



ກະຊວງ ເຕັກໂນໂລຊີ ແລະ ການສື່ສານ
Ministry of Technology and Communications



ກົມຄວາມປອດໄພໄຊເບີ
ບົດສະເໜີ
ຄວາມປອດໄພໃນການໃຊ້ສື່ສັງຄົມອອນລາຍ



ພາລະບົດບາດ

ກົມຄວາມປອດໄພໄຊເບີ ຂຽນຫຍໍ້ວ່າ “ກຄຊ” ຂຽນເປັນພາສາ ສາກົນວ່າ “Department of Cyber Security” ຂຽນຫຍໍ້ວ່າ “DCS” ແມ່ນກົມໜຶ່ງ ທີ່ສັງກັດໃນໂຄງປະກອບການຈັດຕັ້ງຂອງ ກະຊວງ ເຕັກໂນໂລຊີ ແລະ ການສື່ສານ, ມີພາລະບົດບາດເປັນເສນາທິການໃຫ້ແກ່ ຄະນະນຳກະຊວງ ໃນວຽກງານ ການຄຸ້ມຄອງຄວາມປອດໄພທາງໄຊເບີ ໃນຂອບເຂດທົ່ວປະເທດ.



ໄດ້ຮັບຮອງການນຳໃຊ້ຊື່ CERT ຢ່າງເປັນທາງການຈາກ ມະຫາວິທະຍາໄລ ຄາເມລອນ ປະເທດ ສາທະລັດອາເມລິກາ ໃນ ເດືອນ ມິຖຸນາ 2016

ໂຄງຮ່າງການຈັດຕັ້ງຂອງກົມຄວາມປອດໄພໄຊເບີ

ກົມຄວາມປອດໄພໄຊເບີ

ພະແນກ ສັງລວມ
(General Affairs
Division)

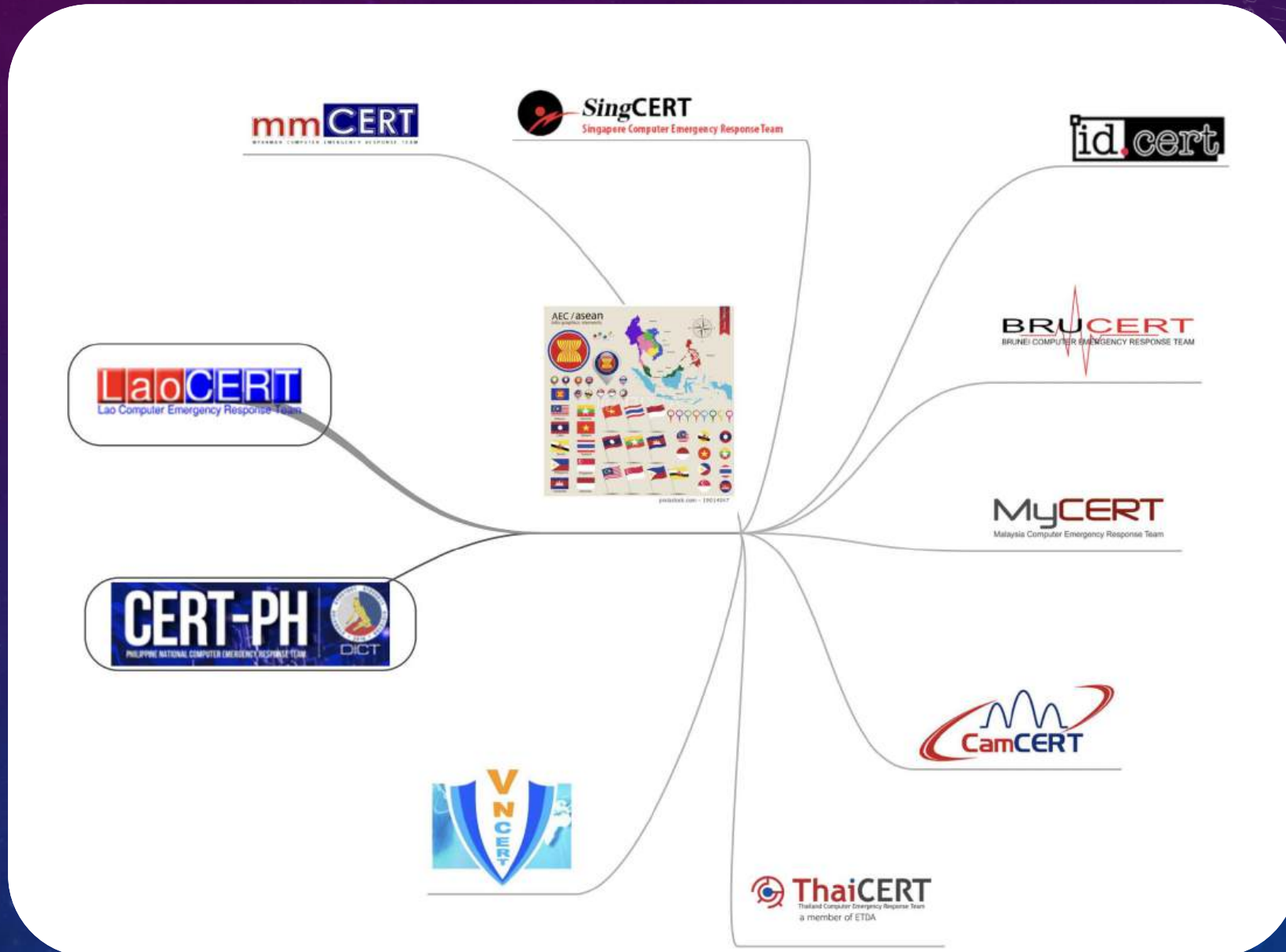
ພະແນກ ວິໄຈຂໍ້ມູນ
ຂ່າວສານ ຜ່ານອິນເຕີເນັດ
(Content Analysis
Division)

