



# Security Awareness Training 2021 v1.7 IT&Users

---

TRAN HONG QUAN ANDY

PEOPLEFIREWALL.COM

# Self Intro

#peoplefirewall

Keywords: people firewall, tran hong quan andy

<https://www.amazon.com/dp/B096N922WJ/> <https://peoplefirewall.com/ebook>

The screenshot shows the Amazon Kindle Store page for the book "People Firewall: Cybersecurity and Hacking Secrets Kindle Edition" by Andy Tran. The page is viewed in a web browser with the address bar showing "amazon.com/dp/B096N922WJ/". The Amazon header includes the logo, delivery location (Tran Hanoi 10000), and navigation links like "All", "Today's Deals", "Buy Again", "Gift Cards", "Browsing History", "Quan's Amazon.com", "Customer Service", "Registry", and "Sell". A search bar is present on the right. Below the header, there's a navigation bar with categories like "Buy a Kindle", "Kindle eBooks", "Kindle Unlimited", "Prime Reading", "Best Sellers & More", "Kindle Vella", "Kindle Book Deals", "Kindle Singles", "Newsstand", "Manage content and devices", and "Advanced Search". A green banner for "Epic Daily Deals" is visible. The main content area shows the book's cover, which features a Spartan warrior. The title "People Firewall: Cybersecurity and Hacking Secrets Kindle Edition" is prominently displayed, along with the author "Andy Tran" and the format "Kindle Edition". The price is listed as \$15.00. There is a "Look inside" link and a "1 rating" star. Below the price, there's a section for "Internet Freedom for individual" and "Trust no one but yourself, don't trust your girlfriends/wife, smartphone and mobile apps." The book's publication date is "1st edition 4/6/2021" and the update date is "2nd edition update 9/8/2021". A "Brief introduction" section follows, explaining the book's purpose and the author's background. The author's name "Andy Tran" is shown with a "Follow" button. On the right side, there's a sidebar with the "Kindle Price: \$15.00" and a "Buy now with 1-Click" button. Below this, there's a "Deliver to" dropdown menu set to "Your Kindle Library". There's also a "Send a free sample" button and another "Deliver to" dropdown menu. At the bottom of the sidebar, there's a "Give as a Gift" button and an "Add to List" dropdown menu. The footer of the page shows the Windows taskbar with various application icons and the system clock displaying "7:22 PM 12/9/2021".

Amazon.com: People Firewall: Cy x +

amazon.com/dp/B096N922WJ/

amazon Deliver to Tran Hanoi 10000 Kindle Store

All Today's Deals Buy Again Gift Cards Browsing History Quan's Amazon.com Customer Service Registry Sell

Buy a Kindle Kindle eBooks Kindle Unlimited Prime Reading Best Sellers & More Kindle Vella Kindle Book Deals Kindle Singles Newsstand Manage content and devices Advanced Search

Epic Daily Deals amazon Shop now

Kindle Store > Kindle eBooks > Computers & Technology

Look inside

PEOPLE FIREWALL CYBERSECURITY & HACKING SECRETS

People Firewall: Cybersecurity and Hacking Secrets Kindle Edition

by Andy Tran (Author) Format: Kindle Edition

★★★★★ 1 rating

See all formats and editions

Kindle \$15.00

Read with Our Free App

Internet Freedom for individual

Trust no one but yourself, don't trust your girlfriends/wife, smartphone and mobile apps.

1st edition 4/6/2021

2nd edition update 9/8/2021

**Brief introduction**

As the book is named **People Firewall**, we must turn ourselves into firewalls to protect us from Internet threats. **Cybersecurity** is not a product, it's a process. Moreover, security is not a technology problem. It's a people and management problem. People are the first line of defense, learning cybersecurity will not be complete if we don't understand how the computer hacking techniques or **Hacking Secrets** are conducted.

The reason for the creation of this eBook is about my curiosity on hacking as well as I want to share my knowledge and experience so that everyone can surf the Internet safely.

This book is designed in a very logical way based on what I learnt during my last job at **Check Point Software Technologies Corp.** I sold **next generation firewall appliances** to protect Enterprise customers. I use **People, Policy, Technology and Hacking** to

Kindle Price: \$15.00 includes free international wireless delivery via Amazon Whispernet

Buy now with 1-Click

Deliver to: Your Kindle Library

Send a free sample

Deliver to: Your Kindle Library

Give as a Gift

Add to List

Enter a promotion code or Gift Card

Share <Embed>

READ ON

Type here to search

20°C Trời quang 7:22 PM 12/9/2021

# Nhận thức về an ninh mạng

---

- Tư duy tiếp cận vấn đề
- Bảo mật cho smartphone
- Bảo mật khi làm việc từ xa (mùa Covid)
- Các cách thức hacker tấn công người dùng
- Kiểm tra ngắn 15 phút.

# Tư duy tiếp cận vấn đề

---

- An ninh mạng không phải là vấn đề của công nghệ mà vẫn là vấn đề con người và quản lý.
- An ninh mạng bao gồm con người, chính sách bảo mật, công nghệ phòng thủ và tấn công (hacking).
- An ninh mạng không phải là sản phẩm mà là một tiến trình (process)
- Con người là lá chắn đầu tiên và là quan trọng nhất.

