Enigmaze User's Guide

Create, store and share strong internet passwords

As we will see, there are many varied ways to use the Enigmaze password log book, and in this short guide we will explore several of them. It is important when creating passwords to use eight characters or more, each successive character adding to the *entropy* of the password. Each character added to a password creates an additional exponential layer of difficulty for a hacker to guess or crack using brute force methods. Another common requirement from many websites is the inclusion of upper and lowercase characters as well as numbers and symbols. The Enigmaze grid allows the creation of longer passwords with symbols, numbers and mixed case letters in an easy and more importantly, easy to remember fashion. One other feature worth mentioning is that every page of the Enigmaze consists of a different grid adding to the security of the passwords.
This holds true even if somebody else has your Enigmaze.

Mental Lines

The easiest method to use Enigmaze is to remember a letter from the vertical outer coordinate system.

For example on page one remember that your password is the letter “A”.

This is your password: cSW'=i”hmc%G

Because this method is probably the first to come in mind, we don't recommend using it, but it is the easiest to illustrate.

A better method is to use a portion of the grid and append it to your current password.

Even if you have the same password for all your websites, this will guarantee unique passwords and is easy to recover.

Example: Remember that you append A60 to your current password (Mike67)

The result is: Mike65i”hmc

UV Pen

The UV pen is used in several different ways to draw an invisible line or lines on the Enigmaze. The lines drawn are visible only when illuminated with a UV light, which is provided with the Enigmaze. When not viewed with the UV light, the Enigmaze page appears to be unmarked.

This method is useful to prevent, for example, a guest at your house or office to sneak a look at your notebook while you are gone for a minute. He will open the book and see nothing. The best way to use this method is to use it to add to your existing password. This will prevent problems even if you lose your notebook or it gets stolen.

- You can draw a line or lines either straight or an angle starting anywhere on the Enigmaze grid, whether it be from the edges or the middle or the top or the bottom.
- You can additionally draw a curved line.
- You can even combine straight, angled, and curved lines.
- You can highlight different letter or symbols.
- You can highlight different letters or symbols as reference points.

When it's time to decode the invisible lines, simply illuminate the Enigmaze page with a UV light. Also, remember that the UV pen is not erasable, so when it's time to change or update the password you need to change the page or mark your lines so you know which one is currently in use.

Overlay Card

Cut a page size clear plastic piece from a product package or buy a plastic sheet from your local office supply store. Open the Enigmaze to your desired page (example on "G" for google) and place the plastic over the page. Using a permanent marker you can:

- Mark a line or lines that will cover a portion of the Enigmaze page showing the password.
- Mark reference letters or symbols to act as a key (alignment) to find passwords.
- Mark a memory device or devices to act as a reminder key to find passwords.

Also, with the overlay cards, it's impossible for anyone to guess or decipher your passwords. Even if they have your Enigmaze. With your overlay card and Enigmaze, it would still be tricky for someone to decipher your passwords because the card can be placed in a specific locations on the page, and it's orientation can be horizontal, vertical, reversed or even placed upside down.

This method is useful if you change your passwords often and keeps your book neat.

Using Various Key words and Phrases

Another popular method for encryption that requires minimal memorization is using the domain name as a legend for generating a password. With this method you would locate each letter of the domain name in the grid either in a row or column and draw a line connecting them. At this point you could use the letters between your target letters or letters above and/or below or any combination of methods as your password as long as you remember and apply your rules consistently. This method makes a very strong password that is very easy to remember. This password would be very difficult to crack (as long, of course, it was eight or more characters). All parts of a URL or domain name are represented on the grid, so this

method can be implemented in varying degrees of complexity. For example: *amazon* or *amazon.com* or *www.amazon.com*, and many other permutations can be used.
Similar to using website domain names as in the previous example, another way to use the Enigmaze is with random legend characters. One example is using the phrase E2K4 where you would draw a diagonal line from The ‘E’ character on the left side column to the number 2 on the top row above the grid. Similarly you would draw a line from the ‘K’ to the number 4. Doing this you have, in this example, created a twelve character password: peNY3!:~%UqT

Yet another way to generate a password is by using a memorable phrase. By locating the letters of the phrase in a column or row you can substitute a nearby character or characters for that letter. For example: *Password* would encode to: B^##%S.)

