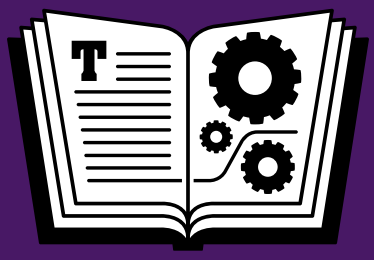

TAKE CONTROL OF

YOUR PASSWORDS

by JOE KISSELL

$15

2ND EDITION

Table of Contents

Read Me First

Welcome to *Take Control of Your Passwords, Second Edition,* version 2.0, published in March 2016 by TidBITS Publishing Inc. This book was written by Joe Kissell and edited by Kelly Turner.

Passwords are an irritating fact of modern life. It's tricky to create and remember good ones, but dangerous to use simple ones (or reuse a password in multiple places). This book helps you overcome these problems with a sensible, stress-free strategy for password security.

If you want to share this ebook with a friend, we ask that you do so as you would with a physical book: "lend" it for a quick look, but ask your friend to buy a copy for careful reading or reference. Also, you can Teach This Book.

Updates and More

You can access extras related to this ebook on the Web (use the link in Ebook Extras, near the end; it's available only to purchasers). On the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy any subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and Mobipocket. (Learn about reading on mobile devices on our Device Advice page.)
- Read the ebook's blog. You may find new tips or information, as well as a link to an author interview.

If you bought this ebook from the Take Control Web site, it has been added to your account, where you can download it in other formats and access any future updates. However, if you bought this ebook elsewhere, you can add it to your account manually; see Ebook Extras.

Basics

Be aware of the following:

- **Credentials:** I frequently use the term "credentials" as a compact way of saying "the combination of your username and password." In some cases, additional pieces of information, such as your ZIP code or the answers to security questions, may be considered part of your credentials—it's whatever a site or service needs to reliably identify you as the authorized user of a given account.
- **Authentication:** The act of proving your identity to a computer system—typically by entering your credentials and having them confirmed as matching the previously stored record—is called *authentication*. I use that term a number of times in this book, so I want to make sure you're familiar with it.

What's New in the Second Edition

Version 2.0 of this book is a major new edition, with updated information and advice that reflects the state of technology in early 2016 and adds extensive details about a variety of increasingly popular products and services. Some of the interesting changes are:

- In Usernames and Passwords: an Outdated Model, added a discussion of approaches involving Biometrics, Authenticator Devices (including EveryKey and Nymi Band), and Passwords on Demand that some people hope will eventually supplant today's way of using passwords as a primary means of authentication
- Updated and significantly improved the accuracy of All about Entropy, which explains the factors determining how likely (or unlikely) a password is to be guessed
- Greatly expanded the topic Multi-factor Authentication, which now covers One-time Passwords and apps that generate them (such as Google Authenticator and Authy), Physical Keys, and Application-specific Passwords, as well as the roles of Trusted Devices

- Added a sidebar explaining why simple passwords are always a bad idea, even for accounts that don't apparently protect any sensitive data; see Why Use Secure Passwords for Throwaway Accounts?
- Significantly expanded the chapter Pick a Password Manager:
  - In Features to Look For, added iOS browser support, Apple Watch support, one-time password support, U2F support, and pricing model, plus new sidebars Three Autofill/Autosubmit Models and Switching Password Managers
  - Updated and expanded the discussions of 1Password and LastPass, both of which have changed markedly since the previous edition of this book
  - Added descriptions of Blur, Master Password, Sticky Password, and True Key—along with a sidebar (Missing Managers) explaining why I don't cover KeePassX or oneSafe
- In Appendix A: Use Two-factor Authentication, added information about Apple's new two-factor authentication system and using two-step verification with Dropbox, Facebook, Microsoft, and Twitter accounts
- Added Appendix C: Calculate Password Strength to help interested readers determine the entropy of passwords they create and understand why such calculations frequently vary

Introduction

Think of a card, any card. Now, keep that card in mind and think of another. Repeat until you've picked twelve cards—but make sure your selection includes all four suits, at least one ace and one face card, and no two instances of the same card. Remember the whole set, because I'm going to ask you again tomorrow…

I'm joking, of course. But have you ever noticed that when magicians pull someone out of an audience to help with a trick, they never make such complicated requests? It's not reasonable to ask someone to create a meaningless string of numbers and letters, remember it indefinitely, and produce it on demand.

But Web sites, banks, and network administrators make exactly that request of us almost daily. Want to buy something online? Sure, but you need more than a credit card—you usually need a password too. Sync this data with the cloud, sign up for that free service, manage your utilities or PTA schedule online…no problem, but you must have a password for that. "Make sure it's between 10 and 14 characters, contains upper- and lowercase letters, at least one digit, at least one punctuation character, and doesn't have any repeated strings. Oh yeah, and don't even think about using a word that might be found in a dictionary or reusing a password you used anywhere else."

Are you kidding me? This is madness. Coming up with unique, random passwords all the time, remembering them, and producing them reliably is not the sort of task the human brain is cut out for.

