



Fact Checked? Be a Smart Citizen

Kelvin Wong
Independent Researcher, Hardware Ninja

Who am I?



- Hardware Ninja <http://hardwareninja.io>
- Speaker @ SANS, HTCIA, HITB and HITCON....
- Hardware Village @ Defcon Vegas and Defcon China



Case Sharing

Case 1



ONLINE SHOPPING



POTENTIAL INFORMATION
LEAKAGE

Story



Opening an online store @
Boutxxxx



Domain Registration @
GoMami




DNS configuration Domain
Binding

Conversation with CS




pls help to change the domain name

11:26



Kelvin 你好，謝謝你的查詢！
我們的辦公時間為星期一至五:10am-11pm；
星期六、日及公眾假期：12pm-6pm；


Thank you for your inquiry.
Our office hour is from 10 am - 11pm from Monday to Friday. 12pm - 6pm on weekends and public holiday. We will reply to your inquiry as soon as possible. Thank you for your consideration.



my email:

new domain:

anna.ns.cloudflare.com
igor.ns.cloudflare.com



anna.ns.cloudflare.com
anna.ns.cloudflare.com



為商戶查看之前已成功綁定為[redacted]，如需要更改域名，我們會收取\$200的綁定費。^^

請在此連結中付款，然後把你的order no. 給我們，我們幫你處理：

<https://bit.ly/32L6iKf>

然後商戶自行到域名平台進行購買，完成購買後，請提供請你將你的domain 管理平台、登入帳號和密碼、boutir 登入email 給我們，我們幫你綁定domain ^^

What? 給你登入帳戶和密碼？



請問是網店"[redacted]"對嗎？

每位年費計劃用戶是享有免費綁定domain服務一次～

我們早前是已經為你的帳號綁定了"[redacted]" 這個domain，如需要轉綁定其他domain的話，是需要收取\$200的綁定費的

如你確認，請透過以下連結付款：

<https://bit.ly/32L6iKf>

然後把order no.給我們，謝謝 ^^

Email from CS

請問貴公司是這樣幫客人做Binding Domain (綁定域名) ？



Inbox x

Updates x



Tue, Feb 23, 12:38 PM



to cs ▾

Dear CS,

Here is the reply from your support department.

請在此連結中付款，然後把你的order no. 給我們，我們幫你處理：<https://bit.ly/32L6iKf>

然後商戶自行到域名平台進行購買，完成購買後，請提供請你將你的domain 管理平台、登入帳號和密碼、boutir 登入email 給我們，我們幫你綁定domain ^^

Is your company collecting the clients' credential data or scamming?

Regards,

Kelvin Wong

Tue, Feb 23, 1:10 PM



文 Chinese (Traditional) > English [Translate message](#)

[Turn off for: Chinese \(Traditional\)](#) x

Dear Kelvin,

你好~

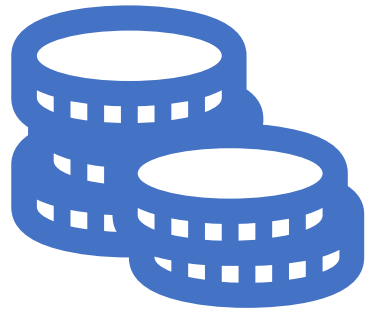
如果商戶自己已擁有Domain，年費計劃用戶可以免費綁定一次，而非年費用戶則可以以\$200綁定服務費，讓同事為你進行綁定~

綁定的步驟非常簡單，升級年費計劃後或完成\$200綁定服務費付款後，把你的Domain管理平台、平台帳號和密碼告訴我們同事，我們同事會進去為你設定，完成綁定後，商戶可以更改返密碼以確保安全~

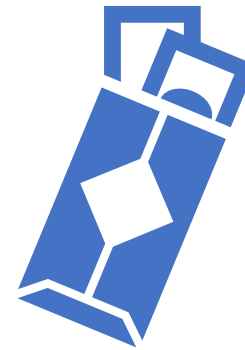
而如果商戶懂得設定DNS，到時亦可請我們同事把相關DNS設定給你，你自行放到Domain設定中~

謝謝~

Case 2



Crypto currency



Gift



Wirex

App Page

 Send Message

Home

Reviews

Videos

Photos


More ▾

 Like



About

[See all](#)

 We're an FCA-regulated borderless payment platform – buy, exchange & spend crypto and traditional currency. I pay my way. I pay by Wirex.

 3 people like this

 3 people follow this

 [Send message](#)

 [App Page](#)

Suggest edits

Does this Page have a phone number?

