

THE ULTIMATE GUIDE TO CREATING, MANAGING AND SECURING YOUR PASSWORDS



BY KHAMOSH PATHAK

The Ultimate Guide to Creating, Managing and Securing Your Passwords

Copyright © 2014 Guiding Tech

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

This book is not affiliated with any firm or company mentioned in the book, and all trademarks are the property of their respective owners.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. The author of this book or Guiding Tech or the resellers or distributors of this book will not be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Contents

Introduction.....	3
How Hackers Get Hold of Your Password (And How to Stop Them).....	6
How to Create a Strong Password – The Basics.....	20
Why And Where You Can Enable 2-Factor Authentication.....	27
The Best Password Management Apps And Why You Should Use Them.....	36
How To Securely Save Passwords Offline And Share Them With Family.....	54
Conclusion – Practical Solutions to Today’s Password Management Problems...	62

Introduction

It's 2014 and I don't need to tell you just how dependent we are on the internet. Everything from communication to shopping to file storage, and work for people like me, takes place online.

All of this translates into important data. Data you don't want to fall into the wrong hands. While we might have transitioned from MySpace to Facebook, Microsoft Word to Google Docs and Windows Explorer to Dropbox, our passwords are still stuck in the past.

Ghosts Of The Passwords Past

[When you look at recent surveys and the most common passwords](#) ("123456" and "password" still claim the top spots) you realize just how ill equipped we are. For all the online privacy and tracking debates, we're missing the most fundamental piece of information. The one that can give it all away. And the way passwords are managed, the hackers don't need to be using sophisticated passwords hacking apps. Just a bit of guesswork will do.



Did you know

8 in 10 adults in US interact with computers somewhere during the day. And 43% [test subjects](#) said giving up internet would be “very hard”.

What You’ll Find in this Ultimate Guide

Hello, reader. In the next few pages I’m going to be the guinea pig and the white coat wearing doctor rolled into one. I’ve spend weeks scorching the corners of the internet, looking for solutions so you don’t have to. In here you’ll find advice from security experts that have been in this field longer than I’ve been on planet Earth.

You’ll also find links to original stories and citations wherever applicable. As this is the “Ultimate” guide, you’ll find more than just advice. You’ll find actionable tips, complete with links and step-by-step guidance.

You’ll also find practical solutions for your everyday security needs. Ones that have been tested by me personally. In the end, once we’ve explored all the options, I’ll talk about solutions that are the perfect balance between security and convenience. I’ll also tell you my experience with using the described methods for weeks. In the end, I’ll drop some no BS truth about internet security.

Intrigued? Jump to the next section and start reading! If that seems too much, skip to the last section for a TL;DR.

Oh, and this mammoth guide is also available as an ebook for you to read offline whenever you want, on whichever device you prefer to, so do check it out.

I’ll see you on the other side.

– Khamosh Pathak, Staff Writer and Content Crafter, [Guiding Tech](#)

How Hackers Get Hold of Your Password (And How to Stop Them)



Before we jump on the strong password crusade, first let's learn about the techniques hackers use to steal or crack passwords.

Phishing

Hackers send emails that **look like** they're from reputable or known websites (like banks you have accounts with), but they're not. The email usually says there's some problem with your account and you need to click a link to change the password.



Many users fall for this trap but there are easy ways to spot phishing mails from the legit ones (because sometimes there really **is** a problem with your account, mostly because of website hacks and you do need to change your password instantly).

- The email will have a similar but not the same address as the real company. For example, it will say *customersupport@amazzon.com* instead of *customersupport@amazon.com*. You should check the email id carefully.
- The link too does not direct to the bank's website, instead it will direct to a website that has a name that's very similar to the name of the legit site.

But if you're concerned about the whole affair and think you need to change the password even after determining it was a phish attempt, go to the site directly and change the password from there (go to the [incognito tab](#) if you want to be extra careful). Do not click on the link in the email.

Tip

If you use Google Chrome as your browser, it'll be worth your time to see [these security extensions](#) for a web browsing experience that's more secure.

Brute Force Attacks

Brute force attacks use automated software to guess passwords. These softwares start small, with "a", then "aa", "ab" etc and eventually get to words and random strings of text. The theory is that given the time, this method will check every possible combination of letters, numbers and special characters in the English language.

But in recent times hackers have gotten smarter and so has hacking software. In late 2009, [32 million plain text passwords from RockYou website were leaked](#) using a backdoor SQL injection attack. Out of which only 14 million passwords were unique. This database gave hackers immense insight into what an average password looks like. And that was just the start. Many websites have been hacked since then and user passwords revealed in either encrypted (which are also crackable) or plain text format.

In the last 5 years, hacking software has become incredibly sophisticated. And we're not making it harder for them. Most of the passwords in the RockYou database were 8 characters or shorter. Using sophisticated hacking software, an 8 character password can be cracked in a matter of days. While simply increasing the length to 14+ characters increases the average time to years.

How Does All This Information Help Hackers?

Instead of starting from “a”, “ab”, hacking softwares now check a password against the huge database of passwords they’ve amassed over time. And they’re smart enough to add variations to dictionary words (for example, “D3tect1ve” for the word “detective”) and to mix and match dictionary words with the available password database.

Cracking Hashed Passwords

A website being hacked and the database of millions of usernames, email and passwords dumped in internet forums does not pose an immediate threat to your security.

Passwords saved on websites are often hashed and not encrypted. The fundamental difference between the two is that while encryption is reversible, hashing is not. Encryption is based on a key. Anyone with the key can decrypt the password quite easily.

Major websites that care about user security hash passwords using a one-way mathematical function that makes it **impossible** to convert them back to letters, numbers and symbols.

In plain text, the word “security” and “security1” has 8 characters in common. For a software, cracking that 1 extra character is not that big of a leap. When both these passwords are converted to hashes, the difference between the two values is immense. This makes the hacking process that much harder.

So how do hackers crack hashed passwords? It comes down to the particular encryption standard a website uses. There are more than a dozen standards, each with varying levels of security and protocol.

Millions of passwords, plain text and hashed that have been stolen from websites for the past couple of years serve as a big help for hackers. Because they now know the hash value for millions of possible password combinations.

Converting a hashed value directly to plain text is impossible.

But the hackers have a repository of plain text password with matching hash values for millions of passwords.

The hackers use brute force attacks to quickly run the hashed database against the one they've amassed during the years. Once the hash value from the hacked website corresponds to their own database, the one with matching plain text passwords, the hackers have cracked the password.

What Does This Mean To You? And How Can You Be Safe?

Now that hackers have a database of millions of users' password practices, you don't just need a password to be "unique" in your own perspective, it should be "unique" to the passwords the hackers already have in their database.



It's also important to note that brute force attacks are not possible with the normal login pages you visit on any given website, as the websites have security measures to stop input after a couple of tries.

Brute force attacks are used to crack encrypted (or hashed) passwords that hackers gain from backdoor exploits or website hacks.

Being safe from brute force attacks is easy as they are not direct attacks.

- Change the password immediately when a website you use is hacked.
- Use long and strong passwords. **Even if they are crackable**, it will take them a lot longer. This gives you enough time to get in and change the password.
- Enable 2-factor authentication.
- Don't use the same password in multiple websites. Once a hacker gets access to an account, the first thing they do is check if the same password works with other accounts using the same email address.

Note: We will discuss all the above points in greater detail in the chapters after this, so don't worry about them right now.

The most important part? **Long passwords.**

The sweet spot is 12-15 characters. Some experts say anything over 14 characters makes the time spent hacking not worth it, even for the hackers.

Brute force attacks, no matter how sophisticated or widespread serve no immediate threat to you if you have a strong password and are aware of website hacks. But some hackers use a more targeted approach to hacking accounts. They first center in on the target and then starting working on cracking the password. These direct hacks pose a larger threat to your data.

Answering Security Questions

You will not believe how much free time a teenager has. You will also not believe that a shocking number of account hacks have nothing to do with passwords whatsoever. The hackers usually get in by answering security questions that you selected while signing up because the service nagged you to.

And I'm using the term "hacker" very liberally here. Most of the time they are just mildly intelligent teenagers with a can do spirit. Once they have acquired a target,

one that's worth spending all their time on, the teenagers then take to the internet to research on the subject. In this day and age of Google search and social media accounts like Facebook and LinkedIn, this is incredibly easy.

All of this is only made worse by the fact that we ourselves aren't making it harder for them. A lot of us use answers like birthdays, where we went to school, our maiden names, city we were born in etc as security questions. All of this was fine in 1995 when Google and Facebook didn't exist.

The problem is that you can't usually type in your own questions, you have to select from the curated few. The best way to tackle this is to answer the security questions with **something totally random and made up**. Type in anything you want in there. But make sure it's something you'll remember.

Security questions data is just as important as passwords, if not more so. Which means you should back them up as well.

Social Engineering



When Wired writer Mat Honan's iCloud account was hacked, he was not only perplexed with the "why?" but also the "how?". The reason turned out to be his valuable @mat Twitter account. And the way the hackers got into the email account, which was linked to the Twitter profile, was even more bizarre.

Read Mat Honan's entire ordeal with Apple, Amazon and one dedicated hacker [over at Wired](#).

As the article says, an impersonator on phone with Apple customer care needs shockingly little proof to reset a password.

Apple tech support confirmed to me twice over the weekend that all you need to access someone's AppleID is the associated e-mail address, a credit card number, the billing address, and the last four digits of a credit card on file. I was very clear about this. During my second tech support call to AppleCare, the representative confirmed this to me. "That's really all you have to have to verify something with us," he said.

The hackers found the associated email address by looking up his Gmail address, which had the Apple ID as the fallback. The billing address came from a Whois search for his website but there are numerous ways to get there. The last four digits of the credit card were the tricky one.

The hackers called Amazon, submitted proof like billing address etc and asked to add a new credit card. Then they called again saying they couldn't get into the account, this time offering the fake credit card details they just created as proof. Once they were in, they could see the last 4 digits of the real credit card associated with the account. The same 4 digits that Apple considers so important.

Post the aftermath, Mat has some suggestions on how we can avoid something like this. Apple and Amazon have both implemented a fix but the last time Wired checked, they weren't as foolproof as they should be.

- The first thing Mat suggests is to not daisy-chain all your accounts. Meaning not to have the same @gmail, @icloud, @yahoo account ids.
- Back up. In the process of the hacking, Mat had the data on his iPhone and Mac wiped off. So, always back up, no matter what.

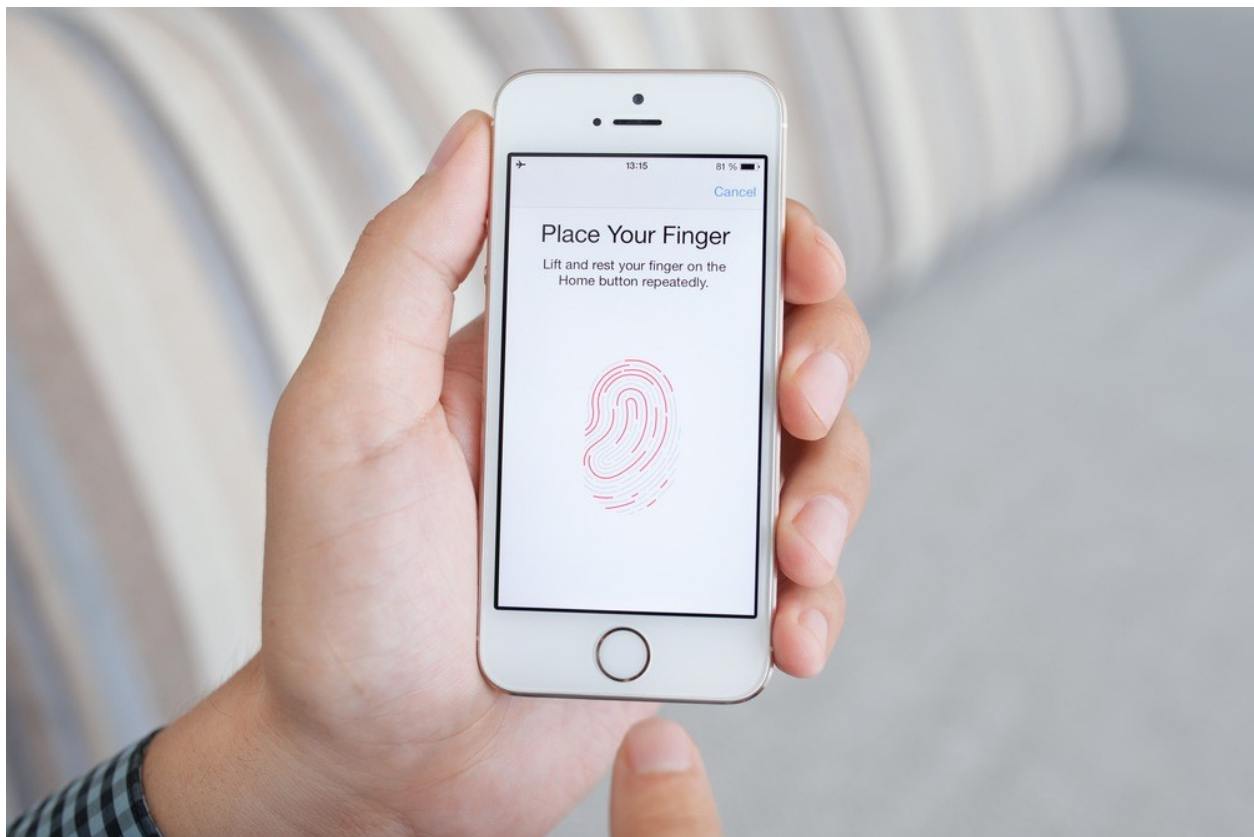
Tip

Photos and videos residing on our phones are usually very dear to us, which is what Mat lost in that hack. That's why better to have them backed up automatically. Check these [8 cool ways to auto-back up phone photos and videos](#).

Can iCloud Be Hacked?

On 31st August 2014, private pictures of several celebrities were leaked on the internet. With time, it was clear that iCloud, in some capacity was responsible for this event dubbed “celebgate”. We don’t know for sure how exactly hackers got into so many celebrities iCloud (and some other cloud) accounts and were able to extract information without any red flags.