# Đạo phật

---

## ■ Con người:

- ❖ Tham sân, si, mạn và nghi
- ❖ Luật nhân quả
- ❖ Tham tiền (tham), quyền lực(tham), bia rượu (tham), ái tình (tham), muốn giàu nhanh (lười)
- ❖ Tốt bụng muốn giúp đỡ người (Đường Tăng)
- ❖ Tin người.
- ❖ Thiếu thông tin và hiểu biết (si)

# Chính sách bảo mật

---

▪ **Zero Trust**, ISO 27001/27701, PCI DSS và **GDPR** cho doanh nghiệp.

Cho Cá Nhân:

- ❖ Mật khẩu mạnh (strong password)
- ❖ Xác thực hai thành tố (2FA)
- ❖ Nâng cấp phần mềm
- ❖ Backup dữ liệu cho máy tính và smartphone

# Mật khẩu mạnh

---

- Dùng nhiều mật khẩu, không dùng một mật khẩu cho tất cả và thay đổi thường xuyên.
- Mật khẩu mạnh lớn hơn 9 kí tự gồm chữ, số, chữ viết hoa và kí tự đặc biệt.
- Dùng cụm câu (passphrase)
  - ❖ Toingudaysom@2002
  - ❖ lamviecThongminh\*1990
  - ❖ Tranthituyet\*2201



# Ứng dụng (thực hành luôn)

<https://haveibeenpwned.com/>

The screenshot shows a web browser window with the URL <https://haveibeenpwned.com/>. The website has a dark blue header with navigation links: Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. The main content area has a large blue background with the text "';--have i been pwned?" in a white rounded box. Below this, it says "Check if your email or phone is in a data breach". A search bar contains the email "quanht@gmail.com" and a button labeled "pwned?". The result section has a dark red background with the text "Oh no — pwned!" and "Pwned in 7 [data breaches](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)". Below this, there is a section titled "3 Steps to better security" with a button "Start using 1Password.com". The Windows taskbar is visible at the bottom with various application icons and system information like temperature (20°C) and time (7:49 PM, 12/9/2021).



20:01

ZP

safe me

WOT Mobile Security Prot...  
Ad • WOT Services LLC  
In-app purchases

Install

4.7★

18K reviews

10 MB

3+

Rated for 3+

11 Down

App Scanning & WiFi Protection

SAFE Me  
Safe Securities Inc. • Tools  
Installed

Secure messenger SafeUM  
SafeUM Communications e... • Communication  
2.9★ 32 MB 5M+

Keep Me Safe: Family Locator Tracker  
Keep Me Safe Inc • Parenting  
16 MB 1K+

Safe Security - Antivirus, Booster, Phon...  
Safe Security Develop • Tools  
4.7★ 26 MB 100M+

F-Secure SAFE Mobile Antivirus  
F-Secure Corporation • Tools  
4.4★ 8.9 MB 1M+

Password Safe - Secure Password Man...  
Robert Ehrhardt • Productivity  
4.7★ 8 MB

Safe Surfer: Porn Filter and App Blocker  
Safe Surfer Ltd • Parenting  
4.7★ 57 MB 500K+

19:55

ZP

4.42  
SAFE Me Score (0-5)

Risk: 

