the password management guide

By Mohammed Al-Marhoon
Table Of Contents

1. Introduction 5
   1.1. What is password management? 5
       1.1.1. Password Forms: 5
   1.2. Your Scenario 6
   1.3. Why? 6
   1.4. Password Breaching/Cracking Stories 6
2. Threats Against Your Passwords 7
3. Common Mistakes 9
4. Useful Tips 10
5. How to Make a Strong Password 11
   5.1. Mozilla’s Methodology 11
   5.2. Microsoft’s Tips 11
   5.3. Google’s Safe Password Methodology 12
   5.4. Putting it all together 12
6. Haystacking Your Password 13
7. Math Behind Password Length & Complexity 14
8. Test Your Password’s Strength 16
9. Password Management Techniques 18
   9.1. Algorithms 18
       9.1.1. Tiered Password System 18
       9.1.2. Password Tree 18
   9.2. What is Password Manager? 18
   9.3 Types of Password Managers 18
       9.3.1. Standalone: 18
       9.3.2. Web-Based 19
   9.4. Examples of Password Managers 20
       9.4.1. KeePass 20
       9.4.2. Mozilla Firefox’s Password Manager 24
10. Two-Factor Authentication 27
11. HTTPS: Added Security 28
12. Password Management Examples 29
13. How to Protect Your Passwords?  
14. Security News  
Security Now  
PwnedList  
15. Points to Remember (Recommendations)  
16. MakeUseOf Links  
Conclusion
1. Introduction

We are all overwhelmed by passwords. Everyone has an account for Google, Facebook, Twitter, LinkedIn, Outlook/Hotmail, Dropbox... the list goes on. Unfortunately, most of us use either one password or a group of passwords for all of our major accounts.

That’s dangerous.

It doesn’t matter if the individual password is unique, or if it’s a long mix of numbers and letters; if you only use one password it won’t matter. When one account is compromised, all of your accounts will likely follow.

The main reason people reuse passwords is that keeping track of many different logins (username and password as shortly both are called logins) is difficult, in fact it’s potentially impossible. This is where password management applications become crucial, especially in a business environment.

You don’t want to use the same password with all of your online accounts, but it is also impossible for you to remember hundreds of passwords. So what should you do?

In this manual, I list all of the steps that may help improve the overall security of your accounts. You will be exposed to a set of rules about how to create a strong password [1.1] to prevent security compromises, and you’ll read a bunch of tips and resources designed to help strengthen your information security.

DON’T PANIC: This manual is not solely for tech-savvy users. Everyone who is concerned about their information security should be able to follow along easily. So what are you waiting for? Read this guide and start improving your password security.

1.1. What is password management?

You know what a password is: it’s a set or string of characters that gives you access to a computer or online account. And management is simply the process of dealing with or controlling things. Consequently, password management is simple to grasp: it’s a set of principles and best-practices that help a user create, change, organize and control passwords so as to be as secure as possible.

1.1.1. Password Forms:

You may hear different terms like passphrase, PIN and password. Many people use them interchangeably, but they differ from each other. For clarity, passphrase and PIN are two different forms of passwords. A passphrase is a specialized form of password that is relatively long and consists of a sequence of words, such as a phrase or a full sentence. “I Luv2readMUO” is an example of a passphrase. PIN stands for Personal Identification Number. Unlike passphrase, it is relatively short (usually 4 to 6 characters) and consists of only digits. An example of a PIN is “1234.”

In the past, it was common for a password to be just one word, usually at least 8 characters long. People used to use their middle name, their pet’s name, the name of their favorite movie or almost anything else as passwords. This concept has been completely changed. When we say password, then we often mean both regular passwords and passphrases.
THE PASSWORD MANAGEMENT GUIDE

Throughout the rest of this guide, PINs will be out of scope and I will mainly discuss the password which is the string of characters that we mostly use everywhere.

1.2. Your Scenario

How many passwords do you have?

Let’s assume that you created your first password when you opened a bank account: a 4-digit PIN code. Soon after that you created another password for your email (most online mail clients don’t allow you to create password with 4 characters, so you cannot reuse your PIN). You came up with something like “12345678,” a passphrase like “John1234,” or a short sentence from your favorite song. After that, you were required to have a password for credit cards, SIM card(s), social networking sites, forums… again, the list goes on, and each new service may require a password.

So what are you going to do? For most people the solution is using the same password multiple times, and using something easy to remember like “12345678.” These are both (common) mistakes. So what is the solution?

1.3. Why?

Passwords are the keys to accessing your computer, bank account and almost everything you do online [1.3]. In other words passwords are the primary means of authenticating a user (authentication being the process of verifying who somebody is). They provide the first line of defense against unauthorized access to your sensitive data. Human memory acts as the safest database – or password manager – for storing all of your passwords.

You may have a good memory. However, with dozens of different websites all requiring their own password for security, is your memory up to the task? For most people memory is not a scalable solution, so if you want to be secure you’re going to need to implement a system for storing your passwords securely. This manual aims to provide you with different techniques for creating strong, easy-to-remember passwords for each one of your accounts.

1.4. Password Breaching/Cracking Stories

A Password Breach is an incident when someone not authorized to do so breaks a password or hacks a database in which passwords are stored, and they’re more common than you may think. Twitter announced in February 2013 that it had been breached, and that data for 250,000 Twitter users was vulnerable. A number of high-profile breaches occurred in 2012; here are a few examples:

Zappos.com, the well-known online shoes and clothing shop, announced in January, 2012 that its customer information database has been hacked and millions of its users’ login credentials were compromised.

Yahoo announced that over 450,000 email addresses and passwords of Yahoo Voices’ users were stolen and revealed (or posted online) by hackers.