While we don’t know how exactly they did it, thanks to the power of free and open internet and some curious tech journalists, we have an idea how it could have happened.



[Ars Technica ran an experiment](#) where they tried to hack into their family members’ iPhones and iCloud accounts. They used military grade software (available to the public for a couple hundred dollars or pirated copies for free as torrents) that has been reverse engineered to hack Apple’s hardware and software.

Once a hacker has the iCloud account's password (gained either by phishing, physical intrusion, public Wi-Fi snooping or malware), it becomes fairly easy to recover entire iCloud backups from devices, to wipe them off or to track the device's movement using Find My iPhone feature.

At the time of hacks and the Ars Technica experiment, 2-factor authentication was not required to restore backups on Windows machine or when logging in to websites. Apple is said to be adding security measures that will notify the user when their iCloud account has been accessed on a new computer. While this won't help stop the hack, it will make the user aware.

Using the iCloud's restore feature, a hacker can clone an iPhone's entire storage. This includes everything from photos, videos, app data to phone calls and messages.

Now, there has been some good news. iCloud has recently enabled 2-factor authentication for restoring iCloud backups. This means ([and Ars Technica confirmed](#)) that the hacking software previously used to restore complete iCloud backups no longer works if the account has 2-factor authentication.

Tip

Now that you know about iCloud's stand on cyber security, check out its [very human readable privacy policy](#). Apple maintains that unlike other competitors, it is not in the business of selling user's private data and the company itself doesn't have access to your messages. But BoingBoing thinks [we shouldn't believe Apple's promises blindly](#).

To conclude, is iCloud safe from hacking? Only if you have 2-factor authentication turned on.

How To Deal With Password Hacks Beyond Your Control?

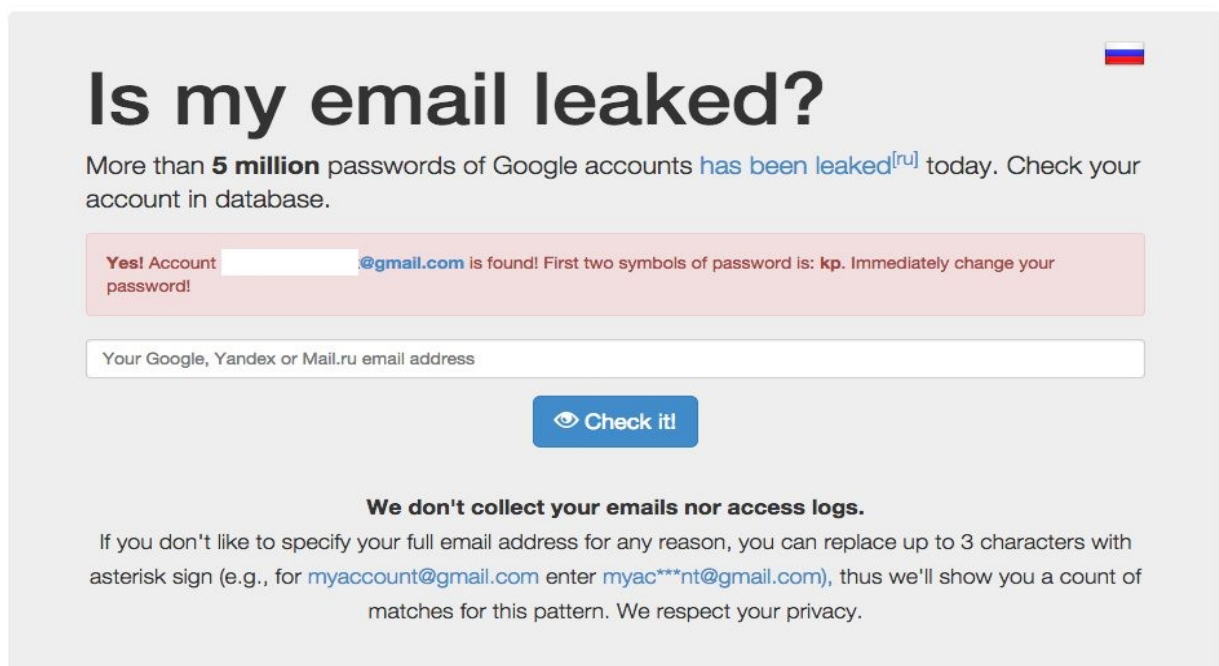
In case of a service-wide hack, step zero is to go to the website in question and change your password as soon as possible. But how do you know when it's time?

First, make sure you've put up a wall in the form of 2-factor authentication. If hackers steal millions of passwords in the middle of the night, you won't be losing any sleep over it because you know they can't get in without the second confirmation code that comes to you via SMS.

Second, be aware of security exploits. When a well known service takes a hit, they send out emails and usually warn users when they visit the site about the hack and urge them to change their passwords, like eBay did this past year. But make sure the email you got is legit and not a phish attempt, as discussed in the phishing section above.

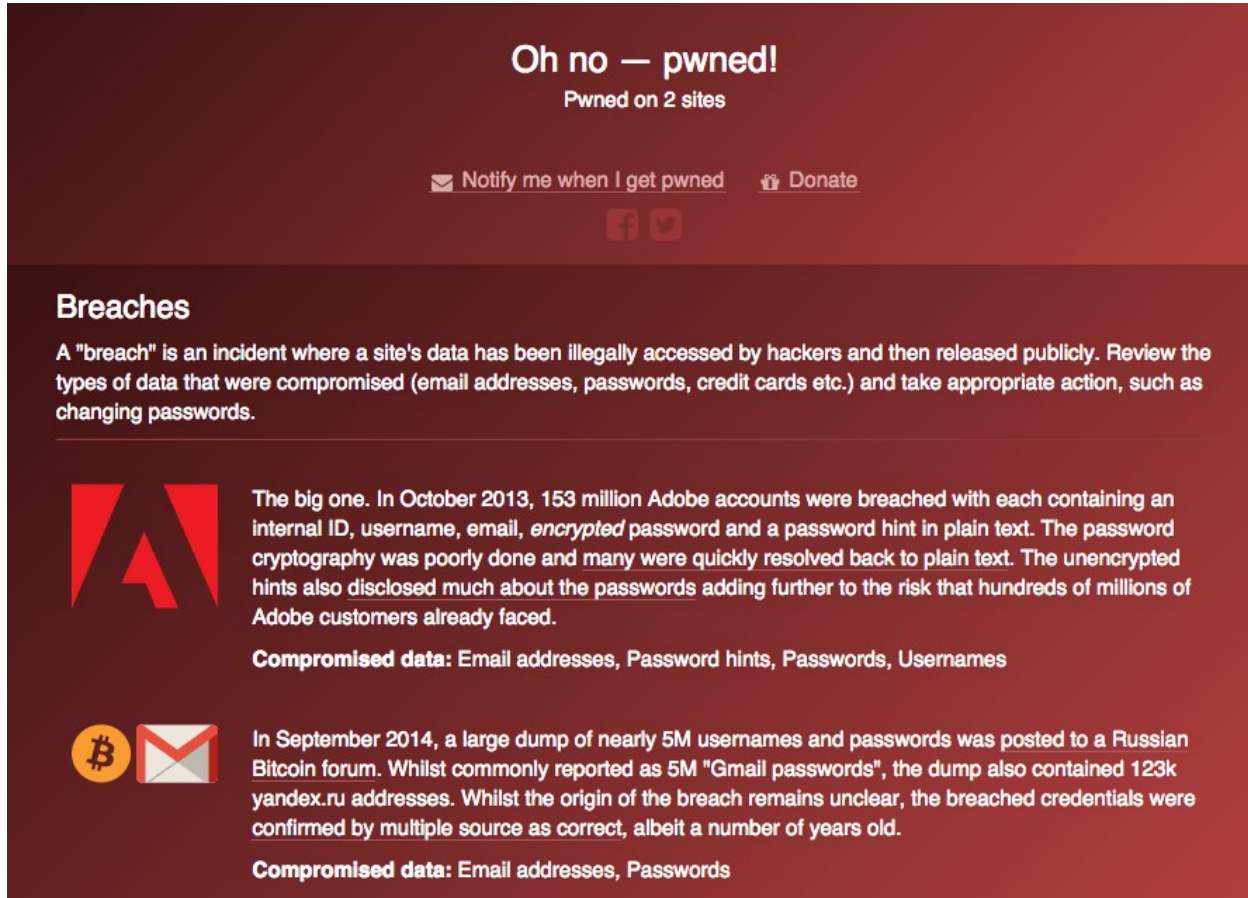
How To Know If A Service You Use Has Been Compromised

As this is the internet, not every company is going to be forthcoming about the security. If you follow sites like Lifehacker, The Verge and TechCrunch, you'll immediately see reports of major break-ins as they happen.



The screenshot shows a web interface for checking if an email account has been compromised. At the top right is a small Russian flag. The main heading is 'Is my email leaked?'. Below it, a message states: 'More than **5 million** passwords of Google accounts [has been leaked](#)^[ru] today. Check your account in database.' A red alert box contains the text: 'Yes! Account [redacted]@gmail.com is found! First two symbols of password is: **kp**. Immediately change your password!'. Below this is a text input field with the placeholder 'Your Google, Yandex or Mail.ru email address'. A blue button with an eye icon and the text 'Check it!' is positioned below the input field. At the bottom, a disclaimer reads: 'We don't collect your emails nor access logs. If you don't like to specify your full email address for any reason, you can replace up to 3 characters with asterisk sign (e.g., for [myaccount@gmail.com](#) enter [myac***nt@gmail.com](#)), thus we'll show you a count of matches for this pattern. We respect your privacy.'

To be more proactive, use websites that compile breaches and the leaked database and let visitors check if their email or username belongs to any of those leaks.



Oh no — pwned!


Pwned on 2 sites

[Notify me when I get pwned](#) [Donate](#)

[Facebook](#) [Twitter](#)


Breaches

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.



The big one. In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

Compromised data: Email addresses, Password hints, Passwords, Usernames



In September 2014, a large dump of nearly 5M usernames and passwords was posted to a Russian Bitcoin forum. Whilst commonly reported as 5M "Gmail passwords", the dump also contained 123k yandex.ru addresses. Whilst the origin of the breach remains unclear, the breached credentials were confirmed by multiple source as correct, albeit a number of years old.

Compromised data: Email addresses, Passwords

Here are three such websites.

- [Haveibeenpwned.com](https://haveibeenpwned.com)
- [PwnedList.com](https://pwnedlist.com)
- [Shouldichangemypassword.com](https://shouldichangemypassword.com)

Haveibeenpwned.com has a newsletter that sends out emails every time a major website hack occurs. This way even if you don't follow the news, you'll still stay up to date.

How to Create a Strong Password - The Basics

When it comes to creating a strong password there's no one straight answer. But there are things you can do to make it harder for hackers. Make it so strong, it's almost not worth the effort for them.

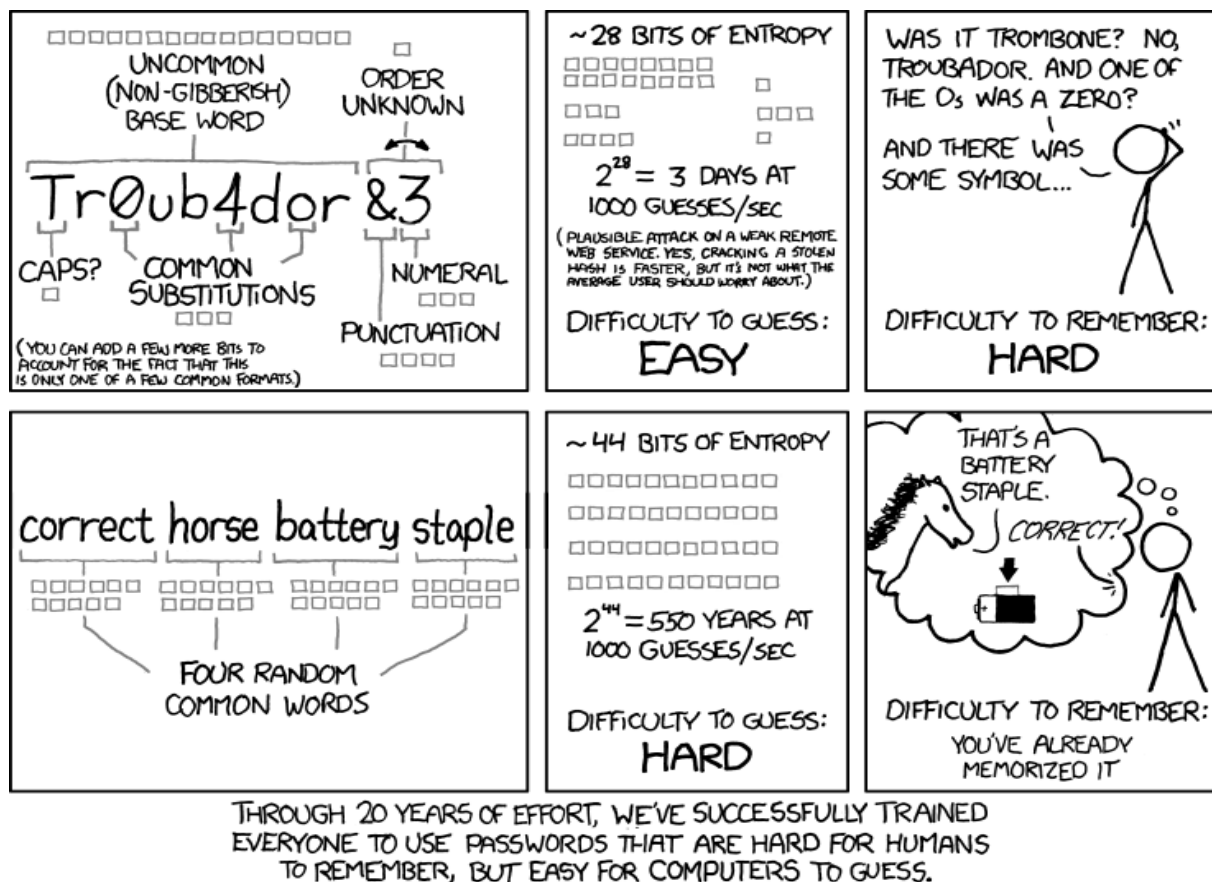
Here are some pointers to start with.

