The Mozilla Pocket Password Primer

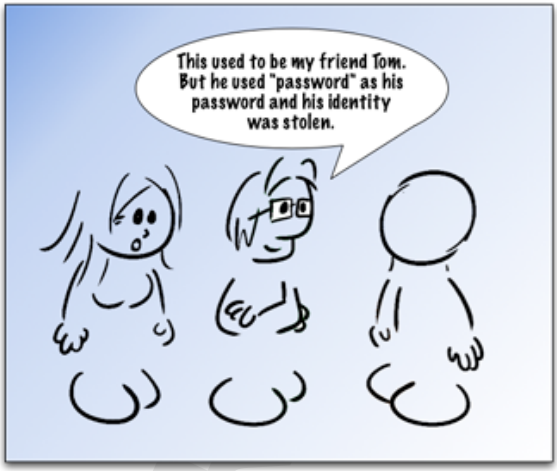
Simple Ways to Keep Your Identity Safe On the Internet

mozilla
Firefox®

The Mozilla Pocket Password Primer

Preliminary Draft

Please visit the Consumer Education page on the Mozilla Wiki to comment on this publication. You will also find links there to ebook versions.



pass·word /ˈpæsˌwɜrd, ˈpɑs-/ **–noun**

1. a secret word or expression used by authorized persons to prove their right to access, information, etc.

-- *Dictionary.com*

Passwords

It's hard to get through a day on the internet without encountering dozens of requests for your username and password. With more and more of our work and leisure time spent online, most people find that remembering a unique password for each account they have is an impossible task. It's made harder when sites have strange rules about how you must form your passwords. Some sites prohibit special characters like &, %, #, and @ in passwords. Other sites require them. Some sites have maximum length limits on passwords that are shorter than the minimum length required by other sites. What is the modern, internet-savvy user supposed to do?

Certainly ***not*** what most of us do now...

Are there little yellow notes stuck to the side of your monitor with usernames and passwords scribbled on them?

Do you have at least one computer or online account where the password is “password”?

Do you use your pet’s name as a password, and tell yourself you’re making it more secure by adding “123” to the end?

Do you have accounts on 387 websites and log into all of them with one of three favorite, easy-to-remember passwords?

Did you last change the password for your bank account shortly after the turn of the century? Before?

If you’ve secretly answered “yes, but...” to any of these, don’t worry. We won’t tell anyone, and in this guide we’ll show you how to create and manage strong, secure passwords without breaking a sweat. We’ll also show you how to memorize only one password and still have a unique password for every site you visit.

You'll sleep better at night knowing you're safer from identity theft, and with the tricks you'll learn here you can help your friends and relatives be safer online as well.

Passwords Are Compromises

Any password is a compromise between a secure (long, random and unique) string of characters and an easy to remember word or phrase. As we need more and more passwords to get through the day, we all tend to push the compromise in the direction of easy to remember more than we should. A bit later, we'll show you a technique creating passwords that will keep your's memorable without making them easy to guess. We'll also show you ways to let your computer manage all your passwords so you don't have to remember them.

Threats to Your Passwords

The threats to your passwords fall into three major categories:

Social Engineering: The more an identity thief knows about you, the less secure passwords associated with your everyday life become. Don't assume that the names of your children, pets or friends make secure passwords. They aren't. Similarly, if you keep passwords written down in a "secret place", anyone watching your day-to-day activity will quickly learn where they're hidden.

Brute Force Attacks: If your passwords are insecure, an identity thief needs little more than your username to mount an attack against your accounts. Cracking software that uses lists of dictionary words in combination with common password configuration information quickly opens accounts with passwords such as "Jennifer3" and "Bobcat123". A security audit of a university computer system found that 20% of the accounts could be accessed using only a list of the 20

most popular female names followed by a single numeric digit.

Breaching Insecure Systems: If the administrators of a website use poor security practices, such as storing passwords unencrypted, identity thieves that manage to breach system security can steal the entire list of passwords and usernames. That's a huge security problem for you if you've used the same password on other sites, particularly ones with access to your bank account or other sensitive information.

