

STT	Người ký	Đơn vị	Thời gian ký	Ý kiến
1	NGUYỄN TRẦN QUỲNH	Phó Giám đốc - Ban Giám đốc - Trung tâm Vận hành khai thác toàn cầu - TCT VNet - Tổng công ty Mạng lưới Viettel	02/08/2023 16:20:32	
2	NGUYỄN THỊ LAN DUNG	Bộ phận Hành chính – Tổng hợp - Phòng Tổng hợp - Trung tâm Vận hành khai thác toàn cầu - TCT VNet - Tổng công ty Mạng lưới Viettel	01/08/2023 10:16:11	
3	NGUYỄN ĐỨC TÀI	Trưởng phòng IP- BRCD - Phòng IP và Băng rộng Cố định - Trung tâm Vận hành khai thác toàn cầu - TCT VNet - Tổng công ty Mạng lưới Viettel	01/08/2023 09:27:21	
4	PHẠM LÊ HOÀNG THÔNG	Phó phòng Điều hành Mạng lưới - Phòng Điều hành Mạng lưới - Trung tâm Vận hành khai thác toàn cầu - TCT VNet - Tổng công ty Mạng lưới Viettel	31/07/2023 09:56:31	
5	TẠ MINH TUẤN	Phó phòng Điều hành Mạng lưới - Phòng Điều hành Mạng lưới - Trung tâm Vận hành khai thác toàn cầu - TCT VNet - Tổng công ty Mạng lưới Viettel	31/07/2023 09:23:08	

## MỤC LỤC

<b>HƯỚNG DẪN GỠ IP BLACKLIST MỘT SỐ LỖI THƯỜNG GẶP.....</b>	<b>1</b>
<b>1. Mục đích, đối tượng và phạm vi sử dụng .....</b>	<b>1</b>
<b>2. Định nghĩa và thuật ngữ.....</b>	<b>1</b>
<b>3. Hiện tượng .....</b>	<b>1</b>
<b>4. Nguyên nhân.....</b>	<b>2</b>
<b>5. Kiểm tra khai báo bản ghi ngược PTR của mail server. ....</b>	<b>2</b>
<b>6. Hướng dẫn gỡ IP Blacklist.....</b>	<b>3</b>
<b>6.1 Lỗi Spamhaus Zen .....</b>	<b>3</b>
<b>6.2 Lỗi Protected Sky .....</b>	<b>10</b>
<b>6.3 Lỗi Uceprotectl2 và Uceprotectl3 .....</b>	<b>11</b>

# HƯỚNG DẪN GỠ IP BLACKLIST MỘT SỐ LỖI THƯỜNG GẶP

## 1. Mục đích, đối tượng và phạm vi sử dụng

- Tài liệu này nhằm mục đích hỗ trợ cho các bộ phận chăm sóc khách hàng hỗ trợ khách hàng thực hiện kiểm tra, gỡ IP Blacklist (IP dùng làm IP server mail) ảnh hưởng đến dịch vụ khách hàng.
- Phạm vi sử dụng: VNet, VTS, VTT.

## 2. Định nghĩa và thuật ngữ

STT	Thuật ngữ	Giải thích
1	VNet	Tổng Công ty Mạng lưới Viettel
2	VTS	Tổng Công ty Giải pháp Doanh nghiệp Viettel
3	VTT	Tổng Công ty Viễn thông Viettel
4	TT VHKTTTC	Trung tâm Vận hành Khai thác Toàn cầu - VNet
5	CSKH	Bộ phận chăm sóc khách hàng
6	IP Blacklist	Danh sách các IP bị liệt kê bởi các tổ chức chống Spam
7	Bản ghi PTR	Viết tắt của từ Pointer Record là bản ghi ngược ánh xạ một địa chỉ IP đến một tên miền
8	Domain	Tên miền (Domain name) là định danh của một website trên Internet
9	Open Relay Access	Máy chủ mail cho phép open relay sẽ mặc định cho phép người dùng không cần phải xác thực vẫn có khả năng gửi mail thông qua máy chủ này
10	BO ISP	Bộ phận BO ISP - P. IP&CĐBR - TT VHKTTTC

## 3. Hiện tượng

Khách hàng sử dụng IP tĩnh không gửi được email đến các email khác do IP đã bị liệt vào danh sách blacklist của các tổ chức chống Spam như: Spamhaus Zen, Protected Sky, Uceprotectl2 và Uceprotectl3... Cần lưu ý IP Blacklist chỉ liên quan đến việc ngăn chặn spam mail, nghĩa là IP dùng làm server mail, không liên quan đến việc truy cập web. Trước khi gỡ IP Blacklist cần hỏi thông tin khách hàng có

dùng IP này làm server mail không, địa chỉ web mail của khách hàng là gì (Ví dụ: mail.viettel.com.vn).

#### 4. Nguyên nhân

IP của khách hàng bị các tổ chức chống Spam liệt vào danh sách blacklist có thể nằm trong các nguyên nhân sau:

- IP của khách hàng có thể bị lạm dụng để phát tán thư rác.
- Nếu khách hàng dùng NAT để chia sẻ đường truyền Internet cho nhiều người dùng đằng sau NAT, có thể một vài người dùng đã và đang sử dụng đường truyền này để phát tán thư rác, thư quảng cáo hoặc email có chứa virus (có thể người dùng đó đã bị nhiễm spyware, trojan, virus...).
- Mail server khách hàng cho phép Open Relay Access.
- Mail server của khách hàng không có bảng ghi ngược PTR.