LinkedIn confirmed that millions of LinkedIn passwords have been compromised. And here’s a must-see link that shows a self-explanatory infographic which highlights the 30 most popular passwords stolen from LinkedIn.

EHarmony, the famous online dating service, announced that some of its members’ passwords have been affected.

The list of hacks is always growing, and should prompt you to ask questions. For example: If I use the same password for all sites (and one of them is leaked) will hackers simply be able to re-use my password for all services? (Yes.) Are there upcoming hacks? (Yes). If yes, which services will be hacked? (Impossible to say). When? (Again, impossible to say). Will my password be involved in the next breach? (Maybe). Are my passwords strong enough? (Probably not). Should I change them? (Yes. Often.)

These recent hacks serve as a warning – and a call to action. It’s time to review and evaluate all of your passwords, and change any that seem weak or that you have used for more than one site. The following parts of this manual will answer and discuss most of your concerns. Go through them and share your feedback after reading.
2. Threats Against Your Passwords

Similar to what is explained in The Simplest Security: A Guide To Better Password Practices, password cracking is the process of breaking passwords in order to gain unauthorized access to a system or account. And password breaching, as defined earlier, is generally the result of password cracking. Passwords can be figured out, broken, determined or captured through different techniques such as guessing and social engineering techniques.

**Guessing:** a method of gaining unauthorized access to a system or account by repeatedly attempting to authenticate – using computers, dictionaries or large word lists. A Brute Force is one of the most common forms of this attack. It is a method of guessing a password by literally trying every possible password combination. A Dictionary Attack is a similar technique, but one based on entering every word in the dictionary of common words to identify the user’s password. Both of these are very similar, but the following table clarifies the main differences between them:

<table>
<thead>
<tr>
<th>Brute Force</th>
<th>Dictionary Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>use every possible password combination of characters to retrieve the password</td>
<td>use every word in a dictionary of common words to identify the password</td>
</tr>
<tr>
<td>large number of password combination</td>
<td>certain number of common keys</td>
</tr>
<tr>
<td>time of cracking depends on the password strength (length and complexity)</td>
<td>time of cracking is depends on the number of common passwords, so it’s a bit faster than a brute force attack.</td>
</tr>
</tbody>
</table>

**Social Engineering:** the art of gaining sensitive information or unauthorized access to a system or account by taking advantage of human (user) psychology. It is also known as the art of deception. In reality, companies are typical targets of social engineering and it is more challenging to manage by IT organizations. Why? Because it relies on the fact that users are:
• naturally helpful, especially to someone who is nice or they already know
• not aware of the value of the information they possess
• careless about protecting their information

For example: an employee in an enterprise may be tricked into revealing his username and password to someone who is pretending to be an IT help desk agent. You can imagine why social engineering is a very successful way for a criminal to get inside an organization: it is often easier to trick someone than to gain unauthorized access via technical hacking.

Phishing attempts are a common example of social engineering attacks. For instance: an email or text message that appears to come from a well-known or legitimate organization, such as a bank, to notify you that you are a winner and they need some personal details (such as your phone number and address) so they can send you the prize. Social engineering relies on weaknesses in humans. So please remember: DO NOT share your passwords, sensitive data and confidential banking details on sites accessed through links in emails.

For more in-depth information about threats against passwords, please read the following resources:

• Guide to Enterprise Password Management (Draft)
• THE RISK OF SOCIAL ENGINEERING ON INFORMATION SECURITY: A SURVEY OF IT PROFESSIONALS
• What Is Social Engineering? [MakeUseOf Explains]
• How To Protect Yourself Against Social Engineering Attacks
3. Common Mistakes

The previous chapter highlighted ways in which our information is vulnerable. What mistakes make this vulnerability worse? The following table shows you the most common mistakes you might be making:

<table>
<thead>
<tr>
<th>Mistake</th>
<th>Example</th>
<th>Risk Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using a Common Password.</td>
<td>123456</td>
<td>Too risky. These are most criminal's first guesses, so don’t use them.</td>
</tr>
<tr>
<td></td>
<td>12345</td>
<td></td>
</tr>
<tr>
<td></td>
<td>123456789</td>
<td></td>
</tr>
<tr>
<td></td>
<td>password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>iloveyou</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the six letters on any row of a keyboard. For example, the first six letters on the top row of the keyboard “qwerty.”</td>
<td></td>
</tr>
<tr>
<td>Using a Password that is based on personal data (often called an easy-to-guess password).</td>
<td>Gladiator</td>
<td>Too risky: anyone who knows you can easily guess this information.</td>
</tr>
<tr>
<td></td>
<td>“Bobby”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>“Jenny”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>“Scruffy”</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Real Madraid or RealMadraid</td>
<td></td>
</tr>
<tr>
<td>Using a Short Password</td>
<td>John12</td>
<td>The shorter a password, the more opportunities for observing, guessing, and cracking it.</td>
</tr>
<tr>
<td></td>
<td>Jim2345</td>
<td></td>
</tr>
<tr>
<td>Using the same password everywhere.</td>
<td>Using one password on every site or online service.</td>
<td>Too risky: it's a single point of failure. If this password is compromised, or someone finds it, the rest of your accounts – including your sensitive information – are at risk.</td>
</tr>
<tr>
<td>Writing your password(s) down.</td>
<td>Writing your password down on a post-it note stuck to your monitor, keyboard or anywhere.</td>
<td>Very high risk, especially in corporate environments. Anyone who physically gets the piece of paper or sticky note that contains your password can log into your account.</td>
</tr>
</tbody>
</table>

Google “Common Password Mistakes” and you’ll find hundreds of results and resources describing different kinds of mistakes – nearly all of which fall into the mistakes mentioned in the above table.