Very low

Device Controls

Screen Lock

OS Version

19:55

ZP

Awareness

Required

All courses

Results

Search

25 Courses

Required

SAFE Laptop Usage - MacBook

SAFE Laptop Usage - Windows

SAFE Password Usage

Importance of Software Updates

SAFE Public Wi-Fi Usage

SAFE from SMS Scams

20:06

ZP

Device

Connection

Enabled

Screen Lock

5 seconds

Lock Timeout

Enabled

Device Encryption

Disabled

Developer Options

5 minutes

Sleep Duration

Enabled

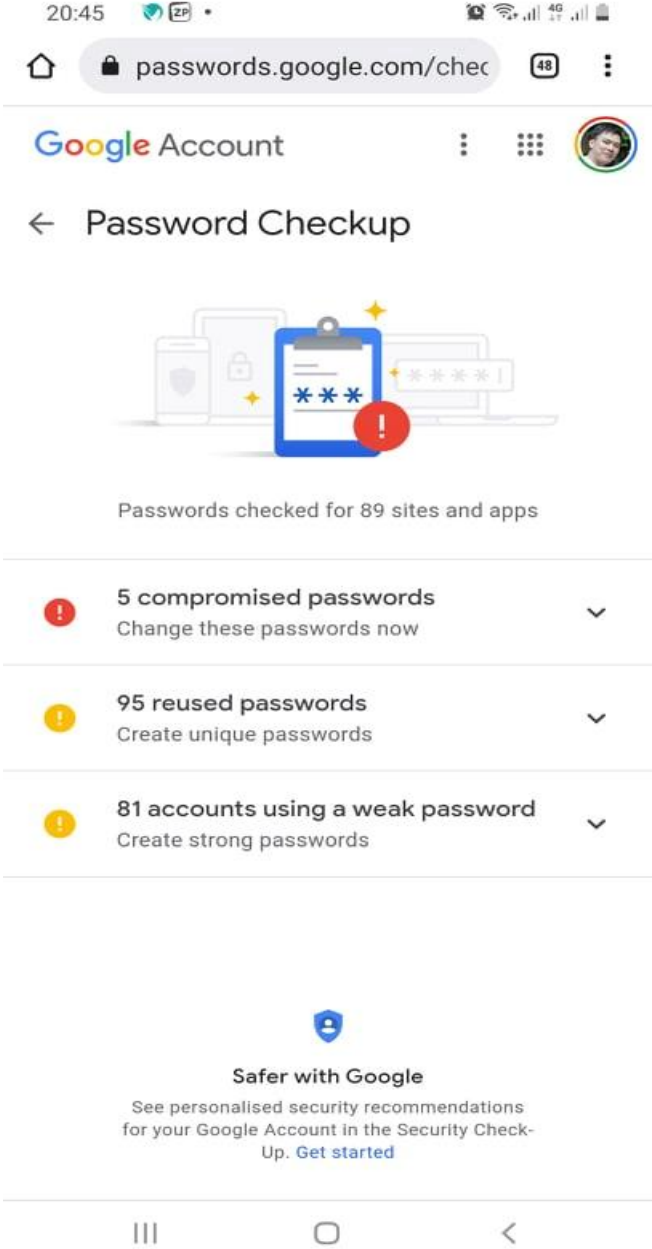
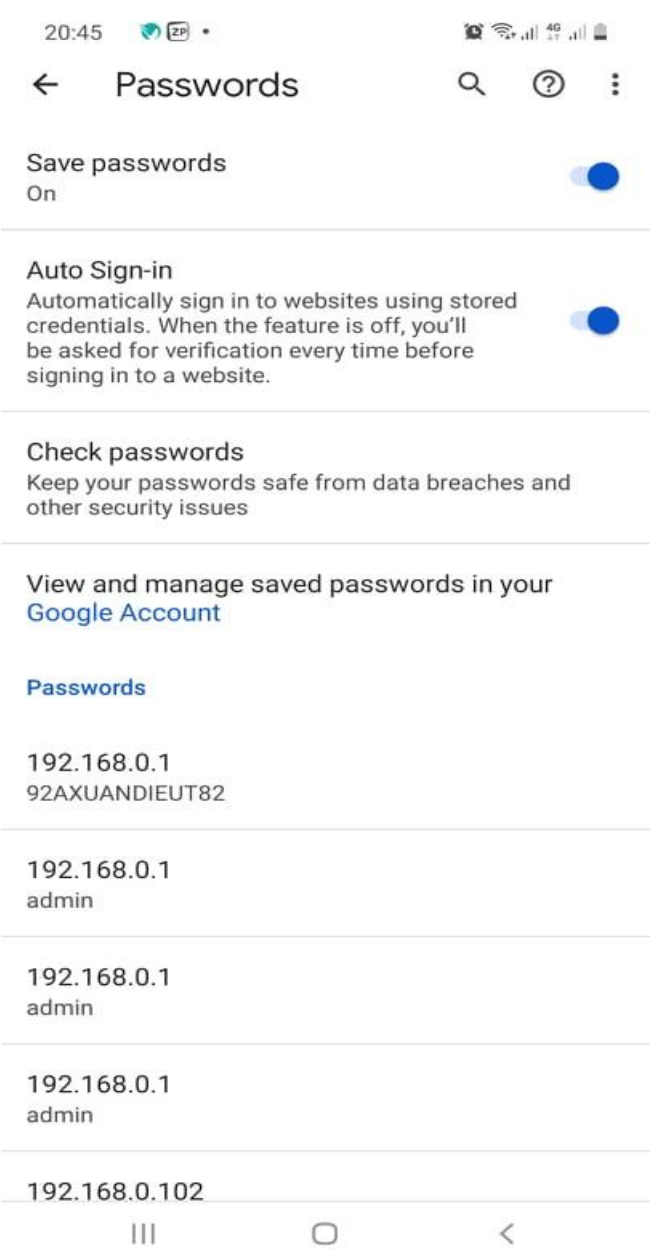
Notification on Lock Screen

