

Next to my wiretapped cell phone, my biggest problem is the attacks that disable my Virtual Private Network (VPN) software. Ensuring my VPN software is rendered inoperative is essential for the illegal surveillance. Without an active VPN I am easily found when I go online. The Army cyber criminals stalk me on and offline, intercept my emails or webpage contacts, and block every attempt I make to connect to local or Mainland agencies for help. The cyber criminals prevent me from conducting sales on eBay or Craigslist to generate revenue.

There are multiple cases of the same VPN attacks HPD purposely ignored and refused to investigate. HPD officers never investigated the cyber crime statements I submitted when my VPN software was compromised. Readily evident VPN compromises I referred to HPD were not acknowledged like they didn't exist. On page 88 of my main/master evidence document titled "Cybercrime 2022", I listed five VPN crime statements HPD ignored.

Here I attached a copy of letters from my 6+ year computer technician who validates the VPN programs on my computers have been hacked. I also attached an email from a VPN vendor validating their software and my computers have been compromised.

I urgently need emergency law enforcement relief from the VPN and all other cyber attacks.

**Thorough cyber crime case investigations by HPD 2016 - 2022: Zero/0/None**





October 6th 2022

**Laine Kohama**

**2165 Aha Niu Place, Honolulu, HI 96821**

**808.673.4749**

**Aloha Detective Inuma,**

**In response to your request to address Mr. Finney's computers please note:**

**I have provided computer technology services to Mr. Finney's computers, tablets and cell phones since September 2016. His computers have been hacked/compromised by cyber criminals. Intrusions we've witnessed did not occur because of user or computer error. Please refer to the the letters Mr. Finney provided to you where I validated software I installed in Mr. Finney's computer was subsequently hacked.**

**I am sure he has suffered targeted cyber attacks, not problems with malware, clicking on a malicious link that could have downloaded a virus. Cyber criminals are targeting Mr. Finney. The most recent cyber attack involved his VPN service, and the credentials automatically filled in by the VPN service was changed, which rendered his VPN service to not work as intended.**

If you would like to contact me please feel free to call me at 808.673.4749. We appreciate your efforts and kokua with Mr. Finney.

**Mahalo,**

A handwritten signature in cursive script that reads "Laine" followed by a long, sweeping horizontal line.

**Laine Kohama  
President/Owner  
808.673.4749**

## NordVPN remotely disabled

3/10/2022

To Whom It May Concern:

On December 15th 2021, we installed a copy of the NordVPN on Mr. Finney's Dell desktop computer and a shortcut for quick opening as part of several software installations requiring an Internet connection. The VPN software prevents online activity from being monitored by a third party conducting online surveillance.

On 1/16/2022, Mr. Finney returned the Dell computer to me and reported that upon his first startup offline from the Internet, the NordVPN program shortcut was missing from the desktop and the NordVPN program would not open when double clicked from within its file folder. Upon receipt I examined the computer and noticed as he did that the shortcut was missing and the NordVPN program did not start up when clicked.


Mr. Finney suspects his Dell desktop computer was compromised again by cybercriminals during our installations to prevent discreet use of his VPN program. These incidents replicate a long series of software installs failing in Mr. Finney's computers after we serviced them.

Findings:

1. NordVPN was one of several applications we installed in Mr. Finney's desktop computer. All other programs functioned normally.

2. I validate the NordVPN desktop shortcut we previously installed was missing and the NordVPN application did not open when accessed from its file folder.

3. This incident is a recurrence of a prior one that occurred on August 7, 2019 when the Express VPN we installed was disabled and the program MITM Guard we had installed was erased from his MacBook Pro laptop computer. Upon inspection I noted the Express VPN program opened to a blank white screen that crashed and the MITM Guard program we installed could not be found.



---

Mr. Laine Kohama



# Malwarebytes remotely disabled

9/24/19

To Whom It May Concern:

On 5/20/19, we installed a fresh copy of Malwarebytes in Mr. Finney's iMac. We verified it was fully operable. On 9/23/19, Mr. Finney returned the iMac and explained the Malwarebytes program had been compromised on 9/4/19 during a screen sharing session with a network administrator from Western NRG, Camarillo, California. Ricardo hired me to capture screen shots to prove the compromise occurred.

I examined the iMac on 9/23/19 and found the Malwarebytes program title was changed from "Malwarebytes" to "Front End Application". Mr. Finney explained the program had been hacked and modified maliciously before. He provided an email dated 4/28/19 from the Malwarebytes company verifying the program written over his original Malwarebytes software was not theirs. This recent incident is a repeat of a prior compromise. We repaired Mr. Finney's computer before when this incident occurred.


This incident replicates a long series of software installs being modified or failing in Mr. Finney's computers after we installed them correctly.

1. We can verify that after our 5/20/19 installation the Malwarebytes program appeared as normal in Mr. Finney's machine.
2. We can verify that on 9/23/19 we observed the program named "Malwarebytes" had been changed to "Front End Application"
3. We can verify Malwarebytes stated a program named "Front End Application" installed on Mr. Finney's iMac was not theirs.