1. Make it long. The longer the password, the harder it is for password guessing apps to crack it. For example, the possible combinations for a 15 character password including alphabets and numbers is much higher than an 8 character password.
2. Use special characters and uppercase letters. Many websites allow users to insert special symbols like "\$", "underscore" etc. Use them to make your password stronger.

Don't Make It Easy For The Computers To Guess

Computers these days are incredibly powerful, and with the help of sophisticated software, some are dedicated to just guess passwords by trying every possible combination, starting with "a", then "aa", "ab" and on and on and on.

[XKCD comic 936](#) explains this very well.



A short password, even with a slew of uppercase and lowercase letters, including special characters is not that hard for a computer to guess.

But a password that's 20+ characters long, is only made of lowercase letters, a combination of words? That would take them years, if not hundred of years to crack.

Also, such passwords, if formed well, are really easy to remember.

The Best Ways To Make A Human Readable Password

The easiest way to remember a password is to associate it with a not-so-easily-guessable part of your life with the service at hand.

Run your imagination wild. Use a quote from your favorite TV show, tie it in with the service, make it funny and you'll never forget it.

For example, there's a bit in Friends TV show where Chandler gets his TV Guide delivered by the name of *Mrs Chanandler Bong*. It's funny and if you integrate it with your primary email address, it can stick. Make it *chanbongmail* or *mrschanandlermail* or any other combination.

This is the time where all the years of watching TV is actually going to help you. It's not quite X-files but it's up there.

Random Text vs Human Readable, Which Is It?

To know how to create a strong password, we first need to know how they are hacked. We've discussed that in detail in the past section. But here is the rundown.

- Using brute force or password guessing apps
- Social engineering
- Phishing
- Backdoor attacks



As the passwords and internet security gets sophisticated, so do the hackers and their software. As normal brute force attacks take so much time, hackers are integrating dictionary words (and variations of them) along with millions of passwords cracked from previous exploits. When you add all the data, it takes shockingly little time for a sophisticated password guessing app to crack the easiest and widely used passwords.

Thanks to all of that, not only do we need to create a strong and unique password that can't be related to our personal life, but we also need to stay away from any commonly used password patterns hackers might already know of.

Did you know

The earliest known use of cryptography is found in non-standard hieroglyphs carved into monuments from the Old Kingdom of Egypt circa 1900 BC.

Hackers use personal information they got either by searching the internet or social engineering means and ask the software to generate passwords based on that. The software spits out combination of your names, date of birth, address etc until it finds a match. If I use "KhAmOSHP4ThaK" as a password thinking how smart I am being having used uppercase, lowercase **and** numbers in a passwords, I would be wrong.

First, I've made the passwords very hard for me to remember. Second, the personalized hacking tool that knows my first and last name won't take long to spew out this combination.

The Answer Lies In The Middle

There's no one true way to make a strong password but there are many ways to get it wrong.

You can create a strong password using "S0M3tHeng" like this or a random phrase that's 25 character long.

The key is to not use any personal information in the password which might be 'recorded' somewhere.

Right, don't use personal details in the password, details that might be recorded somewhere. But you may always use personal information that you never shared with anyone. Stuff that's really weird and quirky. Like the *Mrs Chanandler Bong* example we discussed above.

Another way to go about choosing a 25 character phrase for a password is to put in utter gibberish in there. It can be a quote from a movie or a TV show or a person, but make sure it's nothing personal and nothing too mainstream.

And it's the same advice if you're going the short but complicated-to-read password route. Make sure it's not related to personal data (you might create it using something that's too personal though, as discussed above).

To make short but random passwords easy to remember, security expert [Bruce Schneier suggests using anagrams](#). Where you take a sentence or a famous quote but use the initials as the password.

For example:

Your **T**ime Is **L**imited, **D**on't **W**aste It **L**iving **S**omeone **E**lse's **L**ife becomes YTILDWILSEL. You can make that uppercase, lowercase, turn e to 3, l to 1 etc. You've now got a medium length, complicated password but an easy way to remember it.

The XKCD scheme is still good advice, but you actually need to pick the individual words randomly.

How To Check If Your Password Is Strong

You can check the password strength using [Rumkin's online tool](#). It provides a more detailed feedback compared to the "weak/strong" feedback you see beside the password input box.

Enter your password or passphrase here:

.....*

Length: 19

Strength: **Strong** - This password is typically good enough to safely guard sensitive information like financial records.

Entropy: 85.2 bits

Charset Size: 52 characters

- Warnings are shown if you enter a common password.
- Warnings are shown if your password is very short (4 or less characters) or if it is short (less than 8 characters)
- Password strength is determined with this chart, which might be a bit of a stretch for a non-critical password:
 - < 28 bits = Very Weak; might keep out family members
 - 28 - 35 bits = Weak; should keep out most people, often good for desktop login passwords
 - 36 - 59 bits = Reasonable; fairly secure passwords for network and company passwords
 - 60 - 127 bits = Strong; can be good for guarding financial information
 - 128+ bits = Very Strong; often overkill

The website also has some suggestions, the one we've covered above already like having a long password, with uppercase, lowercase and special characters. It should not be a common phrase or something easily associated to you (like your name or birthday).

Use the text input box to see the strength of the password. You should aim for 60-127 bits entropy. When I entered *mrsChadandlerbong'sTVmailguide* I got a score of 150, which was an overkill, meaning the password is too complicated for its own good.

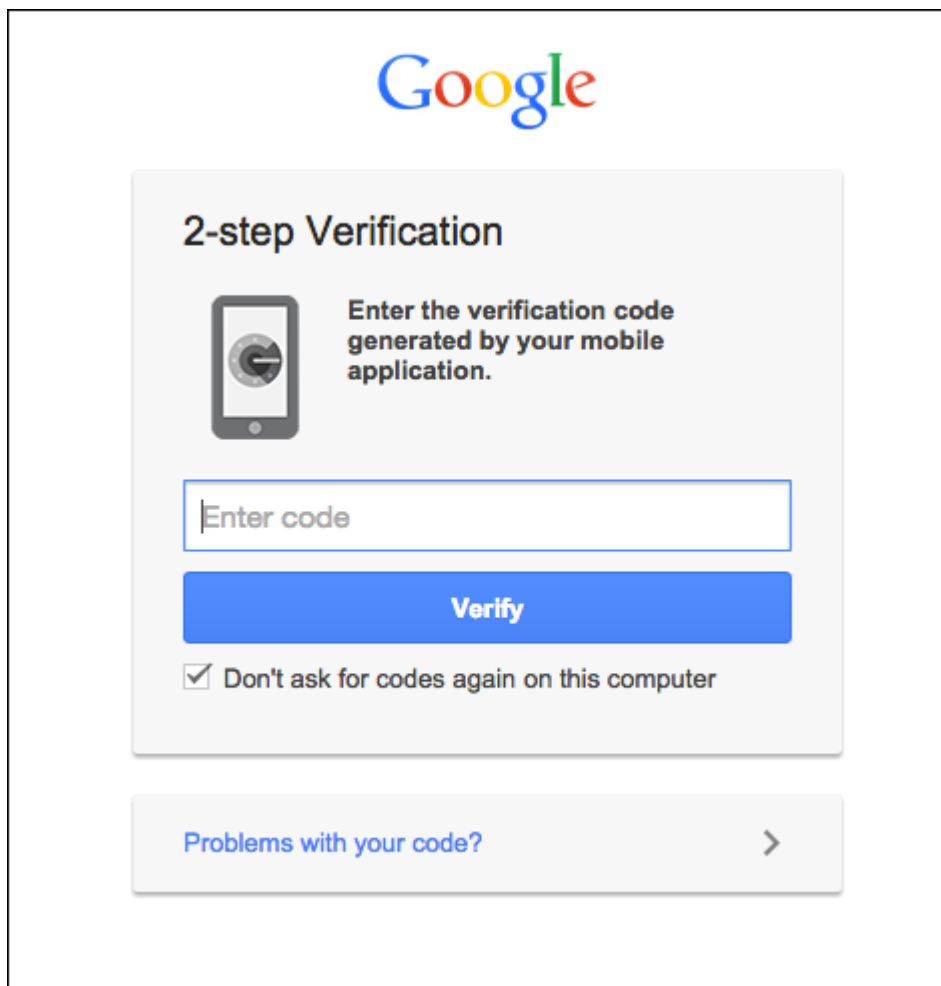
It's far past the point for hackers to randomly generate it while it's not easy enough for me to remember. *MrschanandlerbongTVguide* brought me to a more saner 110 bit entropy level.

Why And Where You Can Enable 2-Factor Authentication

Remember the guy in the movie who would walk away from an explosion, with a stylish and confident gait, putting on his aviators just when everything behind him starts burning to ashes? He knows the fire won't reach him. Something's got his back and he knows it. If he were to be in the utterly boring world of password security, that something would have been 2-factor authentication.

Gmail can be hacked, hackers can social engineer the security questions but unless they physically kidnap you or get hold of your phone, they can't get into your account if you have 2-factor authentication enabled.

Google's ex-spam guru [Matt Cutts said it best](#) when he said "Two-factor authentication means "something you know" (like a password) and "something you have," which can be an object like your phone.



The image shows a screenshot of Google's 2-step Verification interface. At the top is the Google logo. Below it, the title "2-step Verification" is displayed. To the left of the instructions is an icon of a smartphone. The text reads: "Enter the verification code generated by your mobile application." Below this is a text input field with the placeholder "Enter code". Under the input field is a blue button labeled "Verify". Below the button is a checkbox that is checked, with the text "Don't ask for codes again on this computer". At the bottom, there is a link "Problems with your code?" followed by a right-pointing chevron.

2-factor authentication works something like this: When you log in to a website, just entering your password isn't enough. Once you've entered a password, you'll get an authentication code on a physical device close to you. It can be an SMS on your phone or if you're using one of the compatible services, the Google Authenticator app.

What You Need Know About 2-Factor Authentication In General

- You don't always have to use SMS to verify. You can use Google Authenticator app for supported services, on your smartphone or tablet.
- If for some reason you can't receive SMS, you can print out a set of one time backup codes and carry it with you.
- You **don't** have to enter the authentication code every single time you log in. In services like Gmail, there's an option to enter the authentication code once every 30 days when you're using the same computer.
- When you're logging in using a new computer or device, the 2-factor authentication is a must.

A Practical Guide To 2-Factor Authentication

A lot of major websites support 2-factor authentication now. Gmail, Dropbox, Paypal etc are all in. But the reality is that 2-factor authentication is cumbersome. It's important but cumbersome.

So pick your most important services where your files, mails, data and communication is stored and use 2-factor just there.

Services Where You Can Enable 2-Factor Authentication

Google : Google can either send you a confirmation code via SMS or the Google Authenticator app which is available for [iOS](#), [Android](#) and [even BlackBerry](#). Devices can be saved for 30 days. [Click here to enable it](#).

LastPass: We've covered LastPass's 2-factor (hardware and software) authentication in detail in the password management apps section of this guide. LastPass partners with services like Google Authenticator, Toopher and Duo

Security. You can also use YubiKey which serves as a physical USB authenticator. Go to *Settings* on LastPass's website and navigate to *Muiltifactor options*. To know [how to enable Google Authenticator, see this](#).

Facebook: Facebook calls its 2-factor system "Login Approvals" and it sends you a 6 digit code via SMS. It also works with the Google Authenticator app. [Enable it from here](#).

Twitter: Twitter's 2-factor authentication is fairly straightforward. It will send you a 6 digit authentication code when you log in using a new device. That's it. [Click here to enable it](#).

LinkedIn: LinkedIn's process is the same as Twitter where you're sent a 6 digit code via SMS. [Enable it from here](#).

Dropbox: For a lot of us, Dropbox is where we save all our files. You'll want to make sure it's well protected. Dropbox does the usual 6 digit code via the SMS bit but it also has support for apps like Google Authenticator, Duo Mobile and Authenticator app for Windows Phone. Check out Dropbox's [documentation page](#) for a step by step guide on how to enable it.

Steam: If you're a gamer your credit card is already saved to a Steam account. Secure the account using 2-factor authentication by going to *Steam -> Settings -> Manage Steam Guard Account Security* in the Steam app.

Microsoft: Microsoft will send you a seven digit code via email or SMS when you use a new machine. [Enable it from here](#).

Yahoo! Mail: Do you still have to use Yahoo! Mail? You can have a 6 digit authentication code sent in when you start using it on a new machine. [Click here to enable it](#).

PayPal: If you use PayPal for business transaction, you'll want to make it as secure as possible. PayPal will send a 6 digit code via SMS when you use it on a new machine. [Click here to learn how to enable it](#).

Amazon Web Services: Amazon's S3 and Glacier storage services support 2-factor authentication using Google Authenticator. [Enable it from here](#).

Evernote: If you want to sleep peacefully knowing your personal thoughts are safe from the reach of hackers, turn on 2-factor authentication using Google Authenticator. [Check out Evernote's blog post to know how to do it.](#)

WordPress: WordPress doesn't have a direct support for 2-factor authentication using SMS but you can enable it using the [Google Authenticator plugin](#).

More Websites With 2-Factor Authentication

The list of websites that have 2-factor authentication feature is too big to go in detail here. Thankfully Josh Davis, a computer science student, has compiled all the popular websites that have this feature at his site called [Two Factor Auth](#). You'll also find handy links to the corresponding documentation pages there.