#### 5. Kiểm tra khai báo bản ghi ngược PTR của mail server.

Việc khai báo bản ghi ngược PTR có thể là một trong những nguyên nhân dẫn đến việc các tổ chức đưa vào blacklist hoặc bị mail server đầu nhận thực hiện kiểm tra chống spam nếu không khai PTR thì email gửi đến sẽ bị chặn. Vì vậy, trước khi gỡ blacklist cần kiểm tra khai báo PTR của địa chỉ IP.

Truy cập <https://mxtoolbox.com/ReverseLookup.aspx> nhập địa chỉ IP cần kiểm tra.

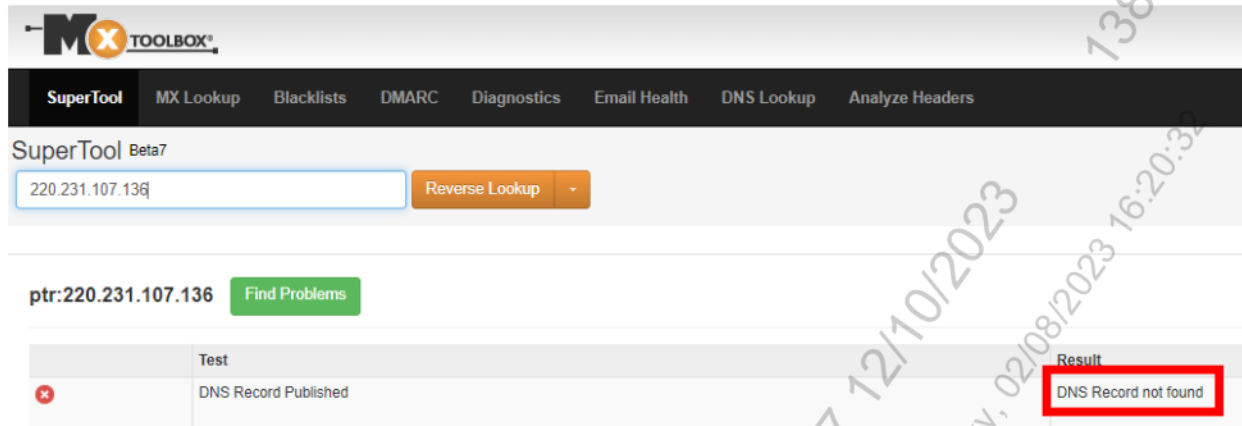
- Nếu kết quả trả về là IP khách hàng có một domain tương ứng, thì chứng tỏ IP của khách hàng đã được khai bản ghi ngược PTR.

The screenshot shows the MXToolbox website interface. The URL in the browser is [mxtoolbox.com/SuperTool.aspx?action=ptr%3a220.231.107.133&run=toolpage](https://mxtoolbox.com/SuperTool.aspx?action=ptr%3a220.231.107.133&run=toolpage). The page title is "SuperTool Beta7". There is a search bar with the IP "220.231.107.133" and a "Reverse Lookup" button. Below the search bar, the results show "ptr:220.231.107.133" with a "Find Problems" button. A table displays the PTR record details:

Type	IP Address	Domain Name
PTR	220.231.107.133 VIETEL-AS-AP (AS7552)	mail.vnua.edu.vn

Below the table, there is a "Test" section with a "DNS Record Published" test, which resulted in "DNS Record found".

- Nếu kết quả trả về là **“no record found”** chứng tỏ IP của khách hàng chưa được khai bản ghi ngược PTR. CSKH thực hiện tạo phiếu yêu cầu gửi đến BO ISP để hỗ trợ khai báo.



The screenshot shows the MXToolbox SuperTool interface. At the top, there's a navigation bar with links like SuperTool, MX Lookup, Blacklists, DMARC, Diagnostics, Email Health, DNS Lookup, and Analyze Headers. Below this, the 'SuperTool Beta7' section has a search bar containing '220.231.107.136' and a 'Reverse Lookup' button. A 'Find Problems' button is also visible. The results table shows a test for 'DNS Record Published' with a red 'x' icon and a result of 'DNS Record not found' highlighted in a red box.

Test	Result
DNS Record Published	DNS Record not found

## 6. Hướng dẫn gỡ IP Blacklist

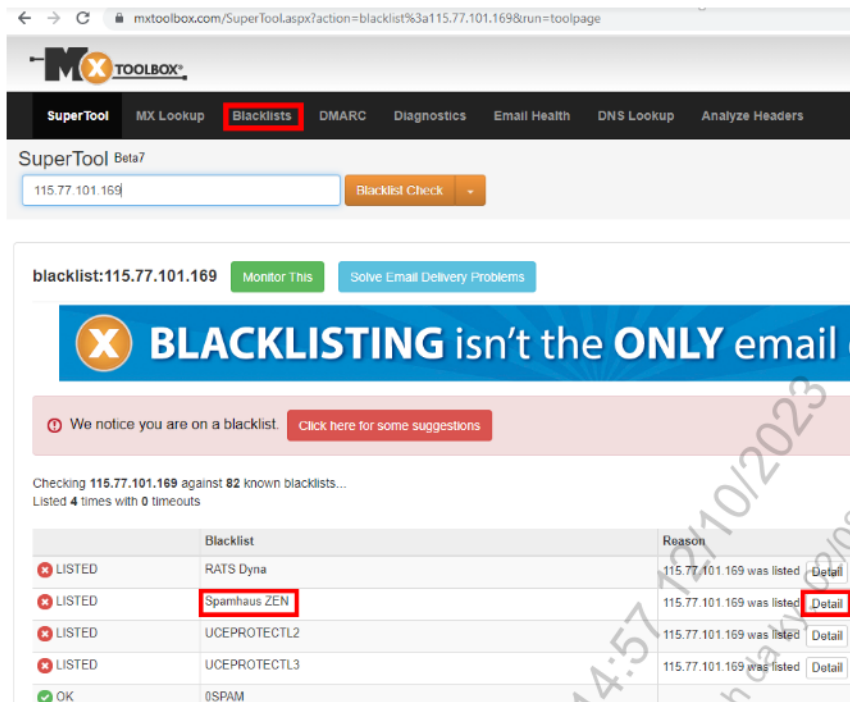
Sau đây là hướng dẫn khắc phục một số lỗi blacklist thường gặp ảnh hưởng đến việc gửi/nhận email của khách hàng. Nếu có các lỗi khác xuất hiện ngoài hướng dẫn này thì cách làm vẫn tương tự, người đọc chủ động làm theo hướng dẫn của website đang gắn blacklist cho IP để thực hiện.