Laine Kohama

Gigalsland

Honolulu, HI



A handwritten signature in black ink that reads "Laine" followed by a stylized flourish.

---

**Malwarebytes** Edit Window Help

Overview Displays Storage Memory Support Service



## macOS Mojave

Version 10.14.4

iMac (Retina 5K, 27-inch, Late 2015)  
 Processor 3.2 GHz Intel Core i5  
 Memory 8 GB 1867 MHz DDR3  
 Graphics AMD Radeon R9 M380 2 GB  
 Serial Number C02RR0CVGG7J

System Report... Software Update...

© 1988-2018 Apple Inc. All Rights Reserved. Licensed Agreement

Force Quit Applications

If an app doesn't respond for a while, select its name and click Force Quit.

- Calendar
- FrontendApplication
- Gigaisland Remote Support Client
- SonicWall Capture Client
- Finder

You can open this window by pressing Command-Option-Escape.

Force Quit

Calendars + Day Week Month Year

## September 2019

< Today >

Sun	Mon	Tue	Wed	Thu	Fri	Sat
Sep 1	2 Labor Day	3	4	5	6	7
8	9 Ashura	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30 Rosh Has...	Oct 1	2	3	4	5
6	7	8	9	10	11	12

Yom Kippur

Applications

Favorites

- AirDrop
- Recents
- Applications
- Desktop
- Documents
- Downloads

iTunes Launchpad Mail

Malwarebytes Maps Messages

**Malwarebytes | PREMIUM** My Account

Dashboard Scan Quarantine Reports Settings



A new and improved version of Malwarebytes is available.  
 Install the new version free of charge.

Install Now

Scan Now


Real-Time Protection ⓘ

- Malware protection: On
- App Block: Off

Scan Status

- Last Scan: Today, 5:20 PM
- Protection Updates: Current
- Scheduled Scans: Settings

You can now schedule scans



View scheduler

# ExpressVPN and MITM Guard remotely

## Apple ID compromised

On August 07, 2019, I examined both apps and found the ExpressVPN software opened to a white page with no content, then quickly crashed. This occurred repeatedly. I saw that there was a "?" icon on the taskbar that read "MITM Guard" but I could find no trace of the program I had moved from his flash drive to his computer. Logs from Capture Client verifies the MITM Guard had been installed in the iMac:

**05/29/2019 12:03:30 PM** sngavm[62:1974] Error RicardoAdmin Failed to open file: /Users/RicardoAdmin/Desktop/MITM Guard.app/Contents/MacOS/MITM Guard

I further inspected Symantec, and after having been connected to the Internet, it appears to be in working order.

Furthermore, Mr. Finney is concerned that his Apple ID for slenderboy@tutanota.com has become compromised. Per his instruction, I changed the password for and removed the Apple IDs from Mr. Finney's iMac. The new password was only recorded on the paper that was supplied by Mr. Finney. Upon inspection of the iMac I do see that there are no Apple IDs associated in the "Internet Accounts" section of his iMac and that, per my research, Game Center does not exist on this version of iOS 10 - thus no remnants of the Apple ID appear to remain on Mr. Finney's iMac. Mr. Finney and our team have attempted to log in to his Apple ID via the online portal, and while it accepts the password that we had changed it to previously, it does not allow further alterations or entry without answering the security questions - which according to Mr. Finney have been changed without his knowledge.

Mr. Finney suspects his iMac was compromised again by cybercriminals during our installations to prevent discreet use of his VPN and to block a MITM attack from being revealed. Without a detailed and expensive examination of the iMac's operating system, we cannot verify both applications were compromised and when, however:

- a. The Express VPN app failed to operate after we verified it was installed correctly.
- b. The MITM Guard app disappeared after our installation.
- c. The Apple ID we deleted from the iMac appeared in the MacBook Pro laptop although we did not install it. The slenderboy Apple ID appeared in Mr. Finney's MacBook Pro computer installed in iCloud in and saved to Internet Accounts. The unwanted Apple ID is also entered in Game Center and attached to a game player account Mr. Finney states he never opened.

These incidents replicate a long series of software installs failing in Mr. Finney's computers after we installed them correctly.

1. We can verify that on May 20, 2019 Express VPN was able to open properly and that on May 22, 2019 MITM Guard was opening to its proper screen.
2. We can verify logs from Capture Client prove the computer was not powered on after we



returned it to Mr. Finney. No opportunity for a compromise arose while the computer was in his possession.

3. ExpressVPN does not properly open as of Lainé and his team's inspection on August 07, 2019. The description when opening is that the program opens to a white screen with the ExpressVPN logo, and after some time will force quit and the program and will then crash. We verified this by several attempts to open this program.

4. We can verify that Symantec was installed on Mr. Finney's MacBook Pro and was operational before returning the computer back to him. At this time we do see that Symantec need to 'Check your subscription', and as Mr. Finney allowed us to connect the computer to the internet, after a brief period it appears that Symantec was fully operational.

