Security Overview

This document is on mitigating security risks for blockchain related businesses.

Date: Thu Sep 13 20:42:15 MDT 2018

Note: This document will be updated periodically.

1. Never have the browser remember a password.

   The browsers do not encrypt the passwords that they save. There are drive-by attacks on the browsers that can reveal the saved passwords. All it takes is visiting the wrong site - or having malicious advertizing on the right site.

   If you have had the browser remember a password in the past, you need to consider that password to have been compromized. Change it.

2. Never use a human-generated password. All passwords must be randomly generated by the computer.

   There is vast evidence that humans can not generate random passwords. Rember that **you** are the weak link in passwords. Use a random password.

   If you have passwords that you created, then change them to computer generated random passwords.

3. Use passwords that are long enough.

   In today's world 12 characters, randomly generated, is sufficient. 14 to 17 characters is better. With modern hardware a 7 character password can be guessed in 0.7 seconds, 8 character password in 30 seconds, 10 character passwords in 3 weeks and 12 character passwords in 157 years. Length matters.

4. Write passwords down in your notebook.

   Don't lose the book. Do make a Xerox copy of the book and put the copy in your sock drawer.

5. Don't change your password unless it has been leaked.

   National Institute of Standards' (NIST) recomendation is that you don't change your password. Good research shows that it is better to pick a good password and never change it.

6. Use a different password for each site/tool.

   This contains the risk of a lost/compromized password.

7. Don't share your password with anybody **ever**.

   Enough said.

8. Sign up for Keybase and use it for securer communication.

   https://keybase.io

   Sign up and create a public/private key-pair. Use Keybase (it is slow and kind of ugly) on both your desktop and on your mobile devices for secure communication. It is designed specifically for transmitting secure data and it works.

9. Use a password manager or write down the password and put it in your wallet.

   Use both a password manager, like 1password, and write down the password on a chunk of paper. The note in you wallet is much more secure than any document on a computer. Somebody actually has to physically see the note for it to be stolen. Every time you are connected to the internet your computer is exposed to over 3 billion potentially dangerous other computers.

   Do **not** install the 1password browser extension. It has known weaknesses. Have 1password save/encrypt/restore your passwords then cut and paste the password from 1password into the password field of the applicaiton/site that you are logging into.

   For developers you may need a command line password manager. I have one that fully encryptes data.

10. Use a service that validates the password has not been pawned.

    NIST has a standard that all passwords should be checked against a database of 500,000,000 million leaked passwords. All new passwords shall be checked against this list. The tool 1password will do this for you automatically.

    https://www.1password.com

    You can check your passwrods at: https://haveibeenpwned.com/Passwords

    A really good page on this subject is at: https://www.troyhunt.com/ive-just-launched-pwned-passwords-version-2/

11. Use 2-factor-authentication (2FA).

    2FA means that you use a password and a PIN that is generated by a device like your iPhone. It verifies that you, the human, knows the password and that you are in posession of the device. This is much stronger authentication.

Google Gmail supports using 2FA. If you are using google, then take advantage of this feature.

Do not use 2FA over SMS. It is not secure. NIST has specificaly banned this practice.

12. Never email anything secure.

    This means don't use email for passwords, keys or anything else that requries security. The only secure system for passing secure data is Keybase. Get a Keybase account and use that.

    Sooner or later your email will leak. Assume that email is public. Assume that all chat systems (other than Keybase) are going to leak at the worst possible time.

    Thyere is a way to use email securly. This is how you do it:

    1. You create an encrypted file. On the Mac you can use Disk Utility to create an encrypted volume. On the PC you can install VeraCrypt.
    2. You encrypt your data.
    3. You send the encrypted data to the destination person.
    4. You use a phone-call to pass the password to the person (or Keybase)
    5. They decrypt the data.

    If you transimit data in this fashion, you can use Email, Dropbox or copy the encrypted file to a public server. Use 256-bit AES encryption with a strong randomly generated password.

    If you need help with setting this up, I can help you to use email securly.

13. Control exposure.

    Let me give you an example. Suppose that we have a value of a token at $1,300.00 for a cow-token. Now we have 10,000 tokens that are associated with real live cows. But we pre-create 100,000,000 tokens (100 million) as our supply for running the business. The 100 million is un-sold inventory - but has a value of $1,300.00 per token. A key for accessing the 100 million in un-sold invetory is on a laptop. If you have the laptop in your possession then you have a $1.3 billion dollar un-sold inventory that you are toting around. What is your risk?! How much of a target have you made yourself into by doing this?