Well, what should we do now to avoid the threats against passwords? And are there any instructions or security procedures to follow to create a strong password without making any one of these common mistakes?
4. Useful Tips

Before discussing the methodologies of how to make a strong and easy-to-remember password, let us have a look at general useful tips which are the cornerstones of any methodology of making a strong password. There are many references – on MakeUseOf and the wider Web – that cover this topic. Here I am trying to go over the most common suggestions.

IMPORTANT: your password should be at least 8 characters long, and it is highly recommended that it’s 12 characters or more.

Select a password that contains letters (both uppercase and lowercase), numbers and symbols.

<table>
<thead>
<tr>
<th>Category</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uppercase letters</td>
<td>A, B, C, D</td>
</tr>
<tr>
<td>Lowercase letters</td>
<td>a, b, c, d</td>
</tr>
<tr>
<td>Numbers</td>
<td>0, 1, 2, 3, 4, 5, 6, 7, 8, 9</td>
</tr>
<tr>
<td>Symbols</td>
<td>! @ # $ &amp; * : ; . ? /</td>
</tr>
</tbody>
</table>

Do not use names or words found in the dictionary.

For business accounts, use a separate unique password for each major service and make sure that none of these passwords are the same as those associated with personal accounts. For example: the password to access your workstation should be different from the password for your personal Google account.

Always enable “HTTPS” (also called secure HTTP) settings in all online services that support it – this includes Twitter, Google, Facebook and more.

Don’t use easy password security questions. In fact, security questions are one of the major weaknesses in email security. Anyone close to you – anyone who knows you – can easily answer the following common security questions:

- What is your mother’s maiden name?
- What is your cat’s name?
- What is your hometown?

These tips all help, but you may come up with a password that meets a few of the points above and is still weak. For instance, as Microsoft mentioned on its website, Welcome2U!, Hello2U!, and Hi2U? are all quite weak, despite including uppercase letters, lowercase letters, numbers and symbols. Each one of them contains a complete word. On the other hand, W3l4come!2?U is a stronger alternative because it replaces some of the letters in the complete word with numbers and also includes special characters. This isn’t foolproof, but it is better than before.
5. How to Make a Strong Password

“Treat your password like your toothbrush. Don’t let anybody else use it, and get a new one every six months.” ~ Clifford Stoll

Before we go any further, keep in mind the following: The stronger your password, the more protected your account or computer is from being compromised or hacked. You should make sure you have a unique and strong password for each of your accounts.

Indeed, there are many articles and suggestions on how to choose strong and easy-to-remember passwords for your various online accounts. Most of these suggestions or methods, if not all of them, agree on the rule of creating passwords based on a mnemonic, such as an easily remembered phrase. However, they have some minor differences in the way they combine the useful tips mentioned above by adding some layers of security to make the password stronger. Let’s summarize these methods, for easy reference.

5.1. Mozilla’s Methodology

Mozilla has published a very useful article, including an animated video, titled “Create secure passwords to keep your identity safe”. The ideas, in a nutshell, are:

Pick up a familiar phrase or quote, for example, “May the force be with you” and then abbreviate it by taking the first letter of each word, so it becomes “mtfbwy”

Add some special characters on either sides of the word to make it extra strong (like #mtfbwy!)

And then associate it with the website by adding a few characters from the website name into the original password as either a suffix or prefix. So the new password for Amazon could become #mtfbwy!AmZ, #mtfbwy!FbK for Facebook and so on.

5.2. Microsoft’s Tips

Microsoft offers an a lot of security information, which forces you to think seriously about the strength of your passwords. Microsoft's tips for creating strong passwords are very similar to Mozilla’s tips, but also highlight four areas to take into consideration; Length, Complexity, Variation and Variety.
We have already explored the first two. For variation, Microsoft has emphasized the importance of changing your password regularly (about every three months). Variety is mainly about avoiding password reuse, which leaves all accounts vulnerable if one is compromised. A study done by researchers in the Security Group at the University of Cambridge Computer Laboratory shows that the rate of comparing stolen login credentials (hashed passwords) for two different sites was as high as 50 percent. So never ever use the same password twice – try to always have different passwords for different accounts for websites or computers.

5.3. Google’s Safe Password Methodology

A part of Google’s recent advertising campaign for online safety, “Good to Know”, is instructions for picking a safe password for each of your accounts. The idea in brief, as Sara Adams mentioned in this short video, is to choose a sentence or line (that you can easily remember) from your favorite song, film etc. Then take the first letter of each word and then try to mix it with numbers and special characters (symbols) and mix letters to constitute your strong but easy-to-remember password. The more unusual the phrase you choose the better. “Good to Know” is a great rich educational campaign and resource that mainly aims to spread awareness of online safety and privacy. Keep your online accounts secure is another amazing video that shows you how to boost your security.

5.4. Putting it all together

While generating a password you should follow two rules; Length and Complexity. Let’s start by using the following sentence: “I like to read MakeUseOf blog everyday”. Let’s turn this phrase into a password.

Take the first letter from each word: IltrMUObes. I will take the letter “d” by considering everyday as two words and in order to lengthen the password. So it will become like IltrMUObed.

Now increase its strength by adding symbols and numbers:

20Iltr.MUO_bed?13

OMG! What is this difficult password?! It is impossible to remember and who is going to add numbers and symbols like this? Wait a minute… I did not add any numbers and I did not put the symbols randomly. Let us analyze this password more fully:

20Iltr.MUO_bed?13

Firstly, 20 and 13 refer to the year, 2013. Secondly, I put a symbol after each three places or characters. What did you notice? Yes, it is a pattern. Design your own special pattern. You may want to use my exact pattern as your base password for most of your online accounts – don’t. Think of your own. But if you would like to go with this option as a base password, then do yourself a favor by rotating portions of your passwords, changing the order, or at the very least using the name of your online account in the password.

