't be too cautious!

At any rate, call into your mobile phone provider and set an account password. Ask them if there is anything else you can do to secure your mobile phone account.

Now, we'll assume you've done everything possible to secure your mobile phone account and thus prevent your account from being hijacked. Let's turn to your phone itself.

Update Your Phone's Operating System

Both Apple and Google Android constantly update and upgrade the security features of the operating systems for their phones. Whatever platform you are using, you want to upgrade your operating system at every roll out. First make sure you are connected to WiFi, since upgrading the operating system over cellular can be slow and costly.

Next, follow these steps.

Apple iOS Phones

Tap "Settings" on your iPhone, then "General," and then "Software Update." Your phone will tell you if there is an available upgrade. If there is, install it.

Google Android Phones

Tap "Settings" on your Android phone, then tap "About Device," and tap "Software Update" and then "Check for Updates." Your phone will tell you if there is an available

upgrade. If there is, install it.

The Weakest Link: You and the App Store

The weakest link is, of course, you. That nifty, fun, "free" app that you've heard about on Google Play or the Apple App store? It could be a Trojan Horse.

Anytime you download and install an app on your phone, you're taking a security risk. Apple does a better job than Google does of policing apps in its store for spyware and malware, but both vendors can't be 100% certain. Therefore, just as on your computer or tablet, be wary of any apps that you install. They could be Trojan Horses that do anything from key logging to hijacking your phone to sending that precious two-step verification code to a third party.

Under no circumstances, install "free" apps that you find not in the App Store / Google Play but through some other means such as an email, Google search, or text message.

Todos

Your phone is a critical piece in your security infrastructure, so your **todos** are:

1. Secure your online web access to your cell phone provider's website (e.g.,Verizon, AT&T, T-Mobile, etc.) with a strong password and two-step verification, if available.
2. Set an account password for call-in activity.
3. Update your cell phone operating system on at least a monthly basis.

SURVEY REBATE

Earn $5.00 via a quick survey. Visit **http://jmlinks.com/pw**, take a quick survey, and earn $5.00. You can even gift a friend a free Kindle copy of the book! Expires 12/1/2017 or without notice.


2015
2016

8
YOUR FINANCIAL ACCOUNTS

"I rob banks because that's where the money is.'"
~ Willie Sutton (Bank Robber)

If your computer, email, and mobile phone are means to an end, your bank accounts and credit cards are the ultimate goal for thieves and scammers on the Internet. **They want access to your bank accounts and credit cards to steal your money!**

Accordingly, in this Chapter, let's review your bank accounts, financial accounts, and credit card accounts to tighten them up to Tier #1 password security.

Your Bank

If you use any form of online banking, your login, password, and verification codes are prime targets for Internet thieves. To tighten your bank security, first login

to your bank account directly. Next, your **todos** are:

1. Upgrade your password to a unique "**Tier #1 Super Secret Password**." You may have to hunt to find where to reset your password; it's often under "My Profile" or "My Account."
2. **Upgrade** all other **information** that is available, such as your phone number, cell phone number, alternate emails, etc. This would include your "secret questions."
3. Look to see if they have "**notification options**" to alert you to suspicious activity.
4. Enable "**Two Step Verification**," which is now offered by most banks and financial institutions.

Write down your bank password in your password book, and be sure to write down the web address of your bank and contact phone number, so you can quickly contact your bank in the event you've been hacked. I also recommend calling into your bank, directly, and asking if they can password-protect you on call in, a so-called "**account password**," which means that you'd have a verbal password to give to the bank when you call in.

Other Financial (Investment) Accounts and Your Credit Cards

Most of us have more than one financial institution. We may have a few different accounts at a few different banks, and we may also have retirement or investment accounts at companies like Fidelity, ETrade, Schwab, etc. The same rules apply to each of your financial accounts. Login to the account, upgrade the password to a Tier #1 super secret password, audit the notification and alert features, and upgrade to two-step verification if they offer it. Set an account call-in password if available.

Credit Cards, Debit Cards, and Identity Theft

Finally, the same goes for **credit cards** and **debit cards**. Inventory which credit cards or debit cards you have, and upgrade each and every one of those accounts accordingly. However, it is interesting to note that under federal law you are only liable for $50 in fraud activity on a credit card, if you notify the lender in ninety days or less. Loss limitations on debit cards are somewhat different. To learn more, visit **http://jmlinks.com/36a**.

