



# Cyber Security



Rattasapa Meeprapai  
Computer Technical Officer  
The Secretariat of the Cabinet

(v2.1 – 10 Nov 2022)

# This is me Rattasapa

## RATTASAPA MEEPRAPAI (Root)

### Education

- **B.Eng. Computer Engineering (Second-Class Honours)**  
King Mongkut's University of Technology Thonburi, Thailand
- **MSc Cyber Security (Distinction)**  
University of Southampton, the UK



### Experience

- Computer Technical Officer  
The Secretariat of the Cabinet (Office of the Prime Minister)
- Interactive Content Developer (Part-time) at T-Stone Co., Ltd.  
Developed Interactive Contents for Museums and Exhibitions



### Certificates

- CompTIA PenTest+
- CompTIA CySA+
- CompTIA Security+



### Contact

- Email: [rattasapa.m@soc.go.th](mailto:rattasapa.m@soc.go.th) | Tel.: (+66)2-280-9000 Ext. 1453



# Today's Topic



Cyber Security  
- And -  
Basic of  
Penetration Testing

# The First Topic

## Cyber Security

- The Definition of Cyber Security
- Cyber Threat Trends in Thailand
- Dealing with Cyber Threat with Cyber Security Awareness



# Cyber Security



What is it?



# Like This?



# Like This?

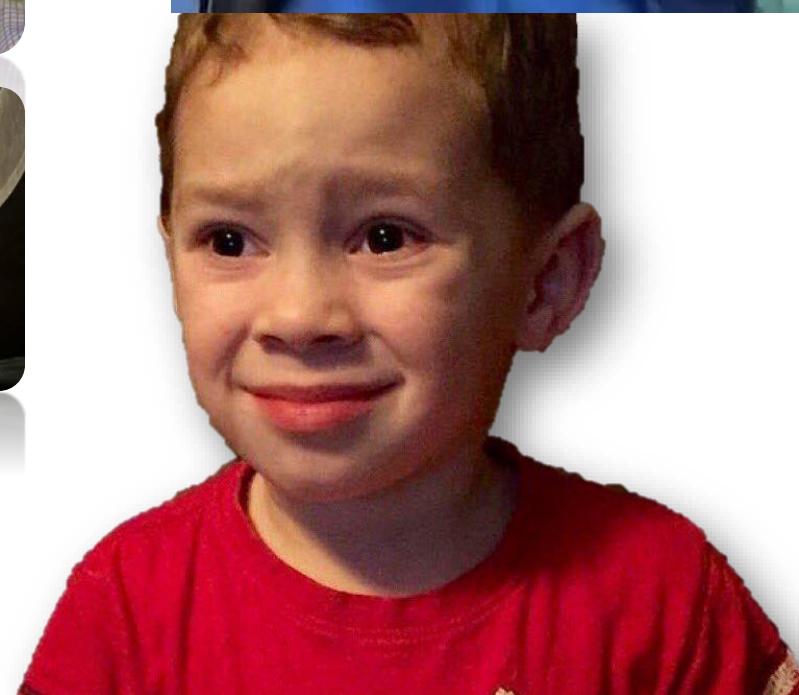
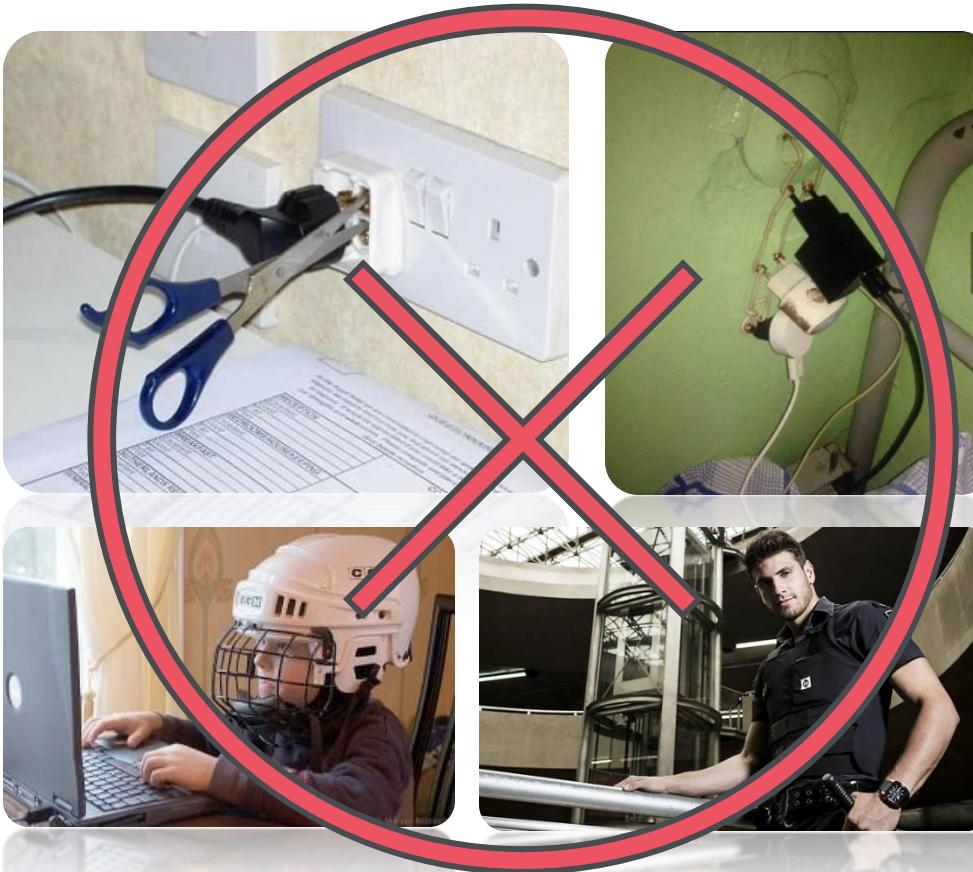


VIA GIGAG.COM

# Or Like This?



# I don't think so...



# The Definition of Cyber Security

- According Cybersecurity Act B.E. 2562 (2019)



- **Maintaining Cybersecurity**



- **Cyber Threats**



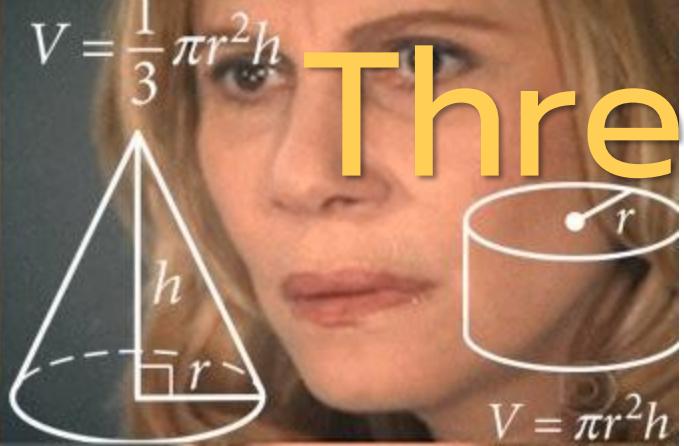
- **Cyber**

# The Definition of Cyber Security

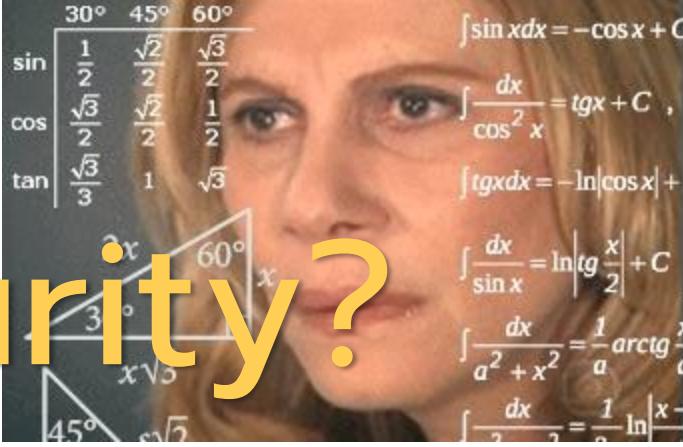
Cyber?



$A = \pi r^2$   
 $C = 2\pi r$



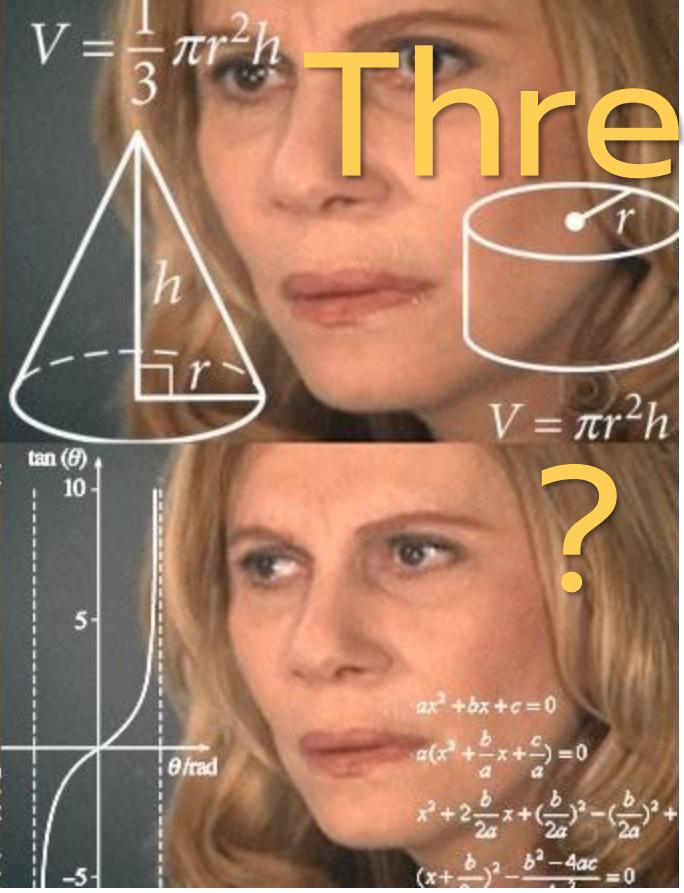
$V = \frac{1}{3} \pi r^2 h$   
 $V = \pi r^2 h$



$\begin{array}{|c|c|c|}\hline & 30^\circ & 45^\circ & 60^\circ \\ \hline \sin & \frac{1}{2} & \frac{\sqrt{2}}{2} & \frac{\sqrt{3}}{2} \\ \hline \cos & \frac{\sqrt{3}}{2} & \frac{\sqrt{2}}{2} & \frac{1}{2} \\ \hline \tan & \frac{\sqrt{3}}{3} & 1 & \sqrt{3} \\ \hline \end{array}$

$\int \sin x dx = -\cos x + C$   
 $\int \frac{dx}{\cos^2 x} = \operatorname{tg} x + C$ ,  
 $\int \operatorname{tg} x dx = -\ln|\cos x| + C$   
 $\int \frac{dx}{\sin x} = \ln\left|\operatorname{tg} \frac{x}{2}\right| + C$   
 $\int \frac{dx}{a^2 + x^2} = \frac{1}{a} \operatorname{arctg} \frac{x}{a}$   
 $\int \frac{dx}{x^2 - a^2} = \frac{1}{2a} \ln \left| \frac{x-a}{x+a} \right| + C$

Security?