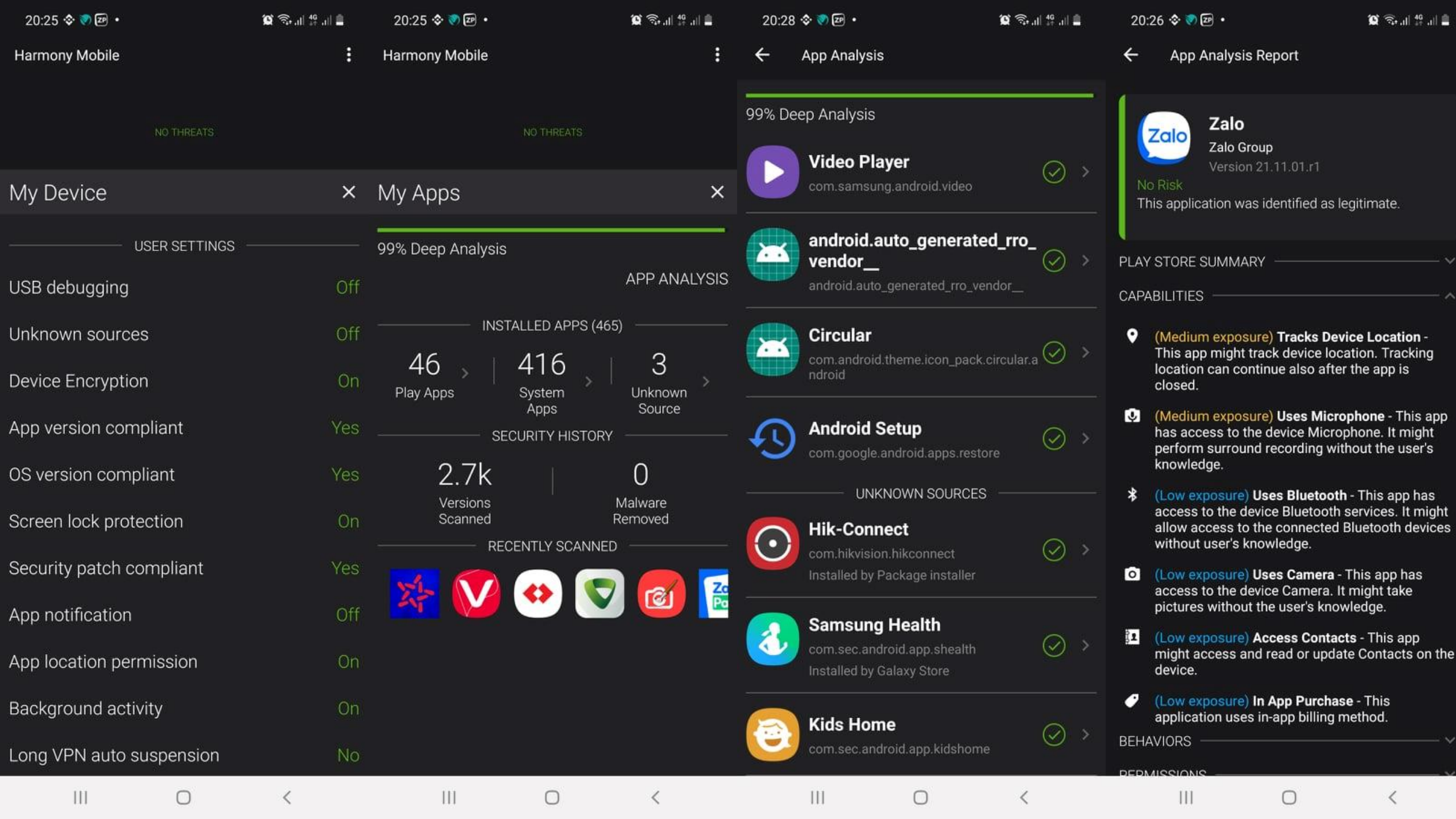
Enabled

Location Services

chrome://settings/passwords

https://passwords.google.com/?utm\_source=chrome&utm\_medium=desktop&utm\_campaign=chrome\_settings





20:25

Harmony Mobile

20:25

20:28

20:28

20:26

20:26

20:26

Harmony Mobile

⋮

Harmony Mobile

⋮

←

App Analysis

←

App Analysis Report

NO THREATS

NO THREATS

99% Deep Analysis



Video Player

com.samsung.android.video



android.auto\_generated\_rro\_vendor\_

android.auto\_generated\_rro\_vendor\_



Circular

com.android.theme.icon\_pack.circular.a

ndroid



Android Setup

com.google.android.apps.restore



UNKNOWN SOURCES



Hik-Connect

com.hikvision.hikconnect

Installed by Package installer



Samsung Health

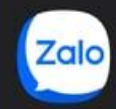
com.sec.android.app.shealth

Installed by Galaxy Store



Kids Home

com.sec.android.app.kidshome



Zalo

Zalo Group

Version 21.11.01.r1

No Risk

This application was identified as legitimate.

PLAY STORE SUMMARY

CAPABILITIES



(Medium exposure) Tracks Device Location - This app might track device location. Tracking location can continue also after the app is closed.



(Medium exposure) Uses Microphone - This app has access to the device Microphone. It might perform surround recording without the user's knowledge.



(Low exposure) Uses Bluetooth - This app has access to the device Bluetooth services. It might allow access to the connected Bluetooth devices without user's knowledge.



(Low exposure) Uses Camera - This app has access to the device Camera. It might take pictures without the user's knowledge.



(Low exposure) Access Contacts - This app might access and read or update Contacts on the device.



(Low exposure) In App Purchase - This application uses in-app billing method.

