

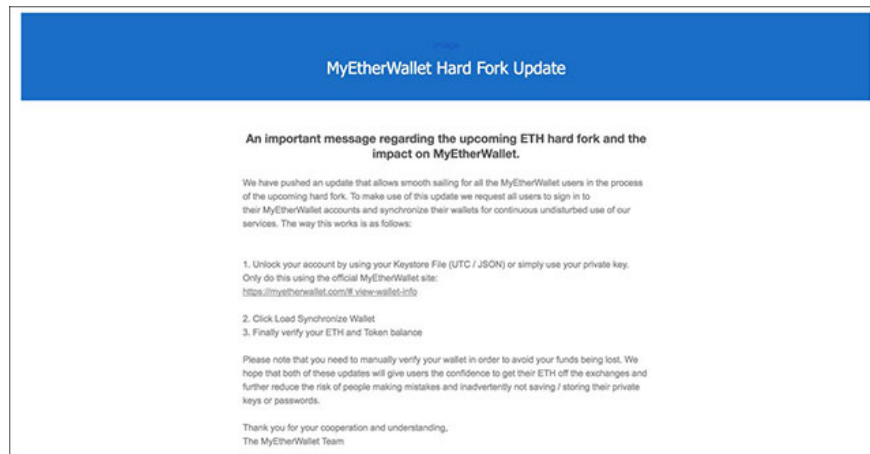
Ethereum phishing attacks help criminals earn \$ 15,000 in 2 hours

As the value of bitcoin is increasing, more and more people are interested in virtual currencies that are created based on bitcoin and have new features that bitcoin does not have.

As the value of bitcoin is increasing, more and more people are interested in virtual currencies that are created based on bitcoin and have new features that bitcoin does not have. One of them is Ethereum with the current value of \$ 296. It is also the time when people seek to cheat to benefit themselves.

See more: All you need to know about Ethereum

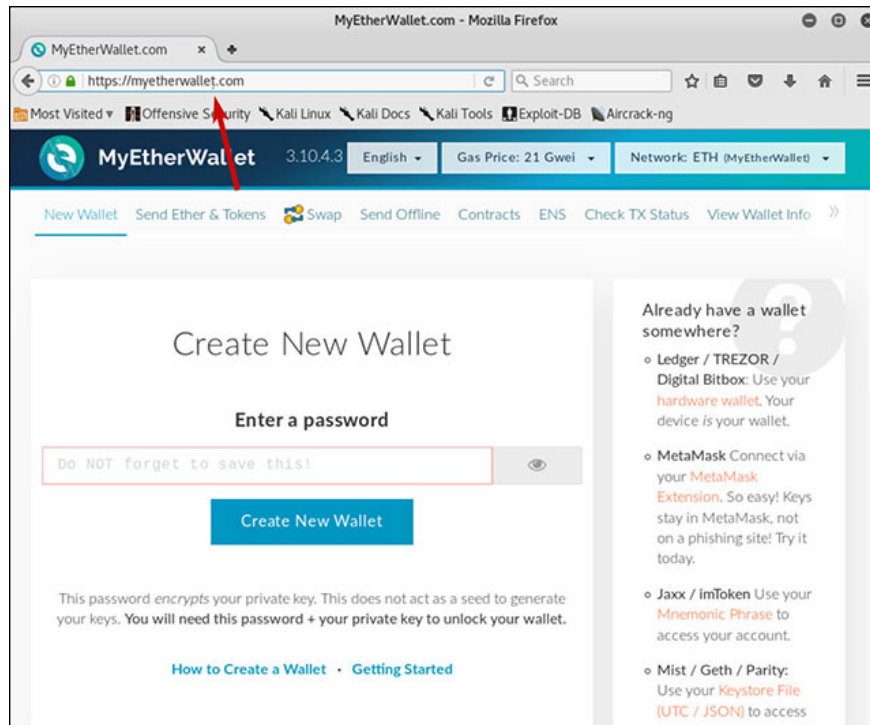
Researcher Wesley Neelen discovered the Ethereum exploit when he received phishing emails from Myetherwallet.com online e-wallet.



Email fraud sent to the victims

This trick says that Myetherwaller has updated and requires users to click on the link available to unlock the account and confirm the balance.

If you click, you will be taken to a page that looks a lot like Myetherwallet.com. But those who notice a bit will see a small comma below the letter t on the page address as shown below.

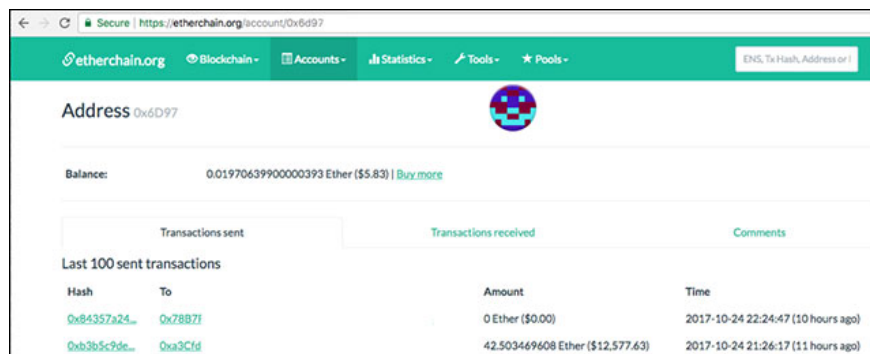


The website address looks just like a small comma

Scammers do this with Unicode tricks, allowing domain names to contain Unicode characters that look like Latin characters, creating a website that looks very real if you don't look closely.

When the victim enters the password, the attacker will use this password to get into their e-wallet and steal money. Neelen did not have this trap but there were some people who got it.

The attacker sent an email to Neelan without knowing that he was a specialist in testing hacking techniques and evaluating safety by attacking the system to make a living. When he received the trap mail, he investigated the page to see if he could find the source code or access history.



The e-wallet was stolen when plotting the fraud

Through investigation, Neelen also found a history file containing a list of all e-wallet stolen by the fraudster. In it an e-wallet contains 42.5 Ethereum, equivalent to \$ 12,500 at the time of the attack. Other wallets also have a

total of \$ 52.56 ETH, or \$ 15,875.65. All are transferred to the scammer's account.

The result is 2 hours of great gain.

You finished reading the article "**Ethereum phishing attacks help criminals earn \$ 15,000 in 2 hours**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
