PASSWORDWRENCH

Password Managers: Devil's in the Details

How Can Giving all your Passwords to a Password Manager be Safe?

AUGUST 2018

Passwords are dead; long live the password! Passwords are unequivocally the most used entry point to anything online, and the most unsecure. Users know this. Companies know this. And hackers certainly know this. To create complex passwords is important, but managing them – remembering them, updating them, etc. – is cumbersome. Password managers help, but are they secure? Given the rampant data breaches that seem to occur every few weeks – and those are only the ones we hear about – how can giving all your passwords to a password manager be smart? Forsaking security for convenience: is there a better way?

Let us dissect why passwords aren't going anywhere – at least not yet, along with a novel solution for solving the problem of password management while still maintaining security.

There are enough vendor-neutral reports today that show that most people, sites, and companies are using or require the use of passwords the wrong ways, posing imminent security risks.

Biometrics Are Different from Passwords

It's important to point out first that a password is something that is created by the user. This sounds simplistic but consider it. A password is something that, when created properly, is associated directly with the user and only the user and the system knows it. Now, if we introduce alternatives, namely biometrics such as fingerprint readings or facial recognition, it's supposed to be data that represents only you. Why is this different? When a system uses biometrics for authentication, the system must rely on third-party software to provide accurate information to indicate whether the fingerprint is a match or not. The software itself could be buggy or contain hard-coded logic to provide false positives.

Even if an open-source biometric matching software is used, which would facilitate the discovery of bugs and incorrect logic, what is used to produce the "match" is not the open source code, but the binaries after that code has been compiled. Therefore, the compiler could be compromised, and this poses a security risk.

And the biggest as-yet-unsolved problem with biometrics is that they are not renewable. In the rush to build accurate biometric analyzers, they are based on the premise that your face, fingerprints, heartrate, gait, voice, etc. are uniquely yours, which currently they are. Until they're not. When your personal biometrics are stolen – which they will be - how do you replace them? Grow new fingertips, alter your voice or buy new retinas? The black market of body part replacement a la the movie Minority Report will be a real thing.

How to Use Passwords to Reduce Security Risks

When a user thinks up a password, there is no need to rely on any third-party software, thus, it's a direct connection between the system and the user. Using a third party software to provide accurate information poses security risks. Therefore, using a password for authentication decreases security risks, **when used correctly.**

How does one *improperly* use a password? Here is where the crux of the problem resides. There are enough vendor-neutral reports today that show that most people, sites, and companies are using or require the use of passwords the wrong ways, posing imminent security risks. The main issues with passwords are well known. A password must be long and complex enough to be secure, and should not be comprised of known words, sequences or repetitions, or used repeatedly. For all of these reasons, a complex password should be long and random, which means that it's difficult to remember and takes a long time to type it in using a keyboard. Thus, a properly created and utilized password has become less convenient to use.

For convenience reasons, people understandably like to use the same passwords that they've memorized over and over. Some people have been using the same set or variations of the same passwords for all their logins for years because it's easy to log in using that same password they can remember. Sometimes people add a few characters to it when a system forces them to change a password. It's done for convenience. Unfortunately, because that same password could have been compromised from a system that failed to report it to anyone, security risks increase every time it's used.

To improve security, systems create minimum password requirement rules, making it harder to memorize passwords. These are usually some combination of upper, lower case characters, numerics and/or symbols. Users may find themselves trying to remember if it was Citibank or their 401k savings account that doesn't allow special characters. Out of frustration many of us just never change them once we get in with a weary shrug and an, "If it ain't broke, don't fix it" attitude.

Website Security

Let's talk a little more about these websites that we log into so gullibly, giving them our credit cards, bank information, logins, mother's maiden names, dates of birth, and so much more. First, many sites are still using plain HTTP for authentication, ignoring industry best practices which have standardized HTTPS/SSL to cover logins. Every user is responsible for taking note of such systems and avoiding using them, or else they are exposing their passwords for anyone to grab. There is at long last momentum in the industry to report such systems and force sites to use HTTPS. This is all good news, and this issue has almost been eliminated by now even though using them across unsecured wifis remains a big problem. But the other issue is that many sites are not encrypting passwords inside their systems, going against all best practices. If hacked, your password will be compromised. We've all heard enough reports of companies being hacked and passwords being exposed, and those are just the ones that are known. Due to the bad publicity, of course, some companies fail to report hacks to their users. This is one of the main reasons you see policy rules in companies that care about security that force you to change your passwords regularly.