BEHAVIORS

PERMISSIONS

# 2FA và chính sách

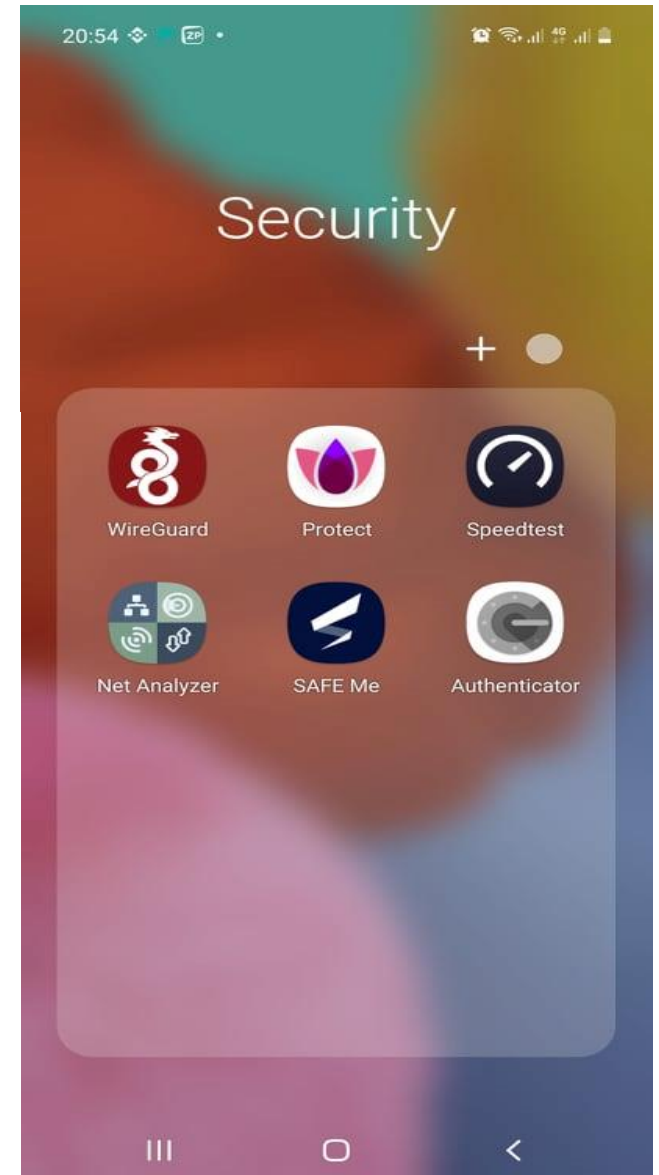
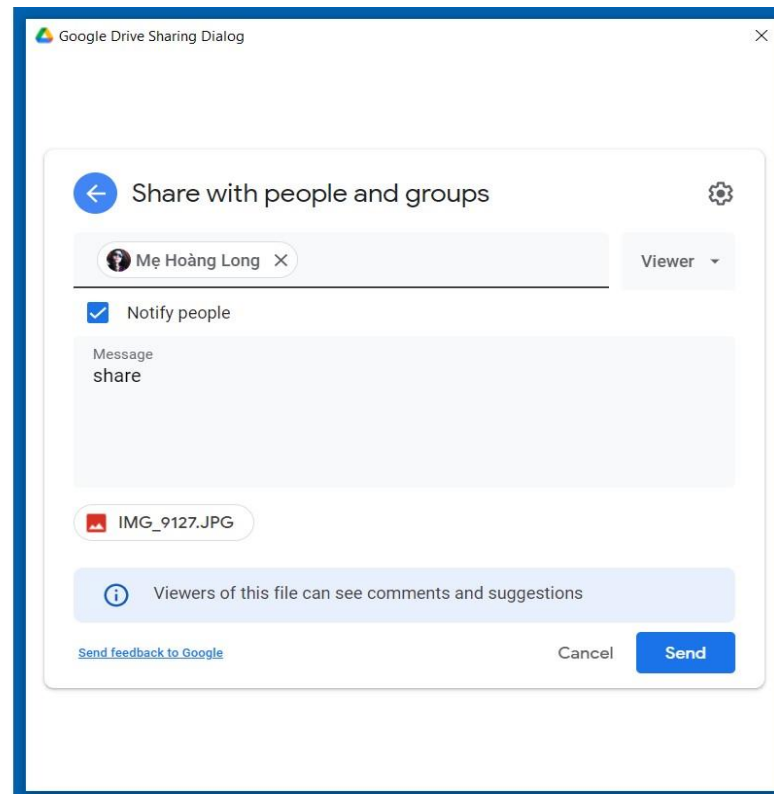
---

- Bật 2FA ở tất cả các tài khoản quan trọng có liên quan tới Tiền.
- Nâng cấp phần mềm thường xuyên.
- Backup dữ liệu lên điện toán đám mây **Microsoft OneDrive** và **Google Drive** và cả ổ cứng di động cá nhân.
- Backup smartphone.



# 2FA và chia sẻ dữ liệu an toàn trên Internet.

- Giới hạn quyền truy cập dữ liệu, Phân quyền cho đúng người
- Google Authenticator



# Phòng thủ (làm việc từ xa)

---

- Dùng phần mềm Anti-Virus
- Máy Mac cũng cần phần mềm Anti-Virus
- Kết nối VPN tới công ty.
- Bảo vệ Smartphone
  - ❖ Không Jailbreak Iphone
  - ❖ Chỉ cài ứng dụng trên Appstore và Play Store
  - ❖ Xóa ứng dụng không cần thiết
  - ❖ Cài phần mềm bảo mật riêng cho smartphone

# Cách thức hacker tấn công

---

- Hacking là cách tìm ra giải pháp thông minh cho một vấn đề.
- Rất nhiều cách thức để hack và kĩ thuật thay đổi hàng ngày
  - ❖ Lừa người dùng mở file ảnh, tài liệu, download file nhạc hoặc video có gắn mã độc để chiếm quyền điều khiển.
  - ❖ Email lừa đảo (phishing)
  - ❖ Lừa người dùng cài ứng dụng di động và giám sát hoạt động của dùng người.
  - ❖ Cho người dùng dùng miễn phí Wifi và dùng phần mềm MITM ở giữa để bắt tên truy cập và mật khẩu.
  - ❖ Người dùng chỉ cần vào trang web film người lớn là bị nhiễm mã độc luôn rồi.





VMware Tools

mac-payload

girl.jpg

exec

osx\_http\_8080

girl.icns

backdoor

Recents

Application...

Desktop

Documents

Downloads

OneDrive

iCloud

iCloud Dri...

Locations

VMwar...