Faced with this difficult and increasingly absurd task, people naturally tend to look for shortcuts their brains can handle. They pick easy passwords, like their kids' names or patterns of keys on the keyboard. Even if they go to the effort of creating something more complex, they use the same password everywhere, because then they have only one thing to remember instead of hundreds.

Speaking as a fellow human being, I don't blame anyone for taking the easy way out. You might try to come up with clever, random-looking passwords the first few times, but once your list of password-protected accounts grows into the dozens, and then the hundreds, it's not plausible to keep following the rules.

However, speaking as a technologist who has spent lots of time researching and thinking about security, I'm terrified for people who do this. I know how easy it is to guess, crack, or otherwise uncover someone's passwords, because I've done it myself. And people with far greater skills and resources than mine spend all day, every day doing the same thing—not for legitimate security research but to steal money and secrets, to cause mischief, or to show off.

Every couple of months I read about another high-profile case in which millions of passwords are leaked, hacked, or stolen. And then I look at that list of now-public passwords and shake my head when I see that thousands of folks thought `password` was a pretty good password! I understand why they did it—they were only trying to manage an unmanageable problem—but I feel sorry for them, as their problems didn't end with the site that was hacked. Because these people invariably use the same password on lots of sites, many of them had money and identities stolen, private email messages read, or hate mail sent in their name. It's a big, scary deal.

Back in 2006, I wrote *Take Control of Passwords in Mac OS X*. In that book, I attempted to explain all the ways passwords are used on a Mac and give advice about managing them. I offered the best guidance I could at the time, based on the available facts. But when I look back at that book now, I get an uneasy feeling because anyone who took my advice then might now be living with a false sense of security. The tools for guessing passwords and breaking encryption have taken massive leaps forward in recent years, with no signs of slowing down. What was safe then may be ridiculously insecure today.

On the bright side, the apps and techniques available to us good guys have improved too. While I can't solve all the world's password problems, with a combination of technology and common sense, I can probably help you solve about 98 percent of *your* password problems.

My goal in this book is to lay out a simple strategy that will keep you as secure as possible with a minimum of effort. Sometimes, I admit, there's a trade-off between security and convenience. You have to choose which is more upsetting: adding another lock to your door or risking a break-in because the neighborhood's gotten worse. But you might be surprised to discover that in many cases, you can significantly increase your security without extra effort. Remember how I said that generating and remembering random passwords is not something the human brain is good at? That's true, but I'll bet every human reading this book has a computer as well as a smartphone or tablet, and those devices are *fantastic* at generating and remembering passwords—if you use the right apps, in the right ways, at the right times. (And yes, I'll also talk about the situations in which your gadgets can't help you. Don't worry; those problems have solutions too.)

If all this talk of hacking and identity theft sounds scary, I'm sorry. I don't mean to frighten you. Much. But I do want you to have a clear understanding of the threats so you're motivated to adopt better password practices. It won't take long, it won't cost much, and it won't be difficult. Once you've done it, you can go back to not being scared, just like me. In fact, that's the point of my recommendations—I want you to be relaxed and confident, knowing that your passwords are solid and that you have an easy, reliable way to create and enter passwords whenever they're needed.

This book is no rehash of *Take Control of Passwords in Mac OS X,* although I've borrowed a few sections that are still useful. Instead, I'm looking at the problem of passwords in a broad, platform-agnostic way. Whether you use a Mac or PC, an iOS or Android device, something else entirely, or—more likely—a combination, you'll find guidance to help you take control of your passwords. By the end of this book, I hope you'll thoroughly understand the vulnerabilities and threats associated with passwords, ways to minimize your risks, and how to use passwords safely without losing your sanity. No one can give you an ironclad promise of perfect, unbreakable security, but with the advice in this book, I can get you pretty darn close.

Before we get started, check out the comic that our friends Nitrozac and Snaggy at the Joy of Tech made for us…it's the *Joe of Tech!*

Provided by the Joy of Tech. Published with permission; all rights reserved. View on the Web.

Passwords Quick Start

I recommend reading this book in linear order, because each chapter builds on what comes before it. In any case, don't skip Apply Joe's Password Strategy, because using just part of my strategy (such as a password manager) may leave important gaps in your security.

Get your bearings:

- Find out what's wrong with passwords and the ways most people use them; see Understand the Problems with Passwords.
- Discover what makes a good password and why that's not all you have to worry about; see Learn about Password Security.

Develop your password toolkit:

- Learn my three-point password strategy—and what to do in situations that don't fit into it; see Apply Joe's Password Strategy.
- Arm yourself with a good app for creating, remembering, and entering random passwords; see Pick a Password Manager.

Tie up loose ends and fix old problems:

- Make sure your passwords don't fall into the wrong hands while remaining available when needed; see Keep Your Passwords Secure.
- Clean up all those awful passwords you created before you saw the light; see Audit Your Passwords.

Handle special cases:

- Deal with systems that use a password plus another authentication method; see Appendix A: Use Two-factor Authentication.
- Get advice for improving password security for someone who's unwilling or unable to follow my regular strategy; see Appendix B: Help Your Uncle with His Passwords.
- Learn the math behind password entropy; see Appendix C: Calculate Password Strength
- Give a talk about password security; see Teach This Book.