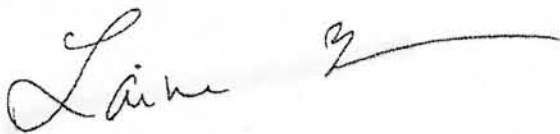
5. No version of Game Center exists on Mr. Finney's iMac and as such no remnant of the Apple ID slenderboy@tutanota.com was found. The password for this Apple ID had been changed previously as per Mr. Finney's request and is documented on the paper supplied by Mr. Finney. Any further alterations done to this account were not done from Gigalsland or from Mr. Finney according to his recount.

6. Upon inspection of the "Full Control" access to Mr. Finney's iMac, we found that there were no services or processes listed. Upon inspection of the "Full Control" access to Mr. Finney's MacBook Pro, we found two apps titled "smbd" and "sshd" installed. We did not install the apps

Laine Kohama

Gigalsland

Honolulu, HI

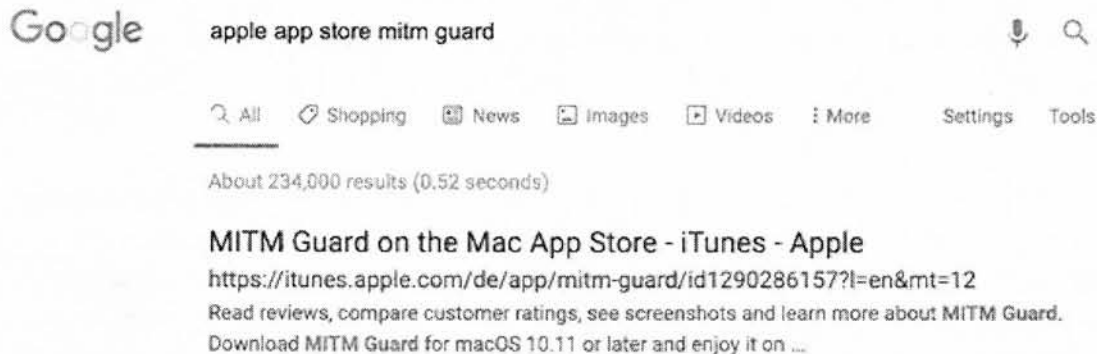
A handwritten signature in cursive script that reads "Laine" followed by a stylized flourish.

---

Laine Kohama

On May 20, 2019, I installed a copy of the ExpressVPN and on May 22, 2019 I installed a copy of MITM Guard from Mr. Finney's flash drive to Mr. Finney's MacBook Pro as part of several software installations requiring an Internet connection. The VPN software prevents online activity from being monitored by a third party through a Man-In-The-Middle (MITM) attack. MITM Guard is a program Mr. Finney researched and found that it blocks Man-In-The-Middle Attacks and notifies him of connections. MITM Guard is listed in the Apple App Store:

MITM Guard is listed in the Apple App Store:



I verified both applications opened correctly with the wireless mode turned off as requested. He returned the computer to me on July 17, 2019 and explained after a long vacation he opened the laptop for the first time since my installation and found ExpressVPN and the MITM Guard app inoperative. He explained he had not connected the laptop in wired or wireless mode and was returning the laptop with Wi-Fi turned off to block any external access.

On July 24, 2019, I examined both apps and found the ExpressVPN software opened to a white page with no content, then quickly crashed. This occurred repeatedly. I found the MITM Guard app would not open at all regardless of the number of activation attempts. I did not connect the laptop in wired or wireless mode before or during my examination.

Mr. Finney suspects his laptop was compromised again by cybercriminals during my installations to prevent discreet use of his via a VPN and to block a MITM attack from being revealed. Without a detailed and expensive examination of the laptop's operating system I cannot verify both applications were compromised and when, however these incidents replicate a long series of software installs failing in Mr. Finney's computers after I installed them correctly.

1. I can verify that on May 20, 2019 I installed and was able to open ExpressVPN and on May 22, 2019 I can verify that I installed and opened MITM Guard on the Macbook Pro.
2. ExpressVPN does not properly open as of Lainé and his team's inspection on July 24, 2019. The description when opening is that the program opens to a white screen with the ExpressVPN logo, and after some time will force quit and the program will crash. I can



verify several attempts to try and open this program.

3. I can verify that Symantec was installed on Mr. Finney's MacBook Pro and was operational before returning the computer back to him. At this time I do see that Symantec need to 'Check your subscription' but per Mr. Finney's request we will not be connecting this to the internet to try and re-establish the connection.
4. The internet account listed for Game Center is [slenderboy@tutanota.com](mailto:slenderboy@tutanota.com) . I did not add this account to the MacBook Pro though I did find this documentation on Apple's Internet Account policies (via <https://support.apple.com/en-us/HT208650>):

"Game Center

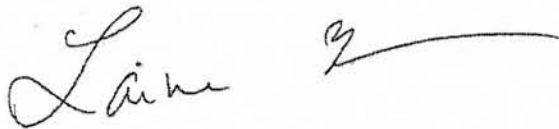
When you sign in with your Apple ID on your iPhone, you will be signed in to Game Center automatically. Game Center allows you to engage in game related activities, including, but not limited to, participation in leader boards, multi-player games, and tracking achievements.