    Don't let yourself get in this position. Don't have all the tokens of the business be issued and carted around. If the same laptop has 100 tokens on it, and the laptop gets stolen we can recover.

    If you have a laptop with a significant value on it - then you will need to use a multi-signature and air-gap the laptop. That means that you never plug it into a network - you never connect to a WiFi network with it. You never let it out of your posession. When you go to the bathroom you

take it with you. When you are in your office you lock it in a safe. The multi-signature means that it takes you and some other person in the business to access the data.

14. Never use a public WiFi without setting up and using a Virtual Private Network (VPN).

    It is always perferable to use a hot-spot that you control over a public WiFi. Verison has hot-spot technology that is wonderful. If you have to use a public WiFi, then immeidately connect to a VPN.

    Understand the limitations of a VPN. This is not total security. A VPN will only keep your communication secure between your computer and the other end of the VPN. This means that all the other security considerations still apply.

    Don't connect to anybody's network without using a VPN. You don't know what the security is on that network.

    If you need to transfer files to somebody's network, then use a USB thumb drive and sneaker net (physically pass them the thumb drive with the information.)

    If a USB thumb drive has been in somebody else's computer then re-format it. If they are sending you files be very careful. Usually I receive files via email and give files via a USB drive. This allows the email virus scanner to have a peek at the incoming file.

    Microsoft Office documents are a significant computer virus vector. I like to scrub them by opening the document in Libra Office, saving it in Libra Office format (this removes all macros), then re-opening it in Libra office and saving into Microsoft Office 2007 XML format.

15. Don't plug into any USB that you don't own.

    Most computers will recoginize a USB network as soon as it is plugged into a computer. For $9.99 you can buy the hardware on Ebay to create a custom USB network adapter with drivers that will get loaded to any PC. A quick Google search will lead to the soruce of the device drivers for this network. A malicious actor can now load a root-kit onto your computer by you plugging into a malictious USB port. This could be packaged neatly into a USB memroy stick that you find or one of the free USB charging ports at an airport. Once the rootkit is loaded your computer is **forever** compromized.

    If you need to charge at an airport, you pull out your charger and plug it into a 110v outlet, then connect to your USB port. You know the origins/background on the charger and that it is not malicious.

16. Use bio-metric authentication only sparingly.

Remember that you can't chagne your fingerprints. Fingerprints have been extracted from camera images off the face of an iPhone with the image taken from 8 feet away. Everything you have ever touched has potentially leaked your fingerpint. Think of most biometrics as a "username" not as a "password."

Good biometrics relys on you activly doing something that has a unique human signature. For example, a system that measures the timing between typing characters in a password. You still have to type the password (the adtive component) and then it verifies that most-likely it is you who typed the password.

17. Don't install un-necessary software.

    I know that the cute-cat screen saver is fun, but it is also a secrurity risk. Use a screen saver with some pictures that you took with your camera. You will have more fun and it will be more secure.

18. Use a fully encrypted laptop.

    With both Mac and PC you can fully encrypt your hard drive. This means that you will need a password to boot your computer. This also means that if your computer is stolen (or lost) it will not expose any secrets.

19. Developers must digitally sign all code changes.

    Developers must use a system like `git` and use a strong (2048 bit or 4096 bit) signature to digitally sign every change to software. Create a public/private key pair in Keybase and use the key pair to sign every commit to the source code.

20. Careful with 3rd party tools like Grammerly.

    Grammerly.com is a wonderful tool - but it is a huge security leak. It will copy every file and every text-box that you enter into its system for checking the grammer. Once the data is out of your hands - who knows what/who has access. Also it is not clear that the tools that Grammerly provides have any built-in security.

    This is in general true of all 3rd party web/based tools. 1password's browser plugin should not be used because it is subject to hijacking.

21. Do *NOT* use a phone number as a recovery for an account.

    All the major carriers (ATT, Verison etc) can be socially engeneered to move a phone number to a new device. This means that your account can be hijacked via a phone number.

    I will add details for how to turn this off with gmail and what to check for. It is in the account settings.

22. Do *NOT* use SMS Messaging for 2FA - it is not secure.

    See the previous note.

23. Get help right away.

    We all make mistakes. If something goes wrong - then - get help. If your computer is comporomized, then get help before you connect to a corporate/home network.

    It is important to quickley classify what the threat is and to deal with it.

    1. Small threats - I lost a computer but it was fully encrypted.
    2. Medium threats - I lost a key but it can be changed on our side.
    3. Large threats - I have detected an intrusion or lost keys and there is evidence of malicious usage.

Rev: 1.0.2