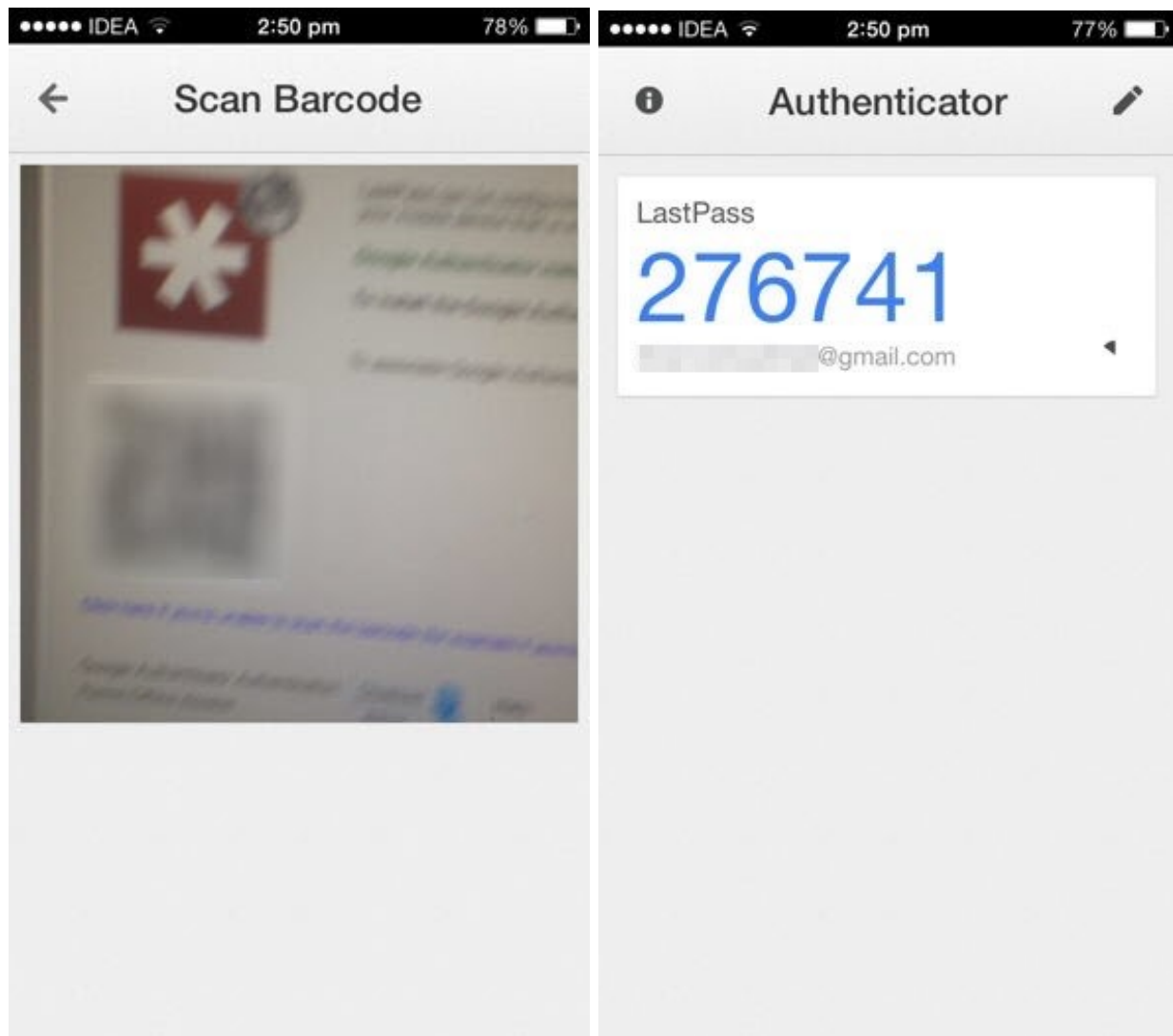
His website also lists sites that don't yet have this feature.

How To Use Authenticator Apps Instead Of SMS

Google Authenticator is one of the most widely used 2-factor authenticator apps. You'll see that most of the websites listed above support it.

But how exactly does it work?

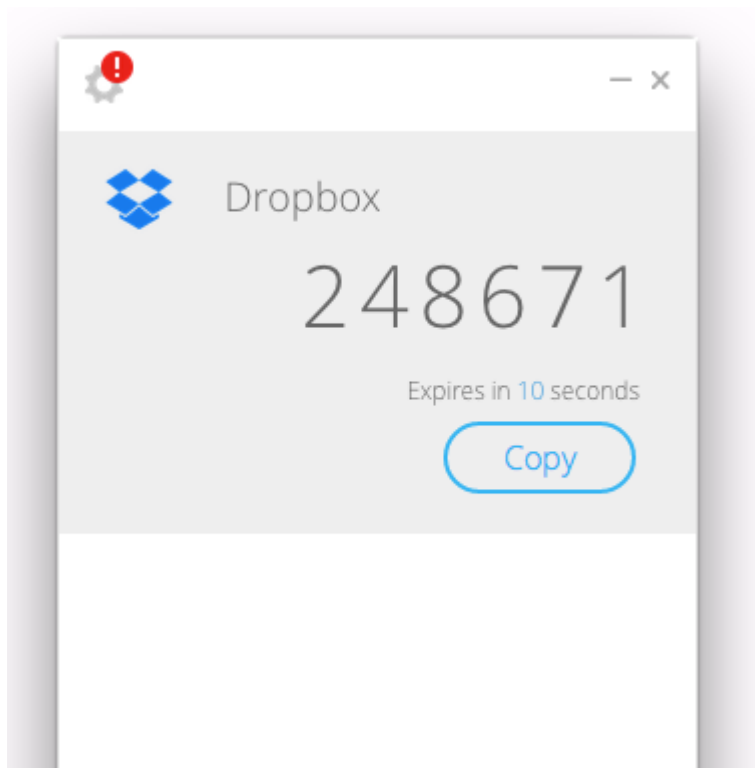
When setting up Google Authenticator with a service, you either need to scan a QR code using the app or input details manually. Most of the time a QR code will do.



When you scan the QR code using the Google Authenticator app, it links the the service with your physical device. Now every time you open the app, it will connect with the service and generate a new verification code that only lasts 30 seconds. The next time you log in using a new device, just open the Authenticator app and a new code will be there waiting for you.

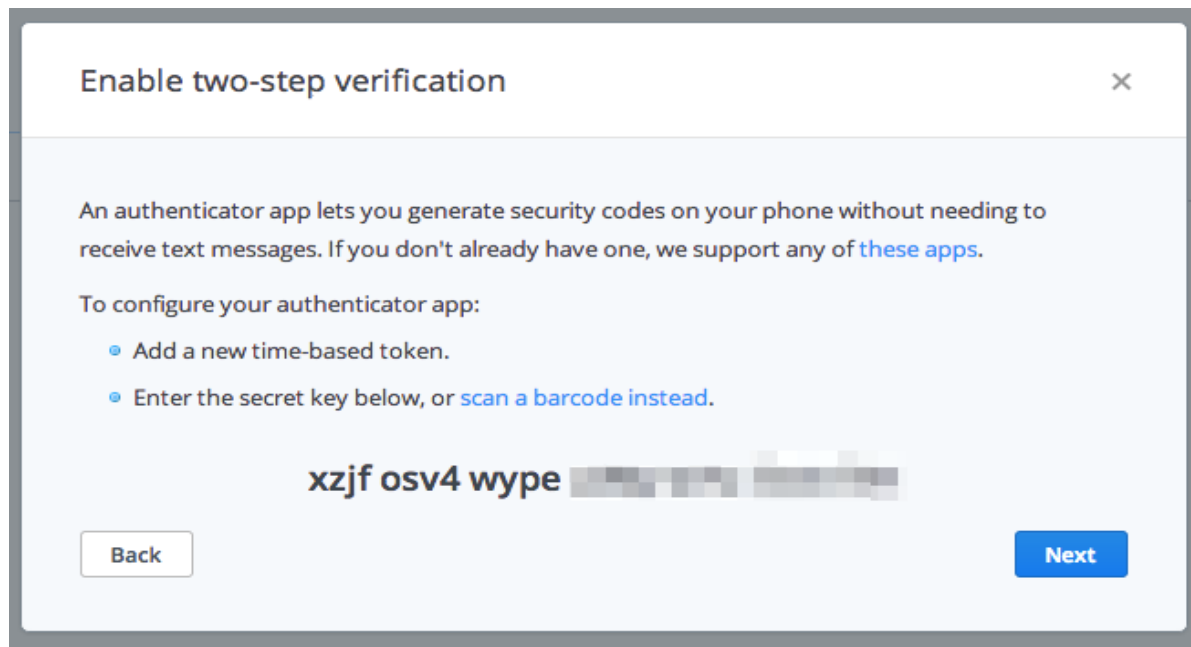
You may add new accounts by going to the *Set up an account* section of the app.

Google Authenticator Vs Authy

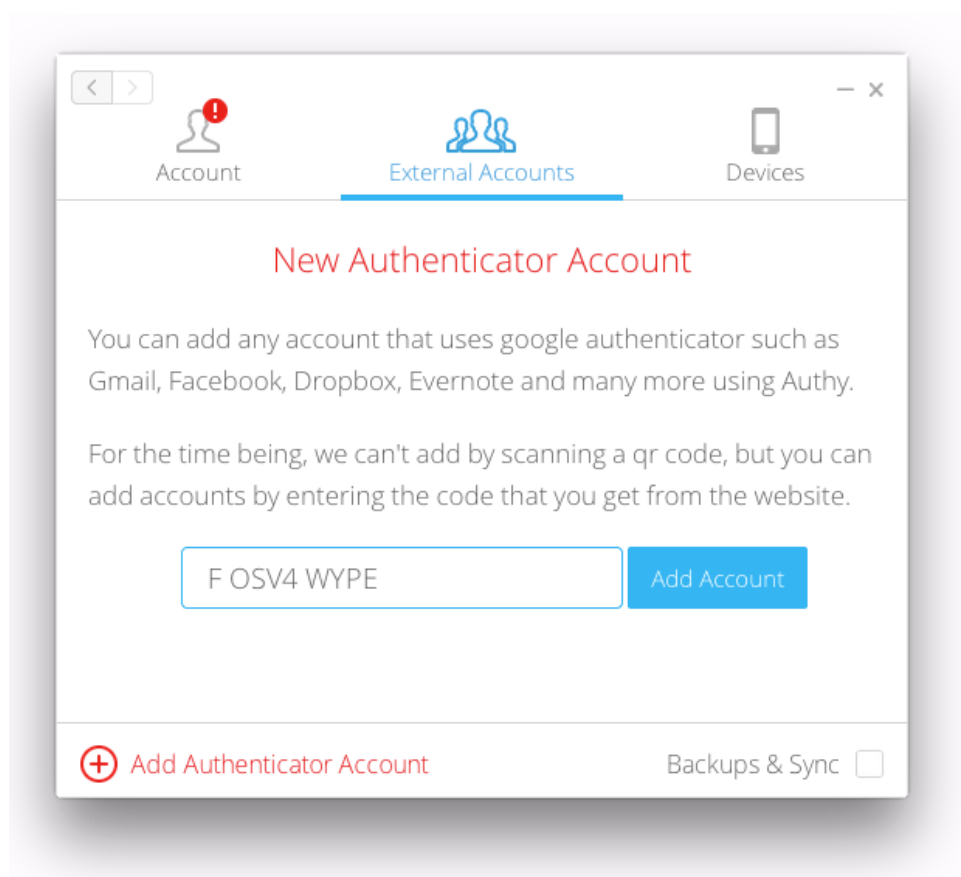


Just like Google Authenticator, [Authy](#) is a free third party service for managing 2-factor authentication codes. Authy has a Chrome app that can be used on Windows, Mac and Linux alongside the iOS, Android and BlackBerry app.

While Authy has security features like device based authentication, master and backup passwords (things that even Google Authenticator does not), it's still a third party app from a company you've never heard of.



It also allows you to manually input the authentication code while setting up a 2-factor authentication account. This is helpful if you don't carry a modern smartphone with application support.



While the tight security is appreciated, it does make the app considerably harder to use. If you're just starting out with 2-factor authentication, this extra barrier might be off-putting.

My advice: Start with Google Authenticator. It's easy to use and despite its lack of features, it just works.

The Best Password Management Apps And Why You Should Use Them

If you want to say screw it to the task of creating unique and strong passwords for different sites and figuring out the best way to remember and store them, password management apps are what you're looking for.

Password management apps will remember username and password for a particular site. These services also have extensions and apps with automatic login functionality. Many of them also offer mobile apps.



But more importantly, the apps have **robust password generators**. When you're signing up for an account, the app/extensions will automatically generate a long and random password and remember it for you. But mind you, these passwords are in no way human readable. They are a jumbled mess of uppercase and lowercase characters, numbers and special characters. It will probably take you longer to memorize them than it will take for brute force attacks to crack it (which is to say a long time).

But is that something you might want to do?

1Password and LastPass both have desktop and mobile apps. So as long as you have your own laptop/phone with you, or a public computer with online access (LastPass has an offline access option), your passwords will be readily available to you.

Did You Know

LastPass also allows you to carry encrypted passwords around in a pen drive if you're heading somewhere remote.

How Does It Work?