Tags

Red

Orange

Yellow

Green

```
319 modules currently loaded
1 listeners currently active
1 agents currently active

(Empire) >
[*] Sending PYTHON stager (stage 1) to 192.168.0.51
[*] Agent OHB1WK8G from 192.168.0.51 posted valid Python PUB key
[*] New agent OHB1WK8G checked in
[+] Initial agent OHB1WK8G from 192.168.0.51 now active (Slack)
[*] Sending agent (stage 2) to OHB1WK8G at 192.168.0.51
[!] strip_python_comments is deprecated and should not be used

(Empire) > agents

[*] Active agents:
```

Name	La	Internal IP	Machine Name	Username	Process	PID	Delay	Last Seen	Listener
7W3V5E1U	ps	192.168.0.79	DESKTOP-OR6DRQQ	*DESKTOP-OR6DRQQ\ DELL	powershell	10004	5/0.0	2021-05-31 11:52:59	http
OHB1WK8G	py	127.0.0.1	Quans-Mac.local	quanht	/Library/Developer	689	5/0.0	2021-06-01 01:56:30	http

```
(Empire: agents) > interact OHB1WK8G
(Empire: OHB1WK8G) > sysinfo
[*] Tasked OHB1WK8G to run TASK_SYSINFO
[*] Agent OHB1WK8G tasked with task ID 1
(Empire: OHB1WK8G) >
Listener: http://192.168.0.10:8080
Internal IP: 127.0.0.1
Username: \quanht
Hostname: Quans-Mac.local
OS: Darwin,Quans-Mac.local,19.5.0,Darwin Kernel Version 19.5.0: Tue May 26 20:41:44 PDT 2020; root:xnu-6153.121.2~2/RELEASE_ARM_T8020
High Integrity: 0
Process Name: /Library/Developer/CommandLineTools/Library/Frameworks/Python3.framework/Versions/3.8/Resources/Python.app/Contents/MacOS/Python
Process ID: 689
Language: python
Language Version: 3.8

(Empire: OHB1WK8G) >
```



21:06

21:10

21:07

21:07

←

🗑️📁⋮

←

🗑️📁⋮

←

🗑️📁⋮

AI

Apple iTunes

quanht@woodfire4.com

Nov 17

🍏

Receipt

APPLE ID

quanht@woodfire4.com

INVOICE DATE TODAY	SEQUENCE NO. 3-654351687	BILLED TO Store Credit	TOTAL £6.99
ORDER ID MNEJ3TNC97	DOCUMENT NO. 126845427		

My World 2.0 Justin Bieber

Album

iPhone

£6.99

Inclusive of VAT at 20%

VAT charged at 20% £1.17

TOTAL £6.99

If you haven't authorized this charge, click the link below to dispute transaction and get full refund.

You can cancel a payment at any time: [Cancel / Refund](#)

[SPAM] Your receipt from Apple

AI

Apple iTunes

purchase@uk.itunes-store.net

Yesterday

To You

quanht@woodfire4.com

Wednesday, November 17, 12:06

🍏

Receipt

APPLE ID

quanht@woodfire4.com

INVOICE DATE TODAY	SEQUENCE NO. 3-654351687	BILLED TO Store Credit	TOTAL £6.99
ORDER ID MNEJ3TNC97	DOCUMENT NO. 126845427		

My World 2.0 Justin Bieber

Album

iPhone

£6.99

Inclusive of VAT at 20%

VAT charged at 20% £1.17

Critical security alert

G

Google

quanht@woodfire4.com

Yesterday

Google

Quan Tran

image

!

Sign-in attempt was blocked

quanht@woodfire4.com

Someone just used your password to try to sign in to your account from a non-Google app. Google blocked them, but you should check what happened. Review your account activity to make sure no one else has access.

CHECK YOUR ACTIVITY

Google

no-reply@useraccounts-google.com

To You

quanht@woodfire4.com

Wednesday, December 8, 12:41

Google

Quan Tran

image

!

Sign-in attempt was blocked

quanht@woodfire4.com

Someone just used your password to try to sign in to your account from a non-Google app. Google blocked them, but you should check what happened. Review your account activity to make sure no one else has access.

CHECK YOUR ACTIVITY

⏮️⏪️⏩️⏭️

⏮️⏪️⏩️⏭️

⏮️⏪️⏩️⏭️

⏮️⏪️⏩️⏭️



# Phần mềm giám sát smartphone

mSpy™ Cell Phone Tracker: Your Id: 000001 Dashboard | mSpy Demo

demo.mspy.com/dashboard.html

**M.SPY** Your Id: 000001

S9 - build 18 - ... PREMIUM

**Dashboard**

**GENERAL FEATURES**

- Contacts
- Text Messages
- Calls
- Events
- Photo
- Video
- Wi-Fi networks
- Keyword tracking
- Keylogger
- Installed APPs

**Dashboard**

**Most Messaging Contacts**

3434857946	Matty	16 times
3444231987	Dad	9 times
3487694712	Mom	4 times

[ALL MESSAGES](#)