So, as you can see, creating a significant number of characters for a password is extremely easy. And in addition to the simplicity of creation, the memorization of the key code is trivial.

One final point to remember, the Enigmaze can be used in many custom ways that are not even documented here. The possibilities are practically endless. Additionally, you are not restricted to just one method of use with the Enigmaze. In fact, multiple methods of encryption are encouraged to increase the security of the generated passwords. Even using multiple methods, the memorization of the keys, phrases, site names, or however you’ve decided to encode your passwords is not extremely difficult. This not only adds to the security of the Enigmaze, but also this adds convenience. A password manager that is difficult to use probably will not get used! Again, the Enigmaze makes security that much more accessible.

Upside down and backwards technique

Use this technique to spell upside down (and/or backwards) your name or another word that is easier to remember. Use letters and numbers. If you are unable to find a number that exactly matches a letter, then use a letter, but write it so that it ends up upside down. Thus, you use many letters and numbers for added security. This technique is heavily dependent on what you consider to be close to the form of a letter.

Imagine that your name 'BORIS', then your password could be SIROB ('BORIS' backwards). 'Steph' could be re-written as HPETS. You can increase security even more by adding punctuation i.e. '!' HPETS!

With the Enigmaze Notebook, you can also make a passphrase and then write it backwards. By locating the letters of the phrase in a column or row you can substitute the passphrase with letters, numbers and symbols in the grid. The benefits are enormous, because it is a highly secure password and very hard to locate, if not impossible.

Drawing randomly on the grid

This is one of the best methods of obtaining a secure password. Using the UV pen, you can draw a line randomly either horizontally, vertically, diagonally or any other way. After drawing the line, you match the grid's characters to their corresponding outer vertical and horizontal coordinate system. In this way, you come up with a very secure password that is hard to crack but easy to store in the Enigmaze. Moreover, the password can only be seen after illuminating the grid with a UV light.

Example:

After randomly drawing the following characters on the grid: peNY3!:~%UqT

Match them to their corresponding outer coordinate system.

This may result to characters such as E2K4.This is your password.

Alphabetic tabs

Another secure way you can use the Enigmaze to create secure passwords involves the use of its alphabetic tabs. Let's say you want to record your gmail account passwords. The most obvious thing to do would be to locate the letter g in the alphabetic tabs. This is a very easy way for intruders to search for your specific passwords in a short matter of time.

With the Enigmaze, instead of using this obvious method, you can substitute the letter in question with the letter which follows it in the alphabet.

For example, we can substitute 'g' with 'h', 'z' with 'a', the list goes on and on. In this way, you can write down even the simplest of passwords without having to worry much about your passwords being compromised.

Create your own mnemonic system to generate unique passwords.You never forget it.

This method involves coming up with your own mnemonic system to create a password. You can then use the Enigmaze to secure your password.

Here's how:
1. Start by defining a complex base password that does not match any word in the dictionary. The best way to remember is to use a word that you know by heart, and use the first letter of each sentence.
Take the lyrics of a song, for example:

"I speak of a time that less than twenty years”
Retrieve the first letter of each word and keep the numbers in digital format:
isoattltty
2. Modify this basic password depending on the site you are using:
For example, you may decide to place the last letter of the name of the site at the end of the password, and the first at the beginning:
To connect to Amazon, you put the letter "n" at the beginning of your password, and the letter "a" at the end:
nisoattlttya
You may also choose to use the letter following the first in the alphabet ("a" becomes "b" and "t" becomes "u"):
nisobuuluuyb

3. After getting your memorable phrase or password from the mnemonic system, it’s more secure mapping your password to corresponding characters in the Enigmaze's grids as shown in previous examples.

The idea is to follow a simple system, and stick to it. You can go even further by using a different model of password creation for each type of service: work, personal, finances. Why not use, for example, the lyrics of a song related to each theme? You'd be sure to always remember your base password.

Leet speak

Create a password you can remember using 'leet speak'. For instance ‘hello’ translates to H3ll0. 'Leet' speak substitutes numbers for many common letters. The most common examples are: 'a' = 4, 'e' = 3, 't' = 7, 'l' = 1, 'o' = 0, 's' = 5.