That said, I highly recommend that you fortify your credit card security as you can become a victim of "identity theft," in which thieves steal not only access to your credit cards but also your financial identify. For this reason, I recommend that you run your credit report at least once a year. You can do this for free at **http://jmlinks.com/35s**. You can also use a paid monitoring service such as Identity Guard at **http://jmlinks.com/35t**. In this way, you'll get an alert if hackers attempt to open new credit cards in your name or alter other parties of your identity.

At the end of this Chapter, you should have audited and upgraded all banks, all financial institutions, and all credit or debit card accounts. Write down the login and password information in your Password Book.

8
FACEBOOK

"Facebook was built to accomplish a social mission – to make the world more open and connected."
~ Mark Zuckerberg (CEO of Facebook)

Facebook is the largest social media network. Nearly everyone is on it. It's a great place to look at and share photos of family – kids, grandkids, parents, friends – as well as timely news and even debate politics or read the news. Facebook is fun!

But Facebook is also dangerous as thieves love to capture your Facebook login and password, and Facebook can be used to authenticate access to other websites. Plus if thieves can take control of your Facebook account, they can then impersonate you (as in my Mom's example pretending to have you stranded in the Philippines) as part of a confidence scam against your friends or family.

FACEBOOK TODOS

#1 – Set up a strong password. Be sure to use a "Level #1 super secret password" for Facebook. You can change your password by logging into Facebook and then visiting **http://jmlinks.com/34d** which will get you to *Facebook* > *Settings* (located at the top right on Facebook) and then click on "Change password."

#2 – Enable "two factor" authentication. When enabled, Facebook will text your phone a code when you login (or use the Facebook app) that you must use in addition to your password. Learn more at **http://jmlinks.com/34c**.

#3 – Review your security settings. Visit **http://jmlinks.com/34d** or in Facebook on the desktop click on the top right > Settings > Security and Login. Pay special attention to "Get alerts about unrecognized logins" which will alert you via email about suspicious activity.

#4 – Choose 3 to 5 friends. Using the settings feature, above, Facebook allows you to identify three to five friends to contact if you get locked out. This is a useful feature if you're hacked, so that you can regain control of your Facebook account.

Finally, on the *Settings* > *Security* tab, on the left column, look for **Apps**. Browse this to see which apps you've given access to your Facebook contacts and other private information. To disable any apps that you don't trust, hover over the icon and click the "x" at the top right. Facebook apps are notorious for enabling all sorts of access that really you shouldn't be giving them in the first place.

Facebook Privacy

Facebook, like all big companies, loves to snoop in your business. Facebook hides this under *Settings* > *Privacy* on the left column, and it's worth reviewing what you've "agreed" to allowing Facebook to make publicly available about you online. After logging into Facebook, navigate to Settings (top right) and then *Privacy* on the left navigation. Review the following elements and set them up to your liking:

> **Who can see my stuff?** Browse and select your options for –
>
> > *Who can see your future posts?*
> > *Who can see your friends list?*
> > *Review all your posts and things you're tagged in* (review this to eliminate non-flattering information about yourself online).
> > *Limit the audience for posts you've shared with friends of friends or Public?*

You should also set "Who can contact me?" and "Who can look me up?" to a desired level of visibility.

Upgrade Other Social Media Networks

While Facebook is the most important social media app by far, you should repeat the exercise above on Twitter, Instagram, Pinterest, LinkedIn or any and all other social sites that you use frequently. Upgrade your passwords and, if possible, enable two-step verification. But most thieves really want access to Facebook because of its universality and its utility in "spoofing" your identity to scam your friends and family.

9
AMAZON

"What we want to be is something completely new. There is no physical analog for what Amazon.com is becoming."
~ Jeff Bezos (CEO of Amazon)

Amazon is the world's third largest retailer. 80 million Americans have Amazon prime memberships, which is approximately 64% of US households, spending on average $1,300 per year on Amazon (**http://jmlinks.com/35u**). That's a lot of people, and a lot of money, and so it's no wonder that thieves and scammers would love to get access to your Amazon account!

To secure your Amazon account, take these steps.

1. Upgrade your password to a Tier #1 Super Secret password.

2. Visit the Amazon security page at Amazon.com > Accounts & Lists > Your Account > Login & security.
    a. Make sure that you have both your email and mobile phone number entered correctly.
    b. Click to Advanced Security Settings and enable Two-Step Verification as well as enter a "Backup Method."
    c. Require codes from all devices.

