# How to Safeguard Your Private Keys and Passwords

*Shôn Ellerton, Sep 04, 2017*

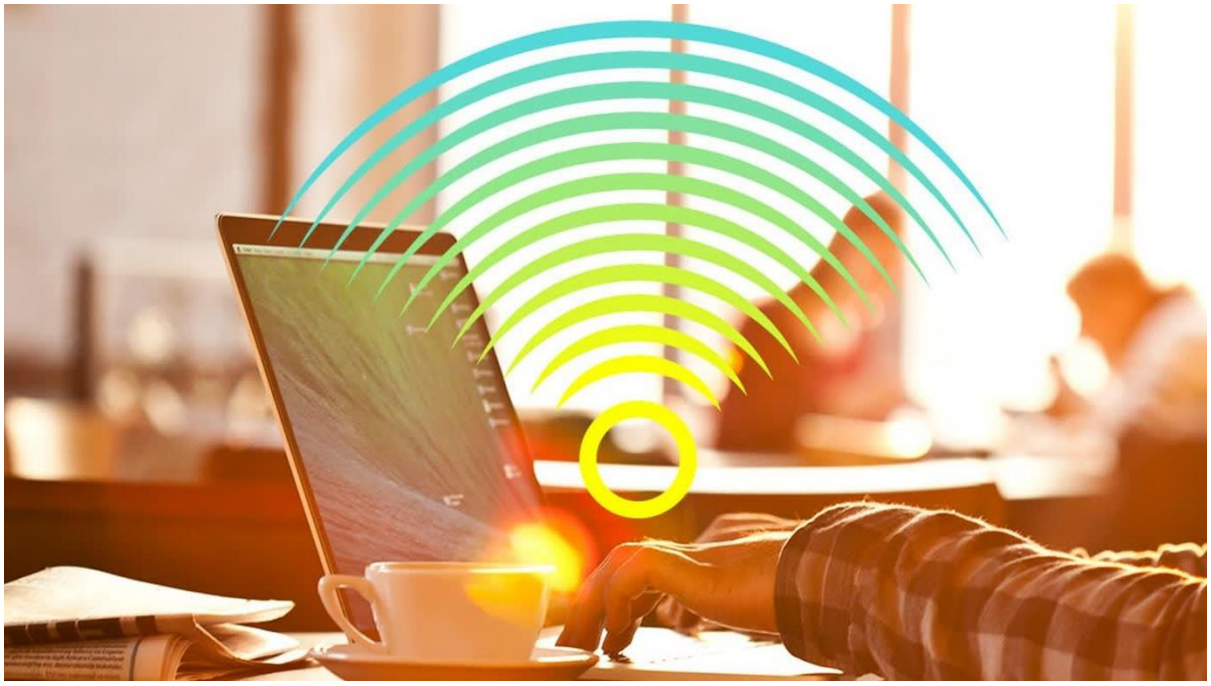
*Don't be an unfortunate victim to an enterprising hacker. Here's a simple way to keep your passwords and private keys safe.*


If you've ever been hacked or know of an attempt by someone to hack your account, it is a very unsettling experience. Here are a few tips I'd like to share with you which you can adopt to decrease your chance of getting hacked.

First, let's start with nine obvious tips.

## 1. Don't set up passwords and private keys on a public or wireless network.

Just don't. This especially includes establishments with free wireless Internet services. If you live around others and want to use your private network, try to use your wired network port. If you have to use wireless, make sure it is highly encrypted (e.g. AES encryption).



## 2. Don’t set up passwords and private keys around other people.

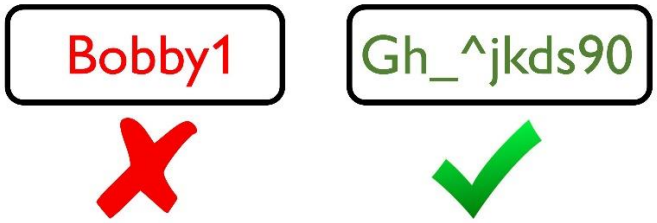
It doesn’t take long for someone to take a snapshot of your screen or scan the QR code if it is revealed. And don’t forget the ‘eye in the sky’. So many establishments have video cameras, some of which have astonishing resolution.

## 3. Always use multiple-step authentication when available

If your account provides 2FA authentication, use it. An example of this is Google Authenticator. Email verification is good practice as well. However, be wary of codes supplied via SMS. There have been cases where hackers have managed to obtain users phone account details and managed to port numbers across to another phone. If your phone or tablet with your authentication app is running on is stolen or lost, immediately disable your account or disable 2FA and then re-enable it immediately. Another note with 2FA: it is good practice to note the key provided and scan to two or more devices. Just ensure your devices are password-protected and secure. More on how to note and mask your key later.