Understand the Problems with Passwords

Because you're reading this ebook, you probably already have a problem with your passwords, such as how to come up with them or how to remember them. We'll get to those sorts of problems shortly.

First, I want to discuss some of the problems with passwords. What's wrong with simple, easy-to-remember passwords? Why do we need so many passwords, anyway? What are the common threats against passwords? And if this whole username/password system is so flawed, what can be done about it?

Simple for You, Simple for Them

The whole idea of a password is that it's private—something known only to you and to the entity with which you have an account (a bank, Web site, cloud service, etc.). If someone else learns your password, that person can access your data, and that's just the beginning.

Once access is granted, the interloper—I'll refer to this hypothetical person as a "hacker" even though that's not necessarily accurate—can change your password so you can't access your own account, impersonate you online, and even change your contact data to theirs. And, if you use the same password for other sites and services, the hacker can get access just as easily to your other accounts and wreak all kinds of havoc, up to and including "stealing" your identity.

Obviously, I'm talking about a worst-case scenario. Most password breaches result in less-serious problems—comparable to someone picking the lock to your house, but not actually taking anything of value. Even so, I think most of us would prefer to avoid that icky feeling that a stranger has been poking around in our personal space, and hassles like changing the locks.

So, your goal when selecting any new password should be to reduce, as far as possible, the likelihood that someone else can discover what it is. You essentially want locks that are strong enough to ward off those unlikely worst-case scenarios, thereby protecting yourself against less-serious risks in the process.

You might be surprised at the ways in which someone could discover your password; I talk about many of these in the remainder of this chapter. But let me start with what I hope is obvious by now: The passwords that are the simplest for you to use are also the simplest for a hacker to discover. Those are the passwords to avoid at all costs.

When someone says that you should never pick a password that's a word in a dictionary, the name of a relative or pet, the date of your anniversary, or another easy-to-remember string, they're pointing out the insecurity of highly guessable passwords. If I wanted to break into an account belonging to someone I knew (a coworker, say), I'd certainly try as many terms like these as I could think of, hoping that what's easy for them to remember is also easy for me to guess.

Of course, you're not merely up against flesh-and-blood guessers. Computers can do an even better and faster job of guessing passwords. You need passwords that are unguessable by human *or* machine. Such passwords are often, unfortunately, hard to remember and type too, which is why they aren't used more often. As this book progresses, I'll explain my suggested strategy for dealing with this problem. For now, remember: a simple password is nearly as bad as no password at all.

The One and the Many

One of the recurring themes in this book—I want to repeat it until you believe—is that reusing passwords is a terrible, terrible idea. Just. Don't. Ever. Do. It.

The basic argument is simple. If your password for one site or service is compromised (stolen, guessed, hacked) and you also used that password somewhere else, then whoever has your password might try it elsewhere and be able to do that much more damage. If you use the

Learn about Password Security

We begin with a brief lesson on password security. I want to keep it short, so I won't go into tremendous detail about encryption algorithms and cryptographic mathematics, and I'm going to do a bit of hand-waving when we get to the geekier concepts (and refer you to Appendix C: Calculate Password Strength if you're genuinely interested in the details). But I think it's important to have a basic grasp of the principles of password usage so you know what you're up against, and why simple-sounding solutions are often extremely unwise.

And, even if you were well-versed in password security basics a few years ago, you should be sure to read about Multi-factor Authentication, which has become increasingly important.

What Makes a Good Password?

To put it simply, a good password is one that you won't forget but that no one else (human or computer) can guess. Behind that straightforward description are two knotty, interconnected problems:

- **Guessability:** Most people have an unrealistic idea of what "guessable" means. You might imagine that no one could connect the password `ninjaboy` with you, but the computer I'm using right now could figure that out before I finish typing this sentence. As I explained in The Major Threats, even if a human who knew everything about you would never guess your passwords, sophisticated cracking algorithms may be able to figure them out unless you take steps to thwart them (discussed at length just ahead). To avoid that risk, your passwords should be far more complex than you might think.
- **Memorability:** If you can't remember a password, it's useless. As a password's complexity (and thus its strength) increases, its

memorability tends to decrease. Let's face it, `iYb48nzJ#;sEoR` may be vastly stronger than `ninjaboy`, but it doesn't exactly trip off the fingertips.

Creating memorable but unguessable passwords—and not just one or two, but potentially hundreds—may sound like an intractable problem. But hang tight; we'll get to a strategy shortly.

All about Entropy

Let's quantify this vague notion of guessability. In ordinary speech, the word *entropy* means disorder, randomness, or unpredictability. Cryptographers use the term *entropy* to refer to a mathematical approximation of a password's complexity based on the method used to create it. A password with higher entropy is harder for a person (and, more importantly, a machine) to guess. So, for passwords, higher entropy is a very good thing.

Note: Cryptographers measure password entropy in bits; a larger number of bits means higher entropy. If you're interested in learning how entropy is calculated—and why it's possible to get numerous conflicting entropy values for a single password—consult Appendix C: Calculate Password Strength. The entropy values I mention in this chapter are derived from the zxcvbn password strength calculator.