Now that you've upgraded your Amazon account, remind yourself of the "human security" necessary to protect your Amazon account. First and foremost, be suspicious of unsolicited emails that pretend to be from Amazon. One of the more clever scams is the scam when they email you "as if" a package has been ordered (usually an expensive TV) with a link to reverify the delivery. You then click through on the link to a "spoofed" Amazon.com site, and enter your login and password to "stop" the order. Presto! They've scammed you out of your Amazon login and password. You can learn more at an official Amazon help file at **http://jmlinks.com/35v**.

As for Amazon privacy settings, you don't have a lot of control. You can learn more about your public profile and privacy at Amazon at **http://jmlinks.com/35w**.

If you're a heavy users of other retailers such as Target, WalMart, or Macys, be sure to login and upgrade your accounts there to the best security possible. Anything that involves money is a target!

10
YOUR PASSWORD GENERATION SYSTEM

"Passwords are like underwear: you don't let people see it, you should change it very often, and you shouldn't share it with strangers.'" ~ Chris Pirillo (Founder of LockerGnome)

Choose a **password generation system**, as explained in Chapter 4. Write it down here:

My password generation system is:

_____

_____

_____

_____

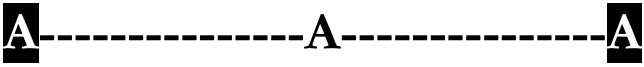
_____

_____

_____

10
YOUR PASSWORDS

Write down your passwords here. If you're super concerned about security, tear out the preceding page on "your password generation system" and store that separately. Then just indicate the "core" or "foundational" password here.



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "A" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

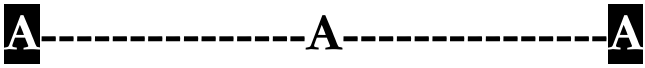
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "A" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

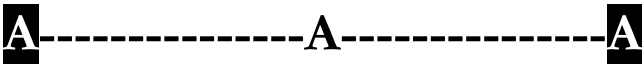
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "A" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

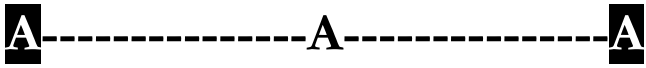
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "A" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

B----------B----------B

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "B" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

B----------B----------B

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "B" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

B----------B----------B

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "B" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

B----------B----------B

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "B" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

C----------C----------C

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "C" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

C----------C----------C

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "C" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

C----------C----------C

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "C" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

C----------C----------C

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "C" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

D----------D----------D

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "D" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

D----------D----------D

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "D" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

D----------D----------D

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "D" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

D----------D----------D

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "D" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

E----------E----------E

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "E" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

E----------E----------E

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "E" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

E----------E----------E

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "E" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

E----------E----------E

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "E" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

F----------F----------F

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "F" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

F----------F----------F

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "F" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

F----------F----------F

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "F" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

F----------F----------F

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "F" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

G----------G----------G

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "G" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

G----------G----------G

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "G" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

G----------G----------G

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "G" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

G----------G----------G

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "G" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

H----------H----------H

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "H" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

H----------H----------H

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "H" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

H----------H----------H

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "H" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

H----------H----------H

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "H" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

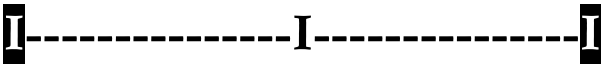
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "I" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

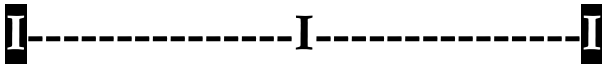
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "I" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

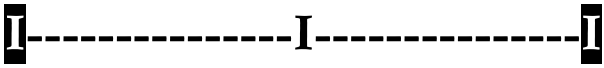
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "I" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

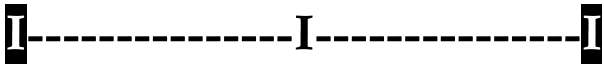
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "I" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

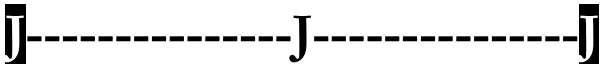
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "J" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

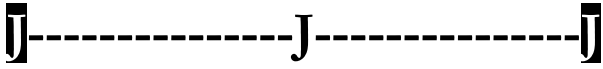
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "J" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

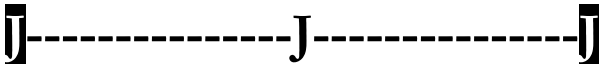
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "J" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

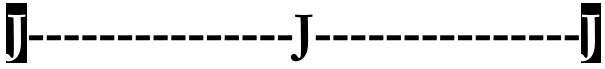
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "J" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

K----------K----------K

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "K" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

K----------K----------K

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "K" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