# Maintaining Cyber Security

- "**Maintaining Cybersecurity**" shall mean any measure or procedure established to prevent, cope with, and mitigate the risk of Cyber Threats from both inside and outside the country which affect national security, economic security, martial security, and public order in the country

# The Balance of CIA Triad

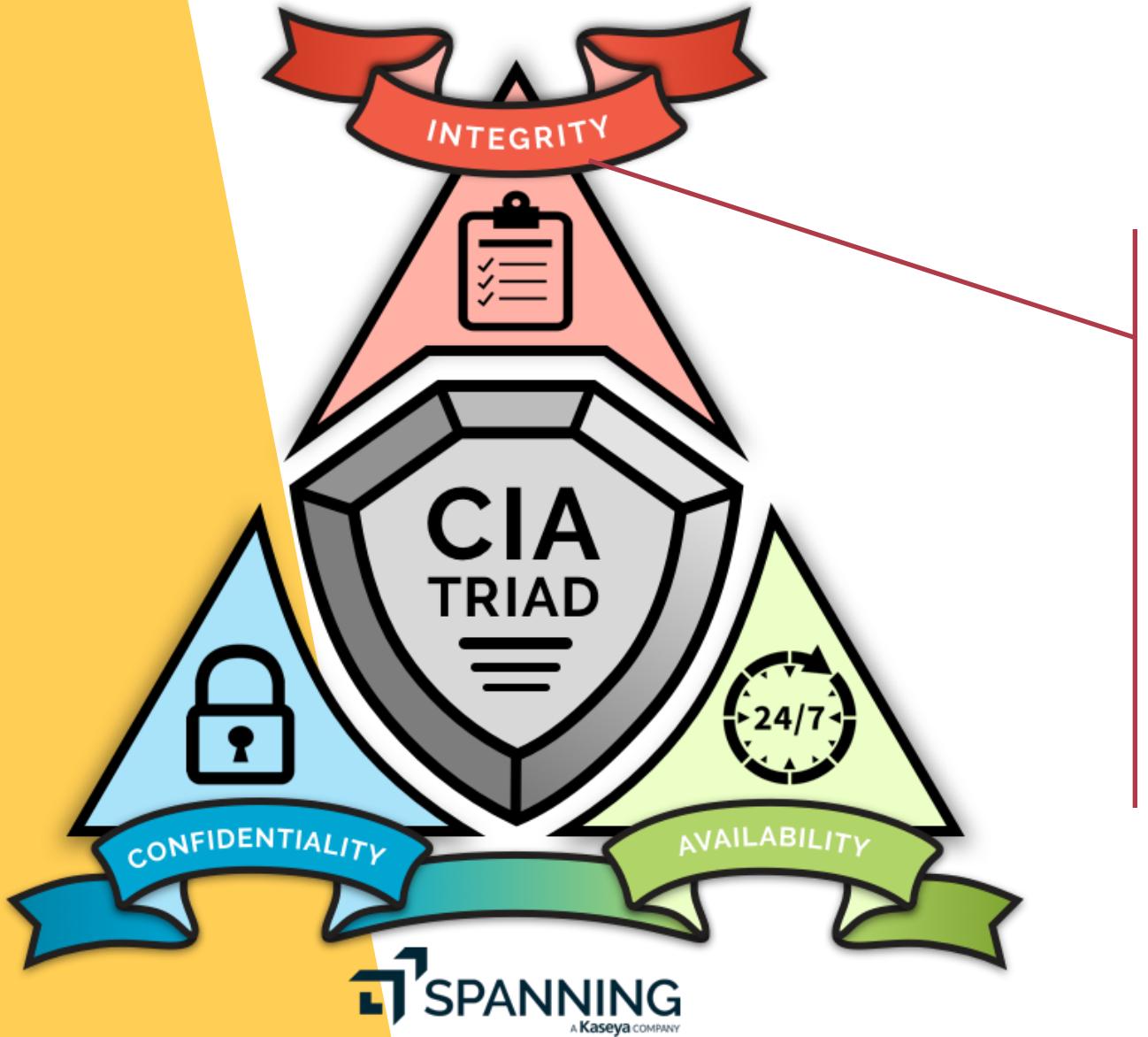


# The Balance of CIA Triad



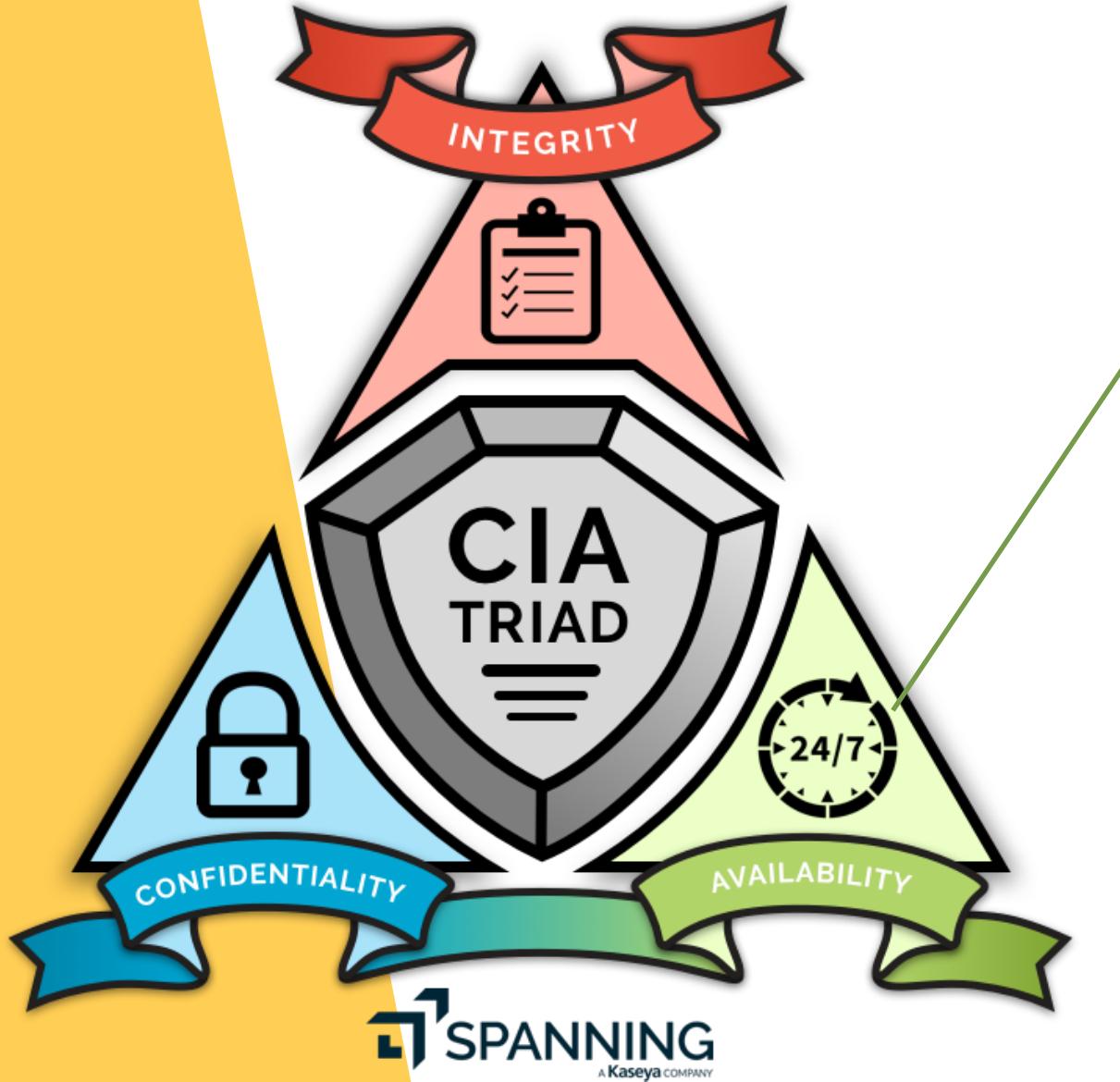
In information security, confidentiality is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes.

# The Balance of CIA Triad



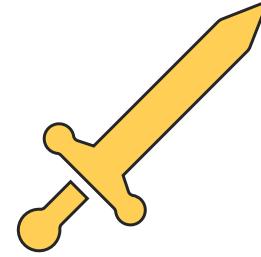
In IT security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner.

# The Balance of CIA Triad

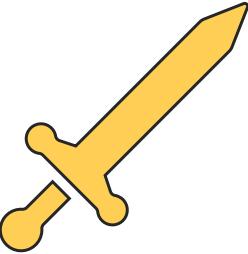


For any information system to serve its purpose, the information must be available when it is needed. This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly.

# Cyber Threats



- "**Cyber Threats**" shall mean any action or unlawful undertaking by using the computer, computer system, or undesirable program with an intention to cause any harm to the computer system, computer data, or other relevant data, and be an imminent threat to damage or affect operation of the computer, computer system, or other relevant data;



# Where do they come from ?

Threat  
Actor

- Criminal
- Competitor
- Hacker
- Government
- Terrorist
- Ethical hacker
- Former employee
- Employee
- Customer
- Contractor
- Whistleblower
- Everybody?

# Clashing between 'Sword' and 'Shield'



The real world might have day and night,  
but cyber world **never sleeps**

# A Few Things to Remember



- We are building fences not walls
- You can lock the door, but it is not good if the window is open
- A secure system is only **as strong as its weakest link**
- And that could be **you...**

# Cyber Threats



What is it?



# Cyber Threat Trends in Thailand



When lifestyle changes to  
the digital era

- Opportunities for accessing to personal information?
- More number of cyber threats?

TOTAL  
POPULATION**+1.0%**

YEAR-ON-YEAR CHANGE

**+80 MILLION**UNIQUE MOBILE  
PHONE USERS**+1.8%**

YEAR-ON-YEAR CHANGE

**+95 MILLION**INTERNET  
USERS**+4.0%**

YEAR-ON-YEAR CHANGE

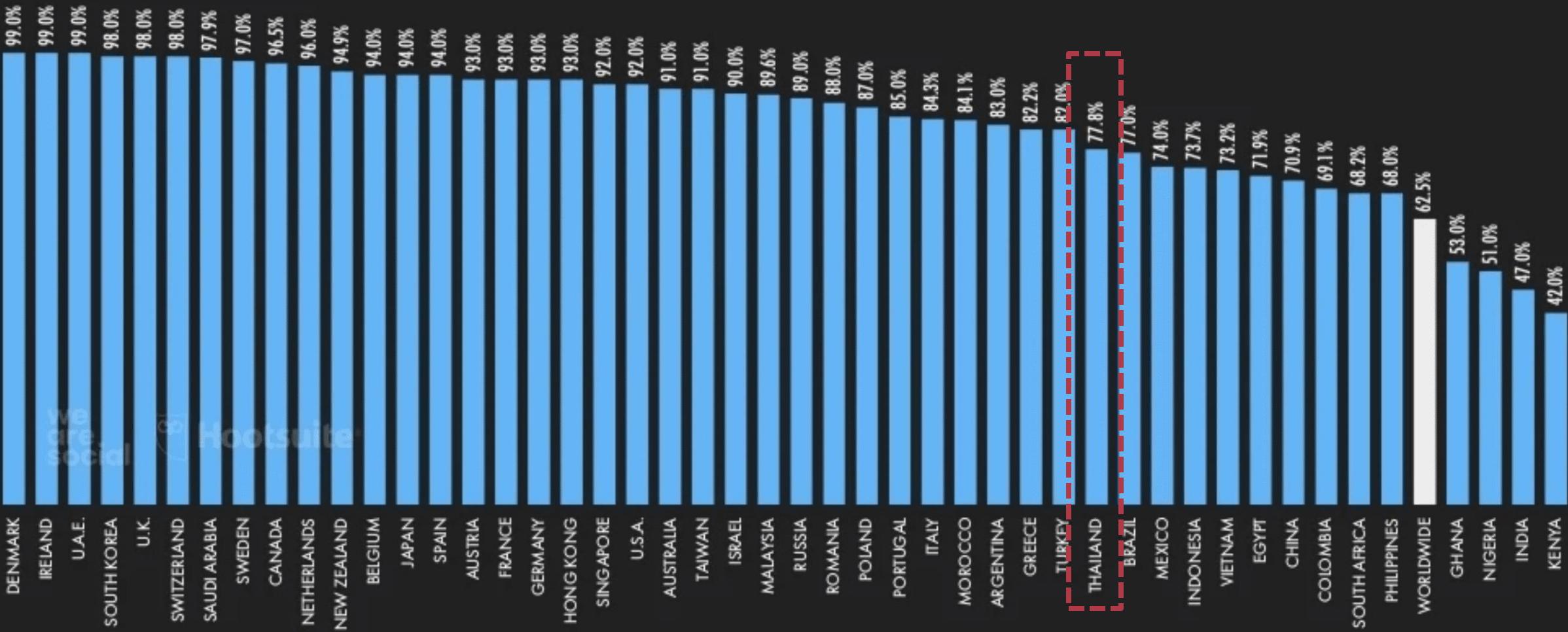
**+192 MILLION**ACTIVE SOCIAL  
MEDIA USERS**+10.1%**

