Master Password

The *stateless* solution
to the world's *biggest* security problem.

http://itunes.apple.com/app/id510296984
http://masterpassword.lyndir.com
masterpassword@lyndir.com

A Revolution in Password Management

Ghent, Belgium, 1 July 2012. Master Password is a revolutionary new way for users to solve the password problem.

Billions of users are actively using the Internet every day, logging into their many accounts. Unfortunately, they don't do enough to protect the security of their accounts, leaving them vulnerable to identity, privacy and financial theft.

Master Password solves this problem by employing an algorithm that enables a user to quickly obtain a unique password for any purpose. To enhance security even further, Master Password is built around the core idea that its operation is entirely stateless. This means that Master Password does not save the user's master password or any of the passwords it generates for future use. When you need to log in to a site later, the algorithm simply re-generates the same unique password for the site, by using the user's master password and the site's name.

- Access to passwords is protected by a master password.
- Generates secure passwords for any purpose.
- Passwords aren't stored, leaving nothing sensitive to be found by thieves.
- No dependency on a device or access to the Internet. No more need for backups.
- Supports different password types to curtail site-specific password policies.
- Easily copy a password by tapping it and switching to the app that needs it.
- Easily transfer passwords to physical objects thanks to readable passwords.
- Optionally save custom passwords using AES encryption.
- Synchronizes between iOS devices using iCloud.
- Never tied down: Passwords can be exported and imported easily.

The Internet is showing an incredible growth. The percentage of the world's population that is connected has grown from 5% in March, 2000 to nearly 33% in March, 2012[1].

What do these billions of people actually do on the Internet? It turns out[2], most of them are either connecting over social networks, browsing around, or playing games.

1 http://www.internetworldstats.com/emarketing.htm

2 http://blog.nielsen.com/nielsenwire/online_mobile/what-americans-do-online-social-media-and-games-dominate-activity/

People's day-to-day activity on the Internet is of such a nature that they're usually logged-in to the sites they use. Twitter, Facebook, Google+, Tumblr, Flickr, Amazon, eBay, et al. aren't much of an experience when the user isn't also registered and logged in to the site. Internet users constantly find new and exciting services that they're eager to sign up for and try out.

Each time, however, they come face to face with that sign-up screen, and consciously or subconsciously, it is a source of great frustration. Yet another password to think of. Yet another password to remember.

This is the point where most everyone[3] gives up on security and re-uses one or a few passwords for all their accounts. Usually, the line of thinking goes like this: "Is this a high-security level site, like a bank account or email address?". A positive answer generally means the user's standard "secure" password will be used. A negative answer usually means the user will re-use their "simple" password for this new account.

This practice makes the user happy again. The mental fatigue involved with having to create and remember yet another password has been averted and the user has successfully logged into their new service. Excitement awaits and the pain of logging in is soon forgotten.

Unfortunately, there are dangerous side-effects[4] the user should know about: for instance , very recently a series of popular social networks have confirmed leaked password databases[5]: *LinkedIn*, *eHarmony* and *Last.FM* to name a few. Hackers have obtained lists of password *"hashes"* for millions of people's accounts.

When a user's accounts are not protected by adequately secure passwords, attackers that obtain *"hashes"* of these passwords can easily[6] discover the user's real password and take over their account.

What's worse, after an attacker discovers a user's password to a certain site, and the user has been re-using this password for many other sites, the attacker can now easily enter any of the user's other accounts as well.

Since Master Password generates strong passwords, the user's accounts are often safe even in the event that a site's password database gets hacked. Additionally, since Master Password generates different passwords for each of the user's sites, the loss of any single site's password does not put the user's other accounts at risk.

When creating a password for a site, there is another hurdle to overcome. Many sites have introduced restrictive "*password policies"*. The idea behind password policies is that they should prevent users from using passwords that are too simple. Password policies can require that the user's password include at least one symbol or number, for instance. Unfortunately, password policies are often abused to restrict the types of passwords users can set in ways that do not improve or even *negatively affect* the security of a user's password. For instance, a site may demand your password start with a letter, or is no longer than 8 characters.

---

3 http://www.zdnet.com/blog/security/survey-60-percent-of-users-use-the-same-password-across-more-than-one-of-their-online-accounts/9489

4 http://www.washingtonpost.com/business/technology/linkedin-eharmony-lastfm-hacks-highlight-bad-passwords/2012/06/08/gJQAq6ktNV_story.html

5 http://www.washingtonpost.com/business/technology/linkedin-eharmony-deal-with-breach-aftermath/2012/06/07/gJQAwqs5KV_story.html

6 http://passfault.com/passwords.shtml#menu

Master Password deals with password policies by allowing the user to choose a password type for a site. The standard password type generates a secure 14-character password. If this password is not accepted by the user's site, a different type of password can be selected that fits the site's password policy. Master Password also supports a "maximum security" password type that generates a 20-character password with increased *"entropy"*. Even the best funded attacker cannot hope to guess such a password.

It happens that users are unable to choose their own password and are instead forced to use a system-generated or administrator-imposed password. Master Password has built-in support for AES-encryption that allows a user to save custom passwords within the app. Passwords are subsequently encrypted with the user's master password. These types of passwords unfortunately do not benefit from the many *unique* advantages that Master Password has to offer.

Finally, and this is a key feature that strongly differentiates Master Password from the competition: since generated passwords don't need to be saved, users of Master Password are no longer reliant on their physical device or its data. **An iPad can break, backup hard disks can become faulty or outdated and an iPhone can easily be left on the night-stand.** Users of Master Password need only a working iOS device (and soon, *any Mac*) with Master Password installed and it can be used to generate any of their passwords simply by recreating their user on the new device (they can, for instance, borrow a friend's device). No backups to restore, no account to sync, and no passwords left behind on a borrowed device.

There exist already a multitude of password management solutions today. Most of these rely on encryption to store a user's passwords, or upload them to the company's servers.
Master Password's stateless approach to security differentiates itself from these solutions by guaranteeing that the user can get his passwords back; even if he loses everything he has.

Master Password is $9.99 (US) and available world-wide from the Apple App Store for any iPhone, iPad or iPod touch with iOS 5.0 or up.

For any questions, media inquiries or application details regarding Master Password, please contact Maarten Billemont at masterpassword@lyndir.com.