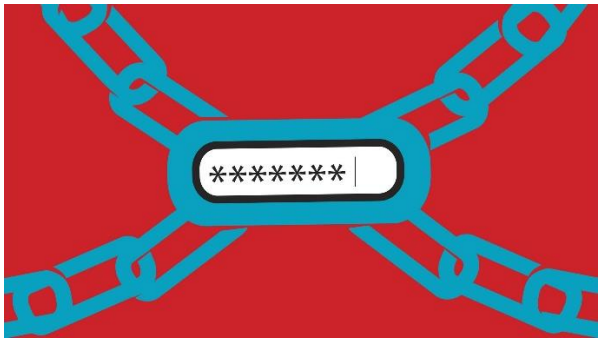

## 4. Always use complex passwords

I am perpetually surprised at some of the passwords that users provide. Seriously, the name of your pet or your kid's name? Use long passwords with a mix of upper, lower, numbers and special characters. For passwords which provide access to important accounts, you should mask these. I will explain this later.



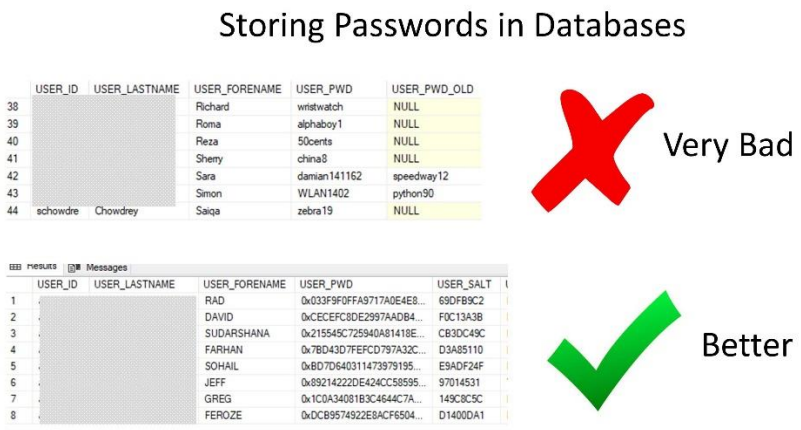
## 5. Don’t use the same password for different sites or accounts

OK. If it is a non-important account like a forum or a site which simply requires you to log in, then perhaps you can get away with a simple password which you commonly use. However, for important sites or accounts, use different complex passwords and mask them. Again, more on masking later.




## 6. Do not assume your passwords are safely stored

I’ve worked in database management before and I can assure you that I have seen databases with completely unencrypted passwords. Most businesses with passwords use the minimum amount of encryption available (for example using MD5 with no salt, if you’re technically savvy on this). Good database security should have far better encryption; for example, AES. If your database administrator knows what your password is; then it’s a FAIL. Banks and password manager sites (e.g. Lastpass) should be using the best encryption possible to protect users’ passwords. There is increasing development on storing sensitive data using blockchain technology; however, your credentials still, somehow, have to get from your browser to the blockchain.



## 7. NEVER send anything confidential to a public or work printer

It is all too easy to print to the WRONG printer. In a multinational company, you could potentially print something out on the other side of the world. Here's an excellent example. Can you imagine if you printed out a paper wallet with a private key to an account; for example, a digital wallet containing a stash of bitcoin. All I can say is you better be quick to set up another account and transfer! Better to physically write down keys and TEST to see you can re-enter them.

## 8. Refrain from using your mobile phone for account access

Try to avoid using mobile phones, if at all possible, to access important accounts. This is especially true regarding access to bank accounts. If you must use your phone to store, say, digital currency, only store a small amount.

## 9. Never share your password

Obvious, but I've heard people on the phone saying, 'Do you need my password?' when calling for IT support or something of that nature. Never reveal your password or key to anyone.

**Note:** There is one occasion where private keys ***should*** be shared, and this applies to digital currency and inheritance. If you unexpectantly pass away or become involved in a fatal accident and you have not shared your private key with a loved one or a family member, there is ABSOLUTELY NO WAY they can ever have access to your digital currency.


And finally, the big one. #10! And this is about masking….

## 10. Avoid writing down or storing important passwords (exactly as they are)

When I mean important passwords or private keys, I mean those which provide access to accounts which can compromise your security, assets or even your safety.

Some background here, but feel free to skip to the simple solution below.

Some examples of important accounts are listed below:

- Bank Accounts;
- Merchant private tokens (e.g. Paypal, Stripe);
- Cryptocurrency private keys (e.g. Bitcoin, Ethereum);
- 2-step authentication keys (e.g. Google Authenticator);
- Pneumonic seed phrases to recover accounts if lost;
- Your main email addresses;
- Your primary social network sites;
- Master password for password vault sites (e.g. Lastpass);
- And any others which can compromise your safety, identity, and so on.