When you use Game Center, your Game Center nickname and any associated data may be visible to other users. When playing a game that supports multiplayer functionality, other users accessing the Game Center from within the same game on the same Wi-Fi network, local area network or within range of Bluetooth will be able to see that you are nearby (unless you turn this feature off), and see your nickname. Only users with whom you have invited into a friend relationship can see your real name; only your nickname will be visible to users who you did not request to be your friend."

This specific article relates to iPhone's, however I believe this to be a similar if not the same policy for the other Apple Products.

5. Upon further research `smbd` is a Daemon used by Samba for file sharing to Windows machines. `Sshd` appears to be the service Daemon that Apple uses for secure remote connection and seems to be added by default from Apple. I did not enable remote access to Mr Finney's laptop. I did not add `smbd` or `sshd` to the Security & Privacy section of Mr. Finney's MacBook Pro.

These are the type of  
"normal" files exploited  
by the cyber criminals



---

Laine Kohama  
Gigalsland Computers  
Honolulu, HI





Nikon <Nikon@precisionphotography.live>

Wed 8/10/2022 7:47 AM

To: linuma, Thomas S <tiinuma@honolulu.gov>

■ 4 attachments (8 MB)

from expressvpn.pdf; 1.png; 2.png; Screen Shot 2022-08-10 at 6.21.53 AM.png;

Aloha, Detective linuma...

I received the attached reply from my VPN technician. Since the font is so small I transcribed the contact and posted it in the attachment titled "ExpressVPN.pdf. The technician explains there is no need for me to access my Mac Settings to install the Express VPN software. He explains further the username, password, and all the fields required by the program will be automatically populated by the VPN app. He again repeats all the VPN controls should be done in the app and not in the Settings. They validate the (unknown) password requirement to continue that prevented me from installing and using the Express VPN program is not part of the normal software process.

This morning the requirement to enter the password to install the Express VPN program disappeared from my computer after I concluded an email session in Outlook. Last night at my final logoff the password requirement was still in place. Now the unknown account name still appears in the network settings but the install process is again seamless. I used my computer for the first time today to send the previous query about Ashley. After finishing in the Outlook email program I noticed the password requirement to continue installing Express VPN had disappeared.

I reported the events to my business network engineers. I attached a copy of my submission and the screen shots I sent them. The reversal came about only after I reported the intrusion and reconfigurations to you and received the reply confirmation from Express VPN.

As the Express VPN technician noted, the software installation process should be seamless. i.e., click, click, click, click to complete the software installation. As I noted previously, the steps shown in the attached screen shots prevented me from continuing the installation process and blocked me from using the VPN. Now the process was reversed after you were notified of the illegal intrusion and Express VPN got involved. I've asked my network engineers to investigate, however they cannot stop the criminals from returning and continuing their illegal, targeted attacks against me.

The proof of intrusion I provided supported by the confirmation from Express VPN that my program does not operate as it is designed to do answers the request you made. The program did not operate because of an illegal intrusion into my business network and computer, and all indications point to a second intrusion to reverse the process since the initial incident was exposed. With these changes coming from an unknown source known to be malicious, although the Express VPN program appears to operate normally I do not consider the program trustworthy. I need to have my entire computer wiped and reformatted, however I cannot do so safely using my home office network or the Apple Store because I

am stalked and my devices attacked through whichever networks they use. As I noted previously, as evidence I provided the systems log from one of my iMac operating system installations when it was compromised at the Ala Moana Apple Store.

Historically, my network engineers have been unable to stop the intrusions. They may be occurring outside my firewall. With the evidence I've provided here combined with the information in my HPD statements and online in my evidence links, will you now proceed with your investigation and take action to stop the cyber criminals and their daily targeted attacks against me at home and away? Thank you for your time.

Respectfully,

Ricardo Finney

---

**From:** linuma, Thomas S <tiinuma@honolulu.gov>  
**Sent:** Tuesday, August 9, 2022 7:54 AM  
**To:** Nikon <Nikon@precisionphotography.live>  
**Subject:** RE: Doc Delivered For My HPD Cases/Request To Access Encrypted Email

Hi Mr. Finney,

Would you be able to meet/contact Ashlyn to go over your recent cyber-attacks in-person? She assists our cyber unit and could be reached at 808-832-3100.

Would you be able to get your VPN or other service providers and obtain a written statement stating that your computer network is compromised? Also, if you have seen a computer/phone repair specialist and if they determined that your devices were hacked/compromised, could you obtain a written statement and their contact information for me?

Our office doesn't fix computers/phones or remove malware, so I would like to know what the specialist says after examining your devices. This will point me in the right direction during my investigation.

Mahalo

---

**From:** Nikon <Nikon@precisionphotography.live>  
**Sent:** Monday, August 8, 2022 5:04 PM  
**To:** linuma, Thomas S <tiinuma@honolulu.gov>  
**Subject:** Re: Doc Delivered For My HPD Cases/Request To Access Encrypted Email

CAUTION: Email received from an **EXTERNAL** sender. Please confirm the content is safe prior to opening attachments or links.