YEAR-ON-YEAR CHANGE

**+424 MILLION**we  
are.  
social

# INTERNET ADOPTION

INTERNET USERS AS A PERCENTAGE OF TOTAL POPULATION

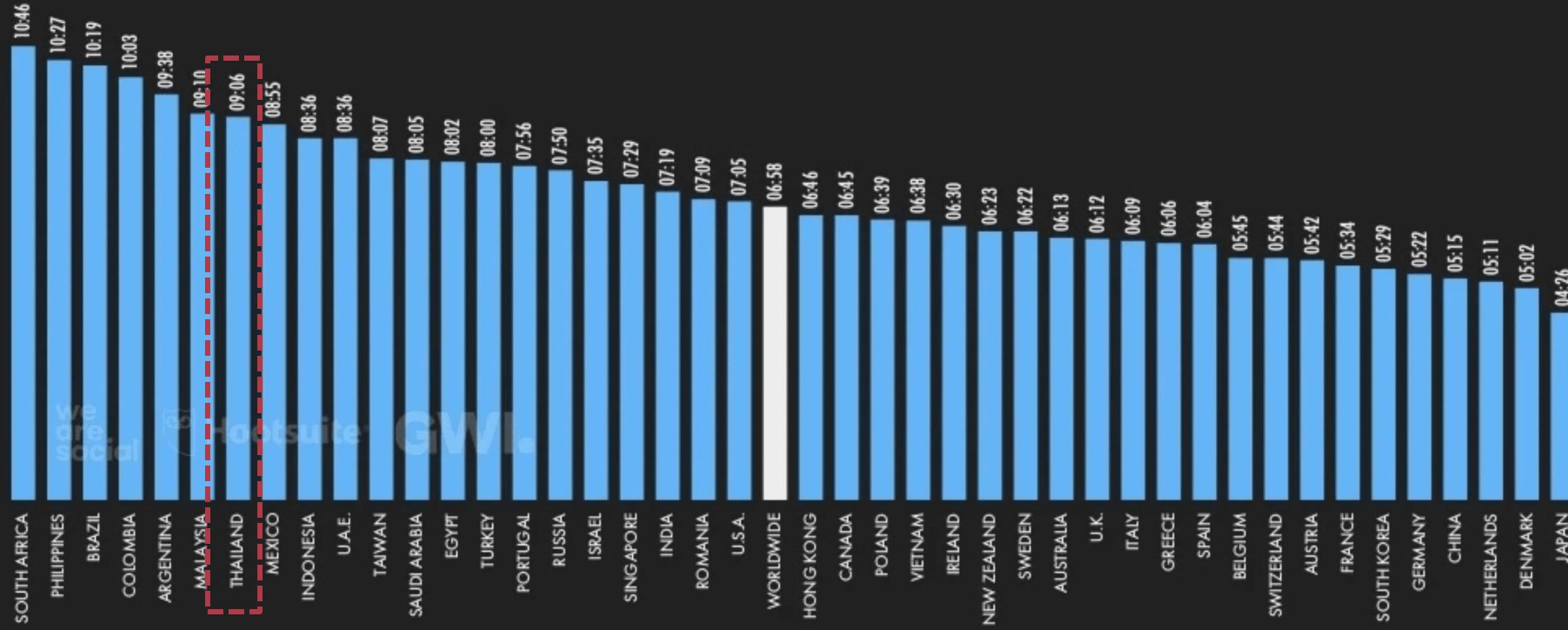


SOURCES: KEPiOS ANALYSIS; ITU; GSMA INTELLIGENCE; EUROSTAT; GWI; CIA WORLD FACTBOOK; ONNIC; APJI; LOCAL GOVERNMENT AUTHORITIES; UNITED NATIONS. NOTE: VALUES HAVE BEEN CAPPED AT 99% OF THE TOTAL POPULATION. COMPARABILITY: SOURCE AND BASE CHANGES.

JAN  
2022

# DAILY TIME SPENT USING THE INTERNET

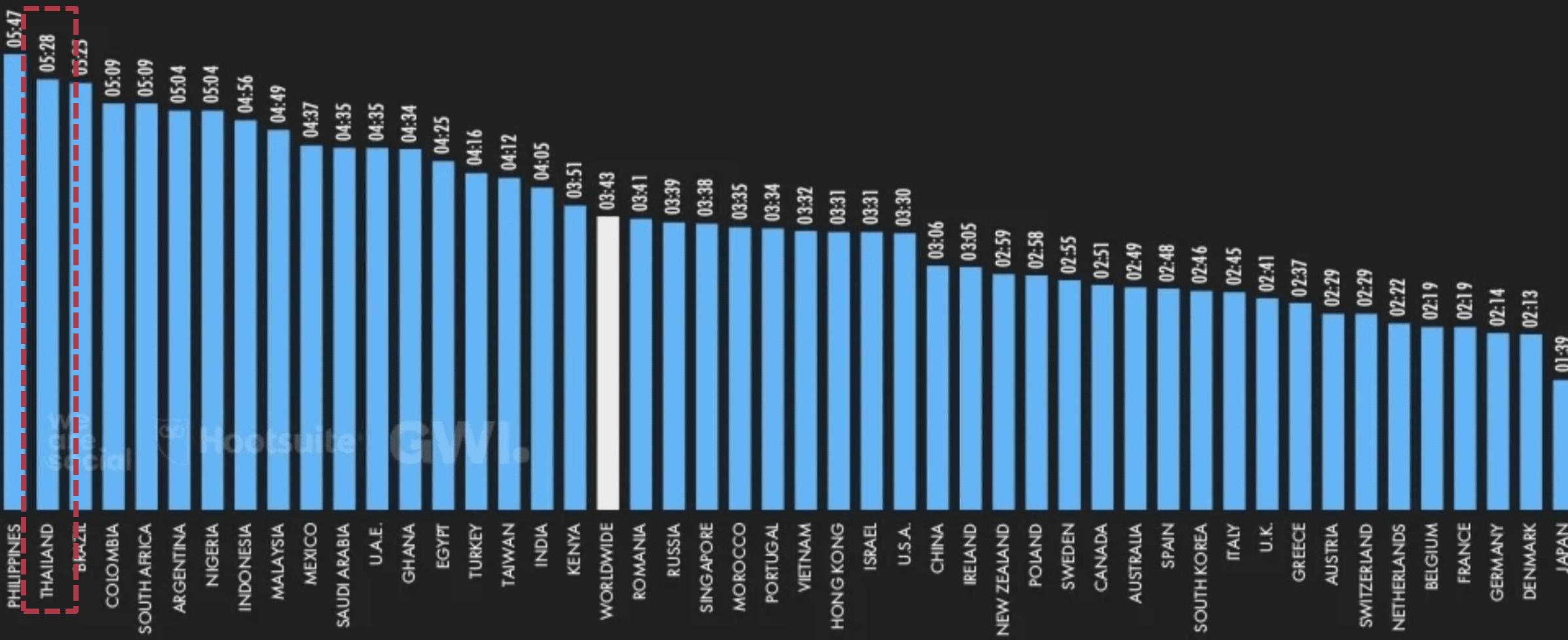
AVERAGE AMOUNT OF TIME (IN HOURS AND MINUTES) THAT INTERNET USERS AGED 16 TO 64 SPEND USING THE INTERNET EACH DAY ON ANY DEVICE