20Iltr.MUO_bed?13Gmail

fb20Iltr.MUO_bed?13 (for Facebook)

20Iltr.MUO_bed?13Tw (for Twitter)

2013Iltr.MUO_bed?Li (for LinkedIn)

That's one password developing strategy. Let's keep adding complexity, while also attempting to keep things possible to memorize.
6. Haystacking Your Password

This technique was developed by security guru Steve Gibson, president of Gibson Research Corporation (GRC). Password Haystack is a methodology of making your password extremely difficult to brute force by padding the password with a pattern like (////) before or/and after your password. Also, Gibson designed a clever interactive calculator, Brute Force Search Space Calculator, which you can use to test the potential of your password. It will show how long it would take for different entities to crack your password, while showing you why your password is either weak or strong based on some mathematical calculations. So how to use this technique?

Here’s how it works:

• **Come up with a password, but try to make it as a mix of uppercase and lowercase letters, numbers and symbols**

• **Come up with a pattern/scheme you can remember, such as the first letter of each word from an excerpt of your favorite song or a set of symbols like (…..////)**

• **Use this pattern and repeat using it several times (padding your password)**

Let’s have an example of this:

**Password:**

I.lto!MUO2012

By applying this approach, the password becomes a **Haystacked Password:**

…../////I.lto!MUO2012…../////  

So for your Facebook account, the password might be:

**fb…../////I.lto!MUO2012…../////**

Further examples of this technique:

818818818JaNe!!

JaNe9999999999//

You get the idea.

It is very easy to insert your password in a container (or a haystack). Now, let us test the strength of the Facebook account’s password by using the brute force search space calculator:

This technique solves two aforementioned problems, which are:

The more complex your password is, the harder it is to remember for the user, and the more likely it will be written down and lost

The most frustrating thing to users is the required regular changing of the password for security reasons, especially in an organization.
7. Math Behind Password Length & Complexity

There are many articles on the web about whether length or complexity is the most important part of a password. You might be wondering: why is it always recommended (or even required) for passwords to be at least 8 characters, and to be a combination of letters, numbers and symbols? And why do others insist that length alone is important? The truth is you have to consider both length and complexity while creating any password. The reason for this is made clear by the following formula:

\[ X^L \] (X to the power of L)

where \( X \) is the number of possible characters that can be in the password and \( L \) is the length of the password.

Roger A. Grimes wrote a fascinating article (Password size does matter) on the analysis of this formula. I will try to keep it simple and not bore you with the pure math calculations. Think back to the most widely used method of cracking passwords, brute force, where all possible combinations of characters are tried one by one in an infinite series of guesses until your password is discovered. The following analysis shows you how both length and complexity affect the password strength, by illustrating the many possible combinations in each number of letters.

Let us focus on passwords of 2 characters. If the password consists only of two letters then we have the following analysis:

- **Password length = 2 characters**
- **First character = lowercase letters (26 possibilities) + uppercase letters (26 possibilities) = 52**
- **Second character = 52 (same as first character)**
- **Total = 52^2 = 52 * 52 = 2704 combinations**

Now let us repeat the process but let us assume that we are allowed to add numbers to the password but with the same length (2 characters only):

- **Password length = 2 characters**
- **First character = lowercase letters (26 possibilities) + uppercase letters (26 possibilities) + numbers (10 possibilities) = 62**
- **Second character = 62 (same as first character)**
- **Total = 62^2 = 62 * 62 = 3844 combinations**

Now let us repeat the last two processes but with a password increased from 2 characters to 3 characters:

- **Password length = 3 characters**
- **First character = lowercase letters (26 possibilities) + uppercase letters (26 possibilities) = 52**
- **Second character = 52 (same as first character)**
- **Third character = 52 (same as first and second characters)**
- **Total = 52^3 = 52 * 52 * 52 = 140608 combinations**

Now let us repeat the process but let us assume that we are allowed to add numbers to the password but with the same length (3 characters only):

- **Password length = 3 characters**
- **First character = lowercase letters (26 possibilities) + uppercase letters (26 possibilities) + numbers (10 possibilities) = 62**
- **Second character = 62 (same as first character)**
• Second character = 62 (same as first and second characters)

• Total = 623 = 62 * 62 * 62 = 238328 combinations

What did you notice? If you look at the number of possible combinations in both parts, you will get the answers to the questions we raised at the beginning. Both complexity and length can make a password hard to crack, but the ultimate strategy is clearly to combine them.

To sum up, the time required to crack a password is dependent on two factors respectively based on their importance:

Length (L): which is how long the password is (Note: each extra character takes exponentially more time to brute force)

Complexity (X): which is how many characters are allowed in each position (uppercase, lowercase, numbers and special characters)
8. Test Your Password’s Strength

You may see creating a strong password as an irritating or difficult job to you. And while you may have come up with a password, you are not sure about its strength. Don’t worry! Fortunately, there are many useful Web-based applications, called password strength checkers (or just password checkers), which can help you test the strength of your password. And provide you with guidelines for creating a stronger one.

How Secure Is My Password is an obvious example. It is a simple, single-purpose Web-based application with a user-friendly interface; basically, one text box. Simply type your password in the text box and it will let you know your password strength (by showing you the time that any desktop PC would take to crack it) as you type the password. But how does it do that? Actually, all of these tools calculate the strength using a simple math calculation or their own weighting algorithms, and come up with the number or measurement that corresponds to the potential strength of your password. For instance, let us try our Haystacked Password: fb…..///I.lto!MUO2012…..///

It is a very useful tool to discover the strength of your password, but as a precaution you probably shouldn’t use this service with your actual password. Instead use it to learn what works and what doesn’t work.