**Most Calling Contacts**

3471629902	Teresa	5 times
3476549120	Lisa	3 times
3456139652	Jessica	2 times

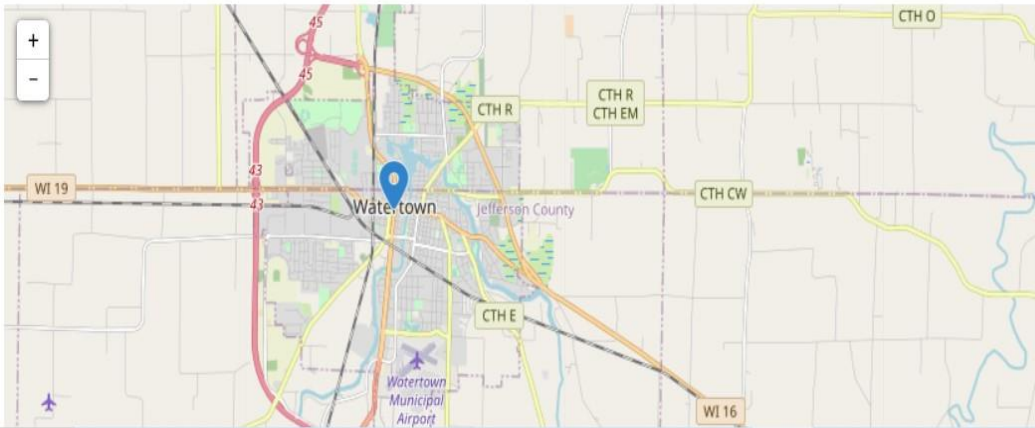
[ALL CALLS](#)

**Most Visited Websites**

The Free Encyclopedia	<a href="https://www.wikipedia.org/">https://www.wikipedia.org/</a>	7 times
Music for everyone.	<a href="https://www.spotify.com/">https://www.spotify.com/</a>	5 times
Gmail   Inbox	<a href="https://mail.google.com/">https://mail.google.com/</a>	3 times

[ALL WEBSITES](#)

**Last Locations**



316 N Washington St, Watertown, WI, 54801  
Apr 9, 2020 6:59 PM

134 Coolidge Ave, Watertown, WI, 54801  
Apr 8, 2020 6:49 PM

813 Scribner St, Spooner, WI, 54880  
Apr 10, 2020 6:36 PM

[Help](#)

Type here to search

27°C Mưa 6:33 AM 8/10/2021

# MITM

ain

File View Configure Tools Help

Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query

APR

- APR-Cert (26)
- APR-DNS
- APR-SSH-1 (0)
- APR-HTTPS (0)
- APR-ProxyHTTPS (0)
- APR-RDP (0)
- APR-FTPS (0)
- APR-POP3S (0)
- APR-IMAPS (0)
- APR-LDAPS (0)
- APR-SIPS (0)

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	192.168.0.1	AC84C63D9664	0	0	20AA4B41E2DA	192.168.0.19
Poisoning	192.168.0.1	AC84C63D9664	0	0	10FEEDAD1675	192.168.0.18
Poisoning	192.168.0.1	AC84C63D9664	0	0	E894F68F7B03	192.168.0.17
Poisoning	192.168.0.1	AC84C63D9664	0	0	B04E26FD667D	192.168.0.29
Poisoning	192.168.0.1	AC84C63D9664	0	0	AC84C621824F	192.168.0.28
Poisoning	192.168.0.1	AC84C63D9664	0	0	704F57066ED7	192.168.0.7
Poisoning	192.168.0.1	AC84C63D9664	0	0	A0F3C19515AF	192.168.0.4
Poisoning	192.168.0.1	AC84C63D9664	0	0	503EAA32BB11	192.168.0.10
Poisoning	192.168.0.1	AC84C63D9664	0	0	503EAA32BB11	192.168.0.51
Poisoning	192.168.0.1	AC84C63D9664	0	0	1C3BF37C9336	192.168.0.55
Poisoning	192.168.0.1	AC84C63D9664	0	0	00D86105DC32	192.168.0.63
Poisoning	192.168.0.1	AC84C63D9664	0	0	B0BE76BD3215	192.168.0.36
Poisoning	192.168.0.1	AC84C63D9664	0	0	402343D37C99	192.168.0.82
Poisoning	192.168.0.1	AC84C63D9664	15	15	023AAEE71F48	192.168.0.81

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Half-routing	192.168.0.70	1C3BF3BC5E15	8	0	AC84C63D9664	103.149.196.173
Half-routing	192.168.0.70	1C3BF3BC5E15	3	0	AC84C63D9664	45.251.33.18
Half-routing	192.168.0.70	1C3BF3BC5E15	7	0	AC84C63D9664	197.210.64.149
Half-routing	192.168.0.70	1C3BF3BC5E15	3	0	AC84C63D9664	185.217.90.190
Half-routing	192.168.0.70	1C3BF3BC5E15	10	0	AC84C63D9664	197.210.65.74
Full-routing	192.168.0.70	1C3BF3BC5E15	15	3	AC84C63D9664	197.210.64.32
Half-routing	192.168.0.70	1C3BF3BC5E15	9	0	AC84C63D9664	197.210.47.246
Half-routing	192.168.0.70	1C3BF3BC5E15	7	0	AC84C63D9664	77.219.1.91
Half-routing	192.168.0.70	1C3BF3BC5E15	8	0	AC84C63D9664	178.50.234.243
Half-routing	192.168.0.70	1C3BF3BC5E15	10	0	AC84C63D9664	197.210.65.151
Full-routing	192.168.0.55	1C3BF37C9336	22	40	AC84C63D9664	17.248.165.40
Half-routing	192.168.0.78	AC84C62A1296	90	0	AC84C63D9664	35.186.224.25
Half-routing	192.168.0.70	1C3BF3BC5E15	8	0	AC84C63D9664	197.210.65.189
Full-routing	192.168.0.70	1C3BF3BC5E15	1	1	AC84C63D9664	116.86.56.230
Full-routing	192.168.0.70	1C3BF3BC5E15	9	1	AC84C63D9664	180.252.122.222
Half-routing	192.168.0.55	1C3BF37C9336	31	0	AC84C63D9664	172.217.26.131
Full-routing	192.168.0.55	1C3BF37C9336	28	25	AC84C63D9664	17.248.165.39
Half-routing	192.168.0.70	1C3BF3BC5E15	16	0	AC84C63D9664	161.117.7.124
Half-routing	192.168.0.70	1C3BF3BC5E15	8	0	AC84C63D9664	197.210.64.212
Full-routing	192.168.0.70	1C3BF3BC5E15	17	1	AC84C63D9664	213.101.14.149