By adding a random letter or symbol the security of your password will increase. For example, you can add the first two numbers of your date of birth in front of the password and the last two at the end of the password. This translates to 19H3ll067.

Using the Enigmaze, map the letters and numbers in the password to their corresponding characters in the grid.

This letter substitution method by numbers is called "Leet Speak." It is used in several hacking programs, which makes it relatively safe. Remember to use this method within a broader password or pass phrase context.

Secure personal details combination

Since our personal details are the easiest passwords to remember, they are prone to hacking through social engineering and other methods. However, with the Enigmaze, you need not worry. You don't have to create complex passwords that are easy to forget.. Just memorize your simple passphrase and the Enigmaze will do the rest.

Find your phone number or postal code on the keyboard of your computer. Read the letters immediately below the numbers. Let's say you chose the number 1. The letter immediately below the 1 key is Q.

Now, let’s say your phone number is 187658880.When you create your password, it will be QIUYTIIIP. Do this for the entire sequence of numbers you intend to convert into passwords.

Now all you have to remember, are the letters instead of the numbers. With the letters memorized, you can now use the Enigmaze.

Pick the letters in your password from the vertical and horizontal coordinate systems and map them to their respective grid entries.

Chronological method

Use this method in case you need to change your passwords frequently. You only need to memorize the simple phrase you created so that you can use it in the Enigmaze to create more secure passwords.

1. Create a Password You Can Remember.
2. Integrate a part of a date within a broader password. This can help when one needs to change the password occasionally.

Use the current year and the first three letters of the current month, then add three letters of your first name. For example, if your first name is Michael, you get something like 2015JulMic. The following month, change it 2015AugMic. This will make it impossible to use the same password twice and you will not forget it.

Next, uses the Enigmaze to create a stronger password through the mapping system discussed in previous examples.

What to avoid – Enigmaze tips

Avoid the use of simple passwords

Avoid the use of simple passwords since they are prone to social engineering techniques used by hackers. For the Enigmaze, it will be easier for intruders to draw several permutations on the grid based on personal details. Therefore, you should avoid the following:

- Avoid passwords that use too obvious identification data (e.g. date of birth, place of birth, phone number)
- Avoid -especially for professionals - to disclose personal information on social net-works, hackers can use it to guess passwords.
- Avoid the use of linear strings: 123456

Never use the same password on different sites

There are means, from the previous method, to have a different password for each site you have recorded in the Enigmaze: You can use a phrase or word related to the site, for example: "your middle name, fb".
Alternatively, use part of the domain name in your password.
For example, if your password is hggghg use:
fbhggghg
(Or any other part of the domain name: the two ending letters, etc. Your choice.)
So:
All you need to remember is a password or phrase (The specific password to the site can be deduced from the name of the site).

Do not use personal information in simple ways

Avoid using any personal information. If the attacker knows your identity, it will be easy to establish your password even with the Enigmaze. Below is a list of types of information to avoid when creating a password. Avoid the following choices:

- Your name
- The names of pets
- The names of family members
- Any birth dates
- Your phone number or zip code

Avoid reversing recognizable words

Though it might take a lot of time, intruders and hackers can decipher your passwords from the Enigmaze if you use simple reversed recognizable words.

Do not use simple leet speak

If you think you are part of the elite because you use hacker terminology - also called 1337 Language (FEL) - in your password, do not use the most common ones! Indeed, many word lists include LEET speak.
For example, avoid the following choices:

- H4X0R
- 1337

Avoid using recognizable words

Avoid using words such as proper names, dictionary words, or even terms from television shows or novels.
For example, avoid the following choices:

- john
- Andrew
- mental

NEVER use one word

One of the most popular password hacking methods is attempting dictionary words. As shown in the manual, it is much safer to use more than one word for the sake of password complexity.

Create a Password You Can Remember

Create compound words. A clever way to create an easy to remember password is to combine three short words with a special meaning to you, into one. For example, you could use "littlecuteralphy".
For added security, you can put a symbol at the beginning of each word. Thus, “littlecuteralphy" becomes "@littleCuteRalphy ". In terms of security, longer passwords are more secure than shorter ones even if they are a random mix of numbers, letters and symbols.

With the Enigmaze, you can always record such passwords securely.