Sharing Passwords

Sometimes we have to share passwords with other people. It's not a best practice, but it happens all the time – consultants, colleagues, family members. If you are the user who creates a password and uses various versions of that password over and over again "JaneDoe1", "JaneDoe11", Jan3Do3" etc., you don't want to share that with anyone lest they figure out that you use variations of "JaneDoe" for everything. Therefore, you have to come up with a new one. It's harder to remember another one. How many can you handle?

And how do you share a password? You can send an email to your colleagues containing the password, but it will expose your passwords for anyone who can see that email. Plus, is your email even encrypted? Most systems aren't. You can simply write it down on a piece of paper or have a conversation over the phone. You call that convenient? If you must modify it because it has been compromised, then you need to do the same steps over again. That's also frustrating.

Why You Need a Password Manager

The longer a password is, the safer it is, but with each character added for safety, it's equally less convenient to memorize it as well as to enter it using a keyboard.

These challenges are the reasons why password managers were created, but not all password managers are secure. Using third-party tools could increase security risks, so it's imperative that you use a secure password manager.

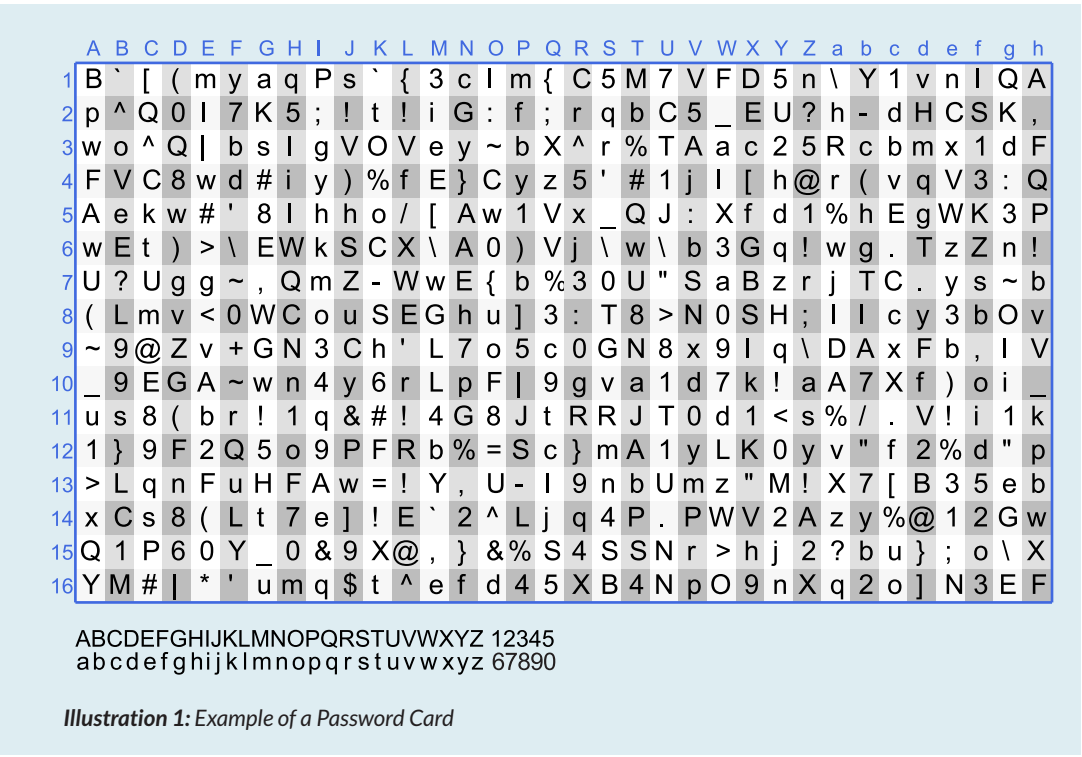
Some of the benefits you should expect from using a trusted password manager include:

- Ability to generate long and complex passwords.
- Ability to reconstruct existing passwords, not storing them in their database waiting to be exposed.
- Ability to share a password with other people safely.
- No need to remember any passwords.
- Convenient enough so that only a few clicks and keyboard keys are used to enter a password. For example, a password of 32 characters would take less than three clicks to enter into a site whereas entering it one by one would take a while and inevitably be bound to be error-prone.
- Encrypted and using HTTPS/SSL. Following best practices.
- Does not force you to reveal your passwords. This is easy to say but not easy to do, since most existing password managers require users to reveal their passwords and by doing that, the passwords are already compromised.