Just to clarify the difference between passwords, private keys and pneumonic phrases:

1) With passwords, you usually have the option of selecting a password and changing it from time to time. Naturally, you would want to select a complex password.
2) Private keys are usually very long strings of characters; something which might look like this: Af76Ej0r980hgYUxfhfd8978fghsj3GHG. Common examples include:
    a. Key created when 2FA (2-step authentication) security is enabled (e.g. Google Authenticator);
    b. Private token key when a merchant third-party payment is activated (e.g. Paypal, Stripe);
    c. Private key when a digital currency (cryptocurrency) address is created (e.g. a Bitcoin address).

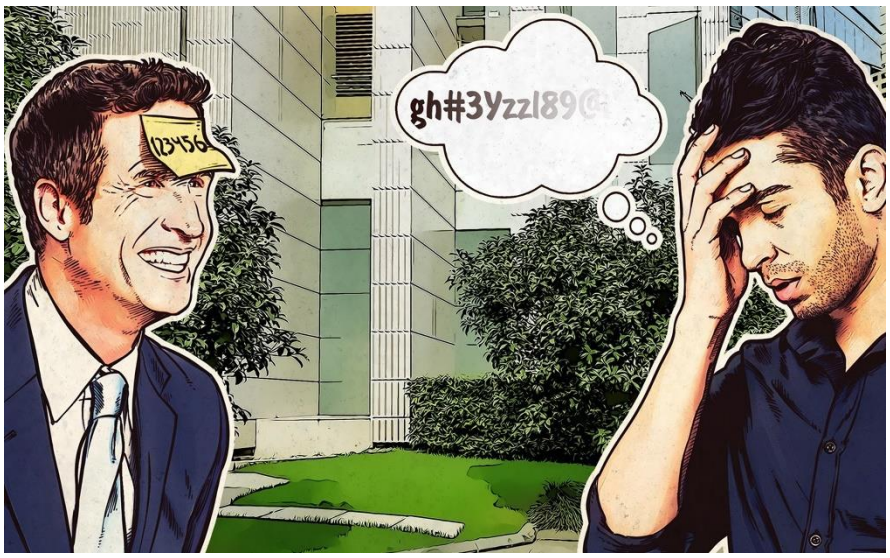
    Private keys are randomly generated and cannot be changed. However, in the case of 2FA authentication, you can disable and re-enable to obtain a new key. Or with digital currency, you can create a new address and transfer your digital currency to the new address.

3) Mneumonic phrases are a randomly generated set of words which enable you to recover your account completely. A typical example would be: ‘stale bread knife windy grey horrible matter’ and you would re-enter the words exactly as they are to recover your account.

Needless to say, if anyone gets their hands on your password AND the key generated by your 2FA authentication, you have compromised your account. Moreover, if you have digital currency and someone else has got your private key, they effectively have access to your assets. The same thing applies with

mneumonic phrases. If someone has your list of words; they can recreate the account and have total access to it.

Therefore, do not write or store these passwords EXACTLY AS THEY ARE.




## Simple solution to mask your passwords and keys

With your complex passwords and/or private keys, think of a pattern *in your head* which you can apply to it. For example, think of a PIN number that you will never forget.

Let's do an example with a 4-digit PIN number. I recommend longer but for the sake of this example, let's keep it simple.

First, think of a PIN number. Don't use this for real of course!

# 1234

Let's say that you are given a key or wishing to mask a complex password which you have created. Let's say you're given a key as below.

# A9bx02Jk78b

You can think of a variety of ways to mask your password but, word of caution. **Keep it consistent and thoroughly test it out beforehand.**

One method, for example, is to *shift* the characters in your password based on your PIN number and repeat the process to the end of the password.

For example, using the PIN number above, let's take the first character of the password: **A**.

To *encrypt* or *mask* the password, choose one direction and be consistent with it. Let's go backwards.

The first number of your PIN is **1**. Therefore, if you go back one character from **A**, you will get **Z**. This is because you start again at the end of the alphabet.

Let's take the second character of the password: **9**.

Now you move on to the second digit of your PIN number, **2**. Therefore, go back two characters from **9** which is **7**.

Repeat for the remaining characters in your password. When you get to the fifth character, start your PIN number over again.

Remember to keep numbers as numbers. Uppercase letters as uppercase letter and lowercase letters as lowercase letters.

Therefore, the *encrypted* version will be:

# Z7yt90Gg66y

Remember, if you go back from 9 you start with 0 again.

To *decrypt* the password, go the *opposite* direction.

Therefore, to decrypt the password using your PIN number, **Z** turns into **A**, 7 turns into **9**, and so on.

Naturally, this is quite secure as long as you remember your PIN number!

You may want to keep it simpler by, say, only involving the first and end characters or whatever pattern you wish to choose.

This technique is especially important for digital currency private keys.

And finally,

**TEST IT OUT THOROUGHLY**. Decrypt your password and test if it works. Please don't forget to do this. I repeat, please don't forget to do this!

So there you have it!

It may not have been that simple at first, but, in reality, it really is!