Facebook's Libra electronic currency has not yet set a launch date but scam tricks are ready

In the past few weeks, scammers have not wasted a minute on registering domain names impersonating legitimate sites for Libra and for Calibra.

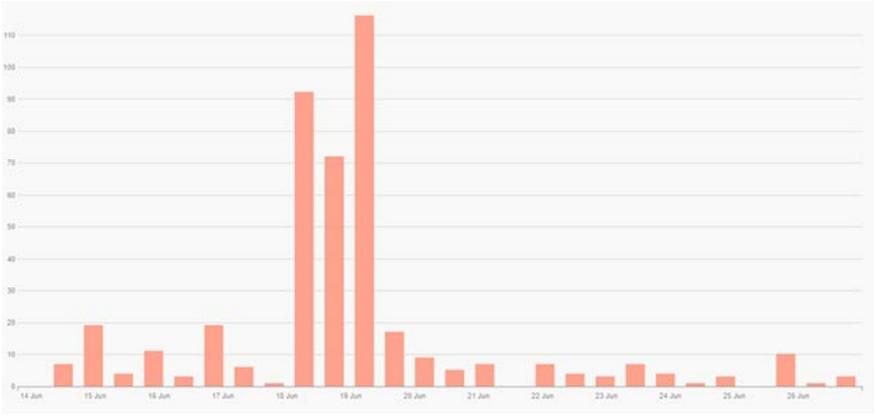
Not long after CEO Mark Zuckerberg officially announced the plan to launch Libra electronic coins and Calibra digital wallet, cyber criminals all over the world immediately embarked on 'creative' tricks. Sophisticated scam dedicated to this promising Facebook brand money.

Since the news about Libra has been officially released, technology and electronic money pages around the world are almost exclusively interested in explaining the nature of Libra, as well as how This currency operates and its impact on the financial-monetary sector, but forgets the inherent importance of capital security.

In the past few weeks, scammers have not wasted a single minute registering domain names for legitimate Libra sites and Calibra - ready to "welcome" the first victims even before when this electronic currency was officially launched.

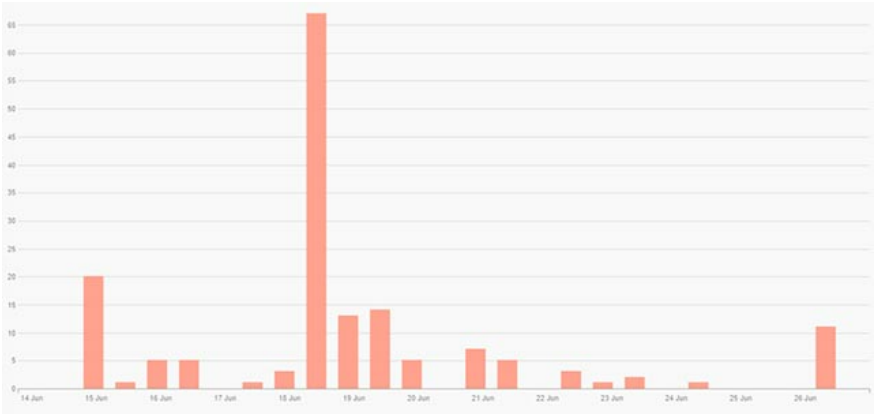
Thankfully some major security groups have not neglected their duties. According to statistics from cybersecurity company Digital Shadows, within 24 hours after Facebook officially announced plans to launch a new electronic currency, the number of domain registration related to keywords 'Libra' around the world has increased many times: from about 20 turns (and less) every day before the news comes, to more than 110 turns on the next day.

1. US lawmakers formally requested Facebook to suspend the Libra electronic money project



The number of domain name registration related to the keyword 'Libra' increased dramatically after Facebook announced the virtual money project

The same situation has been documented for Calibra e-wallet, which is expected to be launched in 2020. There is almost no domain name associated with 'Calibra' registering before Facebook's announcement. This e-wallet project, while on the next day, the number of registrations has skyrocketed to 65.



The same situation appears with the keyword 'Calibra'.

Of course, not all newly registered domain names associated with Facebook's virtual money project are deceptive, or used for bad purposes. In fact, many individuals often rush to buy related domain names before a big project launches in the hope that the domain name they have registered will be bought at a higher price. In this case, too.

The above 'domain hoarding' activity takes place when an agency that manages TLD (top-level domain name), such as .com, does not set the rules necessary to handle name cases. The domain is purchased with a negative purpose, but specifically here is a profit from the official brand.

1. The winning scam from Google: 'The cat game' for the vigilant, 'tragic' for those who are light-hearted

At the same time, there are a number of new domain names registered to serve entirely for the nefarious purpose, the most common of which are impersonation, in this case impersonating the legitimate Libra and Calibra websites to promote reporting scams, stealing personal information, or even phishing, appropriating property.

Instead of using a seemingly suspicious TLD, scammers often take advantage of a homogeneous attack to combine using the Punycode encryption system, thereby creating seemingly more legitimate domains.