**Lưu ý:** Riêng 2 lỗi blacklist **Uceprotectl2** và **Uceprotectl3**, hiện tại đang xảy ra với tất cả các IP Viettel thuộc AS 7552, nhưng không ảnh hưởng đến dịch vụ khách hàng. Trường hợp khách hàng vẫn yêu cầu Viettel gỡ blacklist, thì phải chuyển kinh doanh xem xét vì gỡ blacklist cho hai lỗi này sẽ **mất phí**. Tuy nhiên, tài liệu này cũng có hướng dẫn các bước cơ bản để gỡ blacklist và thanh toán.

### 6.1 Lỗi Spamhaus Zen

**Bước 1:** Truy cập <https://mxtoolbox.com> chọn trường **“Blacklist”**, và điền IP cần kiểm tra.

Các lỗi blacklist sẽ được liệt kê ra, kích chọn **“detail”** để xem chi tiết lý do bị blacklist và tìm link gỡ.



blacklist:115.77.101.169 [Monitor This](#) [Solve Email Delivery Problems](#)

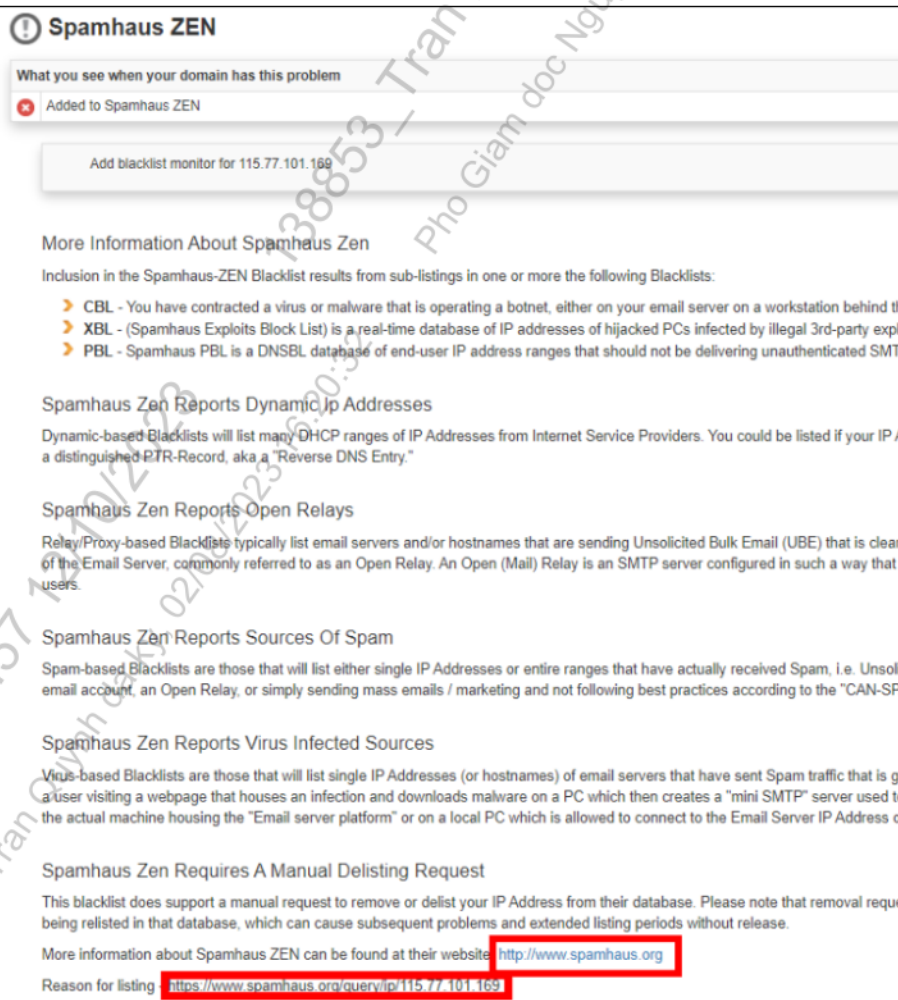
**BLACKLISTING** isn't the **ONLY** email c

⚠ We notice you are on a blacklist. [Click here for some suggestions](#)

Checking 115.77.101.169 against 82 known blacklists...  
Listed 4 times with 0 timeouts

	Blacklist	Reason
✖ LISTED	RATS Dyna	115.77.101.169 was listed <a href="#">Detail</a>
✖ LISTED	Spamhaus ZEN	115.77.101.169 was listed <a href="#">Detail</a>
✖ LISTED	UCEPROTECTL2	115.77.101.169 was listed <a href="#">Detail</a>
✖ LISTED	UCEPROTECTL3	115.77.101.169 was listed <a href="#">Detail</a>
✔ OK	0SPAM	

**Bước 2:** Sau khi kích chọn “detail” sẽ hiển thị như hình dưới, kéo xuống cuối trang xem mục “delisting request” sẽ có link dẫn đến trang chủ, chọn link thứ nhất hay link thứ hai như trong hình đều được.