What Makes the PasswordWrench Approach Different?

Now, we're going to dig into our system, as we've taken a novel approach as a solution: PasswordWrench. Our solution is intriguing because the system does not record passwords, and does not ask users to reveal their passwords, already leapfrogging it ahead to be one of the more secure password managers. But you want to know how it works and if it is easy to use, and whether the balance of *convenience vs. security* is met?

The basis of the system uses an innovative approach, mixing what is termed a "Password Card," alongside a "Password Hint." The Password Card is a grid of random characters, as seen in illustration 1.



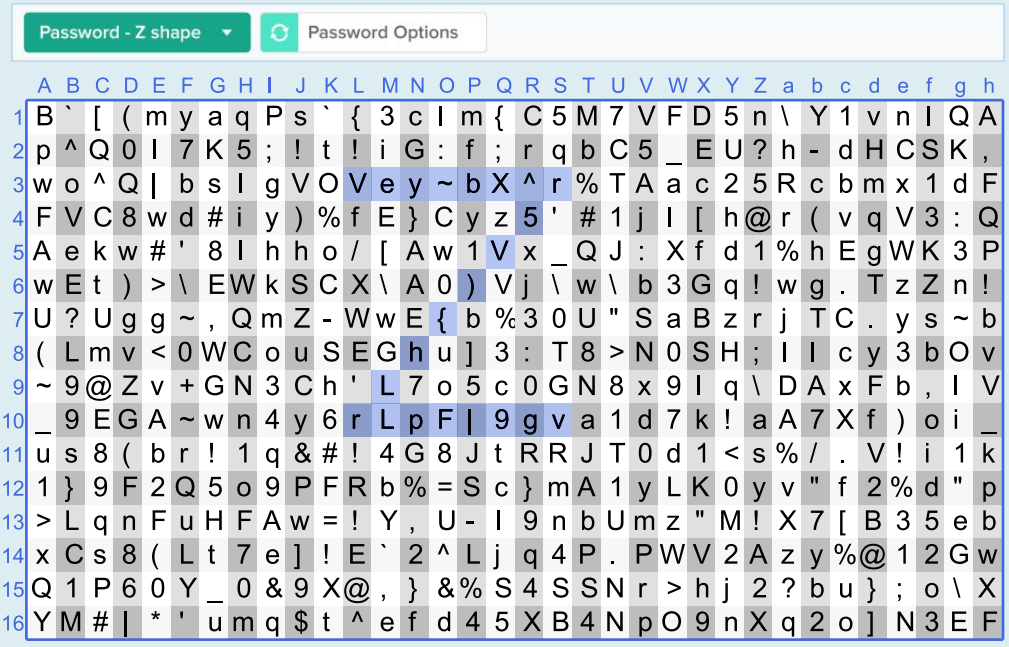
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	a	b	c	d	e	f	g	h
1	B	`	[	(	m	y	a	q	P	s	`	{	3	c	I	m	{	C	5	M	7	V	F	D	5	n	\	Y	1	v	n	I	Q	A
2	p	^	Q	0	I	7	K	5	;	!	t	!	i	G	:	f	;	r	q	b	C	5	_	E	U	?	h	-	d	H	C	S	K	,
3	w	o	^	Q	|	b	s	I	g	V	O	V	e	y	~	b	X	^	r	%	T	A	a	c	2	5	R	c	b	m	x	1	d	F
4	F	V	C	8	w	d	#	i	y	)	%	f	E	}	C	y	z	5	'	#	1	j	I	[	h	@	r	(	v	q	V	3	:	Q
5	A	e	k	w	#	'	8	I	h	h	o	/	[	A	w	1	V	x	_	Q	J	:	X	f	d	1	%	h	E	g	W	K	3	P
6	w	E	t	)	>	\	E	W	k	S	C	X	\	A	0	)	V	j	\	w	\	b	3	G	q	!	w	g	.	T	z	Z	n	!
7	U	?	U	g	g	~	,	Q	m	Z	-	W	w	E	{	b	%	3	0	U	"	S	a	B	z	r	j	T	C	.	y	s	~	b
8	(	L	m	v	<	0	W	C	o	u	S	E	G	h	u	]	3	:	T	8	>	N	0	S	H	;	I	I	c	y	3	b	O	v
9	~	9	@	Z	v	+	G	N	3	C	h	'	L	7	o	5	c	0	G	N	8	x	9	I	q	\	D	A	x	F	b	,	I	V
10	_	9	E	G	A	~	w	n	4	y	6	r	L	p	F	|	9	g	v	a	1	d	7	k	!	a	A	7	X	f	)	o	i	_
11	u	s	8	(	b	r	!	1	q	&	#	!	4	G	8	J	t	R	R	J	T	0	d	1	<	s	%	/	.	V	!	i	1	k
12	1	}	9	F	2	Q	5	o	9	P	F	R	b	%	=	S	c	}	m	A	1	y	L	K	0	y	v	"	f	2	%	d	"	p
13	>	L	q	n	F	u	H	F	A	w	=	!	Y	,	U	-	I	9	n	b	U	m	z	"	M	!	X	7	[	B	3	5	e	b
14	x	C	s	8	(	L	t	7	e	]	!	E	`	2	^	L	j	q	4	P	.	P	W	V	2	A	z	y	%	@	1	2	G	w
15	Q	1	P	6	0	Y	_	0	&	9	X	@	,	}	&	%	S	4	S	S	N	r	>	h	j	2	?	b	u	}	;	o	\	X
16	Y	M	#	|	*	'	u	m	q	$	t	^	e	f	d	4	5	X	B	4	N	p	O	9	n	X	q	2	o	]	N	3	E	F