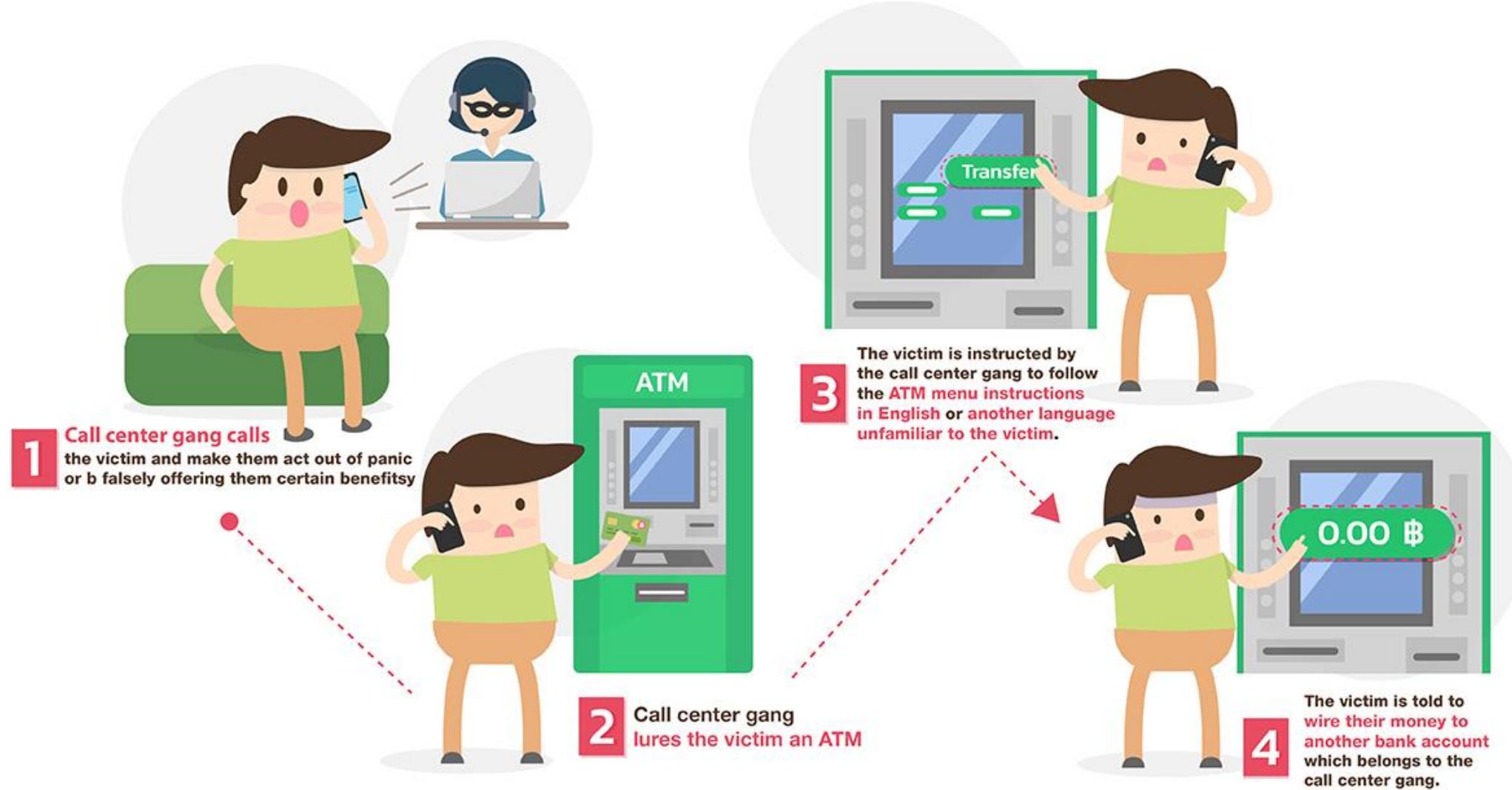
JAN  
2022

# TIME SPENT USING THE INTERNET ON MOBILES

AVERAGE AMOUNT OF TIME PER DAY THAT INTERNET USERS AGED 16 TO 64 SPEND USING THE INTERNET ON MOBILE PHONES



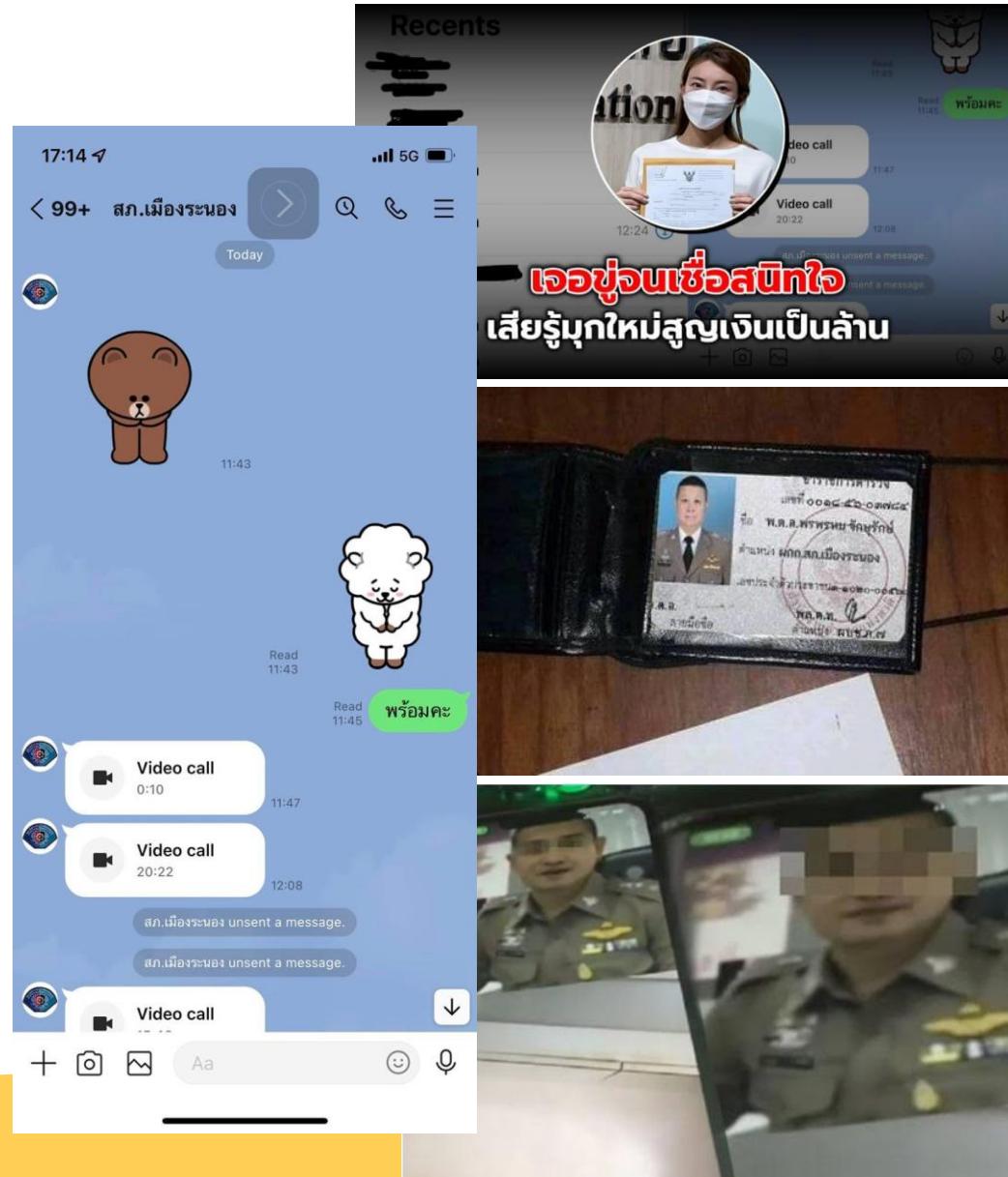
# Traditional Phone Scams



# More internet users, more rooms for hackers

## Call Center Scams in Thailand

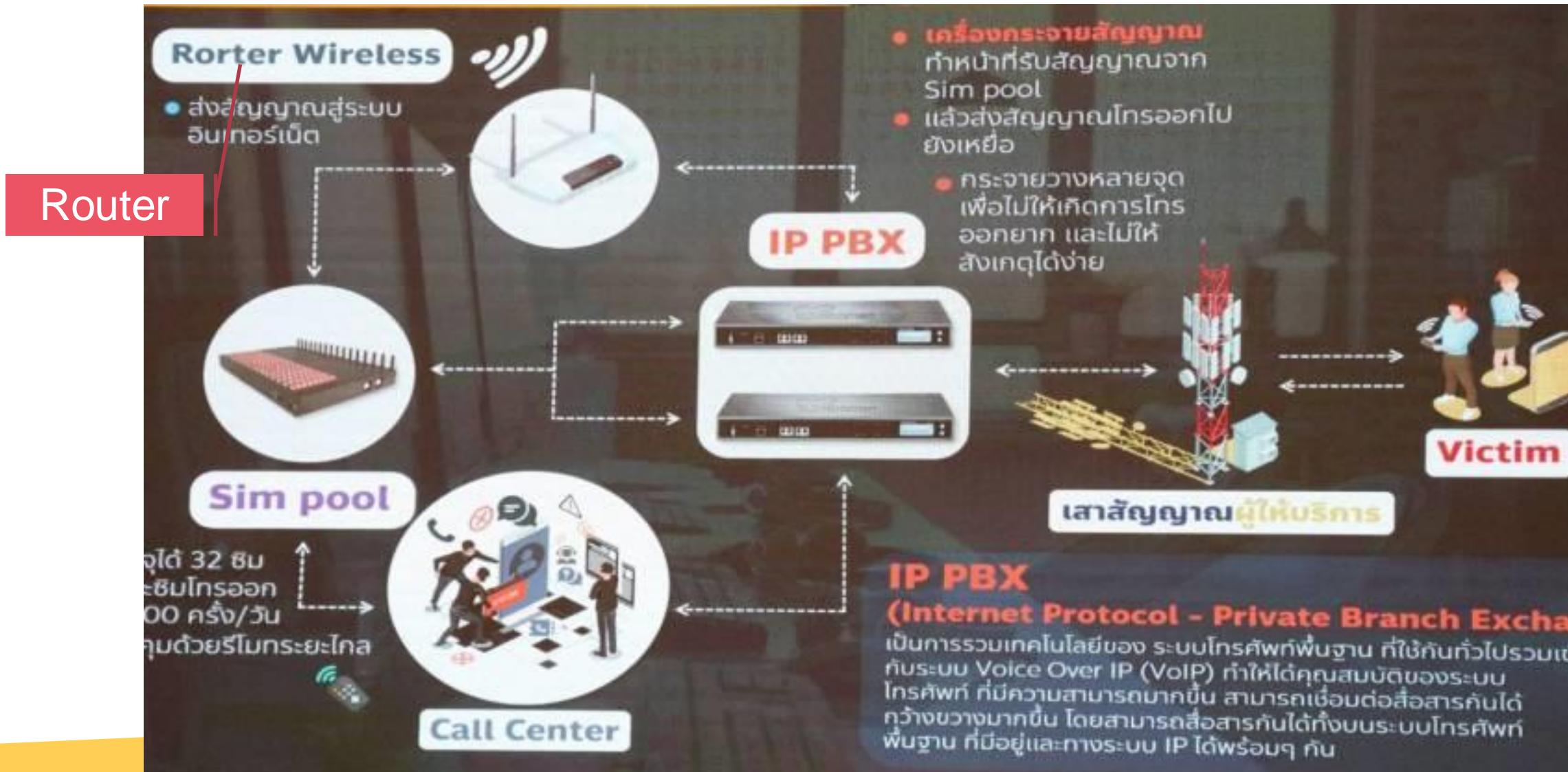
- ▶ Using intimidation, pressure, and scare to make sure that victims will follow every process of scamming
- ▶ Operating from overseas
- ▶ Using other countries or other people phone numbers and luring victims to transfer money into fake bank account



# Call Center Scams in Thailand



# Call Center Scams in Thailand



# Call Center Scams in Thailand

## 10 Chinese 'scammers' nabbed

PUBLISHED : 20 JAN 2022 AT 19:05

WRITER: WASSAYOS NGAMKHAM



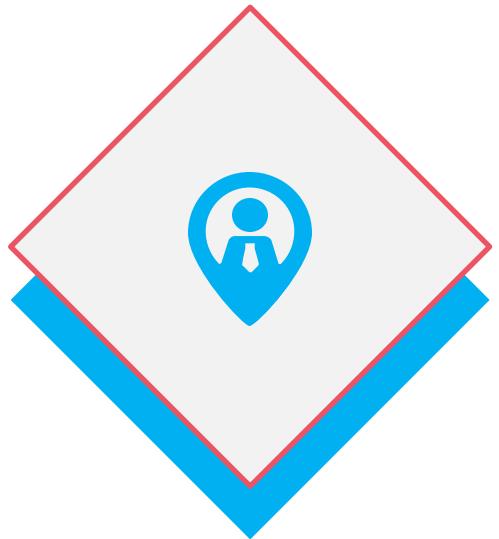
**techhub**  
UPDATE

● กลุ่มวังใหม่ แก๊งคอลเซ็นเตอร์ ขโมยข้อมูล  
หลอกให้โหลดแอปไว้ไมกด้วยดัง

Police arrest 10 Chinese nationals for allegedly operating a call centre scam and online gambling during a raid on two condo units in Bangkok on Thursday. (Photo supplied by Wassayos Ngamkham)



# Types of Cyber Threat



## Cyber Crime

Cybercrime, or computer-oriented crime, is crime that involves a computer and a network.



## Hacktivism

Hacktivism is the use of technology to promote a political agenda or a social change.



## Cyber Terrorism

The politically motivated use of computers and information technology to cause severe disruption or widespread fear in society



## Cyber Warfare

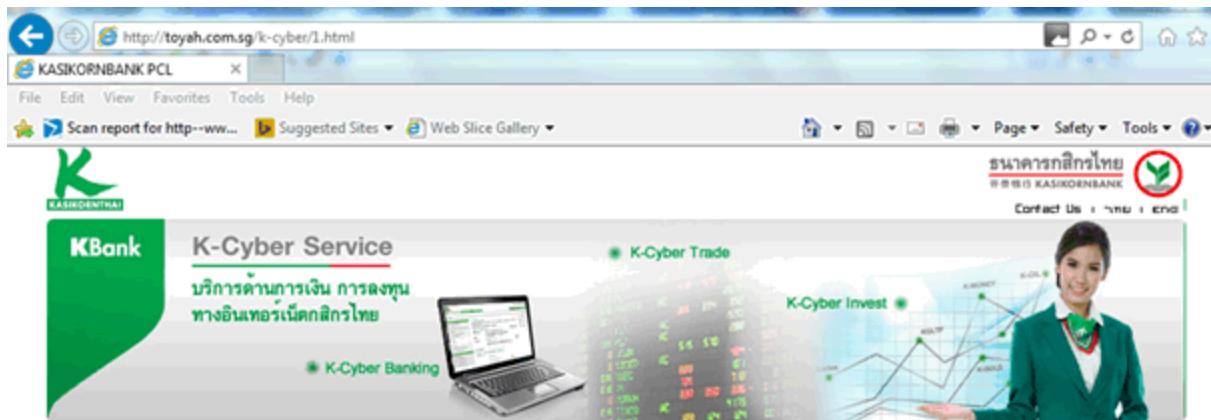
Cyberwarfare is the use or targeting in a battlespace or warfare context of computers, online control systems and networks.