The lessons are clear:

- Use as secure a password as possible
- Change your passwords periodically
- Try not to reuse passwords between sites

If that last rule is impossible to follow, then be sure that sites holding sensitive information don't use shared passwords.

What Not To Use In Your Password

There are some things you should ***not*** use when you're creating a password. All of the following are chosen as passwords so frequently that password cracking software has been developed to take advantage of their inherent weaknesses:

- Your name, or the name of your spouse, parent, child, or pet
- The name of a friend (real or imaginary), your boss or a coworker
- The name of popular fantasy characters or words like "wizard", "guru", "gandalf", etc.
- The name of the operating system you're using, or the hostname of your computer
- Your phone number, license plate number or any part of your social security number
- Birth dates or other easily obtained information about you, your family or your friends
- A proper noun (the name of a particular person, place or thing)
- A dictionary word, either English or foreign

- Passwords of all the same letter
- Simple patterns on the keyboard, like "qwerty"
- Any of the above followed or prepended by a single digit or a sequence of ordered digits (like 123)
- Any of the above spelled backwards

...and one more thing to remember. You should never use a password that has been used as an example in an article about how to create good passwords. That includes this guide. Once a password has been published, it's no longer useful.

If this seems like we've eliminated any password that has a prayer of being memorable, don't worry! We'll show you how to avoid all of those pitfalls.

Choosing a secure password

Good passwords have a fairly simple set of properties:

- They have both upper and lower case letters
- They have digits and/or punctuation characters as well as letters
- They are easy to remember, so they do not have to be written down
- They are at least seven or eight characters long, but the longer the better.
- They can be typed quickly, so someone else cannot easily look over your shoulder

So the puzzle before us is to create a password with all of the good properties without having any of the bad properties.

Strategy #1: Passwords from a Phrase

You can create a secure password starting with a simple phrase. For example, let's use a quote from Ogden Nash:

"Happiness is having a scratch for every itch."

If we use the first letter of each word, and substitute 4 for "for", we get:

Hihas4ei

This is a reasonably strong password but we can improve it a bit by adding some special characters:

#Hihas4ei:

Strategy #2: Associate with a WebSite

We can use our new password on several different websites by adding a suffix with a mnemonic link to a particular site. Let's use the first letter and the next two consonants in the site name.

Just to add a bit more randomness we'll alternate upper-case and lower case, and if the first character in the site name is a vowel we'll start with upper-case. To mix things up a bit more we'll use the same rule to decide whether to add the site mnemonic to the left side or the right side.

#Hihas4ei:AmZ for Amazon

#Hihas4ei:YtB for YouTube

bGz#Hihas4ei: for Bugzilla

dRm#Hihas4ei: for Drumbeat

While this technique lets us reuse the phrase-generated part of the password on a number of different websites, it would still be a bad idea to use it on a site like a bank account which contains high-value information. Sites like that deserve their own password selection phrase, perhaps something like the old English proverb:

"A penny saved is a penny earned."

So for our bank, this would give us a password similar to:

bNk#Apsiape: - Bank

This password lacks numeric characters because our phrase contains neither numbers nor the words “to” or “for”. We could strengthen it a bit by adding a rule to put in a digit or two if none are provided by the phrase:

bNk#8Apsiape2: - Bank

But even without doing that our rule based system gives us strong, easy to remember passwords that are unique to each website.

The Power of Rules

Notice that by using a simple set of rules, we're able to construct a longer than average password that's still easy to remember. Here are the rules we used:

- Choose a memorable phrase and use the first letter of each word.
- Add special characters (we chose # and :).
- Use the first character of the website name and the next two consonants in the name as a site identifier.
- If the website name starts with a vowel, capitalize the first and third characters and add it to the right side of our password.
- If the website name starts with a consonant, capitalize the second letter and add it to the left side of our password.
- If there are no numbers in the password add a digit or two. (we chose to add them at the beginning and end of our phrase).