For more information about this tool and other similar tools, please see the following links:

- [Put Your Passwords Through The Crack Test With These Five Password Strength Tools](#)
- [HowSecureIsMyPassword: Password Strength Checker](#)
- [How secure is your password?](#)
- [Password Meter : Check Passwords for Strength](#)
• **Strength Test: Test The Strength Of Your Password**

Additionally, within Microsoft’s previously-mentioned security service, there is a free tool called [Microsoft’s Password Checker](https://makeuseof.com) for checking your password strength. Just go there, type in your password, and get an instant strength rating: Weak, Medium, Strong, or Best, which appears in the colored bar below the text box as shown in the following snapshot:

![Password Strength Test](http://makeuseof.com)

Read more: [check Your Passwords' Strength at Microsoft’s Password Checker](https://makeuseof.com)

**NOTE:** **Security is your first responsibility.** So for the sake of security, we would strongly and highly recommend you to be careful with using these tools. Therefore, as a best-practice use and consider this kind of web applications (regardless of knowing that web-based application/service uses a client-side script to check the password, without sending anything to the server or not) as an exercise for you to know how to come up with a strong password using different characters, symbols and numbers. Just play with it by constructing fake passwords and testing them.

You **MUST** be the only person who knows your actual password.
9. Password Management Techniques

You may think that creating strong, secure and unique passwords for each of your online accounts is impossible because it will be difficult to remember all of them. Fortunately, there are many different kinds of techniques – including tools and services – available to make your passwords both secure and accessible from multiple computers and devices.

9.1. Algorithms

9.1.1. Tiered Password System

In simple English, tiered password systems are about having different levels of passwords for different types of websites, where the complexity of the password depends on what the consequences would be if that password is compromised/obtained. You may have two or three levels of website or security or passwords. An obvious common example of the tiered password system is the Three-Tiered Password System or Approach, which mainly categorizes the types of website or security into three levels:

- **Low security**: for signing up for a forum, newsletter, or downloading a trial version for a certain program.
- **Medium security**: for social networking sites, webmail and instant messaging services.
- **High security**: for anything where your personal finance is involved such as banking and credit card accounts. If these are compromised it could drastically and adversely affect your life.

Keep in mind that this categorization should be based on how critical each type of website is to you. What goes in which category will vary from person to person.

The point is that you don’t have to memorize hundreds of passwords to ensure your accounts will not be compromised. Use really strong passwords only for your high and medium security accounts.

9.1.2. Password Tree

This is a manual way of creating a tree on a piece of paper in order to categorize the websites while mentioning the passwords underneath each one. Amit Agarwal, the author of *The Most Useful Websites*, offers a nice detailed example in his blog.

9.2. What is Password Manager?

Most people agree that the number of passwords you need on the Web is growing. Therefore having a strong and secure password for each account is more important than ever. This leads to a problem: the difficulty of keep tracking of all your different passwords.

A Password Manager is software that allows you to securely store all of your passwords and keep them safe, typically using one master password. This kind of software saves an encrypted password database, which securely stores your passwords either on your machine or on the Web.

9.3 Types of Password Managers

There are many free as well as paid services, so do your research carefully before deciding which one you want to use.

9.3.1. Standalone:

They store your passwords locally on your computer, and there are three different kinds:
Desktop-Based
These are a type of password manager that stores your personal information - usernames and passwords - on an encrypted local file (or database) on a computer hard drive.

Portable
Passwords will be stored on mobile/portable devices such as smartphone or as a portable application on a USB memory stick or external hard drive.

Browser-Based
Similar to the desktop-based and portable password managers, but built into a Web browser. Examples include the password management tools offered by Firefox and Chrome.

9.3.2. Web-Based
A web-based password management solution enables you to access the passwords from anywhere through a browser, because they store your passwords in the cloud.

9.3.3. Token-Based
They require an extra level of authentication (often called multi-factor or two-factor authentication), such as requiring the user to unlock their passwords by inserting a provided portable physical device (such as a smart card) to gain access to your passwords.

In summary, the following table shows the main features and weaknesses between these types:

<table>
<thead>
<tr>
<th>Advantages (Features)</th>
<th>Standalone</th>
<th>Portable</th>
<th>Browser</th>
<th>Web-based</th>
<th>Token-based</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Desktop</strong></td>
<td>Local central encrypted database</td>
<td>Portability (as a copy of the central encrypted database will be in your USB flash memory)</td>
<td>Ease of use, as it is a part of the browser</td>
<td>Portability accessibility</td>
<td>Much more secure Eliminate the single point of potential failure</td>
</tr>
<tr>
<td><strong>Portability</strong></td>
<td><strong>NOTE:</strong> some password managers of this type don’t provide any protection for stored passwords. Avoid them.</td>
<td>More accessible than the other standalone apps, as the flash USB will be carried with the owner</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Browser</strong></td>
<td>Lack of accessibility away from your computer</td>
<td>Forget or lose the flash drive and you’ve lost your passwords.</td>
<td>Lack of accessibility (unless you use a syncing tool) Not secure, even with a master password</td>
<td>You don’t have control over where the data is stored. Impacted by the security of the server or system they reside on or the security of the company itself.</td>
<td>More expensive Less portable</td>
</tr>
</tbody>
</table>

As Mike Weber wrote in his article “Password Management: How many do you need to remember?”, standalone and web-based password managers are software-based solutions which are impacted by the security of the system they reside on.

As you can see, the table above demonstrates many things that you have to take into consideration:
There is an inverse relationship between usability and security (usability vs. security)

You should not rely totally on any type of password manager

Your single master password must be unique and complex

Be careful when you use the password generator feature included in some password managers. If the password manager uses a weak random number generator, the passwords might be easily guessable.

So which one is the best? Or what should we do? Bear with us and continue reading to find out, but for the time being take into consideration that you have to use different security measures and you should alternate your ways of dealing with passwords.