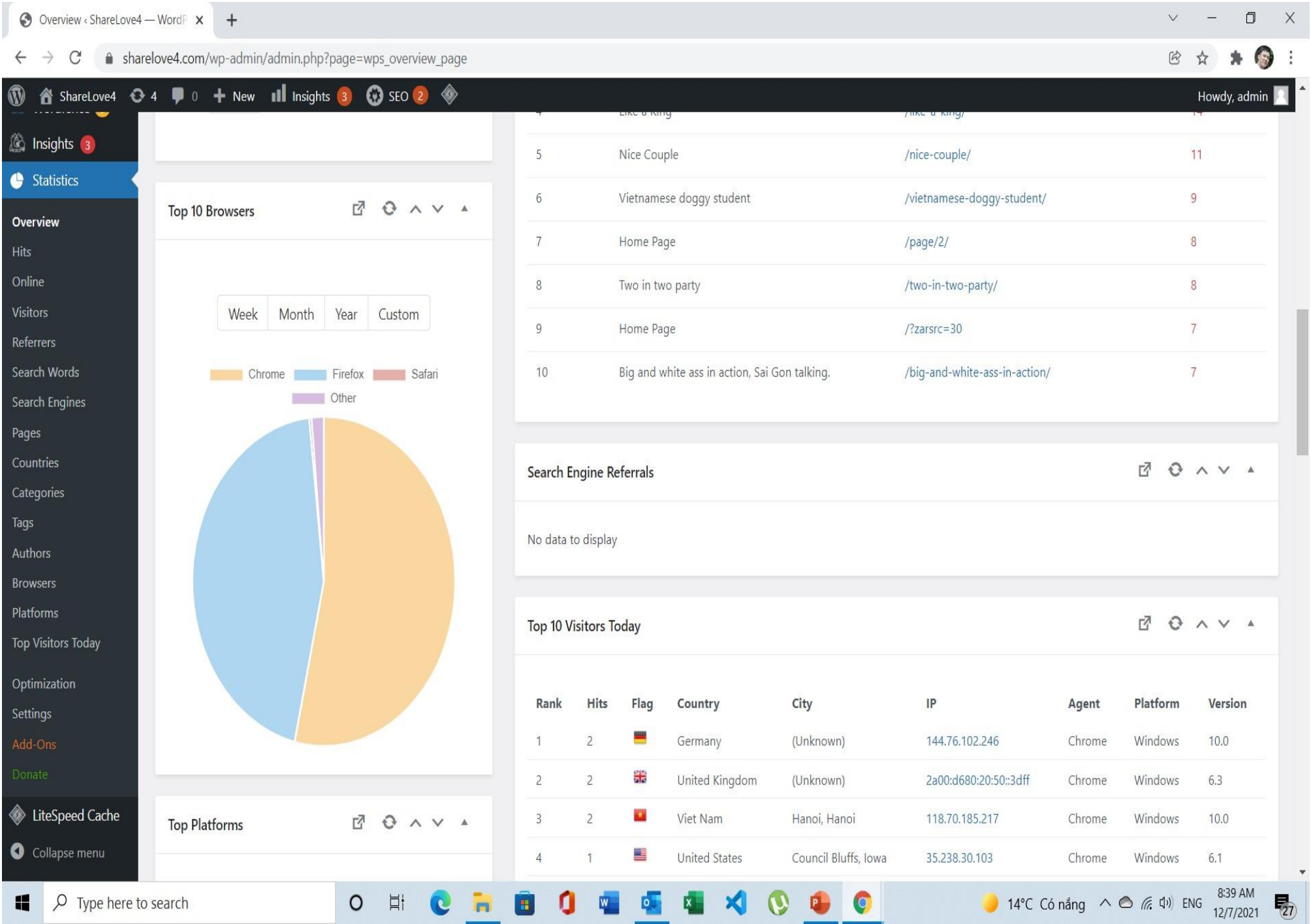
Configuration / Routed Packets

Hosts APR Routing Passwords VoIP

Lost packets: 1%

Windows taskbar: 12:08 PM 5/30/2021

Vào trang web người lớn





# Mã độc như thế nào ?

**Malware/ShellCode/Payload looks like this:**

[illegible]

# Thank you

---

For more contact:

<https://www.facebook.com/quanht2009>

<https://peoplefirewall.com>

[quanht@peoplefirewall.com](mailto:quanht@peoplefirewall.com)

090 419 4242

08666 46 470