**Spamhaus ZEN**

What you see when your domain has this problem

- ✖ Added to Spamhaus ZEN

[Add blacklist monitor for 115.77.101.169](#)

More Information About Spamhaus Zen

Inclusion in the Spamhaus-ZEN Blacklist results from sub-listings in one or more the following Blacklists:

- CBL - You have contracted a virus or malware that is operating a botnet, either on your email server on a workstation behind the
- XBL - (Spamhaus Exploits Block List) is a real-time database of IP addresses of hijacked PCs infected by illegal 3rd-party exploit
- PBL - Spamhaus PBL is a DNSBL database of end-user IP address ranges that should not be delivering unauthenticated SMTP

Spamhaus Zen Reports Dynamic IP Addresses

Dynamic-based Blacklists will list many DHCP ranges of IP Addresses from Internet Service Providers. You could be listed if your IP Address is a distinguished PTR-Record, aka a "Reverse DNS Entry."

Spamhaus Zen Reports Open Relays

Relay/Proxy-based Blacklists typically list email servers and/or hostnames that are sending Unsolicited Bulk Email (UBE) that is clearly of the Email Server, commonly referred to as an Open Relay. An Open (Mail) Relay is an SMTP server configured in such a way that it allows anyone to use it.

Spamhaus Zen Reports Sources Of Spam

Spam-based Blacklists are those that will list either single IP Addresses or entire ranges that have actually received Spam, i.e. Unsolicited email account, an Open Relay, or simply sending mass emails / marketing and not following best practices according to the "CAN-SPAM Act".

Spamhaus Zen Reports Virus Infected Sources

Virus-based Blacklists are those that will list single IP Addresses (or hostnames) of email servers that have sent Spam traffic that is generated by a user visiting a webpage that houses an infection and downloads malware on a PC which then creates a "mini SMTP" server used to send spam to the actual machine housing the "Email server platform" or on a local PC which is allowed to connect to the Email Server IP Address or hostnames.

Spamhaus Zen Requires A Manual Delisting Request

This blacklist does support a manual request to remove or delist your IP Address from their database. Please note that removal request is not instantaneous, and it may take some time for your IP Address to be removed from the database, which can cause subsequent problems and extended listing periods without release.

More information about Spamhaus ZEN can be found at their website <http://www.spamhaus.org>

Reason for listing: <https://www.spamhaus.org/querypip/115.77.101.169>



**Bước 3:** Sau khi vào trang chủ Spamhaus chọn mục **“Blocklist Removal Center”**



**Bước 4:** Điền IP cần gỡ blacklist và nhấn **“Lookup”**

## IP AND DOMAIN REPUTATION CHECKER

115.77.101.169

Lookup

**Bước 5:** Nếu ở bước 2 không chọn link 1 mà vào thẳng link 2 thì cũng sẽ dẫn đến trang bên dưới, sau đó kích chọn **“Show detail”**

✓ This IP is listed in the [Policy Blocklist \(PBL\)](#)

**Don't panic!**

The inclusion of your IP address on the Policy Blocklist (PBL) is standard for the vast majority of internet users and is not the result of your actions. Here are some key PBL facts for your understanding:

- Being on this list does not mean you won't be able to send emails.
- You do not need to request removal from PBL.
- This listing is controlled by your Internet Service Provider (ISP), not Spamhaus.
- Your ISP lists ranges of IP addresses that shouldn't be sending email directly to the internet.
- Typically, IPs of broadband or dial-up customers will be included in this list.
- This is part of Internet best practices enacted to protect all users.

**Run your own mail server?**

If you run your own mail server, and require removal from the PBL, please click on "Show Details" to review your ISP's policy. Once you have reviewed the policy, please tick the "I am running my own mail server" check-box at the bottom of the page to enable removal.

NOTE: Exclusions are only valid for 1 year. If your IP gets listed on another Spamhaus Blocklist, it will automatically be relisted on the PBL.

Show details ▾

**Bước 6:** Tích chọn ***"I am running my own mail server"*** rồi chọn ***"Next steps"***

Hide details ^

**Outbound Email policy of The Spamhaus Project for this IP range**

This IP address range has been identified by Spamhaus as not meeting our policy for IP addresses permitted to deliver unauthenticated 'direct-to-mx' email to PBL users.

Important: If you are using any normal email software (such as Outlook, Entourage, Thunderbird, Apple Mail, etc.) and you are being blocked by this Spamhaus PBL listing when you try to send email, the reason is simply that **you need to turn on "SMTP Authentication"** in your email program settings. For help with SMTP Authentication or ways to quickly fix this problem [click here](#).

**Removal procedure**

If you are not using normal email software but instead are running a mail server and you are the owner of a Static IP address in the range 115.72.0.0/13 and you have a legitimate reason for operating a mail server on this IP, you can automatically remove (suppress) your static IP address from the PBL database.

**About The PBL**

The Spamhaus Policy Block List (PBL) is an international anti-spam system maintained by The Spamhaus Project in conjunction with Internet Service Providers and is used by Internet networks to enforce inbound email policies. The PBL database lists end-user IP address ranges which should not be delivering unauthenticated email to any mail server except those provided for specifically for that customer's use. The PBL lists only IP addresses (not domains or email addresses).

For full information on how the PBL operates please see the [PBL Home page](#) and the [PBL Frequently Asked Questions](#).