Password management tools are really good solutions for reducing the likelihood that passwords will be compromised, but don’t rely on a single source. Why? Because any computer or system is vulnerable to attack. Relying on a password management tool creates a single point of potential failure.

9.4. Examples of Password Managers

9.4.1. KeePass

KeePass is a popular open-source, cross-platform, desktop-based password manager. It is available for Windows, Linux and Mac OS X as well as mobile operating systems like iOS and Android. It stores all your passwords in a single database (or a single file) that is protected and locked with one master key. The KeePass database is mainly one single file which can be easily transferred to (or stored on) any computer. Go to the download page to get your copy.

Here’s how to set it up in Windows:

After opening KeePass, create a database by clicking the ‘New Database’ button

A new window will appear which prompts you for a master password and/or a key file disk, as shown. [9.4.3]

Enter your password in the master password box and click ‘OK’
While you type your password, it will tell you how many bits of encryption it will provide, and there is also a password strength bar underneath the password entry to tell you how secure your password is. **Quick Reminder:** Use a single, unique and strong master password to lock and unlock your database of passwords. Then, you must save that password database.

Then, enter it again in the Repeat Master Password Window and click ‘OK’.

After you have created the password database, you need to configure the database and save it. So click ‘File’ button, then go to ‘Save As’.
Type in a name for your new password database file in the ‘Save As’ window and click ‘OK’.

It is now time to add an entry to your password database. To do that, click the ‘Add Entry’ button (the key-shaped icon).

The ‘Add Entry’ window will be opened. The window has a series of fields and tools such as:

- **Group**: Ready-made folders in which you can organize and sort your passwords. For instance, the Internet group would be a good place to store the password for your Facebook account or other website accounts.

- **Title**: A name that you can use to describe the particular password entry, e.g. Facebook pass-
word and so on.

- **User name:** The name associated with the password entry, such as makeuseof@makeuseof.com

- **Password:** This is one of KeePass’s great features; generating a secure encrypted password. This feature automatically generates a random secure encrypted password when the ‘Add Entry’ window is opened/activated.

To see your password, click the show password button (the button with three dots) on the right side of the password.

To generate a random secure encrypted password either for a new account or to change an existing password, click the button on the right side of repeat entry and directly below the show password button.

- **Repeat:** Type the password a second time to confirm it.

- **Quality:** Displays how secure your password is, with an as-you-type quality (or password strength) meter.

- **URL:** The link (or Web address) to the website associated with the password entry like mail.yahoo.com.

- **Note:** General information about the account or website which might be useful in situations where you are searching for a particular entry or where you have specific settings for your account.

- **Expires:** This is the expiration date which you can use when you want a password entry for a limited amount of time. You can also add a reminder for yourself to change the password at the time specified. And you will see a red cross symbol next to the password’s name when it has expired.

- **Attachment:** This is a file attachment to the password entry. Another great feature about KeePass is having an internal viewer for text files, images and documents. So you don’t need to export the attached file to view it.

Click ‘OK’ once you have entered your information to save your changes. The ‘Add Entry’ screen will be closed and you will be taken to the main window where your password will be displayed under ‘eMail group’.

Then, if you want to use any one of your entries, just right-click on it and select ‘Copy User Name’ or ‘Copy Password’ and paste it in the website.

**Disadvantage:** If you forget the master password, all your other passwords in the database are lost forever, and there is no way of recovering them. Don’t forget that password!
KeePass is a local program, but you can make it cloud-based by syncing the database file using Dropbox, or another service like it. Check out Justin Pot’s article, Achieve Encrypted Cross-Platform Password Syncing With KeePass & Dropbox.

More useful links about this tool:

- KeePassX – Secure Password Management For Linux & OS X
- Using Keepass to Secure Your Online Accounts

### 9.4.2. Mozilla Firefox’s Password Manager

Mozilla Firefox’s Password Manager is a password manager built into the browser. This can save login information (usernames and passwords) that you use while you surf the Web so that you don’t have to enter them again on the next visit to a website or service. You may notice when you enter your login information for the first time in Facebook or other site; a window appears at the top of the webpage.

This window includes a question and dropdown menu. The question says, “Do you want Firefox to remember this password?” and the dropdown menu has three options:

- **“Remember Password”:** if you select it, Firefox will save the login information and it will automatically enter them for you the next time you visit the website.
- **“Never for This Site”:** Firefox will not save the login information, and will never ask you again unless you clear the exceptions in the password manager.
- **“Not Now”:** the browser will skip saving your username and password this time but will ask again next time.

Please note that when you click outside of the Remember Password prompt, it will disappear. So to bring it back, just click the key icon on the left side of the address (or location) bar.

Master password is one of the fabulous features that the secure browser Firefox has. It is a feature to protect saved passwords and other private data. It is highly recommended to use the master password feature if your PC is used by others to prevent them from seeing the list of saved passwords. The master password option is not selected by default. However, you can set it easily by doing the following:

Click ‘Firefox’ button in the top-left-hand corner.
Go to the “Options” menu and select “Options”.

There you will find 8 different settings panels: General, Tabs, Content, Applications, Privacy, Security, Sync and Advanced.

Select ‘Security’ tab.

Check the box next to “Use a master password.”

A new window will appear which prompts you for a master password as shown.
Enter your password in the “Enter new password” box.

Then, enter it again in the “Re-enter password” box and click ‘OK’

One more thing to know - as highlighted on the official Mozilla website - for each Firefox session you will need to enter this master password only the first time you ask Firefox to remember a new password or remove passwords, and then each time you want to see the list of your saved passwords.
10. Two-Factor Authentication

Sometimes a password isn’t enough. Two-factor authentication goes further, requiring both something you know (your password) and something you have (your phone) in order to log in.