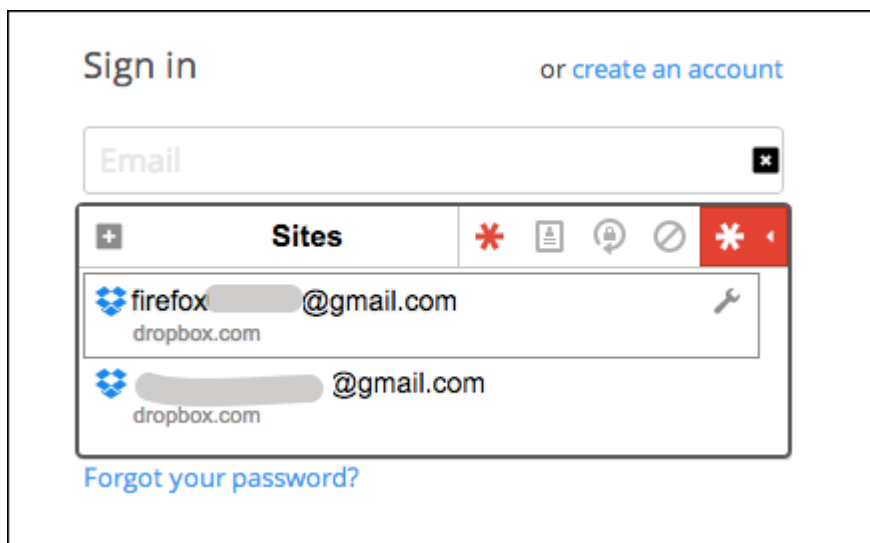
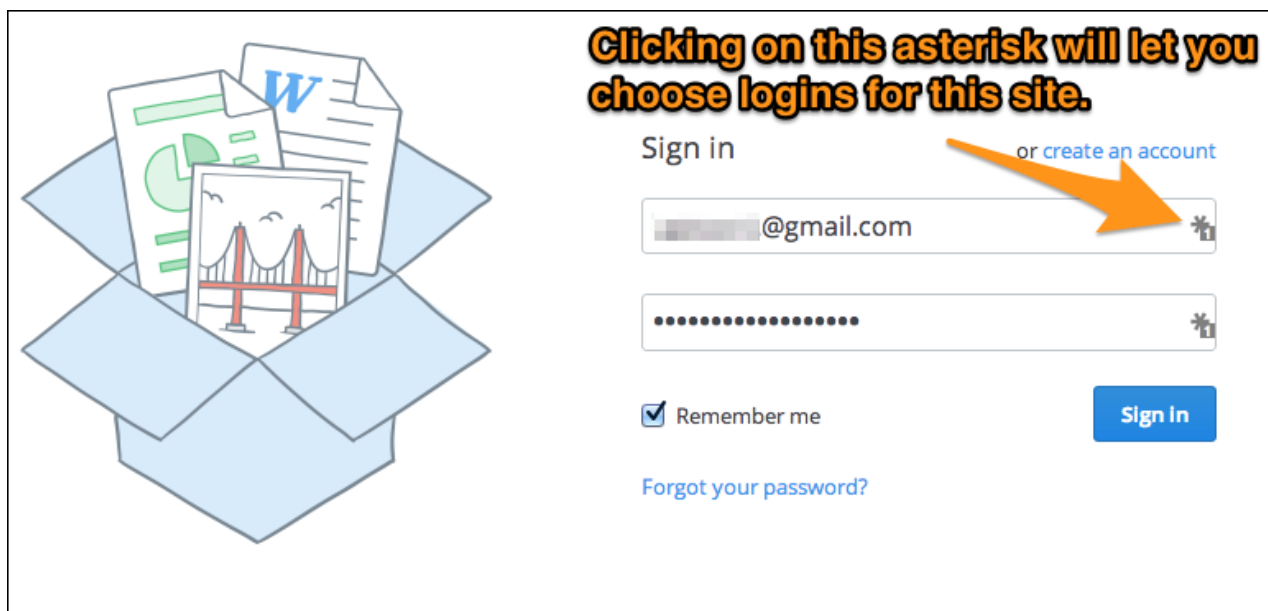
As an example I'm going to use LastPass but the process for apps like 1Password and Dashlane is similar.

When you create a new account, LastPass usually shows a popup after logging in, asking you to save the site, as shown below.



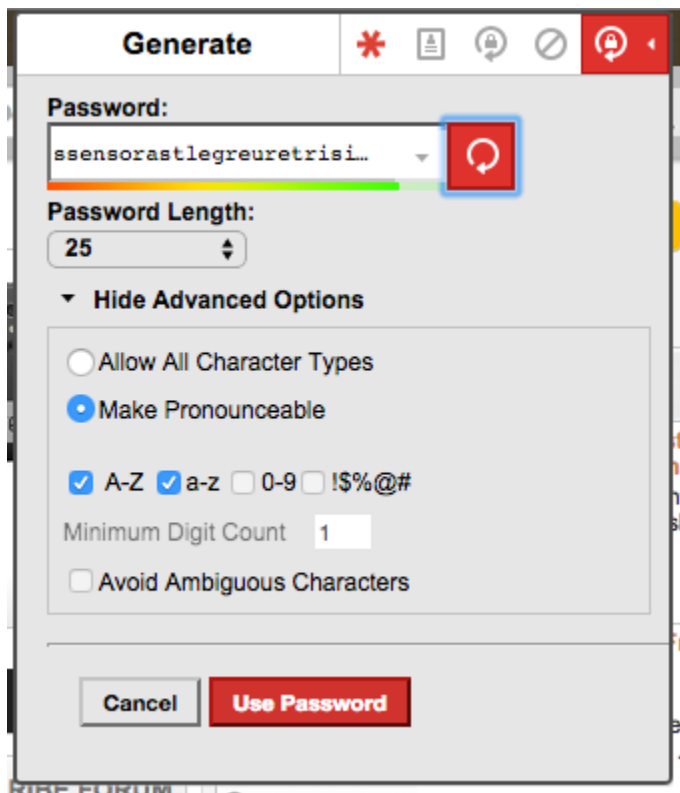
The next time you visit the site's login page, you can choose the username/password saved in LastPass through the asterisk that sits in one corner of the username and password tabs.

If LastPass has stored only one account associated with the site, it will auto-fill the details and show the number 1 on the asterisk. If you use multiple logins for that site, the corresponding number will be shown on the asterisk, and clicking on the asterisk will reveal a dropdown menu from where you may choose the preferred login.



When you're creating an account, LastPass will sense the input fields and will let you generate a password. The password generation has many options that you can customize.

The default length is 12. As this is a random password you're never going to memorize, it's best to go with more than 15 characters. Also enable uppercase, lowercase and special characters.



LastPass Tip

As you see in the above image, there's a *make pronounceable* button which generates a password that's random but still pronounceable, making it possible to remember it.

It's All About The Master Password

When you're using a password manager like LastPass, 1Password or KeePass to save passwords, what matters the most is the master password. The password you use to log in to the password managers.

If all your website passwords are randomly generated and saved with these apps, the master password is the **only** password you'll need to remember.

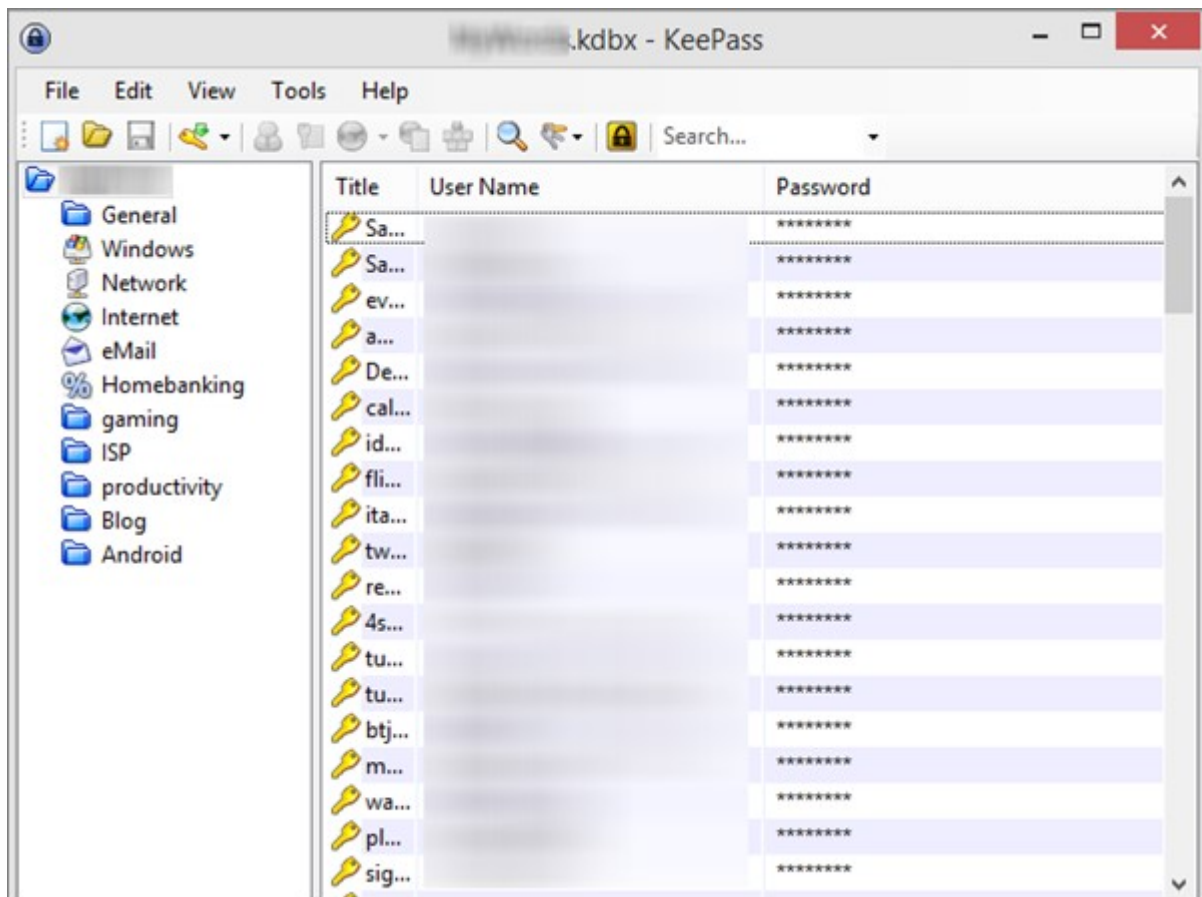
So make this password as strong and long as possible. My LastPass password is more than 40 characters long. You can make it phrase or a sentence.

LastPass Vs KeePass vs 1Password Vs Dashlane

1Password is available as a suite of apps and costs \$50 for the desktop version, \$17 for the Android app and the iOS app is free with paid upgrade for pro features. While 1Password is totally worth it, LastPass presents a better proposition. The desktop browser extension is free to use but you have to pay \$12/year to get access to premium features and mobile app support. If you don't need a password management app on your phone, the free LastPass account will be enough for you.

KeePass is the LastPass without any baggage. It is an open source password protection app with industry leading encryption. It is also just an offline app, basically a password protected database file of your passwords. It is available in the form of Windows, Mac and even Android app. Plus there's also a portable version.

But KeePass is not as convenient as other apps listed here. It doesn't offer auto logins, password generator, auto save, nothing. It is just an app where you save username and passwords and that's it.



When you're starting off with KeePass make sure you build a *.kdbx* file and not *.kdb* file. *.kdb* files are only for KeePass 1.0 apps which is Windows only. *.kdbx* will work on any platform, including Android and iOS.

Tip

Check out our detailed [comparison between LastPass and KeePass](#) and our guide to using a third party [KeePass app with auto logins for Android](#).

Dashlane is just like LastPass, a cloud based password generation, saving and syncing tool, but its free version is not as accessible and the paid version is more expensive. The free Dashlane version only works on one device. Unlike LastPass, the free account doesn't even give you web access to your passwords. And the premium account costs a hefty \$39.99 a year.

Unlike LastPass, 1Password does not save your passwords on its own servers. Much like KeePass, 1Password creates an encrypted database file that you can either store offline or sync using Dropbox or iCloud.

Comparison Table

Features	LastPass	1Password	KeePass	Dashlane
Cross Platform	✓	✓	Via Third Party Apps	✓
Desktop Extension With Auto Log In	✓	✓	✗	✓
Android App With Auto Log In	✓	✓	✓	✓
iOS 8 Extension With Auto Log In	✓	✓	Via Third Party Apps	✓
Open Source	✗	✗	✓	✗
Unique Password Generator	✓	✓	✗	✓
Data Storage Location	On LastPass's Private Servers	Database File That Can Be Saved To Dropbox	Database File That Can Be Saved To Dropbox	On Dashlane's Private Servers
Pricing	Free For Desktop. \$12/year For Mobile Apps.	Mac & Windows App – \$49.99 each. Android App – \$17 Upgrade. iOS 8 App – Free With Pro Upgrade.	Free for all. Everywhere.	Free For 1 Device. \$39.99/year For Multiple Devices And Pro Upgrade.

The Best For Most – LastPass Premium

It's a tough fight between 1Password and LastPass but in the end LastPass wins because of the excellent browser extensions and the Android/iOS apps with auto logins. It's also cheaper and more approachable than 1Password. If you want to use 1Password on desktop, mobile and tablet, you're looking at a 60\$+ bill. LastPass premium on the other hand is only \$1 a month (billed annually). To your mind, 1 dollar a month is an easy sell for all the added security.

But just spending 1 dollar a month won't upgrade your security. For that you'll need to take specific steps.

How To Use LastPass

LastPass Security Check

Before making a change we need a status report. To see how deep in the waters you are, i.e. how bad your passwords are and if any of the sites you use has been hacked recently.

ENGLISH

FEATURES HOW IT WORKS GO PREMIUM ENTERPRISE SIGN IN

LASTPASS SECURITY CHALLENGE

What's *your* LastPass Security Challenge Score?

The LastPass Security Challenge is just one way
LastPass helps you stay safe online

Get Your Score



You will get these results:

- A check of your vault for Heartbleed-vulnerable sites
- A free, fast on-the-spot analysis of your LastPass vault
- An easy to interpret score from 1 to 100
- Easy, actionable ways to increase your security right now
- A comparison of your score against all other LastPass Security Challenge participants to date
- Results of a vault check for vulnerable sites that may have been involved in recent compromises

LastPass Security Check scans all your accounts, emails and passwords against its database of known hacks, bugs, and generic password parameters. At the end you get a score you can act upon and you are ranked against other LastPass users as well.

LASTPASS SECURITY CHALLENGE

70.1%


Your Score

213,058th

Your Rank

100% - Perfect!