But how does higher entropy (or complexity) help make passwords harder to guess?

You already know that cracking algorithms can check billions of passwords per second in an attempt to figure out what yours is. But even brute-force searches don't go in alphanumeric order. (If they did, then `zzzzzzzzzz` would be much stronger than `aaaaaaaaaa`, but it isn't.) Instead, cracking software identifies common patterns of characters that few humans would notice. It uses this information to test more likely passwords before less likely ones, reducing the average time it takes to produce a match. Because higher-entropy passwords are less likely to be used than lower-entropy passwords, a brute-force search tends to take longer to find them.

Apply Joe's Password Strategy

In my earlier book on passwords, I distinguished between "identity" and "security" passwords and outlined elaborate techniques to determine how strong a given password needed to be and create different kinds of passwords depending on context. I now advocate a single approach that's simpler and safer, and that covers the vast majority of cases.

My strategy—and yes, this is what I do myself—has three main points:

- Figure Out Which Passwords You Must Memorize—if you do it right, the number of these passwords will likely be in the low single digits.
- Create Strong but Memorable Passwords for just those few. The passwords should be strong enough to defeat all but the most determined hacker yet easy to recall and type.
- Use a Password Manager for Everything Else. Your remaining passwords will be long, complex, and random. You'll have no idea what they are, but you won't have to, because you'll almost always be able to enter them with an automated tool.

You'll also have to deal with irritating security questions from time to time, as well as other odd exceptions and surprises. I cover all that in this chapter as well.

Figure Out Which Passwords You Must Memorize

First, the bad news: you *must* memorize at least a few passwords, and those few have to be both long and strong.

But the good news is that for most people, with careful planning, the number of passwords that must be stored in the brain is very small. For me, the number is three. Depending on your situation, you might have only one or two, or you might have nine or ten—but if your number gets much beyond a dozen, *you're doing it wrong*. Whatever the number is, I'll refer to this short list as your Very Important Passwords, or VIPs.

Which passwords belong on the must-memorize VIP list? Only those passwords that you need often and can't easily enter using a password manager app (which I discuss two steps ahead). For example, here are my three:

- **The master password for my password manager:** A password manager lets you use a single *master password* to unlock all your other stored passwords. I use that key constantly and I can't very well keep it in my password manager, so I have it memorized.
- **My computer's login password:** Everything on my computer is encrypted, so I can't turn it on or even wake it up from sleep (much less run an app such as a password manager) without entering the login password for my main user account.
- **My Apple ID password:** My Apple ID can get me into all sorts of services—iCloud on my Mac, PC, iOS devices, and Apple TV; my iTunes Store and Mac App Store accounts; Game Center; Apple developer accounts; and so on. I enter it so often that it was well worth memorizing. (I have more than one Apple ID, but I use one much more than the others.) See Devices without Full Keyboards, later in this chapter, for additional advice on passwords—such as an Apple ID password—that must be entered frequently on a tiny virtual keyboard.

Pick a Password Manager

A quick Web search will turn up dozens, perhaps hundreds, of password managers. Because I talk so much about password managers in this book, I want to offer some advice about how to choose one. In this chapter, I introduce you to the capabilities you may find important and then offer a brief overview of more than a dozen representative password managers.

If you're already using a password manager and you're happy with it, you can probably skip this chapter (or skim it, to see if anything interesting pops out). But if you're using a password manager that you aren't entirely satisfied with, use this chapter as a way to find something that may be a better fit. Switching password managers can be a hassle (check out the sidebar just ahead for advice) but it's worth the effort if your new manager makes it easier for you to consistently create—and easily access—strong passwords on all your devices.

Remember, this chapter is only a sampling of your options (both good and bad)—my point is to acquaint you with the variety of choices out there.

Tip: If reading about password manager features makes you drowsy and you'd rather pick one and get on with it, allow me to suggest 1Password. It's what I use, and I think you'll like it. To read about more of my top picks, see Joe's Recommendations at the end of this chapter.

Switching Password Managers

Say you have a bunch of data in a password manager, but you start using a new platform that your current manager doesn't support. Or you find out that your current manager has a security problem. Or you're tempted by fancy new features in another manager. In all these cases, the question is: how easily can you transfer your stuff from the old password manager to the new one?

There's no easy or universal answer. Many password managers (including 1Password, Blur, Dashlane, LastPass, and RoboForm) offer import and/or export capabilities, but even then, there's no guarantee that your new password manager will be able to import the particular format that your old one uses (or exports to). Moreover, even if you can find compatible formats, you might still lose data—for example, if you store custom fields or file attachments in 1Password, those pieces of data will go missing when imported into a password manager without comparable features.

I suggest that before you spend any money, you confirm that the new password manager you're considering can import data from your old one (or from a format the old one can export). You may need to search the support site for each app to see its capabilities—or, better yet, download a free trial version if it's available and try it.

A particular pain point is trying to import data from Apple's Keychain format. It can be done—for example, I just tried it with Dashlane—but there is a catch. Because of Keychain's security design, you must individually approve every single login item as you import it (which sometimes means clicking Allow, and other times may mean entering your password). If you have hundreds of items in Keychain, that can be an enormously time-consuming and tedious process.