Put simply: it is an authentication method that relies on two independent pieces of information to verify who somebody is. Why use this? Because passwords are not enough for protecting important logins any more. Two-factor authentication is stronger because it reduces the chances of having your account stolen or compromised by someone else. Google’s utility “Google Authenticator” is a great example of applying this authentication approach.

If you haven’t enabled two-factor authentication for Google I strongly recommend you do so. Google Authenticator is a service providing you with two-factor authentication (also known as “2-step verification”). It is available as an app for iPhone, Android, Windows Phone and BlackBerry mobile phones. This simple app was developed purposely to provide Gmail users with an extra layer of security to their accounts by providing a secondary six digit code in addition to their username and password to log in to Google apps. This means that besides knowing the username and password, the user would need to have a one-time password (OTP) sent to a phone or generated by the app in order to log in to an account. You can receive authentication codes through the following three options:

- Smartphone such as Android or iPhone by Google Authenticator application.
- SMS Text Message.
- Printed List; for when your phone isn’t working.

Everyone who uses Gmail (or Google Apps), Facebook or other services that offer 2FA should start using this feature as soon as possible. Here’s a great article by Tina Sieber covering everything related to this security method.
11. HTTPS: Added Security

As Matt Smith wrote in his article How To Combat WiFi Security Risks When Connecting To A Public Network:

“As many people now know, connecting to a public, unsecured wireless network can have serious risks. It’s known that doing this can provide an opening for all manner of data theft, particularly passwords and private information.”

A public Wi-Fi network is open, and wireless networks work in the same way as radio works. This means that the information will be sent across the airwaves (like radio broadcasts) in all directions, and anyone within range can read all of it easily – unless it’s encrypted. This is why HTTPS is crucial if you’re using an unsecured network. When you use HTTPS, your personal information – such as usernames and passwords – are encrypted over the network. This means that even if the network is public or open, your logins to any of your accounts are not visible to people who want to capture your login details using some third party tools (or sniffing tools).

So what is HTTPS? As explained on Wikipedia, HTTPS stands for Hypertext Transfer Protocol Secure Turning – you can tell a site is using it when you see “https” in the address bar where “http” usually is. It’s currently a default login option for Web services including Gmail, Facebook and more.

If you want to browse on the Web safely, I strongly recommend you use Mozilla Firefox as your default browser and use HTTPS whenever it is available. Also, I recommend you to use a Firefox extension called HTTPS Everywhere, which will turn on HTTPS whenever possible. For more information about why you should use Firefox as your default browser or how to use its extension HTTPS Everywhere, please see the following links:

- Tackling Firefox: The Unofficial Manual
- Encrypt Your Web Browsing With HTTPS Everywhere [Firefox]
12. Password Management Examples

In brief, **DO NOT PUT ALL YOUR EGGS IN ONE BASKET**. Realistically, putting all the eggs (your passwords) in one basket (like an encrypted database using password manager) means you’ve got a lot of problems once you’re compromised. Instead, try to use all the password management techniques mentioned in this manual, if you can. Here’s a method I’ve used in the past.

Tiered Passwords: I first categorized my passwords based on how critical a given account is:

- **Low security**: forums or newsletters – places where I don’t use any sensitive personal information or data.
- **Medium security**: Facebook, Google+ and emails.
- **High security**: for anything where my personal finance is involved such as banking and credit card accounts.

Now, based on this tiered passwords system, I used different passwords patterns, password managers which is summarized on the following table:

<table>
<thead>
<tr>
<th></th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password Generation</strong></td>
<td>At the beginning I used the same password for most of them, and then I used random passwords.</td>
<td>I used one base password and changed the last or first two letters with the something refer to the website.</td>
<td>Used different strong complex unique password for each account. <strong>It is highly recommended to not use one base password here</strong></td>
</tr>
<tr>
<td><strong>Manual Password Management (piece of paper)</strong></td>
<td>Yes</td>
<td>No</td>
<td>No. <strong>(We strongly recommend you to not use it)</strong></td>
</tr>
<tr>
<td><strong>Password Management Tool</strong></td>
<td>Yes. Browser-based password manager (Firefox’s password manager)</td>
<td>Yes. KeePass password management tool.</td>
<td>No. I am use my brain to remember any password related to any account has any of my personal finance information.</td>
</tr>
<tr>
<td><strong>Additional Security Layer</strong></td>
<td>No</td>
<td>No. I just started using 2FA with my Gmail and I am going to use it with my Facebook and Dropbox accounts.</td>
<td>Yes. I have used 2FA because my bank requires all of its clients to.</td>
</tr>
<tr>
<td><strong>Frequent Password Changing</strong></td>
<td>No</td>
<td>No</td>
<td>Yes. <strong>NOTE: it is Highly recommended to evaluate the strength of your passwords and change them based on that review.</strong></td>
</tr>
</tbody>
</table>

Note: You can use this table as a template for starting your own password management tree or system. However, do not rely on it too much. Try to come up with the system that fits what’s critical for you, and with respect to the latest security standards.

The key take-away from this, of course, is that you should never reuse a password between sites.
13. How to Protect Your Passwords?

Clearly, passwords are the defensive frontline that protects your accounts. Here are some tips that should help you to protect your passwords – whether you’re at work, at home or in a coffee shop:

You should never record or write your password down on a post-it note.

Never share your password with anyone, even your colleagues.

You have to be very careful when using your passwords on public PCs like schools, universities and libraries…etc. Why? Because there’s a chance these machines are infected with keyloggers (or keystroke logging methods) or password-stealing trojan horses.

Do not use any password-saving features such as Google Chrome’s Auto Fill feature or Microsoft’s Auto Complete feature, especially on public PCs.

Do not fill any form on the Web with your personal information unless you know you can trust it. Nowadays, the Internet is full of fraudulent websites, so you have to be aware of phishing attempts.