K----------K----------K

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "K" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

K----------K----------K

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "K" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

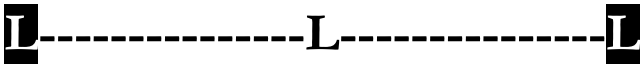
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "L" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

L----------L----------L

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "L" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

L----------L----------L

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "L" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

L----------L----------L

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "L" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

M----------M----------M

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "M" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

M----------M----------M

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "M" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

M----------M----------M

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "M" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

M----------M----------M

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "M" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

N----------N----------N

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "N" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

N----------N----------N

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "N" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

N----------N----------N

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "N" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "N" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

O----------O----------O

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "O" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

O----------O----------O

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "O" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

O----------O----------O

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "O" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

O----------O----------O

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "O" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

P----------P----------P

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "P" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

P----------P----------P

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "P" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

P----------P----------P

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "P" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

P----------P----------P

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "P" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

Q----------Q----------Q

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "Q" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

Q----------Q----------Q

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "Q" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

Q----------Q----------Q

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "Q" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

Q----------Q----------Q

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "Q" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

R----------R----------R

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "R" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

R----------R----------R

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "R" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

R----------R----------R

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "R" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

R----------R----------R

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "R" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

S----------S----------S

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "S" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

S----------S----------S

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "S" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

S----------S----------S

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "S" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

S----------S----------S

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "S" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

T----------T----------T

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "T" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

T----------T----------T

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "T" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

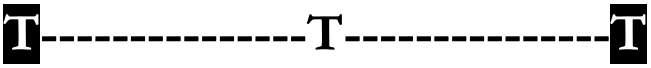
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "T" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

T----------T----------T

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "T" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

U----------U----------U

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "U" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

U----------U----------U

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "U" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

U----------U----------U

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "U" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

U----------U----------U

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "U" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

V----------V----------V

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "V" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

V----------V----------V

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "V" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

V----------V----------V

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "V" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

V----------V----------V

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "V" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "W" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "W" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "W" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "W" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

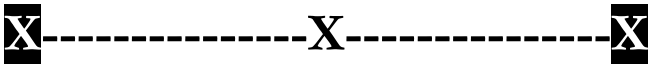
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "X" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

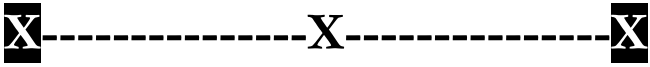
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "X" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

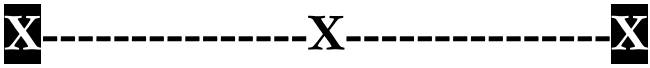
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "X" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

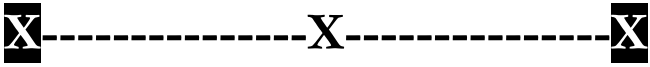
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "X" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

Y----------Y----------Y

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "Y" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

Y----------Y----------Y

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "Y" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

Y----------Y----------Y

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "Y" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

Y----------Y----------Y

WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "Y" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

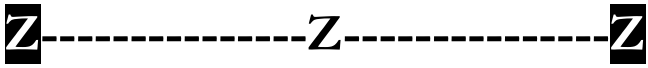
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "Z" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

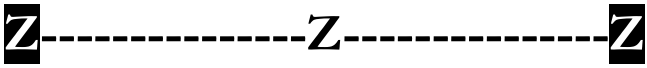
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "Z" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

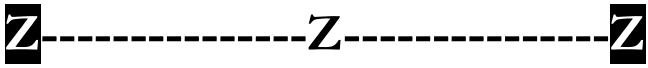
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "Z" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

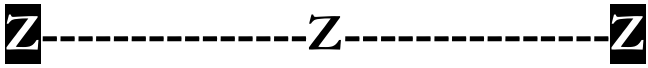
_____

Password:

_____

❑ Two-step verification on

Notes:



WEBSITES & PASSWORDS

Write your passwords for websites or entities beginning with the letter "Z" here:

Organization Name:

_____

Website:

_____

Email Used:

_____

Username (if different):

_____

Password:

_____

❑ Two-step verification on

Notes:

APPENDIX

SCAM RESOURCES

"Reality is easy. It's the deception that's the hard work."
Lauryn Hill (Singer-songwriter)

Want to learn more about scams? Scams are fascinating from a psychological perspective. Here are "scam resources" to learn more about scams on the Internet and how you can protect yourself.