☒ I am running my own mail server

Next Steps



**Bước 7:** Điền các thông tin họ tên và địa chỉ email như yêu cầu để hệ thống gửi email xác nhận theo đúng địa chỉ.

*Lưu ý: email nhận mã ngẫu nhiên trang web gửi về phải là email có định danh, ví dụ: mail @gns.vn, viettel.com.vn. Không được là public như mail của Google, Yahoo...*

Explanation — 2 — Verification — 3 — Conclusion

### Removing (115.77.101.169) from PBL

**We need your details to process your request**

Please fill out and submit the form below. You will receive an email to verify your address (remember to check your junk folder!). Once you have confirmed your email address, we can begin reviewing your delisting request.

Full name\*

Nguyen [REDACTED]

Email\*

[REDACTED]@viettel.com.vn

Confirm email\*

[REDACTED]@viettel.com.vn

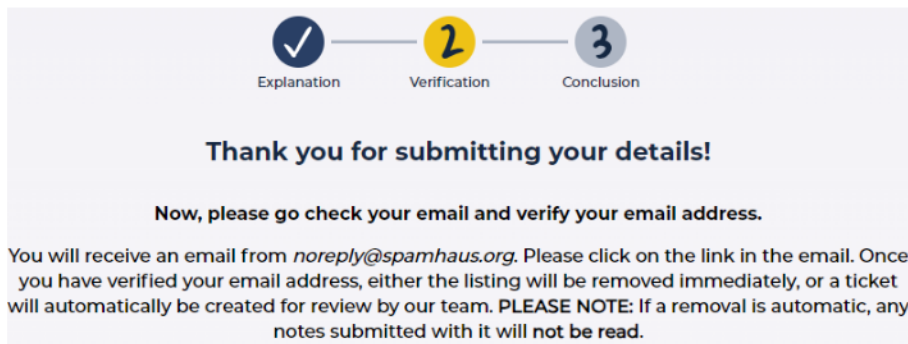
Please provide details regarding the issue\* ⓘ

I can not send/receive the email.

được bảo vệ bằng reCAPTCHA  
Bảo mật - Điều khoản

Submit

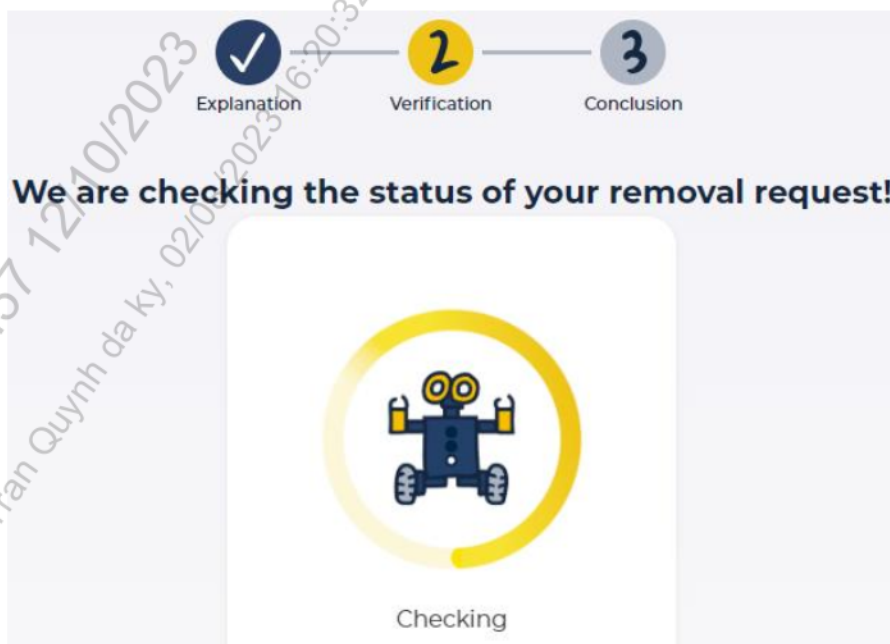
Sau khi **“Submit”** hệ thống sẽ thông báo kiểm tra email để xác thực.



**Bước 8:** Check email sẽ nhận được một thông báo yêu cầu xác nhận và một đường link, ***vui lòng nhấn vào link để xác nhận.***

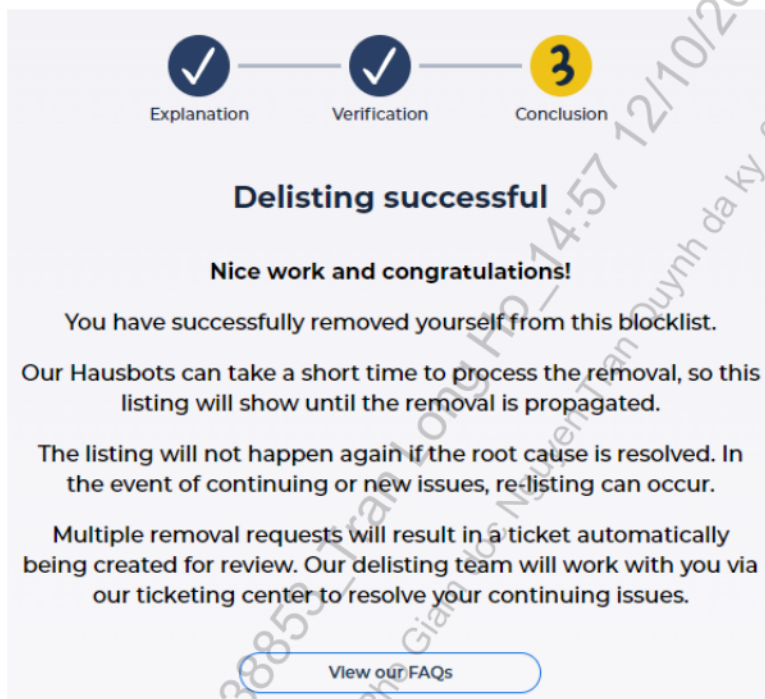


Đợi hệ thống kiểm tra tầm **30s**.