Use a trusted and secure browser such as Mozilla Firefox. Firefox patches hundreds of security updates and makes significant improvements just to protect you from malware, phishing attempts, other security threats, and to keep you safe as you browse the Web.

Keep your eye on the PwnedList database to check if your username or email address is on the list of leaked account data on the Internet.

Keep checking and looking at the recent news and reviews of password manager software and password cracking tools. Based on this, you will be able to decide when you have to change your passwords.
14. Security News

As mentioned in the last tip above, you should stay up to date with the latest security news; security breaches are happening all the time. If you do a quick Google search for the latest security news you will be amazed by the number of resources focused on security. I will not talk about all of them, but I will highlight the most important resources directed at general audiences:

14.1 Security Now

Security researcher Steve Gibson has an interesting podcast called Security Now. I have been listening to this podcast for a few weeks now and I can tell you that this podcast itself is not super technical and it is not directed toward security gurus/programmers. In every episode Gibson explains and answers questions from listeners regarding everything from online authentication, Wi-Fi security, Cryptography to spyware, malware, viruses and so many other things. Surprisingly, you can listen to this podcast on your iPhone or iPad.

By the way, do not worry that you’ve missed any episodes because each podcast is archived with both high and low bandwidth audio, and a full transcript. Just go to the Security Now website to start getting more information about security.

14.2 PwnedList

This tool helps users figure out if their account credentials have been hacked. If you go to the website of the service, you will see up-to-date statistics of the number of leaked credentials, passwords and email addresses.

PwnedList keeps monitoring (or crawling) the Web in order to find stolen data posted by hackers on the public sites and then indexes all the login information it finds. Also, it recently launched a new service that alerts you when your credentials have been posted publicly by hackers. This monitoring tool is available as a free service to the individual. So what you are waiting for? Go to the sign-up page and start getting alerts and updates about your credentials.
15. Points to Remember (Recommendations)

Let's go over the main ideas and points, just to review.

ALWAYS use a mix of uppercase and lowercase letters along with numbers and special characters.

Have a different strong password for each site, account, computer etc., and DO NOT have any personal information like your name or birth details in your password.

DO NOT share any of your passwords or your sensitive data with anyone – even your colleagues or the helpdesk agent in your company. In addition, use your passwords carefully, especially in public PCs. Don’t be a victim of shoulder surfing.

As we mentioned in Password Management Techniques section, it is an excellent step to use password manager applications like LastPass and 1Password to help you in generating, storing and remembering unique passwords. However, for more robust security you should not rely solely on them. Grant Brunner wrote a fascinating article at ExtremeTech about Staying safe online: Using a password manager just isn't enough. In it, he wrote, “using a password manager for all of your accounts is a very sensible idea, but don’t be lulled into a false sense of security. You’re not immune from cracking or downtime.” Broadly speaking, password managers such as LastPass are like any software: vulnerable to security breaches. For example, LastPass experienced a security breach in 2011, but users with strong master passwords were not affected.

And our last recommendation that we strongly encourage is for you to start evaluating your passwords, building your tiered password system, alternating your ways of creating passwords and storing them using password managers or password tree, be up-to-date with the latest security news, and regularly change your passwords.

For more details:

- The guide to password security (and why you should care)
- How to master the art of passwords
16. MakeUseOf Links

I personally highly recommend you go through the following useful how-to articles on MakeUseOf to get more information about password security and protection.

- [How To Create A Good Password That You Will Not Forget](#)
- [How To Create Strong Passwords That You Can Remember Easily](#)

Also, we have a growing repository of useful and helpful security tips that should be viewed in order to be updated in this absolutely vital area.

Those of you who are new to the area of Information Security and want to hear a lot more about security should probably read, "[HackerProof: Your Guide To PC Security](#)", which will give you an overview of information vital to the security of your PC.

Conclusion

In today's information age, passwords are a vital aspect of your security. They are the defensive frontline and the most widely used authentication method that provide protection for the user accounts of your computer or online accounts. However, because of the new techniques used by password crackers and faster hardware, what was considered a strong password a year ago may now be considered an open window to your computer or online account. This doesn't mean that you should be scared, but it does mean that you should keep up to date with the latest security news whenever possible. You’re not immune from cracking or downtime. To be truly safe and secure, you need to keep an encrypted copy of your password database locally, use multi-factor authentication when possible, review the latest security news, evaluate your passwords and change them frequently.

That's it! I hope you have gained a good sense of security awareness and learned new techniques by reading this. Setting up a strong password management system requires time, practice and patience, but it’s worth doing if you are concerned about your security. It makes your life more secure than before. Enjoy!

“TREAT YOUR PASSWORD LIKE YOUR TOOTHBRUSH”
Did you like this PDF Guide? Then why not visit MakeUseOf.com for daily posts on cool websites, free software and internet tips?

If you want more great guides like this, why not subscribe to MakeUseOf and receive instant access to 50+ PDF Guides like this one covering wide range of topics. Moreover, you will be able to download free Cheat Sheets, Free Giveaways and other cool things.

Home: http://www.makeuseof.com
MakeUseOf Directory: http://www.makeuseof.com/dir
MakeUseOf Answers: http://www.makeuseof.com/answers
Geeky Fun: http://www.makeuseof.com/tech-fun
PDF Guides: http://www.makeuseof.com/pages/
Tech Deals: http://www.makeuseof.com/pages/hot-tech-deals

Follow MakeUseOf:

RSS Feed: http://feedproxy.google.com/Makeuseof
Newsletter: http://www.makeuseof.com/pages/subscribe-to-makeuseof-newsletter
Facebook: http://www.facebook.com/makeuseof
Twitter: http://www.twitter.com/Makeuseof

Think you’ve got what it takes to write a manual for MakeUseOf.com? We’re always willing to hear a pitch! Send your ideas to justinpot@makeuseof.com.