Features to Look For

Every password manager starts with the same premise: put all your passwords (and, often, other private information) inside this secure storage place, and unlock it as needed with a single master password. Superficially, most password managers even look similar—they're essentially encrypted databases with predefined fields for username, password, URL, and a few other items.

Keep Your Passwords Secure

If you stored your fortune in a safe deposit box, you wouldn't keep the key hanging on a hook outside your house. The same should be true of your passwords: if you keep them written on a whiteboard by your desk, they're not safe. But even if you don't write them down, there are many ways someone might discover your passwords.

In this chapter, I look at some of the ways your passwords might fall into the wrong hands, and give you tips on keeping them safe. I also discuss backing up your passwords and devising a plan to ensure that your passwords are available in case of emergency.

Avoid the "Weakest Link" Problem

Suppose you have a fantastic password that would take the world's best supercomputers centuries to crack. You've stored the password in your password manager, but it uses a weaker master password that's easier to remember. And because you still worry that you might forget it, you store your master password in an unencrypted text file on your hard disk. You can see where I'm going with this: you've nullified the security of that great password, because someone can get to it by way of the text file that unlocks your password manager, without any guessing or cracking. Even without that file, your super-strong password is reduced to the strength of your master password.

Just as a chain is only as strong as its weakest link, a password is only as strong as the weakest means by which someone can (directly or indirectly) get to it. That concept is straightforward enough, but consider some of the ramifications:

- If you write down a password, the password (and whatever it protects) is only as safe as the written copy. As I explain shortly,

that doesn't mean you should *never* write down your passwords, but if you do, you'd better take extraordinary care to protect those written copies.

- If you click a "forgot my password" link and a site emails you your password or a link to reset it, that password is only as safe as the password used to access your email account (and possibly much less secure; see Use Wireless Networks Safely, just ahead).
- If you type the password into an encrypted file on your computer (or, better yet, encrypt the entire disk), the password is only as safe as the password protecting the encrypted data—and that depends further on the encryption method used, since some methods are easier to crack than others, regardless of the password strength.

Taking all these situations into account, my advice is:

- If you write down any of your passwords, keep them in a very safe place (such as on your person). For increased security, modify them in some way (such as reversing the order of the characters)—but don't forget how you modified them! For ideas about writing down passwords that someone else may need to access, read Prepare an Emergency Password Plan, later in this chapter.
- When typing your passwords, make sure no one watches over your shoulder to see your screen or the keys you press.
- Take appropriate precautions when using wireless networks (see Use Wireless Networks Safely).
- Make all your passwords equally strong (that is, make sure they all have high entropy).
- Store your passwords in a password manager (protected with a strong master password, of course). Lock your password manager when not in use, and back up your data (see Back Up Your Passwords, shortly ahead).

Audit Your Passwords

Perhaps, upon reading this book, you realize that some or all of your passwords are terrible, and you're committed to choosing and using good passwords from now on. Fantastic—but what about all those existing passwords, which may number in the hundreds? How do you find the bad ones and change them? You need to audit your passwords to determine how bad the problem is and where fixes are needed.

There's no quick or easy way to change many different passwords at once, so brace yourself: this is going to be a bit of a slog. But you can make the process manageable by following the steps in this chapter.

Understand the Overall Process

Changing a single password might take you a minute or two, but changing your password for every Web site where you entered `abc123` over the past 10 years is a pretty big undertaking. If you have tons of so-so passwords, you might feel like you should take a week off work, prepare a few gallons of strong coffee, and plow through the enormous process of changing them all at once. And then, realizing how implausible that is, give up and do nothing at all!

I'm a "something is better than nothing" kind of guy, and I'd rather you take small steps toward having somewhat better security now than do nothing in the hope of eventually getting around to having fantastic security. So, first of all, take a few deep breaths. This big task can be broken down into manageable steps, and those steps can be prioritized so that you deal with the most serious problems first, until eventually you have the whole mess cleaned up. Here's what I suggest:

- First, Look for Weak Passwords in order to determine which ones are most likely to be easily guessable or hackable. Make a note of those—but if you've been using poor password practices for a long time, your note might just say "all of them"!

- Working from the list of passwords you consider too weak, Triage Your Passwords—determine which ones pose the most serious security risk right now, which ones are important but not urgent, and which pose a small enough risk that you can put them off until later.
- Next, starting with the most critical one, Update a Password. While you're at it, you'll want to Check Your Security Questions and Answers and Check the Password Reset Procedure. You'll also have to Update Apps and Devices where the original password might have been stored.
- Repeat this process as needed—perhaps changing three or four passwords a day until your entire collection of passwords has been updated.

Look for Weak Passwords

Your first auditing step is to figure out which of your passwords are too weak to provide reasonable security. If you've read What Makes a Good Password? you should have a good idea of what you're looking for—anything that doesn't meet those criteria! In particular, you want to find any passwords that are:

- **Too short:** Anything under 10 characters would seriously concern me, although I generally recommend 12 characters as a safe length for random passwords—and longer is even better.
- **Too simple:** Words you find in a dictionary, keyboard patterns, simple modifications (replacing letters with numbers), and so on make a password easy for a computer to guess, even if it's not short.
- **Repeated:** If there are passwords you've used in more than one place, you should change them so that every one is unique.