ABCDEFGHIJKLMNOPQRSTUVWXYZ 12345
abcdefghijklmnopqrstuvwxyz 67890

Illustration 1: *Example of a Password Card*

The Password Hint is a hint that is recorded in the database in order for users to "reconstruct" their password when needed. Let's show some examples of how this system meets the needs of convenience while still eliminating potential security threats.

The application allows you to generate a password automatically using different shapes such as a line, a Z shape, an L shape and so on. You can pick any shape you like. In this example, here we show a "Z" shape.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	a	b	c	d	e	f	g	h
1	B	`	[	(	m	y	a	q	P	s	`	{	3	c	I	m	{	C	5	M	7	V	F	D	5	n	\	Y	1	v	n	I	Q	A
2	p	^	Q	0	I	7	K	5	;	!	t	!	i	G	:	f	;	r	q	b	C	5	_	E	U	?	h	-	d	H	C	S	K	,
3	w	o	^	Q	|	b	s	I	g	V	O	V	e	y	~	b	X	^	r	%	T	A	a	c	2	5	R	c	b	m	x	1	d	F
4	F	V	C	8	w	d	#	i	y	)	%	f	E	}	C	y	z	5	'	#	1	j	I	[	h	@	r	(	v	q	V	3	:	Q
5	A	e	k	w	#	'	8	I	h	h	o	/	[	A	w	1	V	x	_	Q	J	:	X	f	d	1	%	h	E	g	W	K	3	P
6	w	E	t	)	>	\	E	W	k	S	C	X	\	A	0	)	V	j	\	w	\	b	3	G	q	!	w	g	.	T	z	Z	n	!
7	U	?	U	g	g	~	,	Q	m	Z	-	W	w	E	{	b	%	3	0	U	"	S	a	B	z	r	j	T	C	.	y	s	~	b
8	(	L	m	v	<	0	W	C	o	u	S	E	G	h	u	]	3	:	T	8	>	N	0	S	H	;	I	I	c	y	3	b	O	v
9	~	9	@	Z	v	+	G	N	3	C	h	'	L	7	o	5	c	0	G	N	8	x	9	I	q	\	D	A	x	F	b	,	I	V
10	_	9	E	G	A	~	w	n	4	y	6	r	L	p	F	|	9	g	v	a	1	d	7	k	!	a	A	7	X	f	)	o	i	_
11	u	s	8	(	b	r	!	1	q	&	#	!	4	G	8	J	t	R	R	J	T	0	d	1	<	s	%	/	.	V	!	i	1	k
12	1	}	9	F	2	Q	5	o	9	P	F	R	b	%	=	S	c	}	m	A	1	y	L	K	0	y	v	"	f	2	%	d	"	p
13	>	L	q	n	F	u	H	F	A	w	=	!	Y	,	U	-	I	9	n	b	U	m	z	"	M	!	X	7	[	B	3	5	e	b
14	x	C	s	8	(	L	t	7	e	]	!	E	`	2	^	L	j	q	4	P	.	P	W	V	2	A	z	y	%	@	1	2	G	w
15	Q	1	P	6	0	Y	_	0	&	9	X	@	,	}	&	%	S	4	S	S	N	r	>	h	j	2	?	b	u	}	;	o	\	X
16	Y	M	#	|	*	'	u	m	q	$	t	^	e	f	d	4	5	X	B	4	N	p	O	9	n	X	q	2	o	]	N	3	E	F