LastPass Master Password Strength



Thank you for taking the
LastPass ****
Security Challenge

Improve Your Score

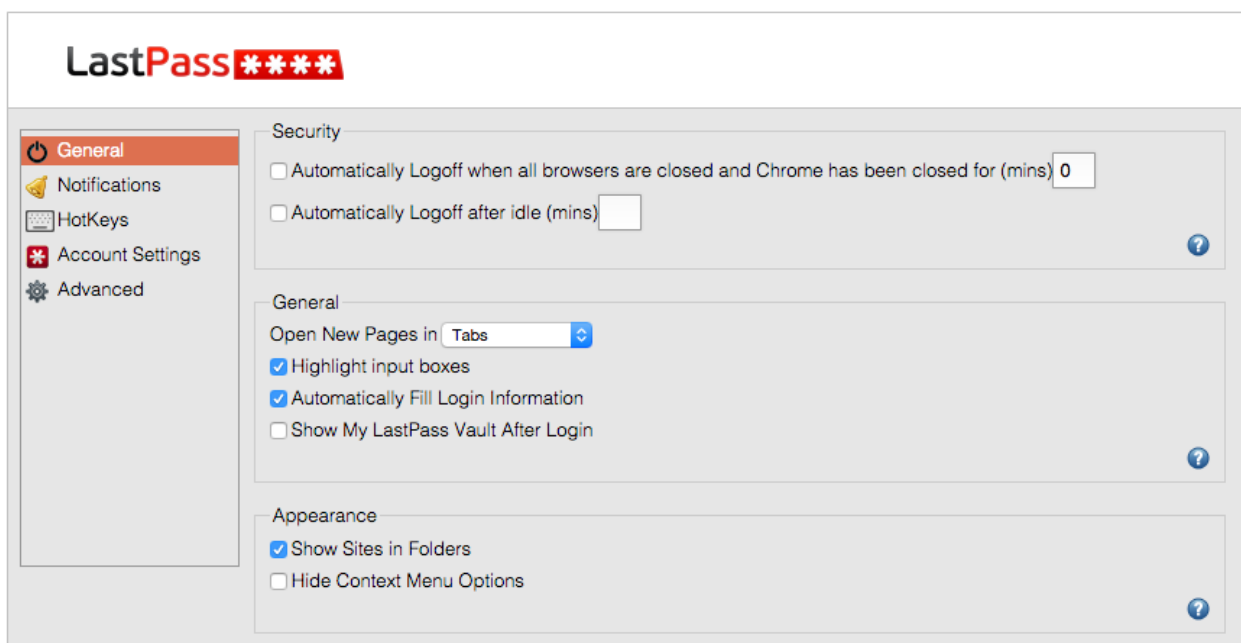
Detailed Results

How it works

If LastPass finds that a website has been compromised and you haven't changed your password, it will email you. I got an email about Adobe's breach with a detailed explanation of what went wrong, what the hackers took and why I should change my password.

Making LastPass More Secure

To make LastPass more secure, click the LastPass extension icon and go to *Preferences*. Here in the *General* tab you can enable options to automatically log off when browser is closed or after a set amount of time.



If you use your computer in a shared office space or you spend a lot of time at cafes, this can act as an added security layer. Because passwords aren't just stolen by hackers from the net, they can be stolen by your co-workers or anyone who can access your laptop.

Increase The Hash Value

We've talked about hashed passwords in the How Hackers Get Hold Of Your Password section. To recap, plain text passwords are hashed in a way that it's almost impossible to revert them to plain text. But some encryption standards are better than others. Hashed passwords go through iterations or cycles of encryption/decryption. The higher the cycle number, the slower it is for hacking software to crack.

Password Iterations (PBKDF2) [Increase Iterations](#)
5000 recommended. [More](#)

Time Zone

Language

Website auto-logout timeout website ONLY, extension auto-logout in [extension preferences](#)

Bookmarklet auto-logout timeout based on last login or last bookmarklet usage

☐ Only allow login from selected countries:

- ☒ India
- ☒ United Kingdom (GB)
- ☐ Afghanistan
- ☐ Aland Islands
- ☐ Albania
- ☐ Algeria

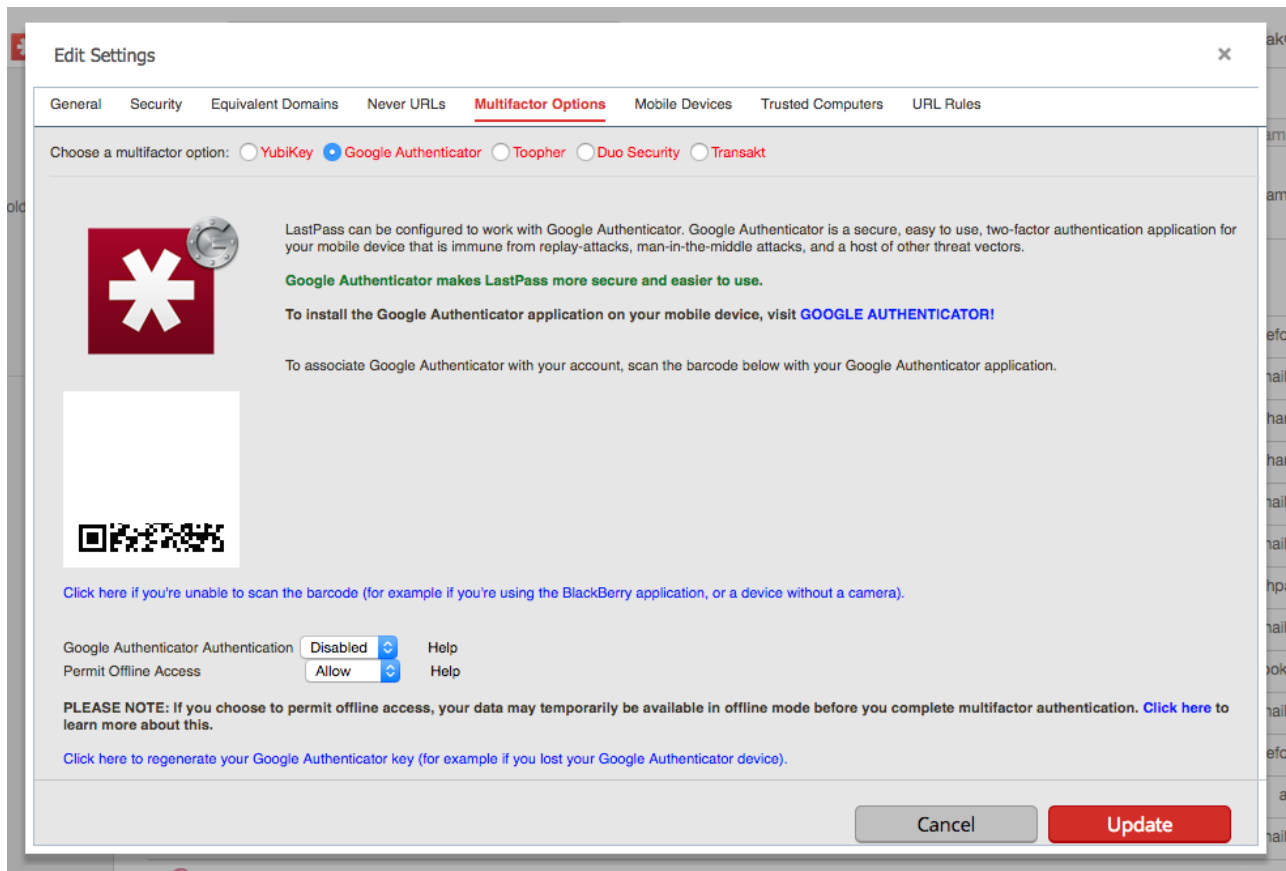
☒ Disallow logins from [Tor network](#)

LastPass uses PBKDF2 protocol from HSA-1 that is slower to encrypt than default protocols. Go to *Settings* from the sidebar on the LastPass website. In the *General* section you'll see a *Password Iterations* option. If you have a new account the default will be 5000 (it's 1000 for old accounts). Increase the iterations to make the password slower for automated apps to crack.

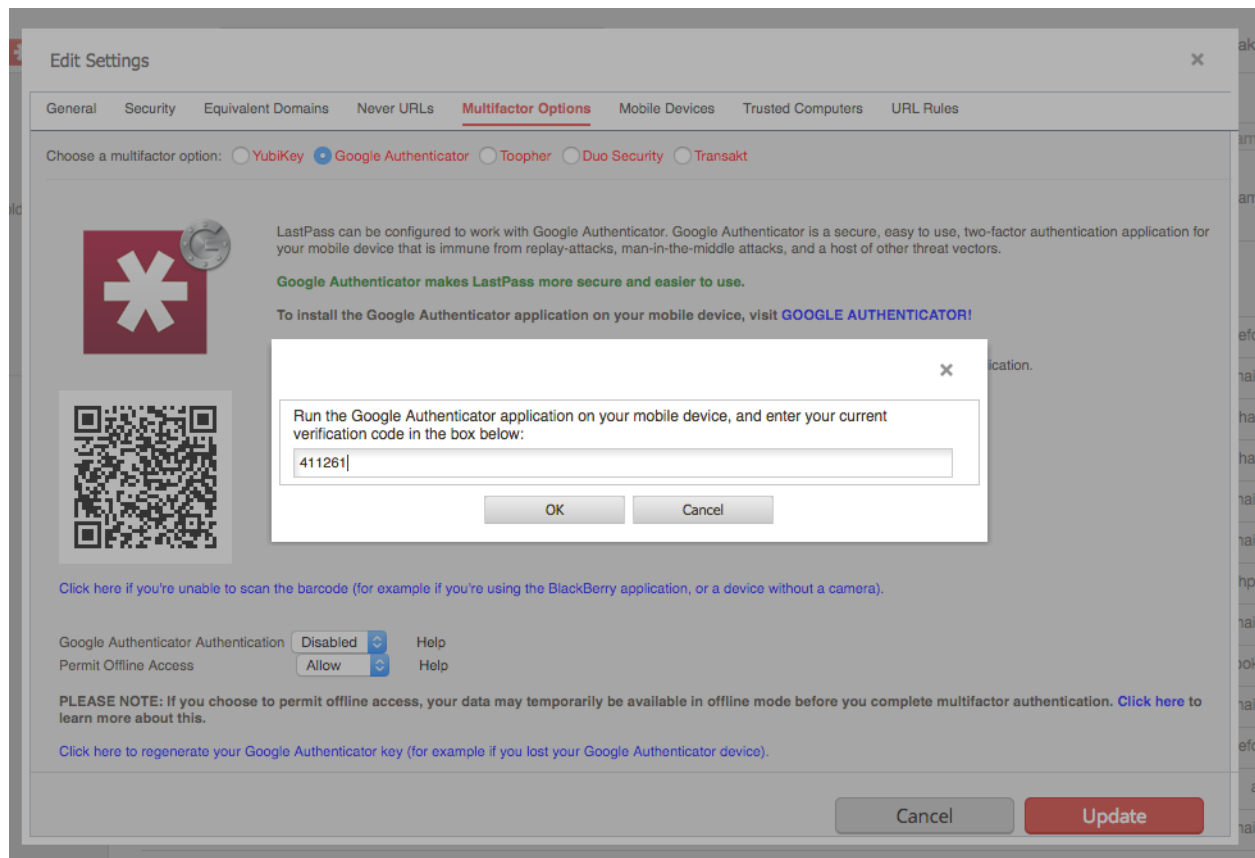
While you can go upto 200,000 cycles, LastPass recommends you don't go above 10,000 cycles because that makes it harder for old IE browsers and mobile web browsers to use.

Enabling 2-Factor Authentication

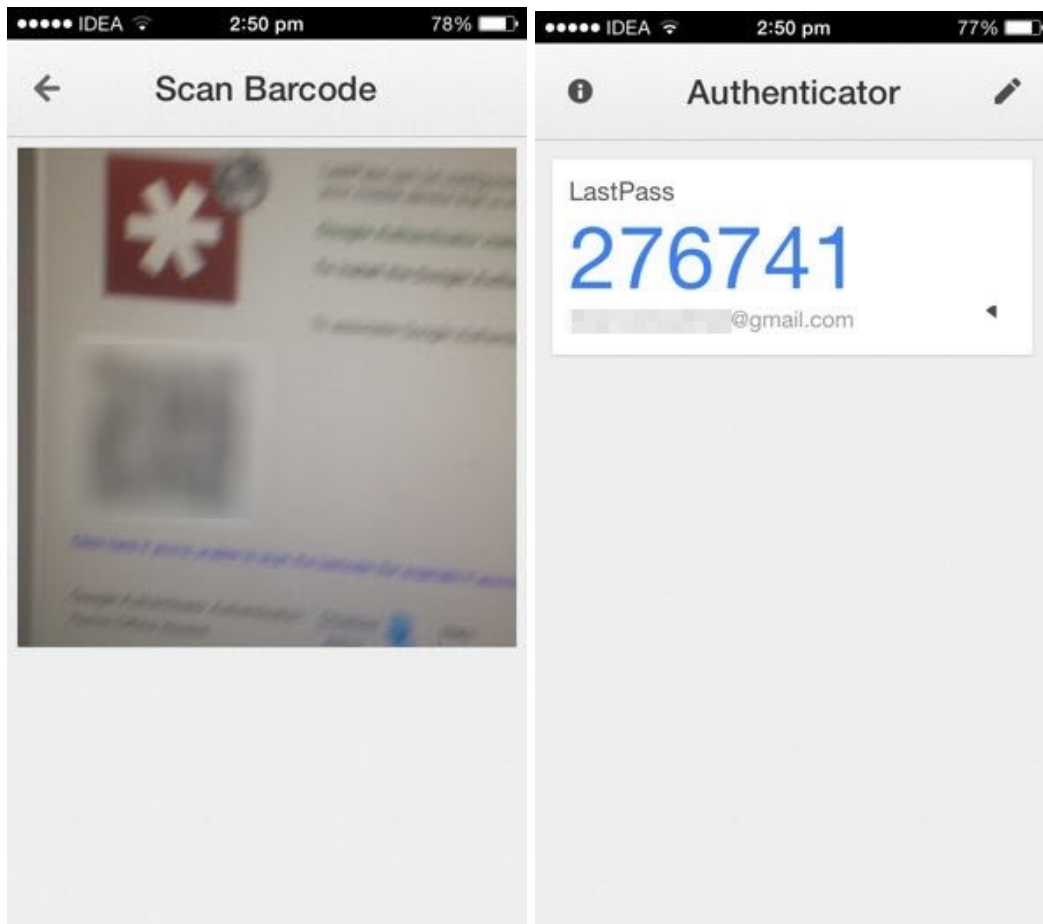
LastPass, just like many other websites, has a 2-factor authentication for the master login. Go to *Settings* from the LastPass website and navigate to *Multifactor options* section.