Aloha, Detective Ilnuma...

Thank you for replying, I sent the 7/29/22 email from my encrypted portal which apparently was not allowed through your firewall. My other email portal I used to send this message is



unencrypted. I do not want to send or receive sensitive information here. These emails are not private since I receive Man-In-The-Middle attacks each login. There's a lot of information in this correspondence I prefer remain out of malicious eyes, however time is of the essence and this mode is fastest. For future sensitive information I have no option other than to continue providing correspondence through the Kapolei Station On-Duty officer.

Daily cyber attacks against my hardware, software, and business network continue. As I noted in my latest and prior HPD statements and my most message to you, the malicious change to my VPN has been the most crippling computer cyber attack I've received. I refer you back to the screen shots I provided in my HPD statements and my August 1, 2022 letter that revealed the malicious installation changes made to my ExpressVPN program after an intrusion ultimately leading to my inability to install the program and use it.

As I noted previously, these requirements not appear during n a clean version of ExpressVPN during installation. Four clicks are made and the software is installed no "Connect", no account name formed from a set of random characters, and no password requirement.

I could easily show you this intrusion and different ones made into my other devices, however that's not possible as you explained since we can't meet in person due to COVIT restrictions. During periods of COVIT in previous months I was able to meet with Detective Pait masked, of course. When and if your restriction is lifted please let me know. It's much more beneficial and easier to interact personally, especially with the limitation requiring unencrypted email to address ongoing cyber crimes.

The successful attacks on my VPN software aid in allowing the online stalking and other intrusions to continue, but as I have listed in great detail it is not the only cyber attack I repeatedly receive. Others are detailed in rank order of impact in my August 1, 2022 letter to you. Details are also in my HPD crime statements filed in January, March, April, May, June, and July 2022 that were not investigated.

My business network and connected components remain compromised. Cyber attacks continue unabated. Again, I urgently need law enforcement intervention to stop the cyber criminals. Please advise when your investigation into my cases will begin. Thank you for your time@

Respectfully,

Ricardo Finney

---

**From:** linuma, Thomas S <[tiinuma@honolulu.gov](mailto:tiinuma@honolulu.gov)>

**Sent:** Monday, August 8, 2022 1:27 PM

**To:** Nikon <[Nikon@precisionphotography.live](mailto:Nikon@precisionphotography.live)>

**Subject:** RE: Doc Delivered For My HPD Cases/Request To Access Encrypted Email

Hi Mr. Finney,

It's best to send your files unencrypted because I am unable to disable any of the City's firewalls. All emails are monitored/maintained by the City, and I cannot make any changes. Also, I have not

receive any email from you dated 07-29-22.

Mahalo

Det. linuma

---

**From:** Nikon <[Nikon@precisionphotography.live](mailto:Nikon@precisionphotography.live)>  
**Sent:** Sunday, August 7, 2022 6:03 PM  
**To:** linuma, Thomas S <[tiinuma@honolulu.gov](mailto:tiinuma@honolulu.gov)>  
**Subject:** Doc Delivered For My HPD Cases/Request To Access Encrypted Email

CAUTION: Email received from an **EXTERNAL** sender. Please confirm the content is safe prior to opening attachments or links.

Good Morning Detective linuma...

I am contacting you from my unencrypted Outlook email account address [nikon@precisionphotography.live](mailto:nikon@precisionphotography.live). This past Monday at 4:10 p.m. I left documentation about my cyber crime reports at the Kapolei Station with Desk Officer Aea with a request to forward all to you. Please confirm you received my submission,.

I receive Man-In-The-Middle attacks in my Outlook email thus it is not private. I sent an encrypted email to you from my Sonicwall encrypted email portal on 7/29/22 at 12:06 p.m. asking for a reply to confirm you can accept my encrypted email. I did not receive a reply.

Are you able to accept encrypted email accessed through a link? If so, please acknowledge the email I sent today at 8:00 a.m. from my encrypted Sonicwall email account, same address. You will need to click on the enclosed link to continue to the email content. Thank you for advising.

Respectfully,

Ricardo Finney

---

**From:** Nikon  
**Sent:** Friday, July 29, 2022 9:03 AM  
**To:** [t.iinuma@honolulu.gov](mailto:t.iinuma@honolulu.gov) <[t.iinuma@honolulu.gov](mailto:t.iinuma@honolulu.gov)>  
**Subject:** Request To Access Encrypted Email


Aloha, Detective linuma...


I will send you an encrypted email from my SonicWall secure email account to ensure private communication. I suffer from Man-In-The-Middle attacks.

Please click on the link received to access the encrypted email. Please confirm you received this message. Thank you.

Respectfully,

Ricardo Finney

 Secured by [Paubox](#) - HITRUST CSF certified

 Secured by [Paubox](#) - HITRUST CSF Certified

Aloha, Detective linuma...