Illustration 2: *Example of an automated generated password, Z shape.*

In illustration 2, you can see the Password Card and a Z shape of selected characters which represent the password that it auto-generated. What PasswordWrench is recording in our database is the "Password Hint" generated (i.e. L3-S3-L10-S10). and not the actual password. All the information recorded is encrypted like any good password manager does, but in this case, if hacked, like many other good password managers have been, the hacker will obtain only an encrypted Password Hint. Without the Password Card, it's useless. The Password Card is generated on the fly and does not reside on the database, so a hacker won't be able to generate the Password Card. It's also convenient to use in this mode since only two clicks were necessary to generate a 22 random-character password.

In general, as security experts, we don't like auto-generated anything, especially not when it comes to our passwords. The attraction is clear for most users, but automated mode is not a high enough priority for people who care about security standards. So, even if it's one of the most secure existing password managers, there are still very real potential security threats that a user might want to eliminate. Let's talk about them and see if and how they can be addressed.

As mentioned above, using the automated feature of PasswordWrench, even if the Password Hint is the only thing recorded (such as L3-S3-L10-S10), in the extremely unlikely scenario where someone gained access to the database AND knew the system's always-changing algorithm. You, as a user, can simply eliminate that threat completely by creating a Password Hint yourself manually. Using the same Password Card above, instead of generating an automatic password, we can enter a hint in the Hint field. In this example, we could write something like "Row 1" which would mean the characters on the Password Card in row 1. Now we obviously want to come up with a Password Hint that is not that easy to reverse engineer, so it's up to you to come up with something strong enough for a reminder, but that would not reveal everything to a possible insider. In our example, if we write "row 1," that could mean all the characters in row 1, but we can do easy things, such as excluding the last character. That way, the threat is eliminated, and even if anyone captures your Password Hint, they would not be able to easily reverse engineer it, which sustains a very high level of security.