# Cyber Crime



## Phishing

Phishing (pronounced: fishing) is an attack that attempts to steal your money, or your identity, by getting you to reveal personal information



UPDATE YOUR KYC DATA AS REQUESTED TO ENSURE UNINTERRUPTED SERVICE

NOTE: To retain your full account functionalities, it is compulsory to complete this authenticity survey which has been provided for all K-Cyber Customers.

# Phishing



- Phishing sounds like fishing
- And fishing needs a “bait”



# Hacktivism



# Cyber Terrorism



## Maroochy Case Study

### Maroochy Waste Water



#### Lessons learned:

- Suspend all access after terminations
- Investigate anomalous system behavior
- Secure radio and wireless transmissions



Homeland  
Security

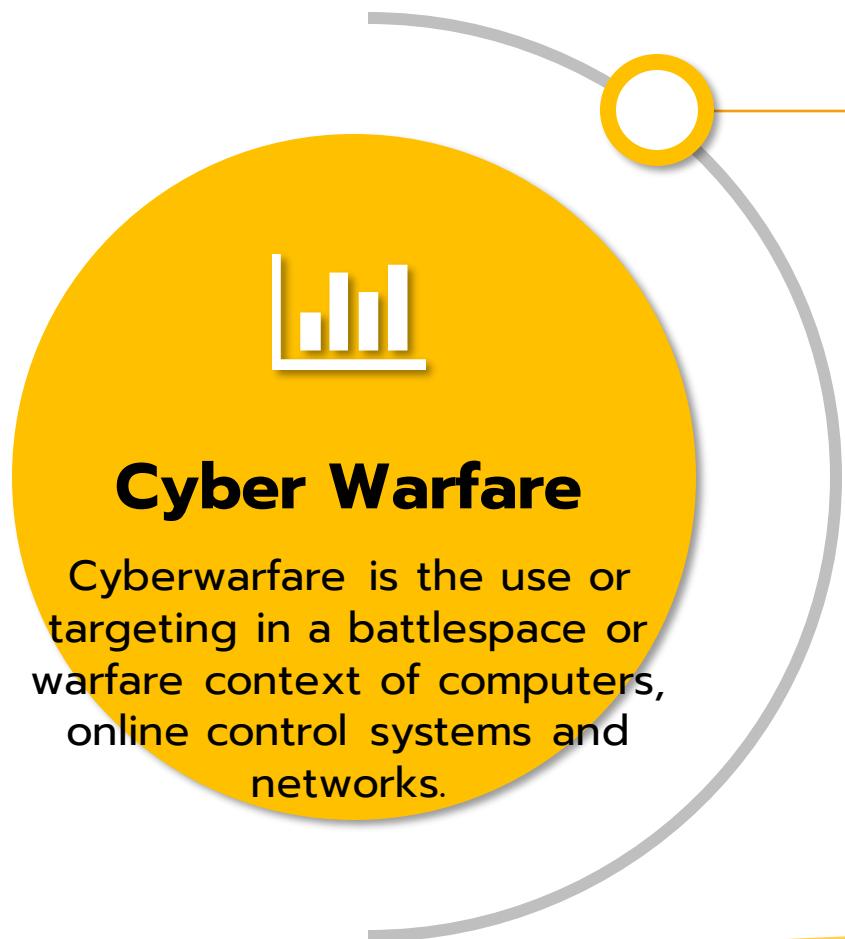
**Event:** More than 750,000 gallons of untreated sewage intentionally released into parks, rivers, and hotel grounds

**Impact:** Loss of marine life, public health jeopardized, \$200,000 in cleanup and monitoring costs

**Specifics:** SCADA system had 300 nodes (142 pumping stations) governing sewage and drinking water

- Used OPC ActiveX controls, DNP3, and ModBus protocols
- Used packet radio communications to RTUs
- Used commercially available radios and stolen SCADA software to make laptop appear as a pumping station
- Caused as many as 46 different incidents over a 3-month period (Feb 9 to April 23)

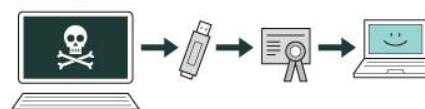
# Cyber Warfare



## STUXNET

### HOW STUXNET WORKED

UPDATE FROM SOURCE



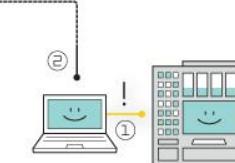
#### 1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.



#### 2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.



#### 3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



#### 4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.



#### 5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.



#### 6. deceive and destroy

Meanwhile, it provides false feed-back to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

# How important of your Citizen ID card?



- Have you ever used your ID card on the internet?
- Have you ever made a copy of your ID card?
  - Back of your ID card?

# How important of your Citizen ID card?



# ลงทะเบียนโครงการราชบัณฑิตย์

กรุณารอข้อมูลของค่านิ่งถูกต้องครบถ้วน เพื่อใช้ในการลงทะเบียน

ค่าเป้าหมาย \*

ชื่อภาษาไทย \*

ชื่อกลาง

นามสกุลภาษาไทย \*

เลขประจำตัวประชาชน \*

\* โปรดกรอก 2 หลักแรกเป็นอักษรภาษาอังกฤษ และ 10 หลักหลังเป็นตัวเลข

รหัสหนังบัตรประจำตัวประชาชน \*



วันเดือนปีเกิดที่ปรากฏในบัตรประชาชน \*

มีวัน/เดือน/ปีเกิด

มีเฉพาะเดือนและปีเกิด

มีเฉพาะปีเกิด

ปี: \*

เดือน: \*

วัน: \*

- Have you ever used your ID card on the internet?
  - Have you ever made a copy of your ID card?
    - Back of your ID card?

# Searching Thai Citizen ID on 'Google'

Google 搜尋結果

搜尋關鍵字: บัตรประชาชน

顯示內容類別: Images

顯示頁數: 1

顯示結果數量: 20

顯示時間範圍: All

顯示地點: Collections, SafeSearch

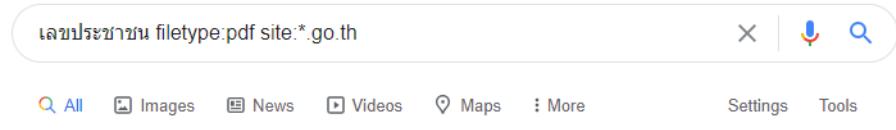
顯示篩選條件: All, Images, News, Videos, Maps, More, Settings, Tools

顯示過濾條件: เลข, ประจำ ตัว, ประจำ จ้า, ชั่ว, ชั่ว, smart card, พก บัตร, ถ่ายรูป, ประจำ หอย, หลัง บัตร, สำเนา บัตร, ทะเบียนบ้าน, เลข บัตร, ตัวเลข, ในปัจจุบัน

顯示結果:

- ความสำคัญของบัตรประจำตัวประชาชน buririamcity.go.th
- ทำบัตรประจำตัว 2021 ใช้เอกสารอะไรบ้าง - ACCE... accesstrade.in.th
- สำเนาบัตรประจำตัว - Jitsupa's Portfolio sites.google.com
- เครื่องกรอกข้อมูลบัตรประจำตัวอัต... rd-comp.com - Out of stock
- หน้าบัตรประจำตัวคนหลุดเดินหายค่าไหน? - Bitdefender... bitdefender.co.th
- ใช้เอกสารอะไรบ้างในการทำบัตร mtp.go.th
- กฎหมายเกี่ยวกับบัตรประจำตัวประชาชน - law of life sites.google.com
- เจอบัตรประจำตัวเดือนสานหนลงครับ... - facebook.com
- เครื่องอ่านบัตรประจำตัว Android... rd-comp.com - In stock
- ไม่พกบัตรประจำตัว : สำเนาบัตรถูกปรับเงินไปหรือ... thamaaya.wordpress.com
- บัตรประจำตัวหอย 2563 ทำใหม่ที่ไหนได้บ้าง และยังด... shopee.co.th
- พอยเด็กบัตรประจำตัวเจ้า... - แมรีน เชียง... pt-br.facebook.com
- ทำบัตรประจำตัวแบบ "New Normal" ก่อนไปร้านค้า... siamrath.co.th
- บัตรประจำตัวและเลขประจำตัวประชาชน - เริ่... coolaun.com
- วันโน้นเจน กลุ่มไม่มีสมาร์ทโฟน ก้าวสู่โลกดิจิทัล news.ch7.com
- ชาวบ้านเรียนรู้ วันโน้นเจน เรียนรู้ กลุ่มไม่มีสมาร์ทโฟน ใจ... news.ch7.com
- ชาวบ้านเรียนรู้ วันโน้นเจน กลุ่มไม่มีสมาร์ทโฟน ใจ... thaiarith.co.th
- ทำบัตรประจำตัวที่สถานีคลีฟาย พ.ร.บ.เทคโนโลยี... atsydney.com
- จากพรมแดน... สังลงทะเบียนคนจน "เลขที่บัตรประจำ... mgonline.com
- ไทยขอสงสัย ความหมายของ 13 ตัวเลข บนบัตรประจำตัว... lifestyle.campus-star.com
- ข้อมูลใดไม่ปรากฏอยู่ในบัตรประจำตัวบัตรบัตร youtube.com
- ข้อมูลใดไม่ปรากฏอยู่ในบัตรประจำตัวบัตรบัตร youtube.com

# Searching Thai Citizen ID on ‘Google’



About 1,400,000 results (0.39 seconds)

- # รหัสสังหนัดและ/o ภาษาของประเทศไทย

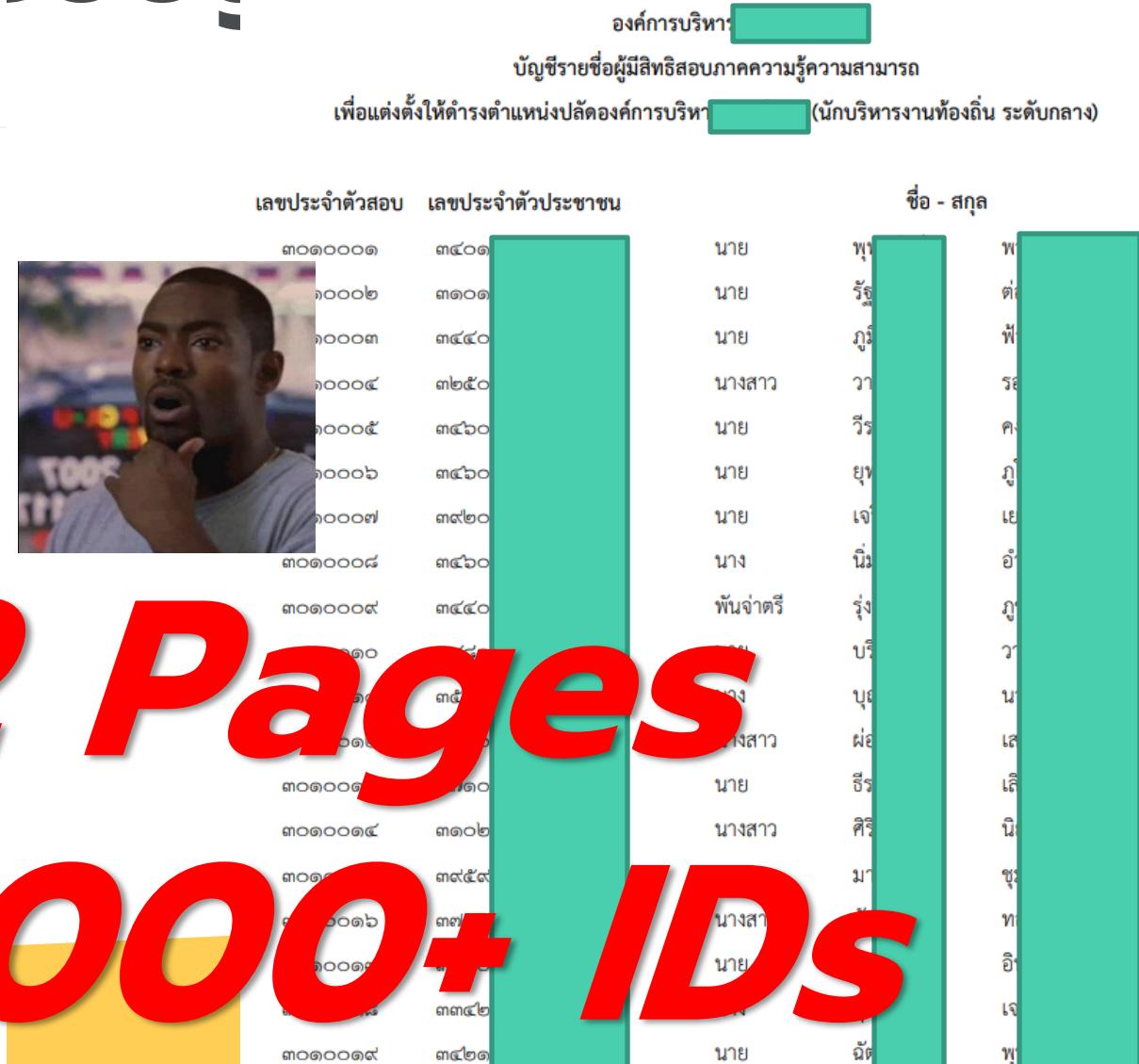
- # ความหมายของเลขประจำตัวประชาชนทั้ง 13 หลัก