If you register your book, you'll get a free PDF copy of the book which has easy, **clickable links** to all resources listed below. To do so:

1) Visit **http://jmlinks.com/pwregister**
2) Enter the password: **2017pw**

Snopes.com - http://www.snopes.com/

Snopes.com has made a name for itself as a website that debunks popular (but untrue) Internet myths. It's more about the latest meme going around Facebook, but an excellent window into what's not true but popular on social media.
Rating: 5 Stars | Category: resource

The Balance Top Internet Scams A-Z –
https://www.thebalance.com/top-internet-scams-a-z-list-2062169

Probably the best online list of all scams, listed from A-Z. Worth a read. Look for patterns as the patterns of scams repeat themselves, even though the content of scams changes over time.
Rating: 5 Stars | Category: article

Microsoft Safety & Security Center -
https://www.microsoft.com/en-us/safety/

Do you have a Windows laptop or computer? If so, be sure to visit Microsoft's informational center on safety and security for windows devices. If you haven't upgraded to Windows 10, it also has links to popular free security upgrades like Microsoft Security Essentials.
Rating: 4 Stars | Category: resource

FTC Online Security -
https://www.consumer.ftc.gov/topics/online-security

Online security information, including scams, hacks, spyware, etc., from the FTC.
Rating: 4 Stars | Category: resource

Scams and Frauds on USA.gov -
https://www.usa.gov/scams-and-frauds
The US government collects information on scams and frauds. This is a useful learning site about the problem.
Rating: 4 Stars | Category: resource

FTC Scam Alerts -
https://www.consumer.ftc.gov/scam-alerts
The Federal Trade Commission (FTC) issues specific alerts on the latest scams out there. This is a useful place to read about the latest scams and look for 'patterns,' so that you can see a scam coming.
Rating: 4 Stars | Category: resource

List of Internet Scams by Heimdal –
https://heimdalsecurity.com/blog/top-online-scams/
Heimdal Internet security, and specifically blogger Ioana Rijnetu, bring you this fun list of Internet scams. Read it and just be amazed at how clever scammers can be.
Rating: 4 Stars | Category: article

Top 10 Ways to Stay Safe On Public Wi-Fi Networks -
http://tinyurl.com/wifisafely
Lifehackers shares ten ways to stay safe on public WiFi. Beware of hackers who use 'free WiFi' to steal logins and passwords.
Rating: 3 Stars | Category: article

Two Factor Auth (2FA) - https://twofactorauth.org/

Who supports two factor authentication? Well, this mega site lists banks, cloud computing, email, education services, and more that support the two-step verification process. Great to look at if your provider does not offer 2FA and you want to switch.

Rating: 3 Stars | Category: resource

Best Antivirus Software and Apps 2017 – https://www.tomsguide.com/us/best-antivirus,review-2588.html

The venerable Tom's Guide reviews and curates a list of the best anti-virus programs for both iOS and Windows.

Rating: 3 Stars | Category: article

Microsoft Safety Scanner (Antimalware) – https://www.microsoft.com/en-us/wdsi/products/scanner

This free tool from Microsoft can scan your PC for infections of both viruses and malware. You have to manually download and run it each time, however. Good if you think you may be 'infected.'

Rating: 3 Stars | Category: tool

Scam Detector – http://www.scam-detector.com/

This is a blog that covers all sorts of scams, and also has an email alert you can subscribe to. The content is good, but there are a lot of annoying ads.

Rating: 3 Stars | Category: resource

Android Security Apps: The Top 5 –
https://www.digitaltrends.com/mobile/top-android-security-apps/

Android phones handle anti-virus and other forms of security differently than Apple, so if you have an Android phone you may want to consider an add-on app for security. Here's a review article.
Rating: 2 Stars | Category: article

Apple Security Updates –
https://support.apple.com/en-us/HT201222

Curious about what security updates are out there for Mac iOS or Apple products? Use this nifty update to see what's worth updating.
Rating: 2 Stars | Category: resource

FIDO U2F Security Key -
https://www.yubico.com/product/fido-u2f-security-key/

If two-factor verification isn't enough for you, you can go to the next level, which is FIDO U2F security. Here's a product from Yubico which is one of the more popular alternatives to two-factor verification.
Rating: 1 Stars | Category: product

A FAVOR

If you liked this book, please do me a huge favor. Go to Amazon.com, search for "The Password Book," and write a short, honest, review.

Thank you,

Jason McDonald
j.mcdonald@jm-seo.net | Tel. 800-298-4065

~ Other Books by Jason McDonald ~

SEO Fitness Workbook
Social Media Marketing Workbook
AdWords Workbook