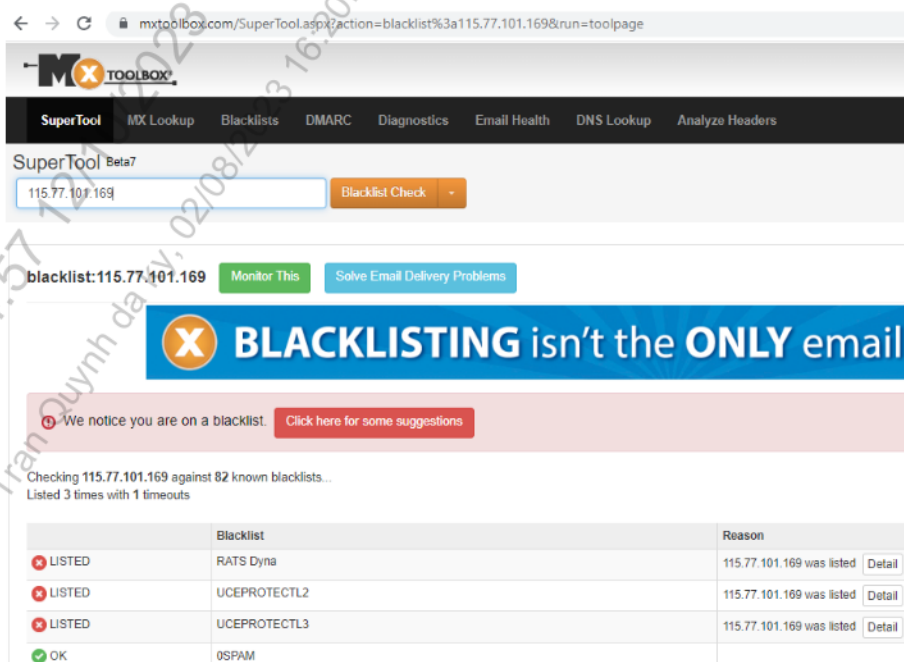


Sau khi hệ thống hoàn tất kiểm tra, sẽ nhận được thông báo delisting thành công như hình dưới nhưng phải đợi tầm 30 phút đến 1h (đối với lỗi này) thì IP mới được gỡ blacklist.

*Lưu ý: các trang web sẽ có thời gian xác thực lại việc yêu cầu delist có phù hợp không, thông thường sau khi delist nên đợi khoảng 24h vào check lại, nên thông báo với KH đợi khoảng 24h, để việc delist có hiệu lực. Ngoại trừ 1 số trang thời gian chờ khoảng 48h (BARRACUDA...)*



**Bước 10:** Vào lại trang chủ <https://mxtoolbox.com> check lại IP sẽ thấy lỗi blacklist Spamhaus ZEN đã biến mất.



## 6.2 Lỗi Protected Sky

**Bước 1.** Tiếp tục truy cập: <http://mxtoolbox.com/blacklists.aspx> để kiểm tra IP có nằm trong blacklist không và chọn “*detail*” như **bước 1** lỗi Spamhaus Zen.

**Bước 2:** Truy cập thẳng link <http://psky.me?125.234.96.163> như hình

### More Information About Protected Sky

A listing by Protected Sky RBL indicates that the IP address has been identified as a spam source. The Protected Sky RBL lists IPs based on reputation scoring using several factors to determine a good, poor or bad reputation. Protected Sky RBL blacklists IP addresses in two categories:

- Poor Reputation: IP address has been seen with a high rate of spam (It advises mail platforms using this RBL to defer the message for later)
- Bad Reputation: IP address has been seen to have a very high rate of spam (It advises mail platforms using this RBL to reject the message at SMTP submission)

More information about Protected Sky can be found at their website: <http://psky.me/>

Reason for listing - Bad Reputation. See <http://psky.me?125.234.96.163>

**Bước 3:** Chọn “*Request a Delisting*”

### Reputation Check

RBL Lookup for 125.234.96.163

Bad Reputation

[Request a Delisting](#)

Spam Level

Non-

Spam

**Bước 4:** Điền một số thông tin cần thiết:

Please complete the form below to delist 125.234.96.163.

The delist process is automated, and you will not receive an email back.

Your Name

ha thuc phuc

Your Email Address

hathucphuc@gns.vn.com

Reason for Delisting

IP is not blacklist

Your relation to the IP:

I'm unsure



I'm not a robot



reCAPTCHA  
Privacy - Terms

Submit

**Bước 5:** Nhận thông báo đã delist thành công.

Thank you for your delist request.  
The IP address 125.234.96.163 has been delisted.  
**Note: If we see heavy spam from this IP again, it will be automatically re-added.**

### Removal Control: Request Accepted

The IP address has been added to the PBL Removals database. Please allow 30 minutes for servers around the world to update their data. Under normal circumstances, in approximately 30 minutes you should be able to send email directly to networks that use Spamhaus' Policy Block List system.

Note that the PBL Removal System will now automatically run a check on the removed IP address and **will re-activate the PBL listing** if the IP address is found to be dynamic, not a real mail server, having any history of sending spam, or if it appears infected with a virus/trojan.