The process of finding passwords like these depends on your current approach to storing them. If they're on a piece of paper or in a text file, for example, a simple glance should tell you. If they're in a password manager that displays a strength meter next to each password, that

Appendix A: Use Two-factor Authentication

Earlier, in Multi-factor Authentication and Manage Email Options, I said that some companies enable (or require) you to use a combination of factors—things you know, things you have, and things you are—to prove your identity. In the most common implementation, one factor is your password (a thing you know) and the second is an object (a thing you have). The result is two-factor authentication (2FA).

A variation on this process requires your regular password plus a time-limited, one-time password (OTP); that password is generated by an app or sent to you via SMS or email. Because the OTP is still, strictly speaking, something you know—and because a single device could unlock your password *and* display your OTP—systems that rely on this process aren't truly 2FA; rather, they're two-step verification (2SV).

With 2SV enabled, the chance of your account being hacked falls dramatically. Even if someone learns your username and password, they need your phone too. (Of course, if someone steals your phone and knows or can figure out your username, the only barrier left is your password, so it still has to be a good one!)

In this appendix, I want to introduce you to several common 2FA/2SV systems you're likely to run across. I won't give detailed, step-by-step instructions for setting up each one, but I'll describe the process generally, direct you to where you can get specific instructions, and say a few words about how to use each system after you set it up.

Two-step Verification Basics

Before I talk about specific services, I want to give you an overview of the general process most of them employ, with minor variations.

To set up 2SV, you'll generally follow steps like these:

1. Log in to your account in the usual way, go to a Settings or Security page on the Web, and enable two-step verification.
2. Make sure you can obtain an OTP when necessary:
    - For services that use SMS, enter your phone number. They'll then typically verify your phone number by sending you a code via SMS you have to enter on the site. Only after you've done this will OTP-by-SMS be available.
    - For services that use email to send your OTP, enter your email address. Then click the link in the email message you receive shortly to confirm that you do indeed own that email account.
    - For services that use an authenticator app such as Google Authenticator, Authy, or 1Password, use your authenticator app to scan the QR code shown on screen (or, in some cases, type or paste in a secret key) to *seed* the authenticator app with a value that enables it to generate the correct OTP every 30 seconds. Usually, after you do this, you'll have to confirm that the authenticator app works by entering an OTP on the Settings page.

Tip: Before you close that browser window or tab, I recommend taking a screenshot of your QR code. Some services let you display it again (for example, if you want to set up a second authenticator app to generate OTPs for you), whereas others require you to turn 2SV off and back on again to see a QR code—a hassle you can avoid with this extra step.

3. Record any backup or login codes the service presents. Some services offer a list of special one-time-use codes you can keep in a safe place (for example, printed out and stored in your wallet)

Appendix B: Help Your Uncle with His Passwords

As much as it pains me to admit this, there are people who will listen patiently to a sober description of the problems with passwords and my simple strategy to overcome them, and say, "Yeah, no, sorry. I'm Just Not Going to Do That."

You, of course, aren't one of those people. You eat your vegetables, work out, drive safely, and have amazing passwords. But you have a friend—or perhaps a much older, much younger, or less technologically sophisticated family member—who's too busy, too set in his or her ways, or for some other reason unwilling or unable to follow my strategy. You want them to be safe, but no matter how much sense it might make, you know they're not going to go for the plan in this book. What to do?

In this appendix, I offer a few suggestions for helping such a person, organized by potential areas of compromise. You may not be able to break every bad habit, but you can perhaps meet your "uncle" halfway and make him that much more secure.

Password Manager Compromises

Your uncle may refuse to use a password manager, considering it too inconvenient or too difficult. Or, he may have so few passwords that a password manager would be overkill. Either way, if a password manager is out of the question, you can make a couple of suggestions:

- For a modest number of passwords, a piece of paper can be a completely adequate password manager. And, if your uncle does all his computing from his home in the country, the likelihood of someone finding and stealing that paper is small. But tell your uncle that keeping it out of sight is still best.

- Even without a password manager, a password *generator* will help your uncle come up with better passwords. He can find lots of free Web-based password generators online—for example:
  - Strong Password Generator
  - Random Password Generator
  - Password Generator

Password Reuse Compromises

I've explained the dangers of using the same password in multiple places and repeated my warning numerous times. But some people—especially if they can't or won't use a password manager—can't accept the notion of having lots of different passwords. "It's too much to remember!" If you encounter such a person, try these compromises:

- If you're going to reuse a password, at least make it a great password (see All about Entropy).
- Ask if your uncle might be willing to remember two (or even three or four) great passwords, and alternate among them for various sites. That'll require either reminder notes or the extra step of guessing on occasion, but at least it'll contain the risk a bit.
- Alternatively, perhaps your uncle would be willing to memorize a single great password like `vGq9&nn3c3#b` and vary a portion of it for each site. For example, maybe the second character, `G`, stands for "Google" but when your uncle logs in to Amazon.com the password becomes `vAq9&nn3c3#b` and at PayPal he uses `vPq9&nn3c3#b`.