Yes

Unsure

No

Photos

[See all](#)



Create Post

 Photo/Video

 Check In

 Tag friends



Wirex

11 November 2020 · 



Dear LiteBit customer,
You have been chosen as a loyal user LiteBit who is lucky to get a bonus of 100 Litecoin LTC (3973.04 €).
In order to improve the Quality of the Platform we give bonuses to 50 loyal users LiteBit .

Get your bonus here:

↳ https://bit.ly/LiteBit_Giveaway

Thank you for being part of us.

Kind Regards

Team LiteBit.eu

[#LiteBit](#) [#Crypto](#)



Message from FB



Wirex Token Rewards's post



Wirex Token Rewards

9 h · 🌐



Dear Wirex Customer,
★Congratulations★

You are one of the loyal users of Wirex who is lucky to get a prize of crypto with 0.63 Bitcoin (BTC) & 50,000 Wirex Token (WXT) from Wirex Bounty Program. To collect your prize and more information available here <http://bit.ly/wirex-token-rewards-info>

* Log in to your wallet, a bonus will be available *
Thank you for being a part of us - Happy Trading!
Copyright© 2021 Wirex Limited. All rights reserved.



All the best,
- Wirex Team
[#Wirex](#) [#BTC](#) [#WXT](#) [#Cryptocurrency](#)

Suspicious URLs

🔍 Wire

✕ 取消

2021年1月20日 星期三

- | | | |
|---|--|---------|
| 0 | https://gift-eth-from-wirex-2021.000webhostapp.com/code.php
https://gift-eth-from-wirex-2021.000webhostapp.com/ | 下午 7:23 |
|  | Wirex Login To Wirex
https://gift-eth-from-wirex-2021.000webhostapp.com/ | 下午 7:22 |
| 0 | https://gift-eth-from-wirex-2021.000webhostapp.com/apps.php
https://gift-eth-from-wirex-2021.000webhostapp.com/ | 下午 7:22 |
|  | Wirex: Crypto & Fiat Multi-Currency Accounts with...
https://sites.google.com/ | 下午 7:20 |

清除瀏覽資料...

編輯

https://gift-eth-from-wirex-2021.000webhostapp.com

WIREX

[Register](#)

Fake

Log in to Wirex

Email

Password



[Forgot password?](#)

Log In



[Register](#)



Log in to Wirex

Email

victim@email.com

Password

password



[Forgot password?](#)

[Log In](#)

victim@email.com
password

A large black silhouette of a person wearing a hood and sunglasses, representing a hacker. The person is holding a laptop, which displays a login page for 'Wirex'.

wirex

[Register](#)

Genuine

Log in to Wirex

Email

Password



[Forgot password?](#)

Log In

OTP safety?



<https://gift-eth-from-wirex-2021.000webhostapp.com/code.php>

Try another confirmation method

Enter code here



Haven't received? [Resend](#) (available in 18 seconds)

Confirm

[Contact Support](#)

Fake

Confirmation

We need to authenticate your request for security purposes. Please enter the 6-digit code we've sent to

****,  

[Try another confirmation method](#)

Enter code here

Haven't received? [Resend](#) (available in 18 seconds)

Confirm

[Contact Support](#)

Genuine

Wirex Account Confirmation

Please confirmation account registered under the email address [REDACTED]

[Confirm](#)

This link expires in 15 minutes.

If you do not immediately confirm the 15 minute grace period after you receive this message, so sorry we will remove your account.

Kind regards,
The Wirex Team

From: Wirex Support <auth.wirextim@gmail.com>

Date: Wed, 20 Jan 2021 18:55:33 +0700

Message-ID: <CALb2bvsDkqgUYpEazRS=GxTnQwJ8vF9vfVGooH24D5wRO3ZhZA@mail.gmail.com>

Subject: Wirex Account Confirmation

To: [REDACTED]

Content-Type: multipart/alternative; boundary="000000000000ab456405b953a2e1"

--000000000000ab456405b953a2e1

Content-Type: text/plain; charset="UTF-8"

Content-Transfer-Encoding: quoted-printable

wirextim@gmail.com

Wirex Account Confirmation

Please confirmation account registered under the email
address [REDACTED]

Confirm <<https://bit.ly/2XWkEpd>>

This link expires in 15 minutes.

If you do not immediately confirm the 15 minute grace period after you
receive this message, so sorry we will remove your account.

Kind regards,

The Wirex Team



Why you?



Question?



Email:
info@hardwareninja.io