I received the attached reply from my VPN vendor. It arrived in very small print so I pasted a larger version of the email content as follows:

Your request ([#19420682](#)) to ExpressVPN has been updated.  
To review the status of the request and add additional comments, follow the link below:

<https://expressvpn.zendesk.com/hc/requests/19420682>

You can also add a comment by replying to this email.

**Sheldon, 10 Aug 2022, 10:03 am GMT+8:**

Hi Ricardo,

Thank you so much for your response.

I believe we have addressed that in the last reply. But in case you have missed it, **there is no need for you to connect to the VPN on your Mac Settings.**

The **IKEv2** connection that you see under the network preference/settings on your MacOS acts as a placeholder for the ExpressVPN app to use. Unless you change the VPN protocol on the ExpressVPN app and switch it to IKEv2, that placeholder will remain disconnected.

**As for the username, password, and all the fields required by that**

**IKEv2** placeholder, it will be automatically populated by the VPN app once you connect using the **IKEv2 Protocol**. Basically, all the VPN controls should be done in the app and not in the settings. I hope this clears up the confusion.

If you have other questions, we'd be more than happy to answer them in real-time on the website:

[\*\*LIVE CHAT\*\*](#)

We look forward to hearing from you.

Regards,

Sheldon

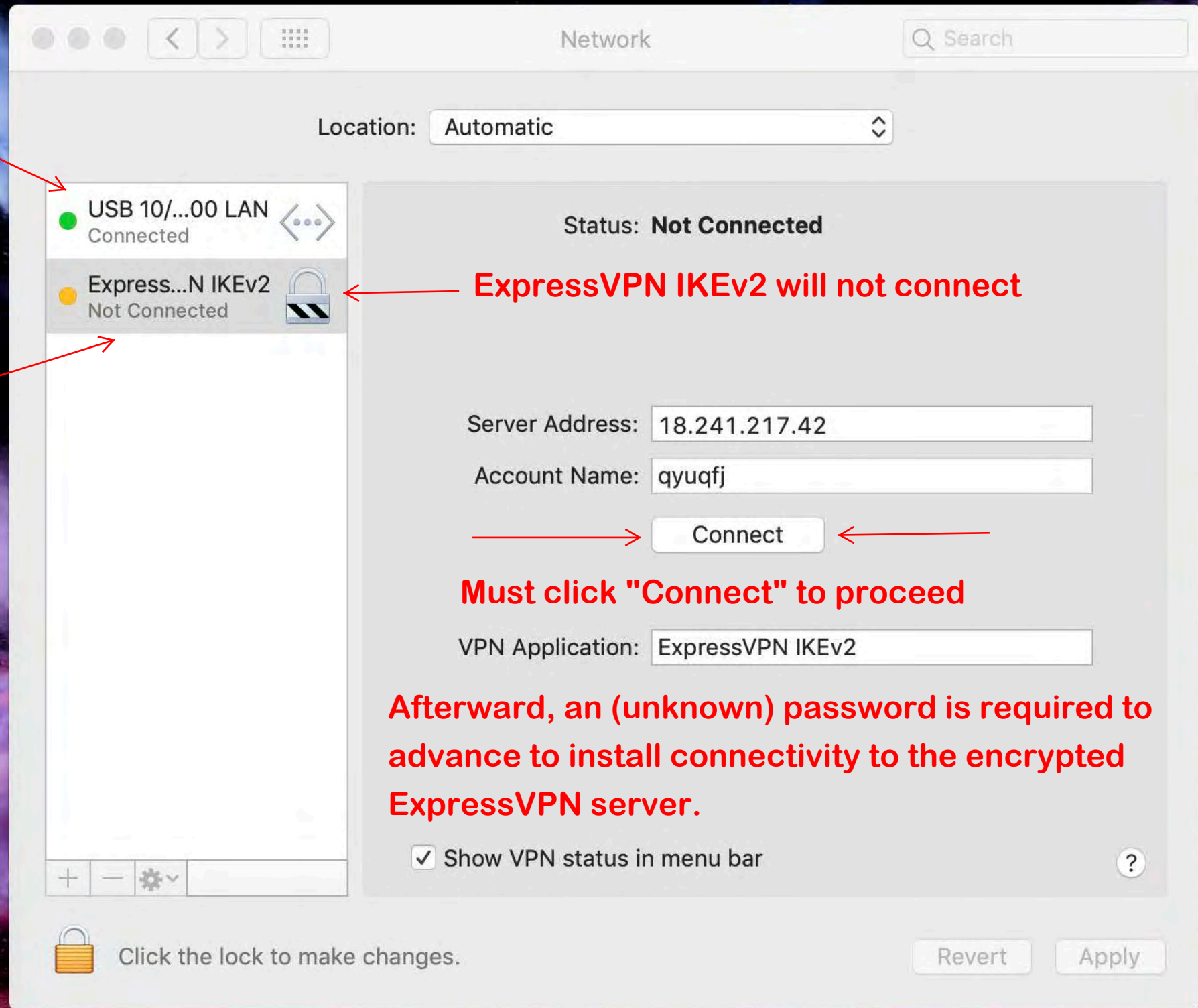
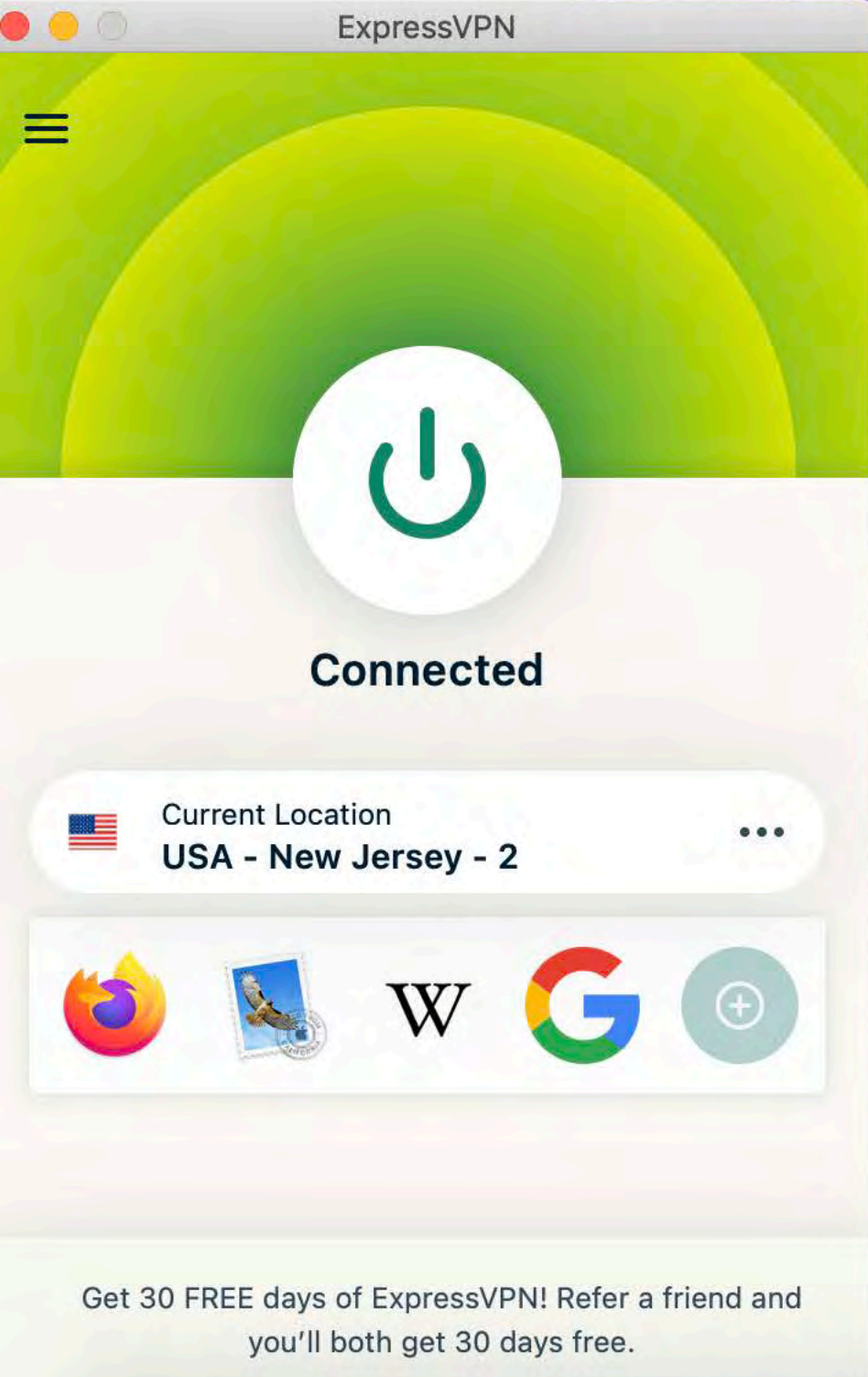
ExpressVPN Support



# Normal Internet connection from my Internet Provider

The connection that is made links to the city and IPs I select. However, this information is immediately visible to the malicious third party stalker's view since there is no stealth connection to the ExpressVPN IKEv2 encrypted server.

After the hack, the Express VPN server will not connect and where I go online is exposed.



ExpressVPN IKEv2 will not connect

Must click "Connect" to proceed

Afterward, an (unknown) password is required to advance to install connectivity to the encrypted ExpressVPN server.

Without a connection to the ExpressVPN encrypted server all that occurs when the software is running is an IP address change which appears instantly when a web page or website opens. With the knowledge of my location, stalkers then redirect or block my access to sites and online sales, cause emails to bounce, exploit unsecure/http connections to disable my computers and software, and much more.



"Connecting", Not "Connected"  
NEVER connects requires unknown  
password..

