Однажды я зашел на свой аккаунт на Kraken.com. И увидел, что мой баланс близок к нулю, а еще пару дней назад был равен почти 1 Биткойну. На моём аккаунте был создан API ключ, который был создан не мной, а злоумышленниками. В истории торговых операций были отображены множество торговых операций приводящих к уменьшению моего баланса, в итоге мой баланс был практически обнулен. Очевидно что хакеры создавали заявки на продажу по заниженным ценам на моем аккаунте через API, а на своем аккаунте создавали встречные заявки на покупку. Таким образом мой депозит перелился на аккаунт хакеров. (2FA не спасла)   
Какие выводы я сделал?.  
ВЫВОД 1 : Я очень долго не менял пароль. Меняйте пароль раз в месяц.

Хакеры могут подобрать пароль используя брутфорс.  
Вывод 2 – никогда не сохраняйте пароли в браузере. Поставьте запрет на сохранение паролей.  
Регулярно чистите Куки и данные сайтов. Почти во всех браузерах это можно установить автоматически после выключения браузера.  
Вывод 3 - Поставьте в браузере отметку «Показывать полный URL-адрес в комбинированной адресной строке и строке поиска». Всегда проверяйте адрес сайта. Может быть следующая ситуация:  
 kraken.com/4867034795125?hfo=4351654321 – true

Kraken.com.4867034795125.hfo.hakers.com - false

Вывод 4. Используйте VPN. Хакеры могут понять, что с вашего ip часто заходят на биржу и отслеживать ваш трафик. VPN предотвращает это. Можно использовать операционную систему Кодачи, здесь имеется встроенный VPN который динамически меняется.  
Вывод 5. Заведите отдельный девайс для работы с криптовалютой. В идеале это отдельный ноутбук с операционной системой Кодачи или VPN с которого вы только заходите на биржу и работаете с вашей криптовалютой, больше ничего.

Вывод 6 Заведите отдельный е-мэйл, с которого регистрируется аккаунт на бирже. Больше нигде этот е-мэйл не регистрируйте. С этого е-мэйл аккаунта сделайте пересылку на мобильный телефон, что бы в случае несанкционированного входа вы могли об этом узнать.

Вывод 7 Выходить в интернет с отдельного ноутбука, отведенного только для работы с криптовалютой, лучше с отдельного интернет соединения. В общих сетях могут быть вирусы, члены вашей семьи могут принести вирус и подсоединиться к сети в которой вы работаете .  
Вывод 8 Поставить антивирус на роутер. Либо, поставь простенький ПК, настрой его как прокси и поставь на него антивирус.

Вывод 9 Храните 2FA на отдельном устройстве не подключенном к интернету. Купить какой-нибудь дешевый смартфон установить на него 2FA и никогда не подключать его к интернету.

Вывод 10 Традиционный совет – хранить крипту на холодном кошельке и использовать Ю-бикей.(правда тогда вам будут недоступны такие опции как лендинг крипты и маржинальная торговля).  
  
Вывод 11 если на бирже Kraken.com , то поставьте 2FA на:  
 - вход  
- торговлю  
- вывод средств  
 - создание API  
 - Заблокируйте все свои настройки Global Settings Lock. Это длинный пароль который запрашивается если вы или хакер захотят изменить настройки вашего аккаунта.  
 Работайте только на биржах с проверенной и хорошей репутацией. Желательно что бы на бирже была система отслеживания unusual activity.  
  
Вывод 12 . Меняйте адреса кошельков в рамках аккаунта биржи как можно чаще. Транзакции в блокчейне сохраняются навсегда. Хакеры могут увидеть что некоторый кошелек часто пополняется а вывода с него не происходит. И этим кошельком заинтересуются. То есть, как можно чаще генерируйте новый кошелек на бирже а предыдущий удаляйте.

P.S. Хакеры зашли с ip адреса США, а я всегда заходил с ip адреса республики Беларусь. Мне на почту пришло сообщение «если это были не вы, немедленно измените пароль и 2FA». Теперь Kraken усовершенствовал защиту, и в случае входа в аккаунт с неизвестного ip, требуют ввести 6ти-значный код. Жалко что, это нововведение не установили до хака моего аккаунта.  
P.S.S. Биржей Kraken.com пользуюсь до сих пор – в целом не плохая биржа.

I once logged into my account at Kraken.com. And I saw that my balance was close to zero, and a couple of days ago it was almost 1 Bitcoin. An API key was created on my account, which was created not by me, but by hackers. As a result, my balance was almost zeroed. Obviously, the hackers were creating sales orders at low prices on my account via the API, and they were creating buy orders on their account. Thus, my deposit was transferred to the hackers' account. (2FA didn't save).   
What conclusions have I made?

**CONCLUSION 1**: I haven't changed my password for a very long time. Change your password once a month. Hackers can guess the password using brute force.   
**Conclusion 2** - never save passwords in the browser. Prohibit saving passwords. Clean cookies and website data regularly. In almost all browsers this can be set automatically after shutting down the browser.  
 **Conclusion 3** - Check "Show full URL in combined address and search bar" in your browser. Always check the website url. The following situation may be:  
 kraken.com/4867034795125?hfo=4351654321 - true   
 kraken.com.4867034795125.hfo.hakers.com - false

**Conclusion 4**. Use a VPN. Hackers can understand that they often go to the exchange from your ip and track your traffic. VPN prevents this. You can use the Kodachi operating system, there is a built-in VPN that changes dynamically.

**Conclusion 5**. Get a separate device for working with cryptocurrency. Ideally, this is a separate laptop with the Kodachi operating system or VPN from which you just go to the exchange and work with your cryptocurrency, nothing else.

**Conclusion 6.** Create a separate e-mail from which an account is registered on the exchange. Do not register this e-mail anywhere else. From this e-mail account, make a transfer to your mobile phone, so that in case of an unauthorized entry, you can find out about it.

**Conclusion 7**. It is better to go online from a separate laptop, set aside only for working with cryptocurrency, from a separate Internet connection. Shared networks can have viruses, your family members can bring a virus and connect to the network you work on.

**Conclusion 8.** Put antivirus on the router. Or, put on a simple PC, configure it as a proxy and install an antivirus on it.

**Conclusion 9**. Store 2FA on a separate device not connected to the Internet. Buy some cheap smartphone to install 2FA on it and never connect it to the Internet.  
 **Conclusion 10**. The traditional advice is to store the crypt in a cold wallet and use U-Bikey (though then you will not have access to options such as crypt landings and margin trading).   
**Conclusion 11**. if using the Kraken.com exchange, then put 2FA on:   
- input   
- trade   
- withdrawal of funds  
 - API creation   
 Lock all your settings by Global Settings Lock. This is a long password that is requested if you or a hacker wants to change your account settings. Only work on exchanges with a proven and good reputation. It is desirable that there is an unusual activity tracking system on the exchange.

**Conclusion 12**. Change wallet addresses within your exchange account as often as possible. Transactions on the blockchain are saved forever. Hackers can see that a certain wallet is often replenished but no withdrawal occurs from it. And they will be interested in this wallet. Generate a new wallet on the exchange as often as possible and delete the previous one.

P.S. Hackers logged into account using United States`s IP address, and I always logged using IP address of the Republic of Belarus. I received a message in the e-mail "if it was not you, change your password and 2FA immediately." But it was deep night and I decided to read it later. Now Kraken has improved the protection, and in case of logging into an account from an unknown ip, they are required to enter a 6-digit code. It's a pity that this innovation was not installed before the hack of my account.

P.S.S. I still use the Kraken.com exchange - in general, not a bad exchange.