LastPass provides software and hardware multifactor authentication. You can buy a YubiKey that can be configured to a specific LastPass account. [They cost around \\$60](#) but if you're truly paranoid or your LastPass data is immensely valuable, it might be worth looking into.



The second option is software based authentication and it's more practical. LastPass works with many secure mobile apps like Google Authenticator, Toopher, Duo Security. Google Authenticator is the most trusted option around. Install the app on your iPhone, [Android](#) or even Blackberry phone and the next time you try to log in to LastPass, you'll get a validation code sent to your phone via the Google Authenticator app.



But beware that this is not an SMS, which means it will need internet to work. But if you're already trying to access LastPass website, internet should be available.

Is LastPass Secure?

The answer to that question is not a straight yes or no. LastPass is as secure as a web service in this day and age can be. But that answer is as cryptic as LastPass's encryption.

[In 2011 LastPass noticed a security issue](#) and immediately urged users to change their master passwords. When you're asking a company to save, sync and sometimes even generate passwords for you, the biggest thing you need is trust and transparency. And LastPass delivers on both regards.

In the 2011 incident, the company said that there was no data loss and no accounts were compromised. But this can happen again. You can choose to not

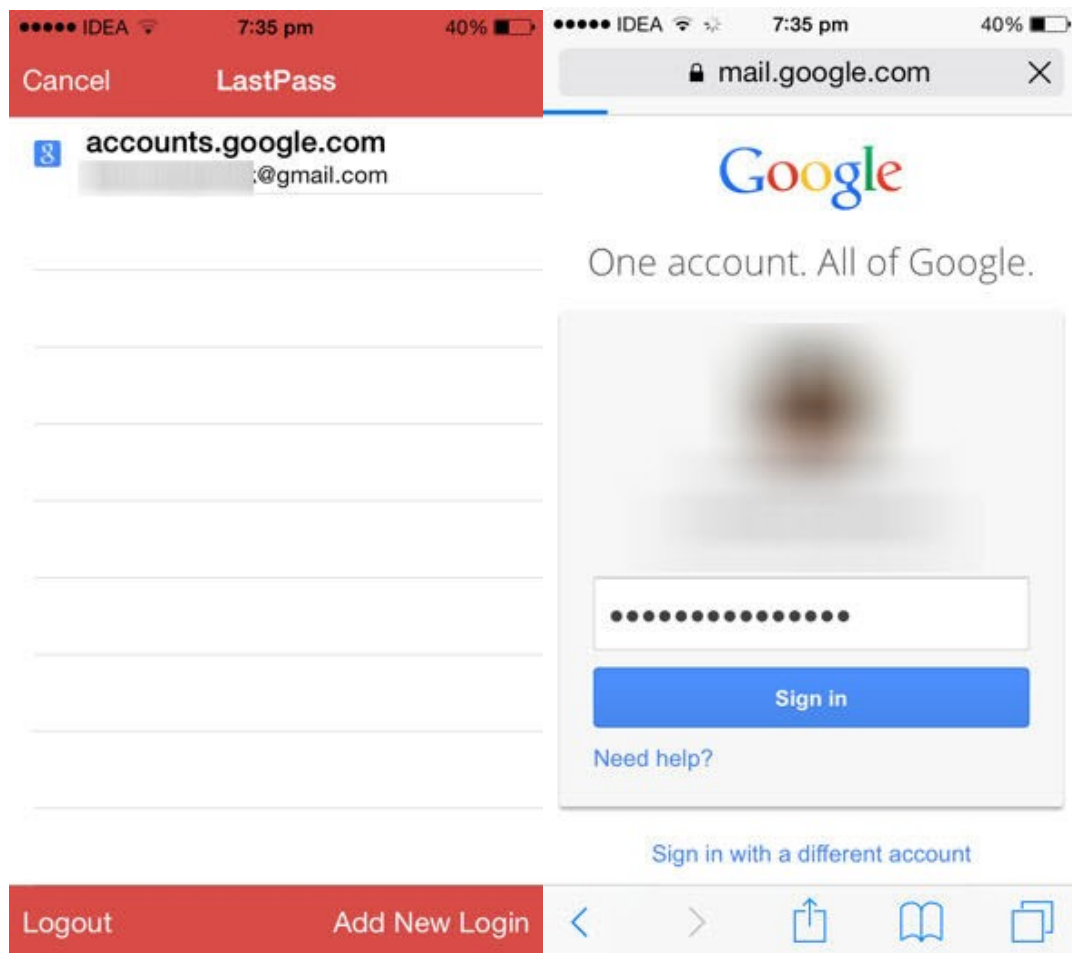
use cloud syncing password managers altogether or you can take steps to make your personal account more secure using 2-factor authentication and other tips given above.

Password Management For Mobile – 1Password for iOS, LastPass Android & iOS



With iOS 8, Apple finally introduced extensions. Once the 1Password and LastPass extensions are enabled, you can go to any page in Safari or Chrome, bring up LastPass or 1Password, open the secure vault using Touch ID or the master password and select the account name and password you want to fill in.

Both apps have APIs that allow developers to add 1Password or LastPass options during app login.



On Android, this is even easier. LastPass's Android app integrates with app login screens directly. There's no need for developers to integrate special functionality like iOS 8. The same goes with in-browser logins. Just as their desktop counterparts, the mobile apps also allow you to generate unique passwords.

LastPass's pricing policy is simple. It's free for desktops but if you want to use it on mobile devices (any number of them), you need to pay for a \$12/year subscription. With iOS 8, 1Password's iOS app is free to use for basic features but it has in-app purchases for pro features. The Android app gives you 1 month free access after which you have to buy a licence. And the 1Password Mac and Windows apps are \$50 each.

How Do You Choose Between 1Password and LastPass?

If you're going to be using it on desktop **and** on iOS or Android, LastPass just makes more sense.

But if you get most of your work down on iPhone or iPad and don't really care about managing passwords on the desktop, go with 1Password.

The Problem With Password Management Apps

When you use a password management app, you're trusting a third party more than yourself. Yes, the apps are heavily encrypted but in case of LastPass, the passwords are stored in a server far away from your reach and knowledge. And just like any other web based service out there, it can be hacked (though not as easily).

When a website like eBay is hacked, you change the password, remove the stored credit card details and you're done. But when LastPass gets hacked, not only do you need to change the LastPass master password, you need to worry about **every single website** that was saved with LastPass.

The question you need to answer is "is it worth the risk?". I'd say it probably is. No password is uncrackable. No system is truly secure. Software can never be bug free. Someone, at some point is bound to find an exploit. But when you use LastPass's encrypted storage along with a strong master password and 2-factor authentication, you've got a fighting chance.

How To Securely Save Passwords Offline And Share Them With Family



If you intend to have your family or friends have access to your passwords in your absence, then here are some ways to save passwords securely offline and also share them when needed.

Write It Down And Put It In A Safe

When technology gets a bit too much for you, you can always go back. As a last resort or the ultimate backup, write down your most important passwords and put it in your safe or a bank locker. Make sure only your most trusted family members get access to it.

KeePass Database In A Pen Drive

As we discussed in the password management section, KeePass is the LastPass without any baggage. KeePass is a simple database app that just stores an encrypted copy of usernames and passwords. The database file can be opened in

KeePass clients for Mac, Windows and even Android. A [portable version of KeePass](#) app also exists.

What this means is you can carry a portable install of KeePass app and a KeePass 2 database file in a pen drive as a backup. KeePass databases can be opened via either a master password or a key file. If this is going to be passed on to someone you know in case of emergency, you can put in the key file in the pen drive as well and eliminate the need to communicate the password.

If having the KeePass database and the key file in the same place doesn't sound too secure, you could always follow the 'put it in a locker' route for the key file too, and store it separately somewhere while ensuring that people you trust have access to it.

Store It In A Cryptic Manner



It's time to add a bit of Indiana Jones (or to be a bit more historically accurate, [Julias Caesar](#)) to our Matrix lifestyle. Going analog with the passwords isn't going to be enough. Because passwords written out one by one in plain text – as is – are enough of a giveaway. Even if you don't specify which accounts they are for, it wouldn't take long for an interested party with time on their hands to figure it out.

Here are a few ways to hide passwords in plain sight (inspired by my favorite treasure hunt movies).

- Form patterns by adding letters at specific positions.
- You can write them backwards as well but that might be easier to figure out than a dedicated pattern.
- Write an essay, on any topic you like and if you're using phrases or words as passwords, hide them in there in plain sight. But then you'll have to remember where to look later on. Or make a key and save it somewhere safe.

Using Passwords on Public Computers: How to be Safe

When you're using a public computer or a cafe's Wi-Fi network, you never know who might be snooping on your data. For safe browsing on a public computer, do the following:

- Use private browsing (incognito) mode.
- Use Windows' built-in virtual keyboard to stay safe from key logging attacks.
- To mask your internet data, use VPN. Apps like [Hotspot Shield](#) and Chrome extensions like Hola can help you out.

Tip

Check out Chrome extensions [that help you browse securely](#) and our coverage on [VPNs](#) to know more.

LastPass One Time Password

If you're using LastPass, it has an OPT function where you can generate a one time password. As the name says, **that password will work only once**. You can generate a log of these passwords and use it when you're accessing accounts on a public computer.

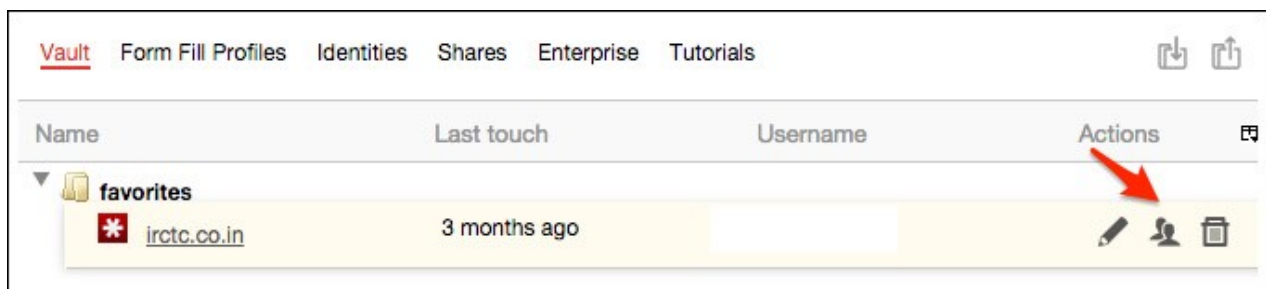
Sharing Passwords With Family With LastPass Premium

If you're a LastPass premium subscriber, you can share passwords with family members easily. Of course, you'll need to have that kind of trust between the people you're readily sharing passwords with. But in case of emergency, it's better to give your loved ones access to important things like bank passwords or credit card details beforehand.

You can escape weak passwords but not death. ReadWrite has a great round up on [how to prepare for death in the digital age](#).

Before getting started, make sure your significant other already has a LastPass account set up.

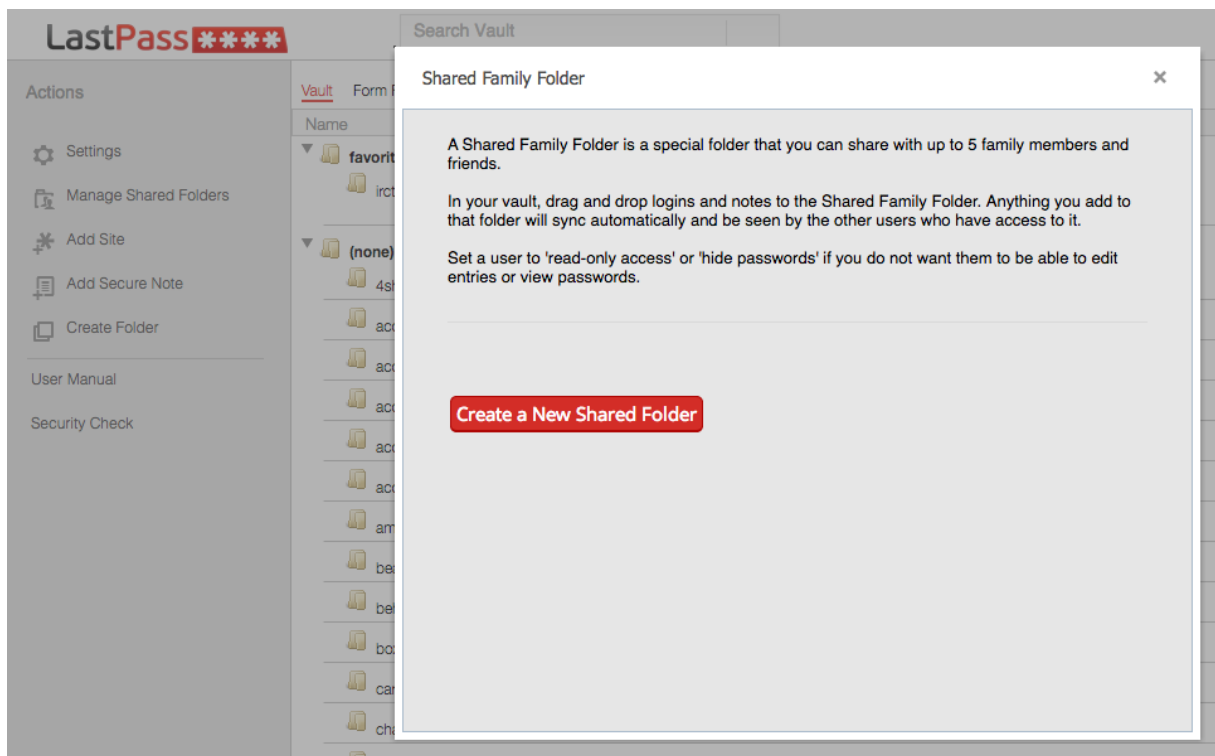
Now go to your LastPass vault and next to a website you'll find a *Share* button.