- www.dla.go.th > upload > document > type2 PDF

- www.surin3.go.th > data > 953\_รายชื่อผู้เรียก... ▾ PDF หน้า 32  
รหัสโรงเรียนโรงเรียน รหัสโรงเรียนเลขบัตร 13 หลัก ๑ สาระฯ ... เรียนรู้ภาษาไทย วิทยา 32030053 1 3205 78940 00 4 จุฬารัตน์ ราชวิถีสำรอง ๒๔๗ ถนนสุขุมวิท แขวงคลองเตย เขตคลองเตย กรุงเทพมหานคร ๑๐๑๑๐ โทร. ๐๘๑-๖๙๙๕๓๒๒๒



- www.ptt2.go.th › plan › images › data › แก้ไข  
**7.แบบฟอร์มขอแก้ไข**  
แบบฟอร์มนี้ขอแก้ไขเลขประจำตัวประชาชน พลเมืองไทย ซึ่งเป็นผู้เดินทางต่างถิ่น มีค่าปรับประชารัฐที่ต้องชำระ ไม่เกินหกสิบบาทถ้วน แต่ต้องตรวจสอบว่าไม่ใช่กรณีที่ต้องจ่ายค่าปรับประชารัฐด้วยกฎหมาย ดังนี้ ๑.



# How important of your Citizen ID card?



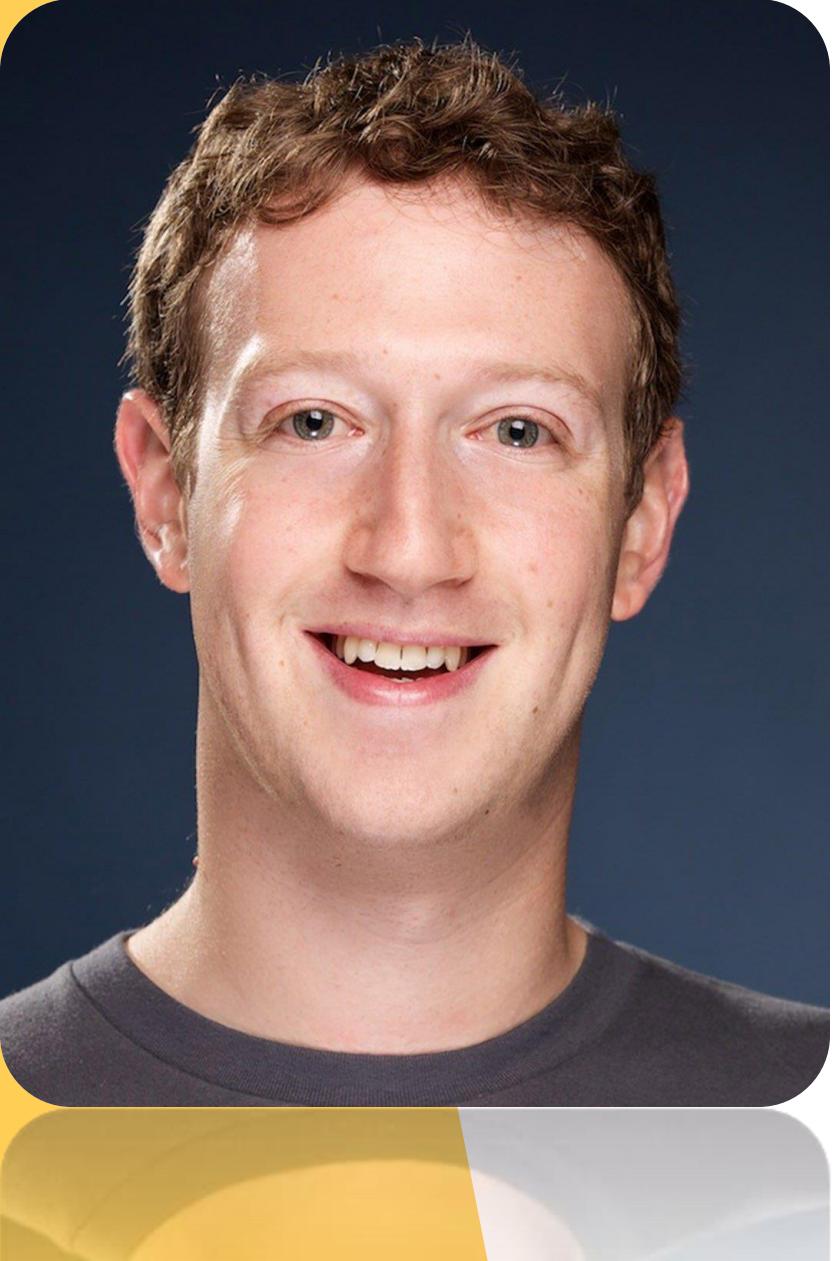
- Examples of Thai Government Agency Website that needs only ID number
  - Checking farmer status <http://farmer.doae.go.th/>
  - Checking your voting rights <https://stat.bora.dopa.go.th/Election/enqelectloc/>

- Dealing with Cyber Threat with Cyber Security Awareness



Behaviours that lead to cyber risks

- Have you ever done this before?



**“Good behaviour will  
keep you safe from  
cyber threats”**

**- MARK ZUCKERBERG, FACEBOOK FOUNDER**

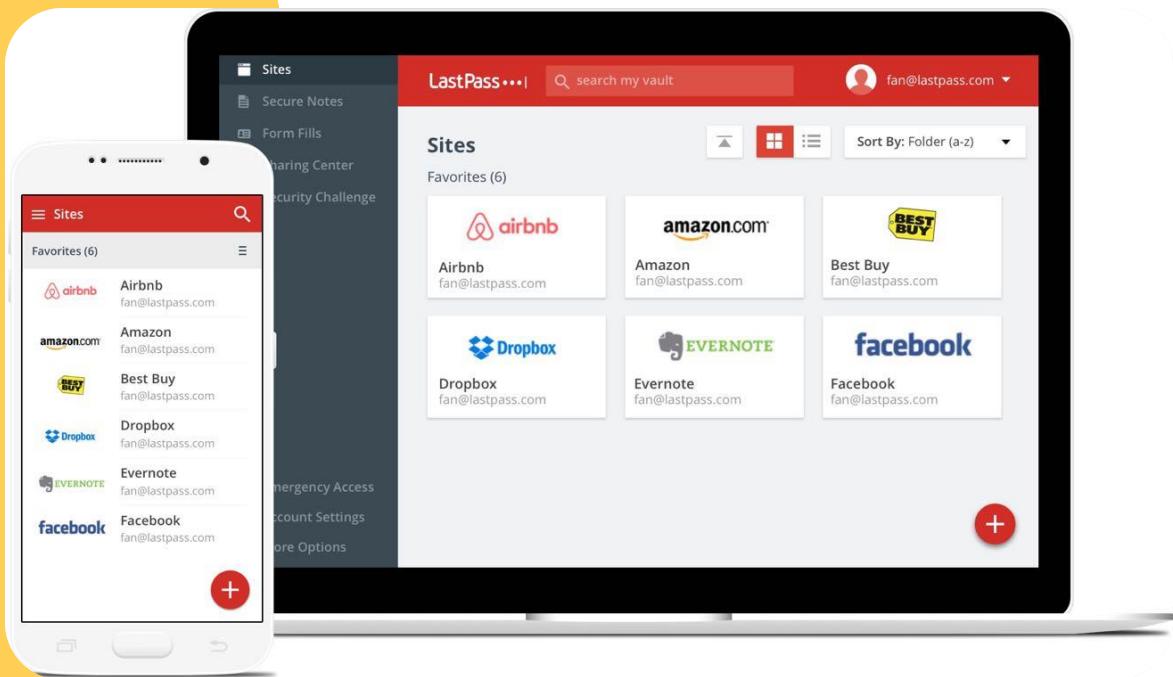
*HE NEVER SAYS THAT BUT I JUST WANT TO USE HIS PHOTO TO MAKE THIS TOPIC MORE INTERESTING AND TRUSTWORTHY*

# 1. Stick passwords on desktop



A password of Hawaii emergency agency was hiding in a public photo, written on a Post-it note

# 1. Stick passwords on desktop



A screenshot of the LastPass desktop application's vault interface. The main pane displays a list of items categorized by type: Logins (45), Secure Notes (11), Credit Cards (5), Identities (2), Passwords (8), and Documents (2). A specific item, 'CBC.ca', is selected and expanded, showing its details: account (CBC.ca), vault (Wendy Appleseed), personal information (username: wendy.c.appleseed@gmail.com, password: redacted, website: http://www.cbc.ca/), and audit details (last modified: 10/24/16 3:05 PM, created: 10/24/16 3:04 PM). A 'Show web form details' button is also visible.

**LastPass and 1Password**  
**freemium password manager that stores encrypted passwords online**

## **2. Let others know your password**



**Your password is your responsibility  
When a crime commits with your account,  
it is your guilty**

# 3. Using commonly passwords



## Worst passwords of 2022

# 3. Using commonly passwords



## Worst passwords of 2022

# Creating a good password

- ▶ Do not let anyone know your password
- ▶ Change your password every 6 months
- ▶ Your password should have at least 12 characters
- ▶ And it should be complex...
  - ▶ Capital Letter and Lowercase Letter (A-Z, a-z)
  - ▶ Number (0-9)
  - ▶ Special Character (!@#\$%^&\*()\_+)

# Creating a good password

- ▶ Examples of password which is “Difficult but Easy”
  - ▶ Type another words in English
    - ▶ อันบอกไม่ได้หรอก -> Cyo[vdw,jwfhsivd
  - ▶ Create your own pattern
    - ▶ โอ้ว!เพสบຸກ -> Fvh;!gal[6Ud
  - ▶ A short phrase from your favourite songs
    - ▶ อันจะพาเรอลอย -> Cyo0trkgTv]vp

# Creating a good password

HOW SECURE IS MY PASSWORD?