A connection is made to IP  
addresses by name, however  
there is no connection through

The screenshot shows the macOS Network settings window. The location is set to 'Automatic'. Under the network list, 'USB 10/...00 LAN' is connected, and 'Express...N IKEv2' is in the 'Connecting...' state. A modal dialog titled 'VPN Connection' is open, asking for authentication information. The text 'Password unknown to me' is displayed in red above a password input field. Below the input field are 'Cancel' and 'OK' buttons. At the bottom of the dialog, 'VPN Application: ExpressVPN IKEv2' is shown, and a checkbox for 'Show VPN status in menu bar' is checked. The main Network settings window has a lock icon and the text 'Click the lock to make changes.' at the bottom, along with 'Revert' and 'Apply' buttons.

After clicking  
"Connect"  
the password  
requirement  
appears.

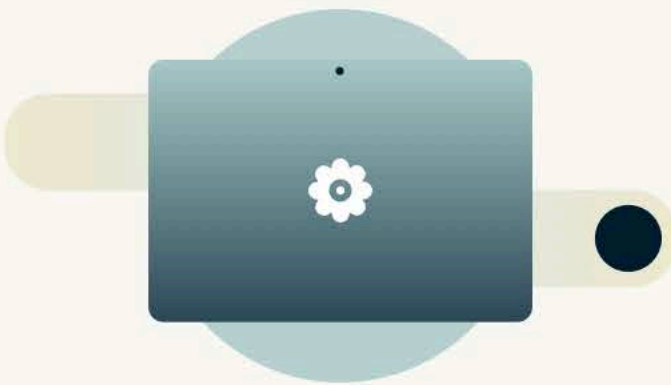
In ExpressVPN software that is NOT compromised  
the connection to the ExpressVPN servers go  
through automatically during the initial install,  
No password is required.

The screenshot shows the ExpressVPN application interface. At the top, there is a green header with a power button icon and the word 'Connected' below it. Below this, the 'Current Location' is shown as 'USA - New Jersey - 2' with a US flag icon and a menu icon. A row of application icons (Firefox, a mail icon, 'W', Google, and a plus sign) is displayed below. At the bottom, a promotional message reads: 'Get 30 FREE days of ExpressVPN! Refer a friend and you'll both get 30 days free.'

Without a connection to the Express  
VPN IKEv3 server, the location and IP  
address for any city I choose is  
immediately visible to the stalkers.



ExpressVPN



## Set Up Your VPN

Your Mac will ask permission to complete the configuration. ExpressVPN will not filter or monitor your network activity.

ExpressVPN IKEv2 connects to VPN servers

**Continue**

Network

Location: Automatic

USB 10/...00 LAN  
Not Connected

Status: **Cable Unplugged**  
Either the cable for USB 10/100/1000 LAN is not plugged in or the device at the other end is not responding.

**"ExpressVPN IKEv2" Would Like to Add VPN Configurations**  
All network activity on this Mac may be filtered or monitored when using VPN.

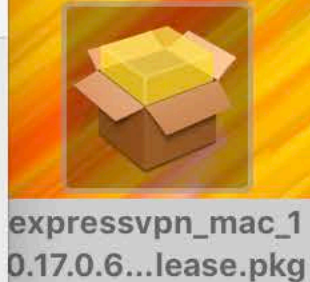
Allow Don't Allow

Search Domains:

Advanced... ?

Click the lock to make changes. Revert Apply

Normally, the ExpressVPN software automatically configures the IKEv2 configuration and connects. Click "Allow", and the connection to the secure ExpressVPN server is done without any action required by the user.





Security & Privacy

General FileVault Firewall Privacy

A login password has been set for this user [Change Password...](#)

Require password 5 minutes after sleep or screen saver begins

Show a message when the screen is locked [Set Lock Message...](#)

Disable automatic login

---

Allow apps downloaded from:

App Store

App Store and identified developers

Click the lock to make changes. [Advanced...](#) [?](#)



Binder1.pdf



express input vpn




expressvpn\_mac\_1  
1.3.0.67...lease.pkg

Install ExpressVPN

The installation was completed successfully.

- Introduction
- Destination Select
- Installation Type
- Existing Account
- Installation
- **Summary**




**NOT!**

**The installation was successful.**

The software was installed.

Normally, after "Allow" is clicked, the encrypted connection is made and ExpressVPN hides IP addresses.

In my hacked computer, when I click close and return to activate ExpressVPN, I go back to the panel requiring a password to advance.



[Go Back](#) [Close](#)



Internet connected

ExpressVPN encrypted servers not connected  
No privacy/No hidden IP's

ExpressVPN

Not Connected

Selected Location  
Mexico

Smart Location  
USA - Los Angeles

Our router app just got a major upgrade:  
Connect to multiple locations at the same time.

Find out how it works

Network

Location: Automatic

USB 10/...00 LAN Connected

Express...N IKEv2 Not Connected

Status: Not Connected

Server Address: 18.241.217.42

Account Name: qyuqfj ??????

Connect

VPN Application: ExpressVPN IKEv2

Show VPN status in menu bar

Click the lock to make changes. Revert Apply

But I go back to this page with a connection to the Internet, not to the ExpressVPN encrypted servers and a requirement to enter an unknown password to advance.