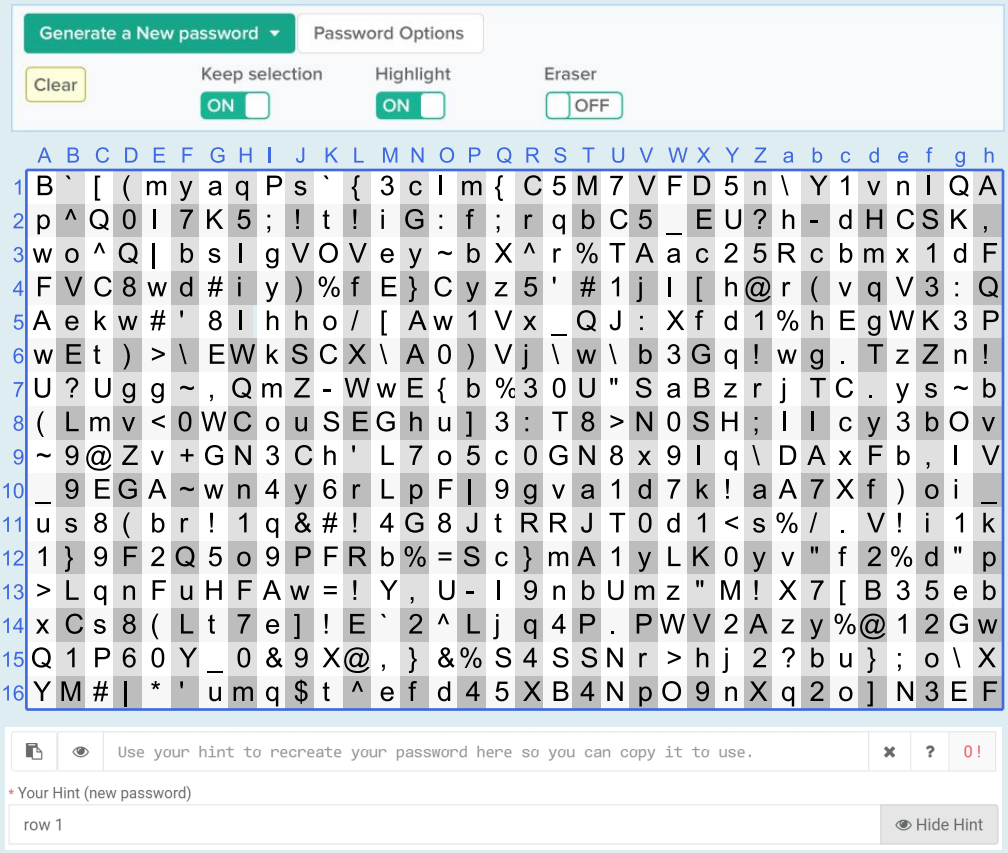


Illustration 3: *Example of a manual Password Hint.*

In our example above, when it's time to reconstruct the password, you can click on the row 1 header, it will select the characters

B`[(myaqPs`{3c|m{C5M7VFD5n\Y1vn|QA

with 1 click. Then you enable the "Eraser" and select the last character of the row which is located at h1, removing the character "Z." The password obtained is then

B`[(myaqPs`{3c|m{C5M7VFD5n\Y1vn|Q

Another convenient way that would still eliminate threats is to use the PasswordWrench tools to mix the auto-generated password with a few characters that you add after it has been constructed. Those extra characters that you add manually could be from a pattern on the Password Card. If you use a pattern on the Password Card, and you use a different Password Card for every site you log in to, so that even if you use the same pattern, the characters will be different. A very simple pattern example would be to use the character in position A1. If you use two different Password Cards, the character at position A1 is different.

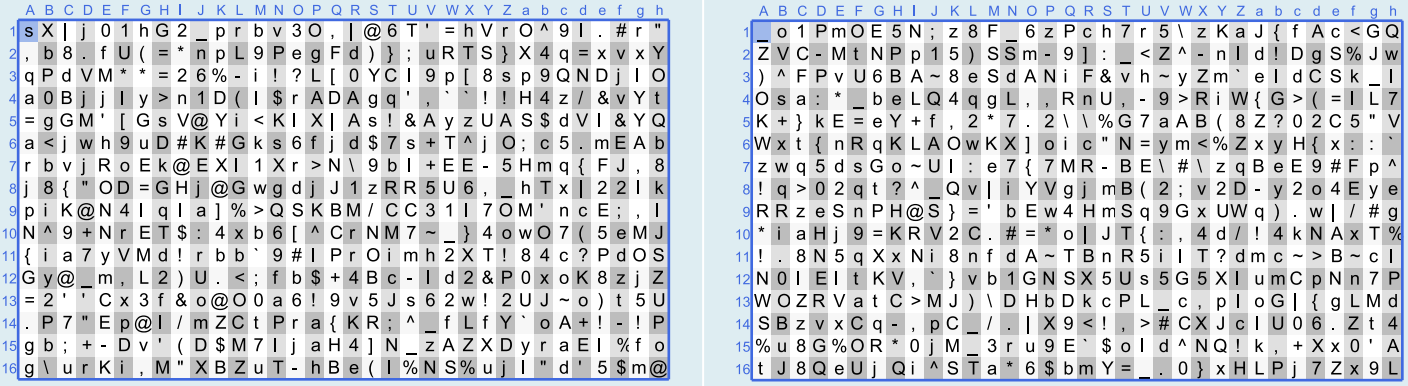


Illustration 4: *Example of 2 different Password Cards side by side with character A1 selected.*

So, in this example, we were able to generate a password of 32 characters with one click, then we added one character using position A1 which is easy to remember, we were able to obtain a password of 33 characters with one click and one keyboard key press. This is very convenient and eliminates the security threat. Additionally you could add your own characters to every password at the beginning or end, such as initials or a special number or date.