.....\*

SHOW SETTINGS

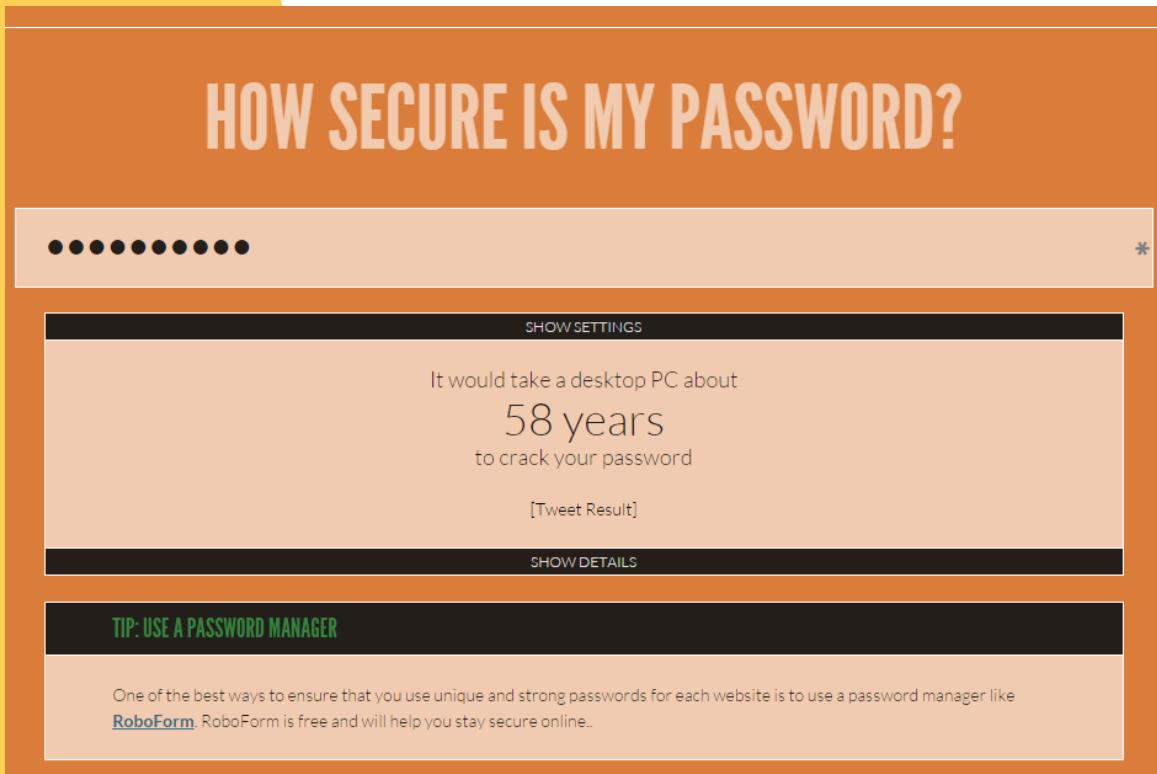
It would take a desktop PC about  
58 years  
to crack your password

[Tweet Result]

SHOW DETAILS

**TIP: USE A PASSWORD MANAGER**

One of the best ways to ensure that you use unique and strong passwords for each website is to use a password manager like [RoboForm](#). RoboForm is free and will help you stay secure online.



- ▶ How secure is your password?
- ▶ <https://howsecureismypassword.net/>

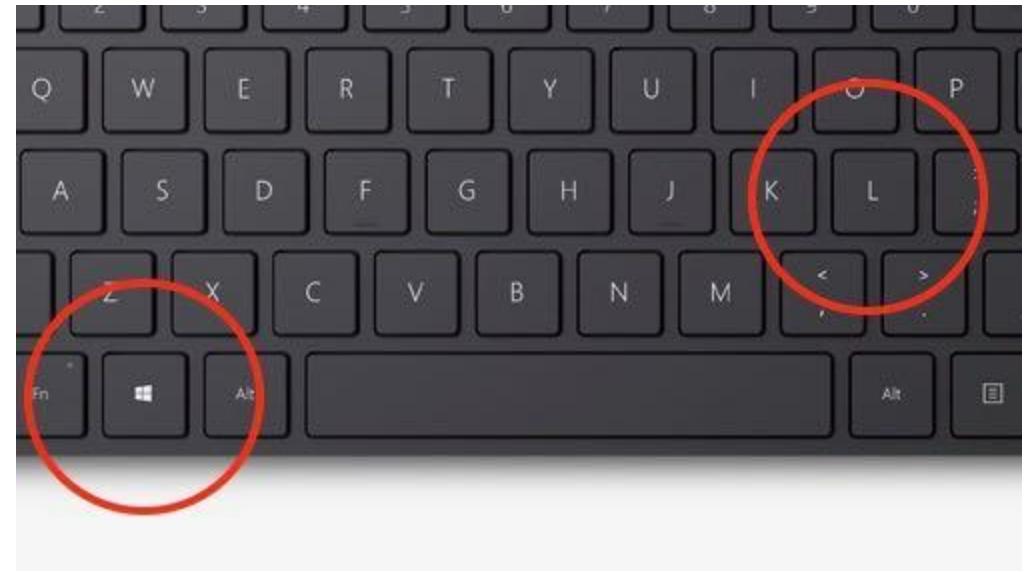
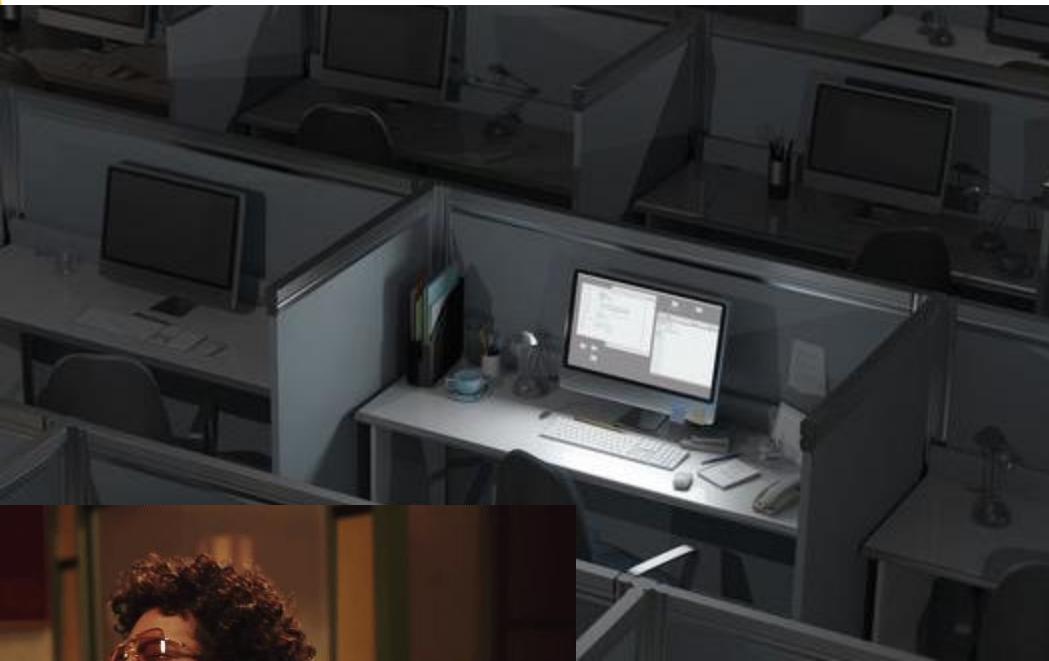


# 4. Never run a virus scan



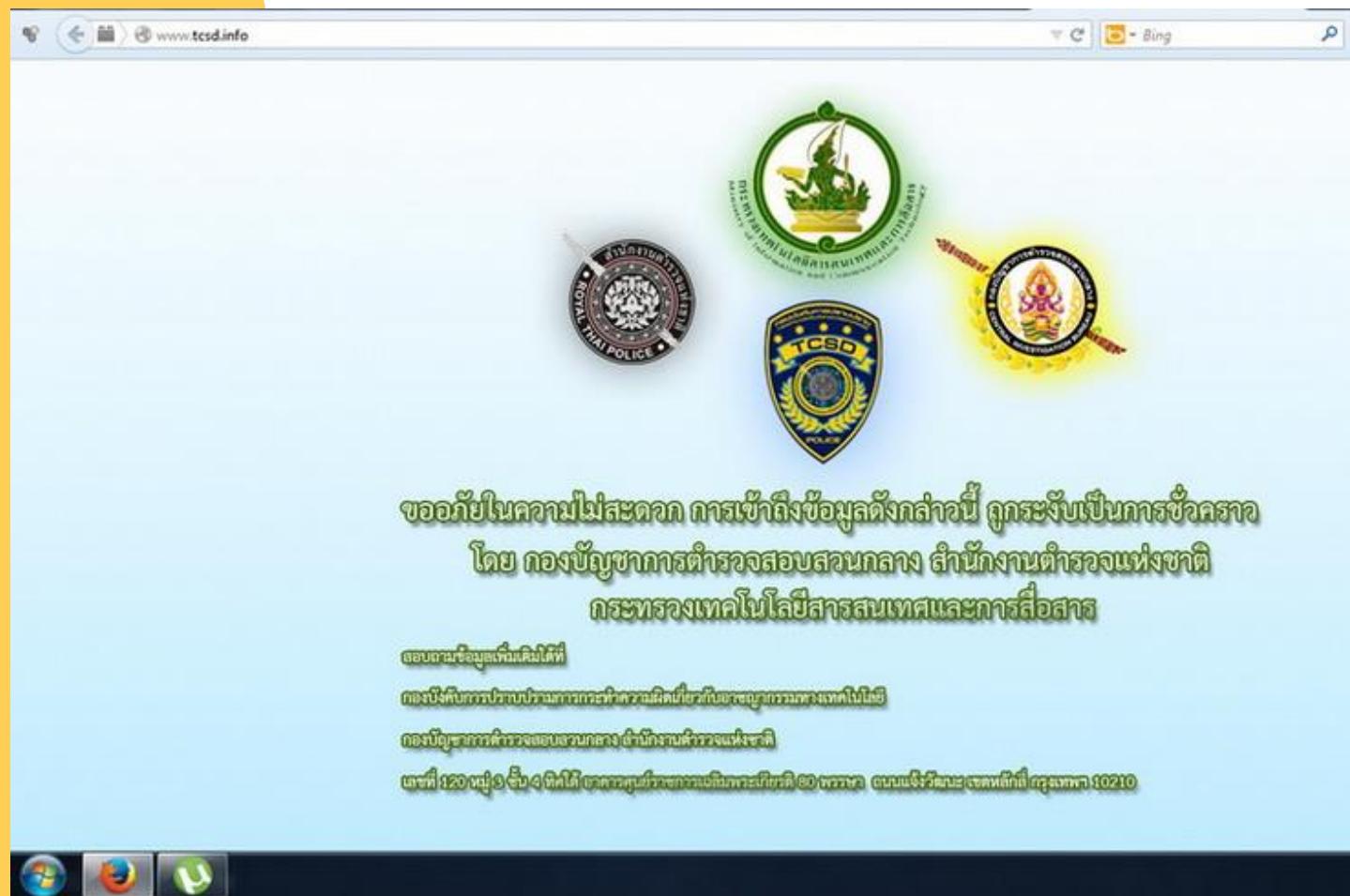
**“Scan before using it”**

# 5. Leave the door screen open



**"Windows + L"**

# 6. Accessing to risky websites



เนื้อหาดังกล่าว เป็นข้อมูลที่มีความผิด

ตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550  
และที่แก้ไขเพิ่มเติม และ/หรือข้อบัญญัติกระทำความผิดตาม  
ว.ร.บ.การพนัน พ.ศ.2478 และที่แก้ไขเพิ่มเติม