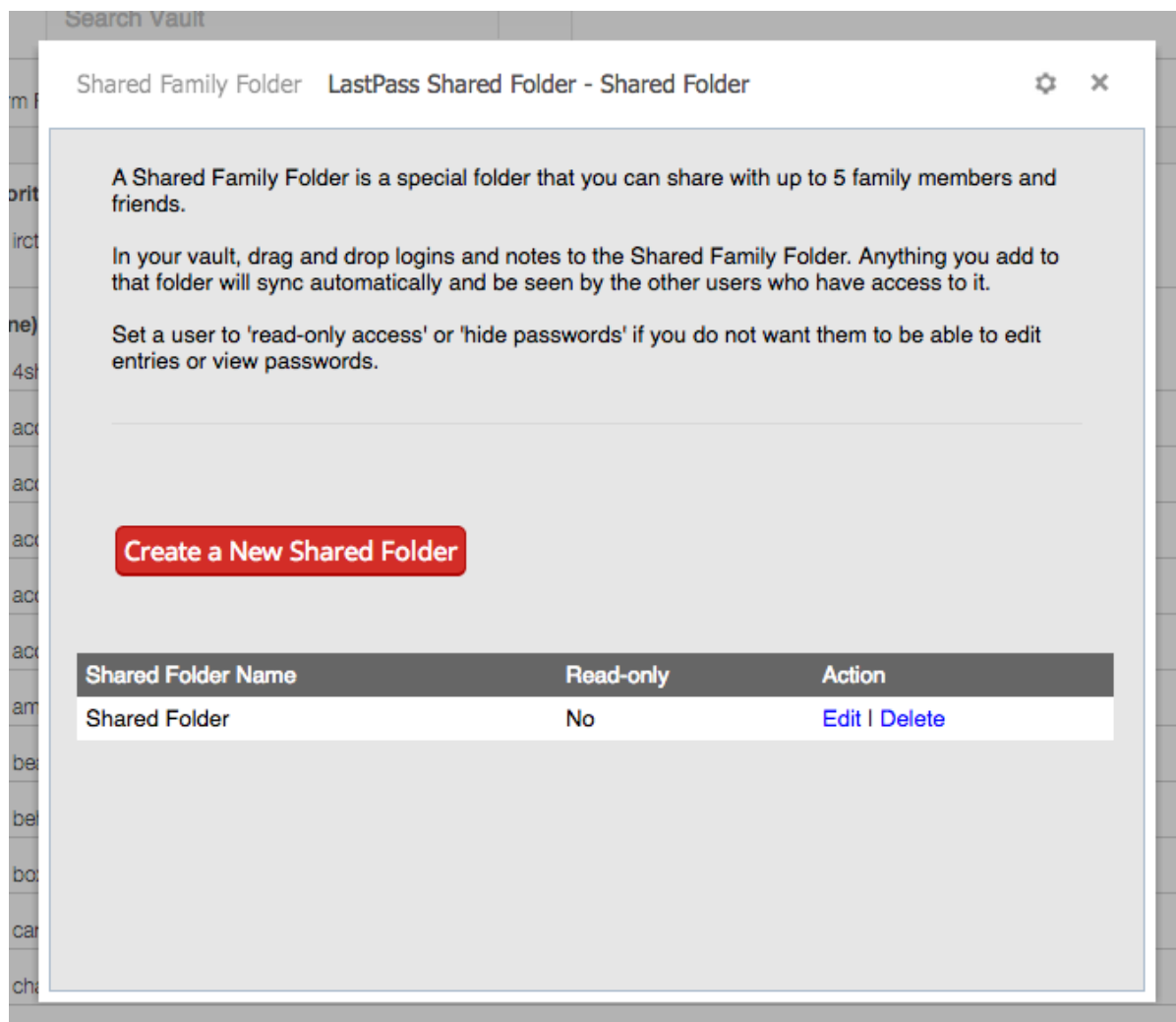
Add the email of the person you want to add and click *Share*.

If they already have a LastPass account, they'll receive a sharing invitation that they can choose to accept.

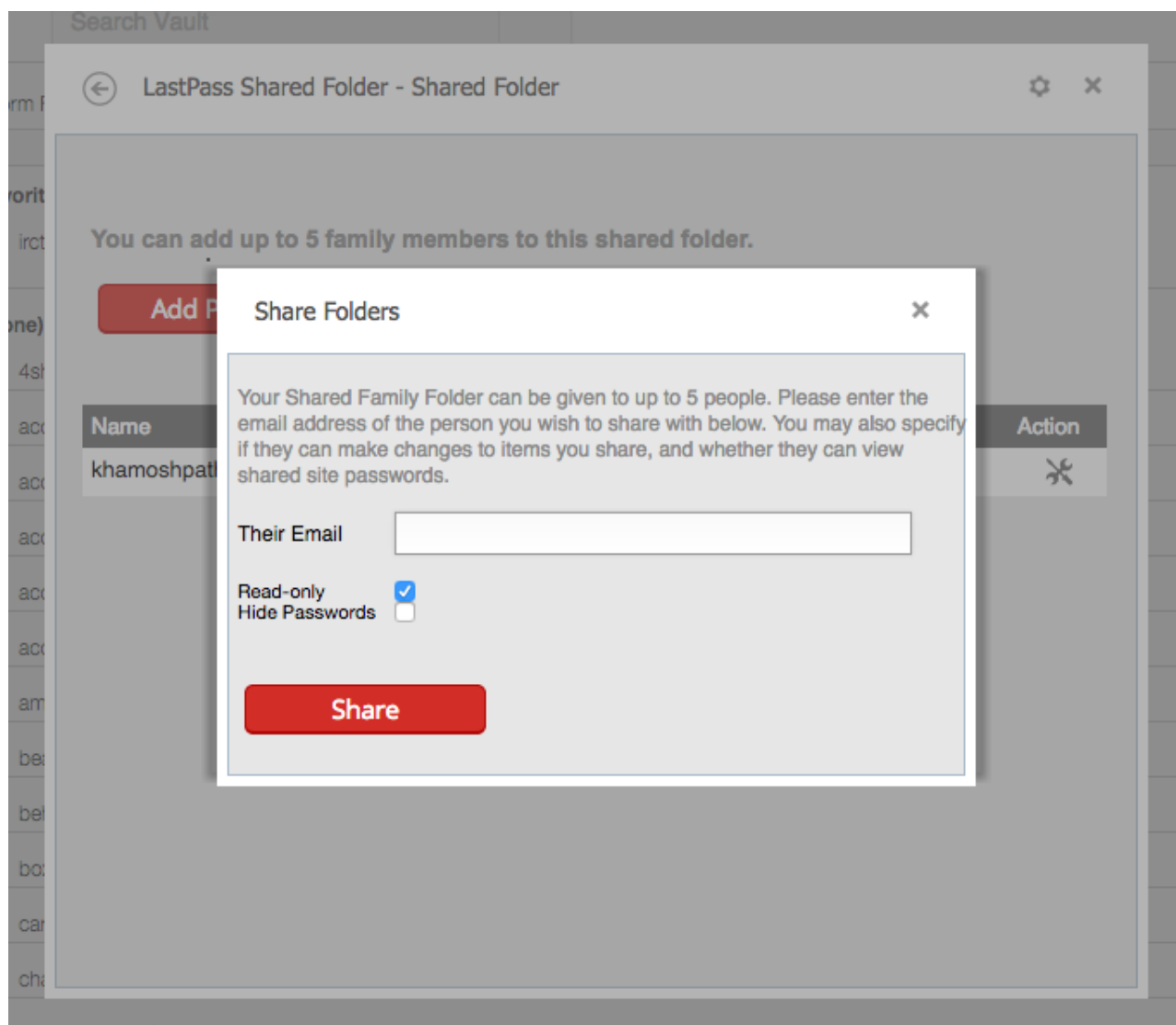
To create a shared folder, go to LastPass's website, log in and from the sidebar select *Manage Shared Folder -> Create New Shared Folder*.



Give the shared folder a name and now from the *Action* menu, select *Edit*.



From here input the email addresses of your family members. You can add up to 5 of them.



The great thing about LastPass's shared folders is that you can share specific sites like your iCloud login or bank details but choose to keep Gmail or other work related stuff personal.

Conclusion- Practical Solutions To Today's Password Management Problems

In the past few pages, you've learned what makes a strong password, the different methods hackers use to crack passwords and how you can be safe from them. There's a lot of advice back there, some varied, some contradicting. Like every other technology problem, there is no one true answer. There is no "one ring to rule them all". If there is, I'm sure it's resting deep inside Mordor.

In this concluding section, I want to offer practical solutions and some alternatives to how you currently manage your passwords. Alternatives that strike the right balance between security and practicality.

Here's the TL;DR.

1. You Can't Create Strong Passwords For Every Single Site..

Currently my LastPass account is filled with more than 100 sites. And that's just the sites I found important enough to save. The number of apps and web services have exploded in the recent years and creating a strong password pattern to include all of them might not be feasible.

And this problem leads us to the next one: Remembering them all.

2. And You Can't Remember Hundreds of Unique Passwords.

But you certainly **need** unique passwords. Having the same password for any two services is never recommended. Never.

3. So Prioritize the Most Important Accounts...

What's most dear to you? Which passwords do you reset when you realize your phone has been stolen?

Select 10-12 of the most important websites and assign them strong passwords. Ones that can survive both brute force and social engineering/guessing attacks. Again, don't make them too complicated. If your wife wakes you up at 3 AM to ask for your bank login and if there's a sale going on (believe me she will one day), your reply shouldn't be "let me fire off LastPass real quick".

Even when you can access LastPass/1Password, these passwords should be something you always remember.

4. And Let A Password Manager Take Care Of The Rest.

After Caramel Frappuccinos, password manager is another thing you can't live without. At this rate of development, you're not going to stop trying new web services, apps or platforms.

And remembering every single password for each of these accounts is just not possible (unless you are using the same password everywhere which, as we've established, is a rookie mistake).

So what do you do? Let LastPass or KeePass or 1Password take care of it. All of it. Let them generate a long (12-15 character), unique password for you. They will also save this password so the next time you want to log in, either on the desktop or on your phone, it will already be filled out.

5. And Please, Oh Please Use 2-Factor Authentication

Again, you don't need to use this on every single site. Just the ones that are important to you. Once 2-factor authentication is enabled, you'll get a 6 digit SMS code on your phone every time you try to log in on a new machine. And most websites let you save a login for 30 days. Which means if you log in and out of Gmail fairly often, you won't have to wait for a confirmation code every time, just once a month.

2-factor authentication, or as I like to call it "the wall" stops hackers from gaining access to your account even if they've managed to crack your password. Because the final piece of the puzzle is on your phone, physically close to you.

Wrap Up: The Internet Security Manifesto

Internet has made us lazy.

I have a theory that more than sophisticated hacking software, security loopholes or just plain guessing, our laziness is the biggest threat to our internet security.

Everything is so much easier now. We stream movies instead of renting them from stores, we check our friend's Facebook statuses instead of having an actual conversation.

Sure internet **has** made our lives easier. Bills are paid online. You don't need to wait in lines to file your taxes. Information has never been easier to exchange. Some people don't even need to travel to an office to work. You can start a business from your laptop and turn it into something profitable.

But internet also forces us to take things for granted. Because for the most part, things on internet are supposed to "just work". When you click the *Send* button in Gmail, you know it will be sent.

The problem is that we as consumers have little to no idea what's going on back there, on a website's server.

Ignorance also plays a big role. "It won't happen to me." "My data isn't that important anyway." "I've got nothing to hide." "I **hope** my journal gets hacked, at least someone will read my writing." I've said it all to myself.

In the weeks I spent researching, testing and writing this ultimate guide, my attitude towards internet security changed. I realized that big multinational corporations are just as susceptible to hacks as the small guys.

If you can't always put 100% trust in a company that stores your important and personal data, what do you do? Take matters in your own hands. Do as much as you can. The purpose of this neatly designed, 9000 word guide isn't only to make you aware; it's also to urge you to take steps in the right direction to manage and secure your passwords.

So, if you haven't started with it yet, now would be a good time.

About Guiding Tech

[Guiding Tech](#) is a blog that publishes descriptive how-to articles, guides, lists and tips that make the life of an everyday computer and mobile phone user easier and fun.

[Visit our about page](#) to know more about what we do and the team behind GT. Also go through [our other eBooks](#).

About the author



Khamosh Pathak is a staff writer at Guiding Tech and has a passion for all things tech. He loves keeping himself abreast with the latest developments in the field of personal technology and has fun writing about them.

He's also a podcast freak and a wine aficionado. When not indulging in geeky stuff, he can be found reading a book on his Kindle Paperwhite or biking around the city while listening to his favorite podcasts.

Image Credits

- <http://www.shutterstock.com/pic-178664063/stock-photo-female-hands-using-tablet-pc-protected-with-password.html>, shutterstock, page 4
- <http://www.shutterstock.com/pic-200320085/stock-photo-silhouette-of-a-hacker-uses-a-command-on-graphic-user-interface.html>, shutterstock, page 7
- <http://www.shutterstock.com/pic-178605110/stock-photo-phishing-fish-hook-in-an-envelope-email-phishing-spam-mail-computer-threats.html>, shutterstock, page 8
- <http://www.shutterstock.com/pic-151558676/stock-photo-safety-first-sign-on-caution-strip.html>, shutterstock, page 11
- <http://www.shutterstock.com/pic-175540514/stock-photo-lisbon-portugal-february-photo-of-icloud-homepage-on-a-monitor-screen-through-a.html>, shutterstock, page 14
- <http://www.shutterstock.com/pic-209983420/stock-photo-simferopol-russia-july-touch-id-the-scanner-of-fingerprints-developed-by-apple.html>, shutterstock, page 16
- <http://www.shutterstock.com/pic-161451770/stock-photo-warning-road-sign-cyber-attacks-ahead.html>, shutterstock, page 23
- <http://www.shutterstock.com/pic-132593639/stock-photo-password-security-for-safety-from-mobile-phone.html>, shutterstock, page 51
- <http://www.shutterstock.com/pic-156979568/stock-photo-close-up-of-a-safe-lock-with-blur-effect-and-focus-on-the-number-one-blue-tones-conceptual-image.html>, shutterstock, page 55
- <http://www.shutterstock.com/pic-200144711/stock-photo-blue-cryptography-encoding-screen-computer-binary-code-pixels-background-raster-copy-of.html>, shutterstock, page 56