> **Note:** If you do a pattern-based substitution like this—and remember, this is only for your uncle, not for you!—don't be blatant (as in `Goog&nn3c3#b` and `Amaz&nn3c3#b`), because if anyone learned one of those passwords it would be obvious what all the rest were!

- Suggest that your uncle set up an extra, non-public email address to use as his standard username (as discussed in Manage Email

Appendix C: Calculate Password Strength

Lots of Web sites and password generators have little meters that claim to tell you how strong a password is—they want you to keep adding characters until the bar is long enough or turns green or whatever. The problem is, each meter uses its own method to estimate password strength. The results vary wildly, and a tool may give you a false sense of security by suggesting that your password is stronger than it really is. (For more on this problem, read Does your password pass muster? Password strength meters not all created equal at ScienceDaily.)

Although not perfect, the best online password meter I've found (and one that ScienceDaily likes too) is an open-source tool from Dropbox called zxcvbn. Not only will it tell you a password's strength and the estimated time to crack it, it will also point out specific areas of weakness (such as dictionary words and patterns in the password). And don't worry, it does all this safely within your browser—it doesn't transmit your passwords over the Internet.

We'll come Back to zxcvbn in a moment. First, we need to cover a little bit of math. Honestly, it's *very* little, but I want to explain briefly how one goes about calculating password strength mathematically—and in particular, how to arrive at this mysterious concept of *entropy* (a password's resistance to being guessed), measured in *bits*. It's a calculation you can do easily, all by yourself, with a calculator or a Web browser—and it lets you prove to yourself how strong any given password is. (It's also subject to a lot of qualifications and caveats, as we'll soon see, but first things first.)

The Entropy Formula

If you're mathematically inclined, you may be able to make sense of the formula for entropy without an extensive explanation. Here it is:

$$\log_2(\text{possible characters}^{\text{length}})$$

If that doesn't make sense to you, don't worry; it didn't make sense to me either before I started writing this appendix! But I think I can unpack it in a way that anyone with basic knowledge of algebra can understand. So if that looks like so much gibberish to you, read on!

If cryptographers and mathematicians were a bit more inclined to think like the rest of us, they'd tell us how hard it is to guess any given password using an ordinary number—a number that represents the total *search space* for any given password, or the maximum number of guesses that could be required to match it, if you had to try every possible combination of characters. This number would probably be pretty big, but at least it would be just that—a straightforward number.

Note: I specify "maximum number of guesses" because if you're running through every possible combination of characters, it's highly unlikely that the particular password you're searching for will be the very last one you check. On average, you'll find it about halfway through your search.

For example, if you have a password made up of all lowercase letters, and it has 6 characters, then the total number of possibilities is 26 × 26 × 26 × 26 × 26 × 26, or 26^6, or 308,915,776. Call it 300 million and change. That's the maximum number of guesses it could take to find a password meeting those criteria.

But, since mathematicians make things "simpler" by making them harder, they don't just toss out a number like 300 million. They perform a calculation to reduce very big numbers like 308,915,776 to smaller numbers that are—even I, as a layman, must admit—easier to work with, especially when the number of possible passwords starts getting into the billions, trillions, and beyond.

Teach This Book

This book helps you develop a simple and secure method for dealing with your own passwords. But what if you need to help other people solve password problems? If you'd like to base a presentation, class, or other teaching opportunity on this book, we'd like to offer assistance:

Share a Cheat Sheet

Lots of people won't read a book like this—not just your "uncle" but even your coworkers who desperately need better password security. So we've developed a free, one-page PDF handout to cover the main points and key tips in this book. You can give it to anyone who needs quick advice on working with passwords. Download it here, and you can print copies for colleagues, send it to them via email, or pop it in a shared Dropbox folder.

Order Classroom Copies

You can buy discounted copies of this book for classroom use. If you want to teach a group about passwords, classroom copies are an inexpensive way to ensure that each participant has a copy of the book.

Download Training Materials

Not sure what to say in a course about passwords? You can download a free, simplified presentation (in an iPhone- and iPad-friendly PDF format, with the option to purchase an editable PowerPoint or Keynote file) that covers the main points in this book (contact us for purchasing details). Be sure to download the cheat sheet for your students too.

Hire the Author

For the ultimate experience, you can hire Joe Kissell to speak to your group about passwords in person (or, if you prefer, by video). He's an entertaining and engaging speaker and is happy to work with groups of any size. Besides teaching the material in this book, he can customize a presentation to meet your group's needs, answer participants' questions, and work with you to develop effective ways of dealing with passwords. For more information and a price quote, contact Joe.

About This Book

Thank you for purchasing this Take Control book. We hope you find it both useful and enjoyable to read. We welcome your comments.

Ebook Extras

You can access extras related to this ebook on the Web. Once you're on the ebook's Take Control Extras page, you can:

- Download any available new version of the ebook for free, or buy a subsequent edition at a discount.
- Download various formats, including PDF, EPUB, and Mobipocket. (Learn about reading on mobile devices on our Device Advice page.)
- Read the ebook's blog. You may find new tips or information, as well as a link to an author interview.
- Find out if we have any update plans for the ebook.