**Bước 6:** Sau 30 phút như thông báo trên, vào lại trang đầu tiên kiểm tra xem còn blacklist không.

**SuperTool Beta7**

125.234.96.163 [Blacklist Check](#)

**blacklist:125.234.96.163** [Monitor This](#) [Solve Email Delivery Problems](#)

**BLACKLISTING** isn't the **ONLY** email

We notice you are on a blacklist. [Click here for some suggestions](#)

Checking 125.234.96.163 against 82 known blacklists...  
Listed 2 times with 2 timeouts

	Blacklist	Reason
✖ LISTED	UCEPROTECTL2	125.234.96.163 was listed <a href="#">Detail</a>
✖ LISTED	UCEPROTECTL3	125.234.96.163 was listed <a href="#">Detail</a>
✔ OK	0SPAM	

### 6.3 Lỗi Uceprotectl2 và Uceprotectl3

**Bước 1:** Tương tự check blacklist như các lỗi bên trên sau đó click vào **“detail”** để xem chi tiết và tìm link dẫn đến web chính.



## Uceprotectl2 Reports Sources Of Spam

Spam-based Blacklists are those that will list either single IP Addresses or entire ranges that have actually received Spam, i.e. Unsolicited Bulk Email (UBE) in their Spamtraps from an IP-Address. This could be a result of a compromised email account, an Open Relay, or simply sending mass emails / marketing and not following best practices according to the "CAN-SPAM Act of 2003" (ref: [https://en.wikipedia.org/wiki/CAN-SPAM\\_Act\\_of\\_2003](https://en.wikipedia.org/wiki/CAN-SPAM_Act_of_2003))

## Uceprotectl2 Automatically Delists Entries

This blacklist does not offer any form of manual request to delist. Your IP Address will either automatically expire from listing after a given timeframe, or after time expires from the last receipt of spam into their spamtraps from your IP Address.

## Uceprotectl2 Accepts Payments Or Donations

This blacklist does support a manual request to remove, delist, or expedite your IP Address from their database upon Payment or Donation of fees to their organization. Please note the following; 1) MxToolBox does not in any way advocate the paying of removal from any blacklists. 2) Removal requests that are submitted without addressing the core problem will likely result in your IP Address being relisted in the database which can cause subsequent problems and extended listing periods without release.

More information about UCEPROTECTL2 can be found at their website <http://www.uceprotect.net/>

Reason for listing - Net 115.77.64.0/18 is UCEPROTECT-Level2 listed because 171 impacts are seen from VIETEL-AS-AP Viettel Group VN/AS7552 there. See <http://www.uceprotect.net/rblcheck.php?ipr=115.77.101.169>

### DMARC is the key to improving Email Deliverability!

Email is the key to your customer communication strategy. But, what is your email reputation?

Setting up and managing your DMARC configuration is the key to getting insight into your email delivery. MxToolbox is the key to understanding DMARC.

## Bước 2: Kích vào “Test and remove listings”

# UCEPROTECT NETWORK

Bitte wählen Sie Ihre gewünschte Sprache - Please choose your preferred language

DEUTSCH

[Hauptseite aufrufen](#) oder [Einträge prüfen und entfernen.](#)

ENGLISH

[Visit Mainpage](#) or [Test and remove listings.](#)

**UCEPROTECT**  
Do not send SPAM to us,  
otherwise your IP will be  
BLACKLISTED.

Sau đó nhập lại IP và chọn “Start testing”

## UCEPROTECT-NETWORK

Spammer listings within the last 7 days:

Level 1: 🚩 92522 IP's, Level 2: 🚩 19183 Allocations, Level 3: 🚩 1050 ASN's. Last Updated: 08.07.2023 11:06 CEST  
[Realtime Outbreakmonitor](#)

**SPECIAL OPTION FOR PROVIDERS:**  
**GET ALERTS WITH EXACT TIMESTAMPS AND IP'S OF YOUR ABUSERS BY EMAIL**  
[Subscribe our feedback-service here.](#)

Users please test your IP addresses. Providers please test your AS number instead.

AFTER YOU CLICKED START TESTING, PLEASE WAIT FOR THE PAGE HAS FULLY LOADED AND READ IT COMPLETELY!

Only manual queries are allowed.  
IP's abusing this page with automatic or excessive queries will be locked out.

Test : IP value: 115.77.101.169 Start Testing

**Bước 3:** Sau khi chọn “*Start Testing*” kéo xuống dưới sẽ thấy đường dẫn và trang add whitelist, kích chọn link như hình.

uceprotect.net/en/rblcheck.php

Networks this IP belongs to				
Networks	Status	Level 1 listed abusers within the last 7 days	Impacts in this net within the last 7 days	Level
🚩 115.72.0.0/13	LISTED	69	661	
🚩 115.77.0.0/16	LISTED	8	159	
🚩 115.77.64.0/18	LISTED	4	134	

### What does it mean to be listed at the UCEPROTECT-Level 2?

UCEPROTECT Network operates three levels of blacklisting, so our users can make the decision how strong they want to filter. While UCEPROTECT-Level 1 lists single IP's only, UCEPROTECT Level 2 is an escalation list. According to the table above allocations get listed at Level 2 if there were too many Impacts from Level 1 listed IP's in that ranges. In other words: Too much abuse was seen from one or several networks which your IP belongs to, within the last week. That is the reason why your mail has been blocked.  
[Click here to see the Policy for UCEPROTECT-Level 2](#)  
Level 2 is basically nothing more than pure mathematics based on the number of Impacts from Level 1 listed IP's.

### Who is responsible for this listing?

YOU ARE NOT! Your IP 115.77.101.169 was NOT directly involved in an abuse, but has a bad neighborhood. Other customers within this range did not care about their security and got involved in a serious problem.  
We are sorry for you, but you have chosen a provider not acting fast enough on abusers.