Changing Your Passwords

If you work for an organization that requires you to change your password periodically, you should consider changing all of your passwords at that time as well. You don't have to visit all your sites, just choose a new secret phrase and as you visit each site make the change.

If nobody requires periodic changes, you should consider changing your password at least twice a year. A convenient way to remember to change is to pick a new secret phrase when you set your clocks when the time changes in the spring and autumn.

Managing Your Passwords

Even with tricks like using phrases to generate passwords, remembering passwords for dozens of

sites can be a bit taxing. There are software tools that will manage your passwords for you. There are online services and stand alone programs that will save your passwords, and you can ask most modern web browsers to remember passwords. But you should choose your password management software carefully and only use a program or service that you're sure you can trust with your most sensitive information.

The Firefox browser from Mozilla, the most trusted name on the Internet, has secure, world-class password management. When you enter a username and password into a website, Firefox asks if you want to remember that password. If you answer yes, Firefox stores the password in your user profile. You can (and should) turn on Firefox's Master Password feature to ensure that your saves passwords are securely encrypted.

Combining Firefox's Master Password with Firefox Sync lets you manage all your passwords on all the machines you use securely and effortlessly. ***Best of all,***

if you use the password manager, the Firefox Master Password is the only password you'll ever have to remember yourself.

The Firefox Master Password

To keep the passwords you save in Firefox's password manager secure, you should turn on the Master Password. If you haven't already set a Master Password, it's easy to do.

Before you start, carefully choose a phrase to create your Master Password. Since the Master Password is used to secure all of your other passwords, a long phrase would be advisable.

In Firefox for Windows:

1. From the ***Tools*** menu select ***Options***.
2. Click on the ***Security*** icon and check the "Use a master password" checkbox.
3. The Master Password dialog box will appear.

4. Enter your Master Password into the "Enter new password:" and "Re-enter Password:" text boxes and hit the OK button.

in Firefox for MacOS:

1. From the ***Firefox*** menu select ***Preferences***.
2. Click on the ***Security*** icon and check the "Use a master password" checkbox.
3. The Master Password dialog box will appear.
4. Enter your Master Password into the "Enter new password:" and "Re-enter Password:" text boxes and hit the OK button.

Many people prefer to have Firefox ask for the Master Password only once at the beginning of each session. There is a Firefox Add-on called StartupMaster that enables this behavior. To add StartupMaster to Firefox, pick **Add-ons** from the **Tools** menu, click on **Get Add-ons,** and then type StartupMaster into the search box.

All Your Passwords On All Your Computers

Firefox Sync can ensure that all your passwords are saved on all the computers you use. Tell Firefox to remember a password on your desktop computer at home, Firefox Sync will make that password available to Firefox on your notebook computer, and any other computer (or mobile device) on which you use Firefox.

Firefox Sync not only synchronizes your passwords, but also your bookmarks, browsing history, preferences, and tabs across all of your browsers.

One thing that Firefox ***does not sync*** across all of your computers is your Master Password, so be sure to set that up on each machine when you configure Firefox Sync.

Firefox Sync is built into Firefox 4, and is available as an add-on for Firefox 3.5 and later. To add Firefox Sync to Firefox, pick **Add-ons** from the **Tools** menu, click on **Get Add-ons,** and then type Firefox Sync into the search box.

When you set up Firefox Sync, it will ask for a password and pass phrase. You can safely use your Master Password and the phrase you used to create it here.

When you have Firefox Sync installed on all your machines it will ensure that passwords you remember on one machine are available on all of the machines on which you run Firefox. That includes Smartphones and mobile devices running Firefox Mobile and Firefox Sync , so you can carry all your passwords with you all the time.

Become a Password Security Ninja

Faithfully using the tips and techniques in this guide will put you in the top 10% of all internet users when it comes to password security awareness.

Use your newfound power wisely and help spread the word by showing your friends and family how they can be safer online by using more secure passwords.

Colophon

The ebook versions of this publication were prepared using the Sigil open source editor for ebooks. Learn more about Sigil at http://code.google.com/p/sigil.