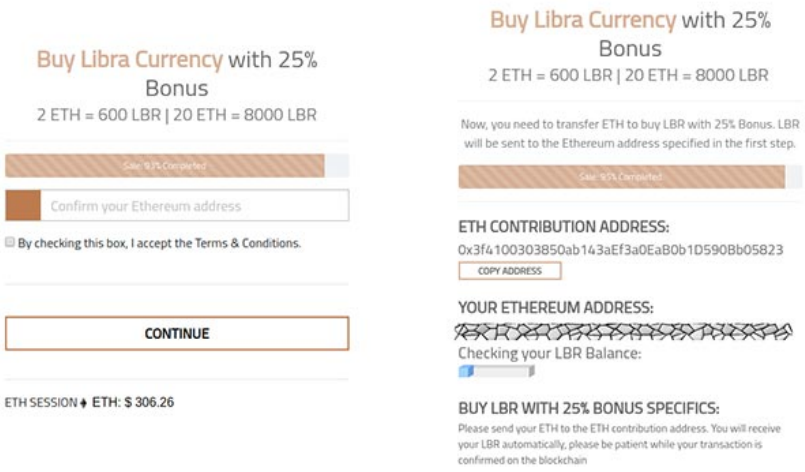
Digital Shadows has found 6 domains that mimic Facebook's "genuine" Libra website, some of which are active and simulate the actual site to the exact point of each dot, including:

1. calìbra [.] com (xn - calbra-yva [.] com)
2. lypbra [.] org (xn - lbra-vpa [.] org)
3. calibra [.] ooo - is active
4. canlibrawallet [.] com - is active
5. libracoins [.] co [.] il - is active
6. libra-ico [.] org - is active

'Cunning cyber criminals can copy the entire original site and only change certain elements to suit their nefarious goals,' said network security engineer Alex Guirakhoo of the Digital team. In addition, there are some differences that we need to keep in mind.

For example, even visually, a well-designed phishing site, a perfect copy of the original Calibra page, is essentially hard to provide a secure connection. . This feature, along with a number of other distinct factors, is quite clear but can easily deceive those who lack concentration or lack of experience, leading to becoming victims of sophisticated tricks. but the crooks have been prepared. In it, the most common is still the game of reward exchange or enter information to receive incentives.

1. New Android Trojans lead users to phishing websites by notification on the application

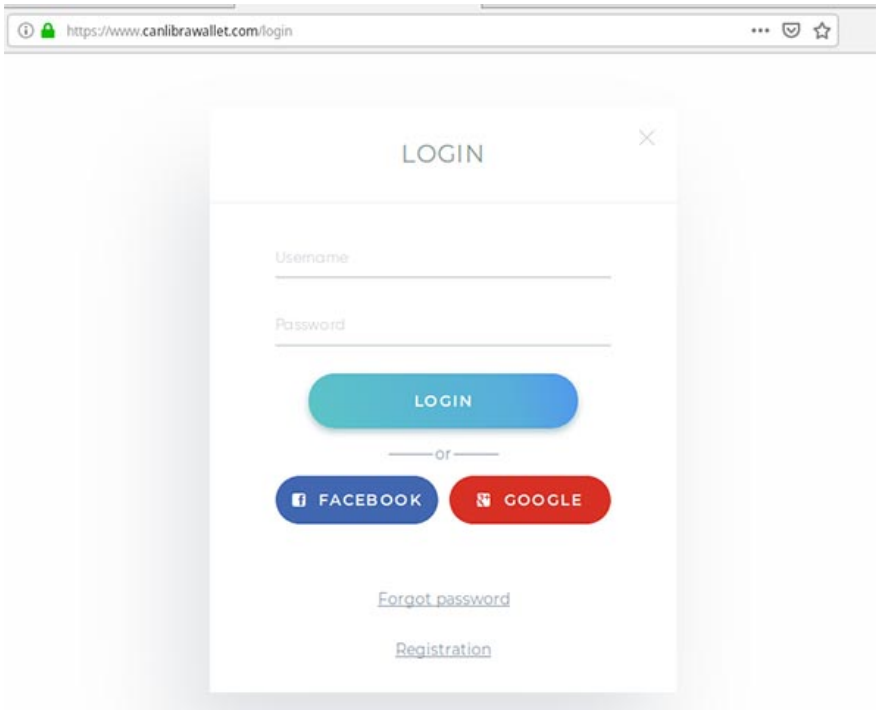


Phishing transfers money to the crook's wallet

As illustrated above, crooks offer an electronic money exchange program with attractive incentives. This is obviously an offer worth considering, but the ultimate goal will be to trick Ethereum into moving to their wallet. Fortunately, not many people have become victims of this trick because according to the information in the photo above, the wallet of the crook has only 0.2ETH.

However, it is still not the most sophisticated trick. Such as the case of canlibrawallet [.]. This site has an extremely similar interface to Libra.org - the official website that Facebook has registered, and even includes links to legitimate whitepaper on electronic money, as well as many other URLs that navigate to the site. Libra official.

1. Kaspersky Lab recommends that users be wary of fraudulent methods of targeting job seekers



This login page helps crooks collect victims' account information

However, you will also see the presence of a login page, where fraudsters provide personal login information to Facebook or Google accounts. This is their ultimate goal.

There is also another type of phishing that provides virtual private servers (VPS), claiming that they have access to the Libra block, although the electronic currency has not been officially deployed.

For example, on the libra-vps page [.] Com, you can see the most attractive offer starting at $ 200 (discounted) for Debian-based VPS, and up to $ 350 for a high-end server with 4GB of RAM and 128GB of storage. At the same time advertising information that crooks offer is also very attractive:

"With these VPS, you will have full access to Libra protocol and all functions of this currency. In just a few seconds, you will be able to create wallets, send / receive money Libra and Mintcoin!" .

1. Detecting new electronic phishing malware, redirecting payment transactions to attackers

Phishing to sell VPS at an attractive price

More seriously, the goal of many fraudulent websites does not stop at appropriating a few hundred dollars of victims, but also trying to trick them into providing personal information or accessing resources. Unknown. Attackers can take advantage of this connection to install many types of malicious software, malicious code into their systems. This behavior can cause countless damages.

Before you want to be a great virtual money investor, be a wise and awake internet user first!

You finished reading the article "**Facebook's Libra electronic currency has not yet set a launch date but scam tricks are ready**" 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.