### Therefore we recommend:

Please send a complaint to your provider and request they fix this problem immediately.  
Think about this: You pay them so that you can use the Internet without problems;  
If they are ignoring your complaint or claiming they can't do anything, you should consider changing your provider.

### Can't you make an exception for me?

We never make exceptions. Requests to us are futile. Only your provider can fix this problem.  
Anyway our system respects IP's which are registered at [ips.whitelisted.org](#) these are excluded from Level 2.

### How can this netrange be removed from Level 2?

After your provider has fixed his problems, the UCEPROTECT-Level 2 listing will be removed automatically and free of charge as soon as the causal Level 1 listings and with them their Every IP temporary listed at Level 1 expires 7 days after we have seen the last abusive action originating from it.  
Automatic expiration is free of charge, because it does not require manual work.  
If your provider don't want to wait for free expiration, they can optionally order expedited express delisting if offered, which is charged a total of 249 CHF per Level 2 listed netrange.  
Orders for expedited express delisting are processed by external service providers, therefore it cannot be offered for free.  
It is necessary that all problems which have caused the Level 2 listing are fixed in first place, otherwise this netrange might end up in Level 2 again within a short timeframe.

#### Bước 4: Nhập IP, chọn “go”.



Welcome to Whitelisted.org

If you are not an abuser, you have the chance to add your Mailserver-IP to our whitelist zone.

This whitelistzone is available by DNS as ips.whitelisted.org and registered IP's are also excluded from neighborhood blocklists such as UCEPROTECT Levels 2 and 3.

This means if your Netrange or Provider gets listed in UCEPROTECT Level 2 or 3, then your IP will be excluded and marked as clean, if registered with us.

This is done as long as your subscription is valid and your system is NOT listed in UCEPROTECT Level 1 for abuse.

**If your IP gets listed at UCEPROTECT-Level 1 for abuse, it can and will no longer stay in ips.whitelisted.org!**

Check status of IP:

Sau đó số chọn thanh toán theo tháng, năm sẽ hiện số tiền tương ứng rồi chọn “continue”



Result:

### WHITELISTING IS RECOMMENDED FOR IP 115.77.101.169.

Your IP is listed in UCEPROTECT Level-2 Netrange 115.77.64.0/18.  
Your IP is also listed in UCEPROTECT Level-3.

Since your IP wasn't directly involved in abuse, you can exclude your IP from neighborhood blocklists as UCEPROTECT Levels 2 and 3 and others that are importing our whitelist, by registering your IP with us.

Registration is available for 1 Month (25 CHF), 6 Month (50 CHF), 12 Month (70 CHF), 24 Month (90 CHF)

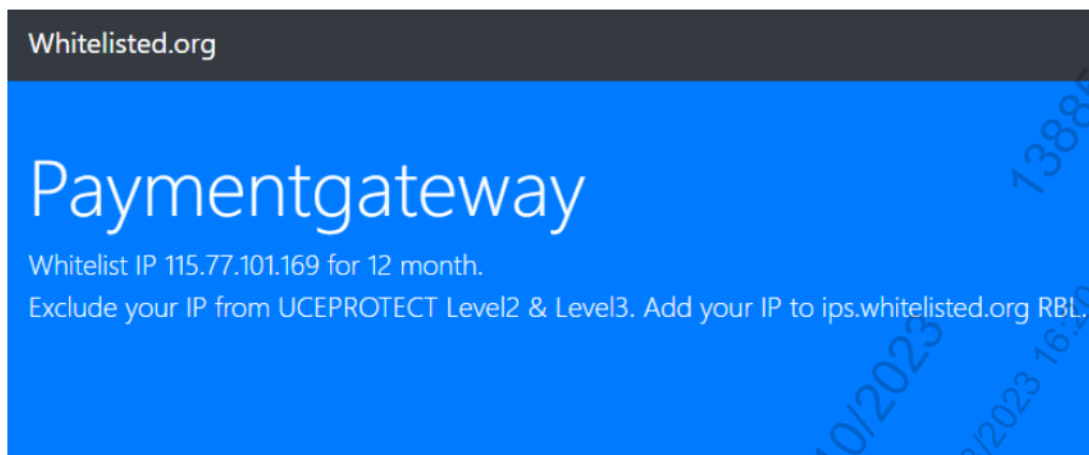
**PLEASE NOTE: Registering your IP with us doesn't give you a free ride for spamming / portscanning / hacking. Exclusion from UCEPROTECT Levels 2 and 3 will only affect the DNSBL Zones if no abuse originates from your IP. If your IP is seen spamming / portscanning / hacking after you registered with us, we will drop your IP from our whitelist-zone ips.whitelisted.org immediately and we will list your IP at our blocklist UCEPROTECT-Level 1 for abuse instead.**

You will get notified to your Paymentsserviceaccount's E-Mailaddress if that happens or in case your subscription ends.

Register my IP 115.77.101.169 with ips.whitelisted.org and exclude it from UCEPROTECT Levels 2 and 3 for

[contact](#) | © 2009-2023 by UCEPROTECT-Network

**Bước 5:** Điền thông tin như yêu cầu và chọn thanh toán.



All payments will be processed through [www.stripe.com](https://www.stripe.com).

*You will be redirected to their checkout page.*

A creditcard with active 3-D Secure and a valid emailaddress or Apple Pay is required.

If your creditcard is not 3-D Secure enabled yet, you will have to activate it in first place. Contact your bank for assistance in activating 3-D Secure.

Also note and remember that all payments to us will show up as UCEPROTECT-Network on your creditcard invoice.

Please enter a valid emailaddress:

[click here to pay 70 CHF using stripe](#)