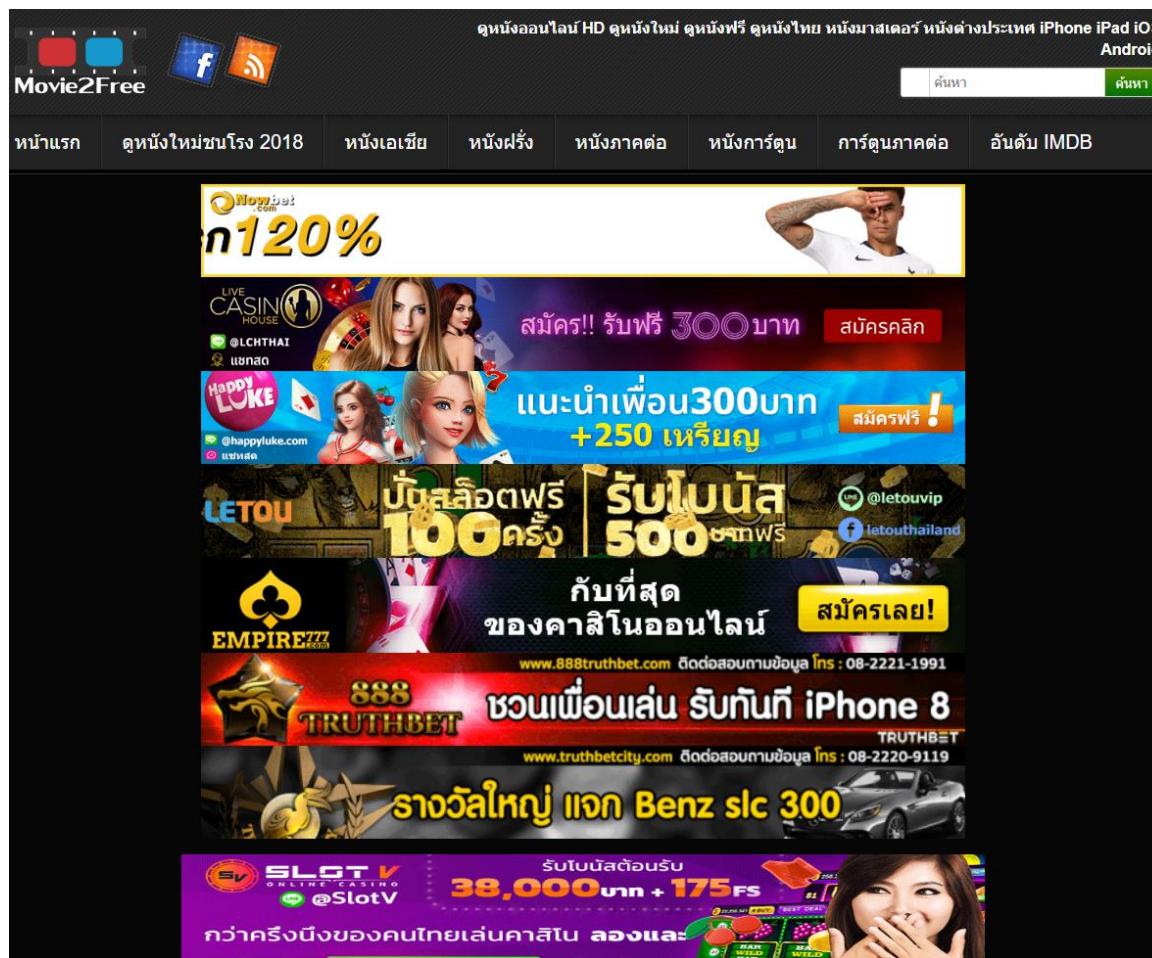
This content has been suspended

due to its illegal acts in accordance with  
the Computer-related Crime Act 2007 (B.E. 2550) and additional amendments  
and/or the Gambling Act 1935 (B.E. 2478) and additional amendments



กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม  
MINISTRY OF DIGITAL ECONOMY AND SOCIETY

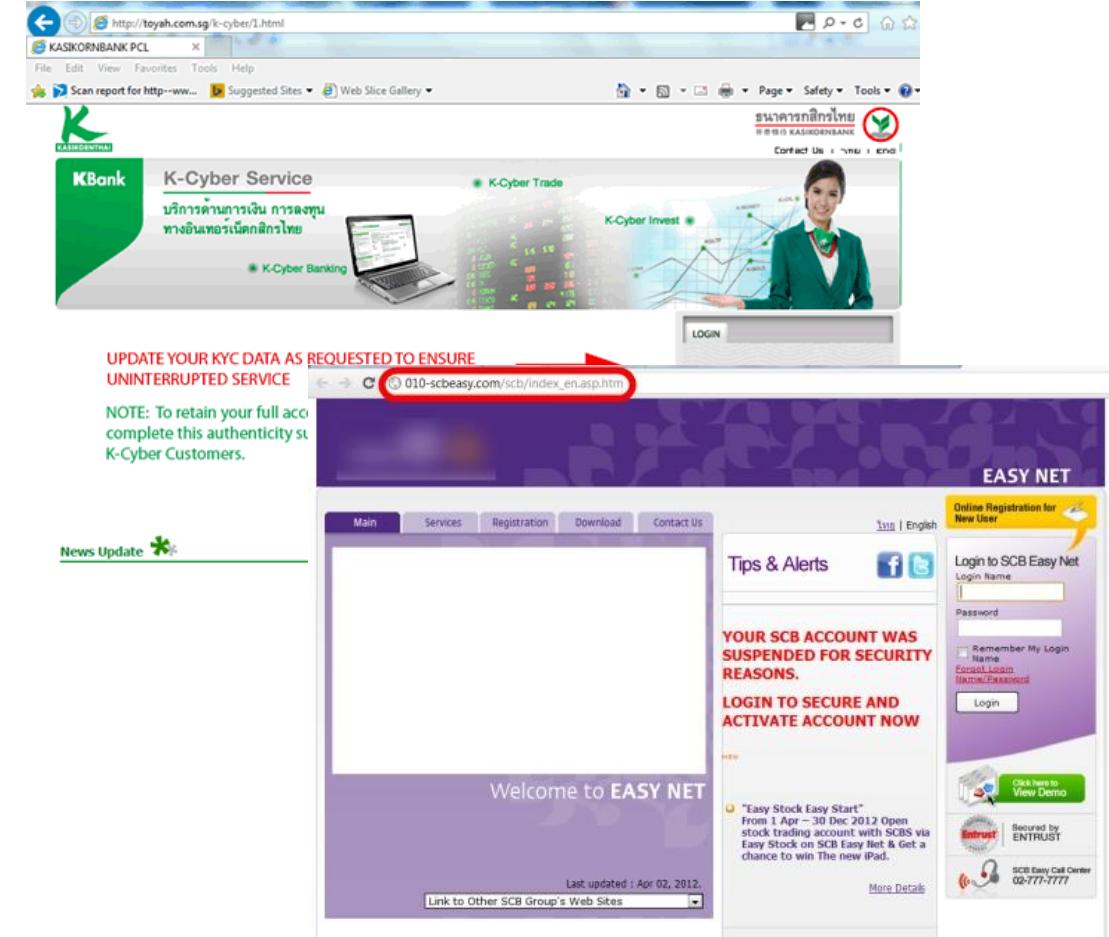
# 6. Accessing to risky websites



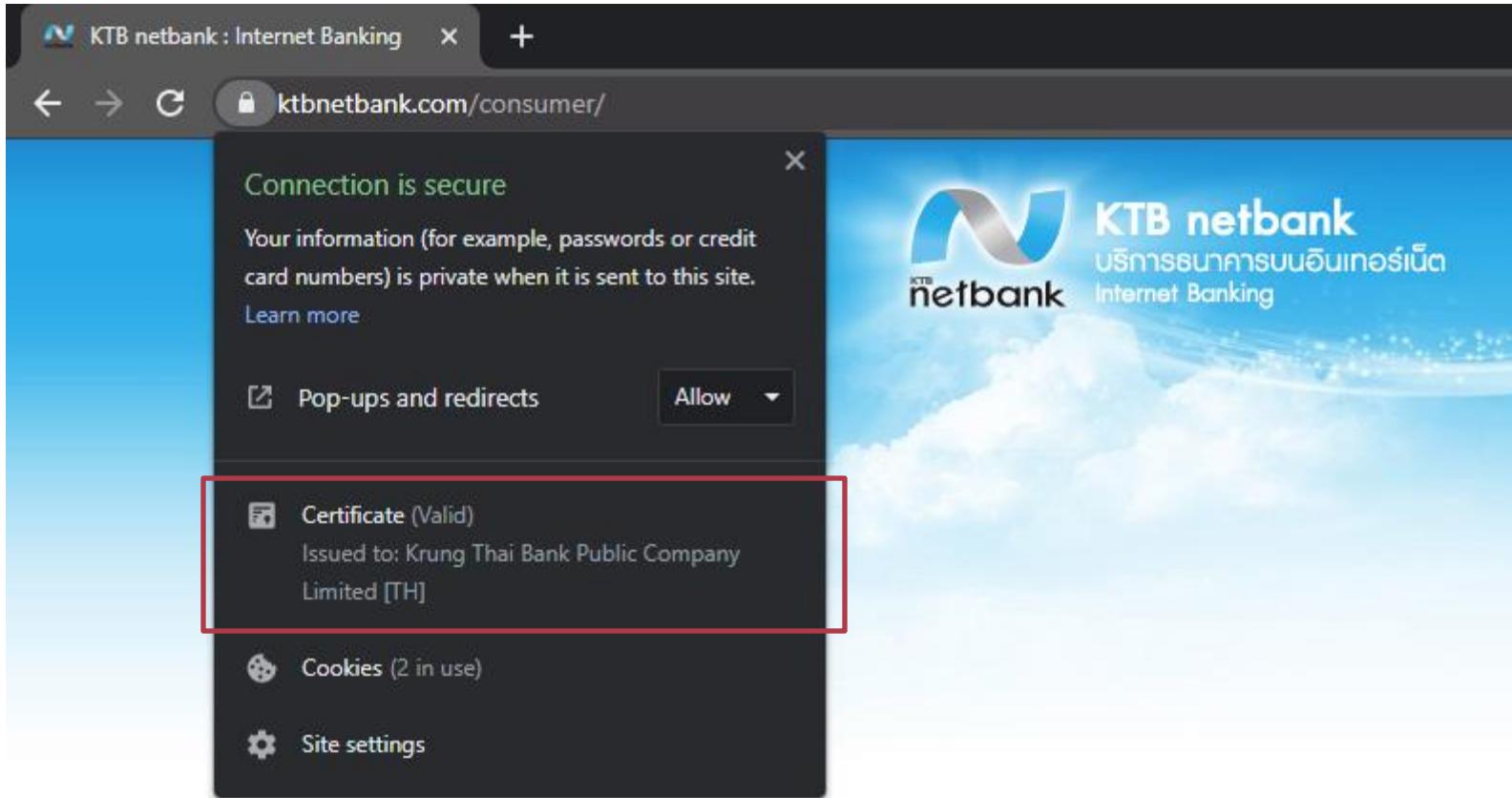
# 6. Accessing to risky websites



# 6. Accessing to risky websites



# Make sure you are using a real website



**Always check website's certificate first  
Issued to: <Web Owner>**

# 7. Using pirated software



**Using pirated software = crime**

# What do we NEED?



- We need to carry out the research to come up with systematic countermeasure, with security frameworks and infrastructures able to react quickly to new attacks. We need to identify and develop the cyber security professionals to go out there on the network and patrol it, to be the good guys in the cyberspace.

**EDUCATION is an EMERGENCY**

“You were the Chosen One! You were supposed to destroy the ~~Sith~~ cyber crime, not join them. You were supposed to bring balance to the force, not leave it in darkness.” Obi-Wan Kenobi

- I am Obi-Wan and now you are my padawan, Obi-two.....





# Q&A