If you bought this ebook from the Take Control Web site, it has been automatically added to your account, where you can download it in other formats and access any future updates. However, if you bought this ebook elsewhere, you can add it to your account manually:

- If you already have a Take Control account, log in to your account, and then click the "access extras..." link above.
- If you don't have a Take Control account, first make one by following the directions that appear when you click the "access extras..." link above. Then, once you are logged in to your new account, add your ebook by clicking the "access extras..." link a second time.

Note: If you try the directions above and find that your device is incompatible with the Take Control Web site, contact us.

About the Author

Joe Kissell is the author of numerous books about technology, including *Take Control of Your Online Privacy* and *Take Control of Dropbox*. He is a contributing editor to TidBITS, and a senior contributor to Macworld. He has also appeared on the MacTech 25 list (the 25 people voted most influential in the Mac community) since 2007.

When not writing or speaking, Joe likes to travel, walk, cook, eat, and practice t'ai chi. He lives in San Diego with his wife, Morgen Jahnke; their sons, Soren and Devin; and their cat, Zora. To contact Joe about this book, send him email and *please* include `Take Control of Your Passwords` in the subject.

Shameless Plug

On my site Joe On Tech, I write about how people can improve their relationship with technology. I'd be delighted if you stopped by for a visit! You can also sign up for joeMail, my free, low-volume, no-spam mailing list, or follow me on Twitter (@joekissell). To learn more about me personally, visit JoeKissell.com.

Acknowledgments

Kelly Turner did an amazing editing job. I appreciated her enthusiasm, attention to detail, and thoughtful comments. I'm also grateful to all the beta readers who provided helpful feedback and perspective. In particular, thanks to Rich Mogull, Will Porter, Oliver Habicht, Adam Engst, Tonya Engst, and Lauri Reinhardt.

About the Publisher

TidBITS Publishing Inc., publisher of the Take Control ebook series, was incorporated in 2007 by co-founders Adam and Tonya Engst. Adam and Tonya have been creating Apple-related content since they started the online newsletter TidBITS in 1990. In TidBITS, you can find the latest Apple news, plus read reviews, opinions, and more.

Credits

- Publisher: Adam Engst
- Editor in Chief: Tonya Engst
- Editor: Kelly Turner
- Production Assistant: Lauri Reinhardt
- Take Control logo: Geoff Allen of FUN is OK
- Cover design: Sam Schick of Neversink
- Comic: Provided by the Joy of Tech. Published with permission; all rights reserved.

More Take Control Books

This is but one of many Take Control titles! Most of our ebooks focus on the Mac, but we also publish titles that cover iOS, along with general technology topics. You can buy Take Control ebooks from the Take Control online catalog as well as from venues such as Amazon and the iBooks Store. Our ebooks are available in three popular formats: PDF, EPUB, and the Kindle's Mobipocket. All are DRM-free.

Copyright and Fine Print

Take Control of Your Passwords, Second Edition
ISBN: 978-1-61542-469-6

TidBITS Publishing Inc. 50 Hickory Road, Ithaca, NY 14850 USA

Why Take Control? We designed Take Control electronic books to help readers regain a measure of control in an oftentimes out-of-control universe. With Take Control, we also work to streamline the publication process so that information about quickly changing technical topics can be published while it's still relevant and accurate.

Our books are DRM-free: This ebook doesn't use digital rights management in any way because DRM makes life harder for everyone. So we ask a favor of our readers. If you want to share your copy of this ebook with a friend, please do so as you would a physical book, meaning that if your friend uses it regularly, he or she should buy a copy. Your support makes it possible for future Take Control ebooks to hit the Internet long before you'd find the same information in a printed book. Plus, if you buy the ebook, you're entitled to any free updates that become available.

Remember the trees! You have our permission to make a single print copy of this ebook for personal use, if you must. Please reference this page if a print service refuses to print the ebook for copyright reasons.

Caveat lector: Although the author and TidBITS Publishing Inc. have made a reasonable effort to ensure the accuracy of the information herein, they assume no responsibility for errors or omissions. The information in this book is distributed "As Is," without warranty of any kind. Neither TidBITS Publishing Inc. nor the author shall be liable to any person or entity for any special, indirect, incidental, or consequential damages, including without limitation lost revenues or lost profits, that may result (or that are alleged to result) from the use of these materials. In other words, use this information at your own risk.

It's just a name: Many of the designations in this ebook used to distinguish products and services are claimed as trademarks or service marks. Any trademarks, service marks, product names, or named features that appear in this title are assumed to be the property of their respective owners. All product names and services are used in an editorial fashion only, with no intention of infringement. No such use, or the use of any trade name, is meant to convey endorsement or other affiliation with this title.

We aren't Apple: This title is an independent publication and has not been authorized, sponsored, or otherwise approved by Apple Inc. Because of the nature of this title, it uses terms that are registered trademarks or service marks of Apple Inc. If you're into that sort of thing, you can view a complete list of Apple Inc.'s registered trademarks and service marks.