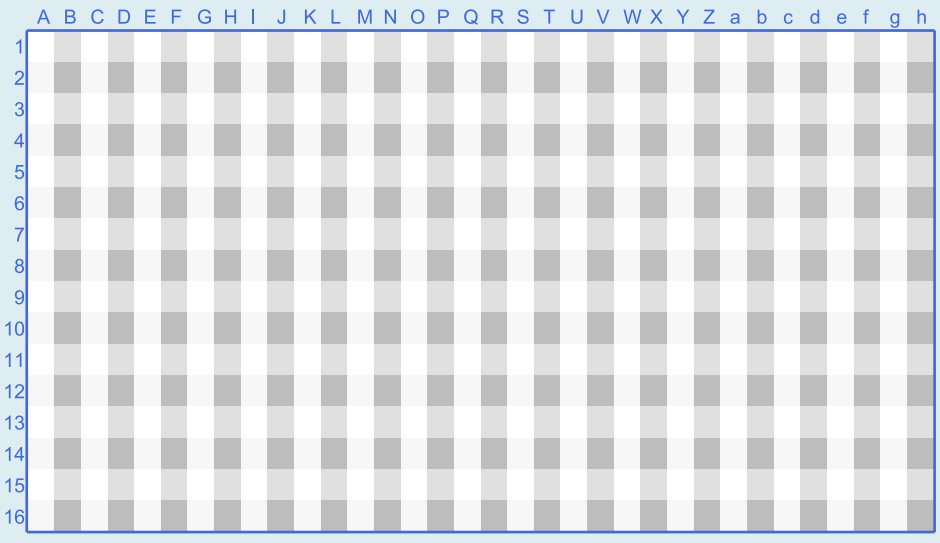


Illustration 5: *Example of a Password Card without characters.*

How PasswordWrench Protects Against Other Threats

There are of course also other threats. What if you are somewhere and a camera, hidden or not, can record everything you see on your monitor? Eliminating that threat is possible. There are actually a few ways to do this. The most convenient way would be to disable the highlight feature so that the characters are no longer selected on the Password Card when reconstructed. Another option would be to disable showing

the characters on the Password Card. That way, no one would know the Password Card, but the password will still be generated.

The issue here though is that we wouldn't know what the character is at the position A1 from our previous example. We can either print the Password Card, and we could see what that character in A1 is, or we can click on the square at the position A1 and the system will add that character into the password. This is a convenient way to reconstruct your password without displaying your Password Card on your screen.

Since working in cyber security has made us all inherently suspicious, we know that someone still might be able to figure out your pattern, because there are still UI cues that a camera could capture. The camera won't know what the password is when generated automatically, but the character you click at A1 will be known since the mouse is pointing there, and when you click at that position your password length increases. Ultimately, for the hardcore users, the ones who require absolute security, the PasswordWrench team has actually thought about this possibility and introduced a mode called "Stealth." When turned on, there are no UI cues shown whatsoever. It's a little bit difficult to use at first, but after a few times it becomes more natural.

Protect your Password Manager login

Now that you are familiar with the concept of the Password Card and Password Hint, the next question is how do you protect your master password? The one that you use to login to PasswordWrench? There are many possibilities, with pros and cons for each. Let's explain.

- You can use a simple password that you can memorize. The benefit is that it's easy to remember. The downside is that you are going to have to change it at some point to meet all the website requirements, and you should not use the same password over and over. You should be taking advantage of a Password Manager.
- You can use PasswordWrench and print out a Password Card and/or download an image of it to use. We've conveniently made the printed version the size of a credit card so you can slip it in your wallet. The negative of that is if you lose the printed Password Card or the downloaded image, you won't be able to log in and you will be forced to go through the "forgot password" process. The benefit is that it's very secure and you can manage your login Password Card within PasswordWrench.
- You can also use the "Password Assistant." When you log in, you will see a button beside the password field called Assistant. What this does is generate a Password Card from a PIN or code you enter. The downside to this solution is that using the same code for any user will generate the exact same Password Card. Of course, a user wouldn't have your password, just the card. The pro is that it's like having a Password Card that can never be lost. It's obviously important you use a code that only you know, but it doesn't need to be complex. You can still add or subtract characters to it as well.

Do You Want Security?

Passwords are effective at protecting users' credentials when used responsibly. They are a direct link between a user and the system to authenticate without the need of using third-party tools, keeping security threats to a minimum. It's clear that everyone should make an effort at protecting their data, and most of us naively tend to believe that big companies are going to take care of it for their users and the government is going to track down the criminals and the world is safe. Security is a collective effort, and that's the bottom line. There are tools out there worth adding to your list of "must have" tools, and you should make PasswordWrench one of them. It's a tool that gives you flexibility on how you want to protect yourself, making protecting yourself convenient without compromising security. If you want security, PasswordWrench is there for you. There is even a FREE plan available.

We offer FREE plans, try it today!