ພະແນກ ຄົ້ນຄ້ວາ ແລະ ພັດທະນາ
(Research and Development
Division)

ພະແນກ ຮ່ວມມືຄວາມປອດໄພໄຊເບີ
(Cybersecurity Cooperation
Division)

ພະແນກ ຕອບໂຕ້ເຫດສຸກ
ເສີນທາງຄອມພິວເຕີ
(LaoCERT Division)

ໂຄງຮ່າງການຈັດຕັ້ງຂອງກົມຄວາມປອດໄພໄຊເບີ



Google

facebook

amazon

SURFACE WEB
PUBLIC

DEEP WEB
PRIVATE

DARK WEB
ANONYMOUS

Competitor Information
Legal documents
Medical Records

Academic Databases
Skipped over websites
Conspiracy theories

Special Browser (TOR)
Killers for hire
State Actors
Hidden Websites
Guns. Explosives

Drug Trafficking
Hacking Services
Credit Cards
Illegal Activities
General Market Place

RED WEB
ANONYMOUS GROUPS

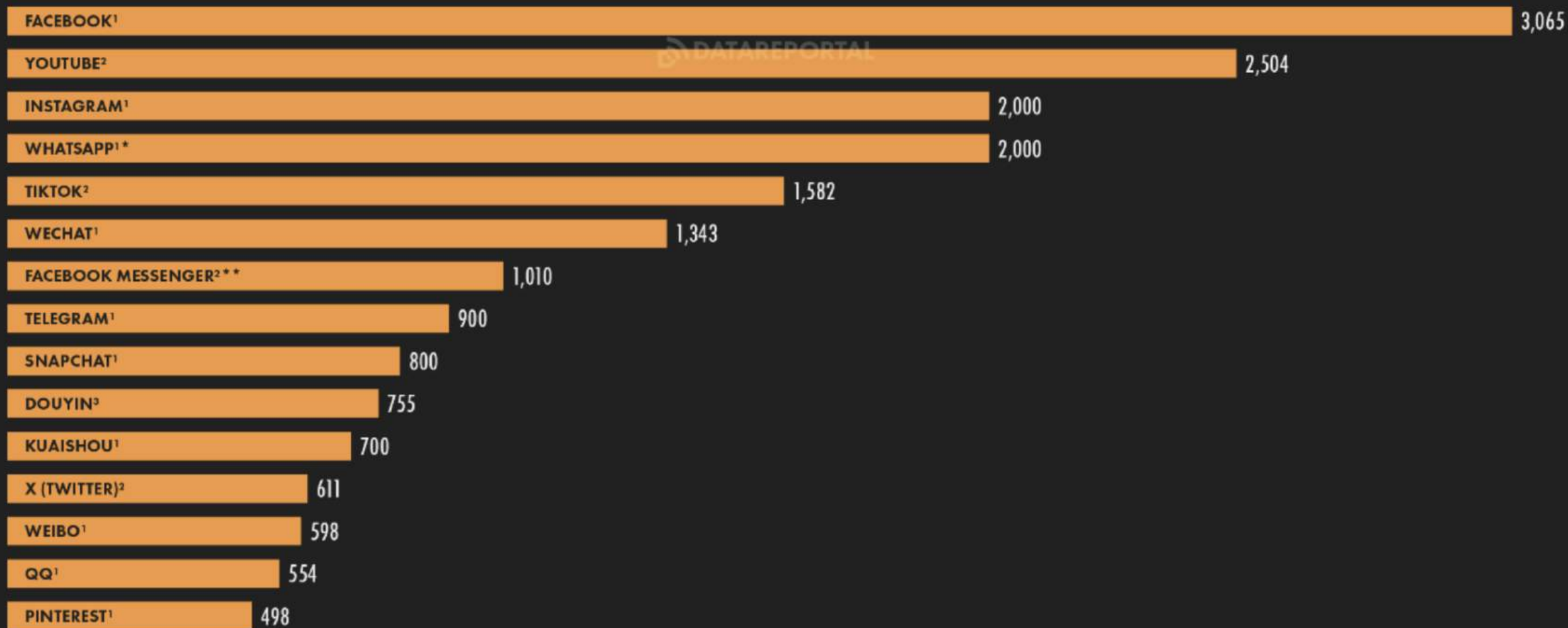
APR
2024

THE WORLD'S MOST USED SOCIAL PLATFORMS

RANKING OF SOCIAL MEDIA PLATFORMS BY GLOBAL ACTIVE USER FIGURES (IN MILLIONS) (NOTE: USERS MAY NOT REPRESENT UNIQUE INDIVIDUALS)

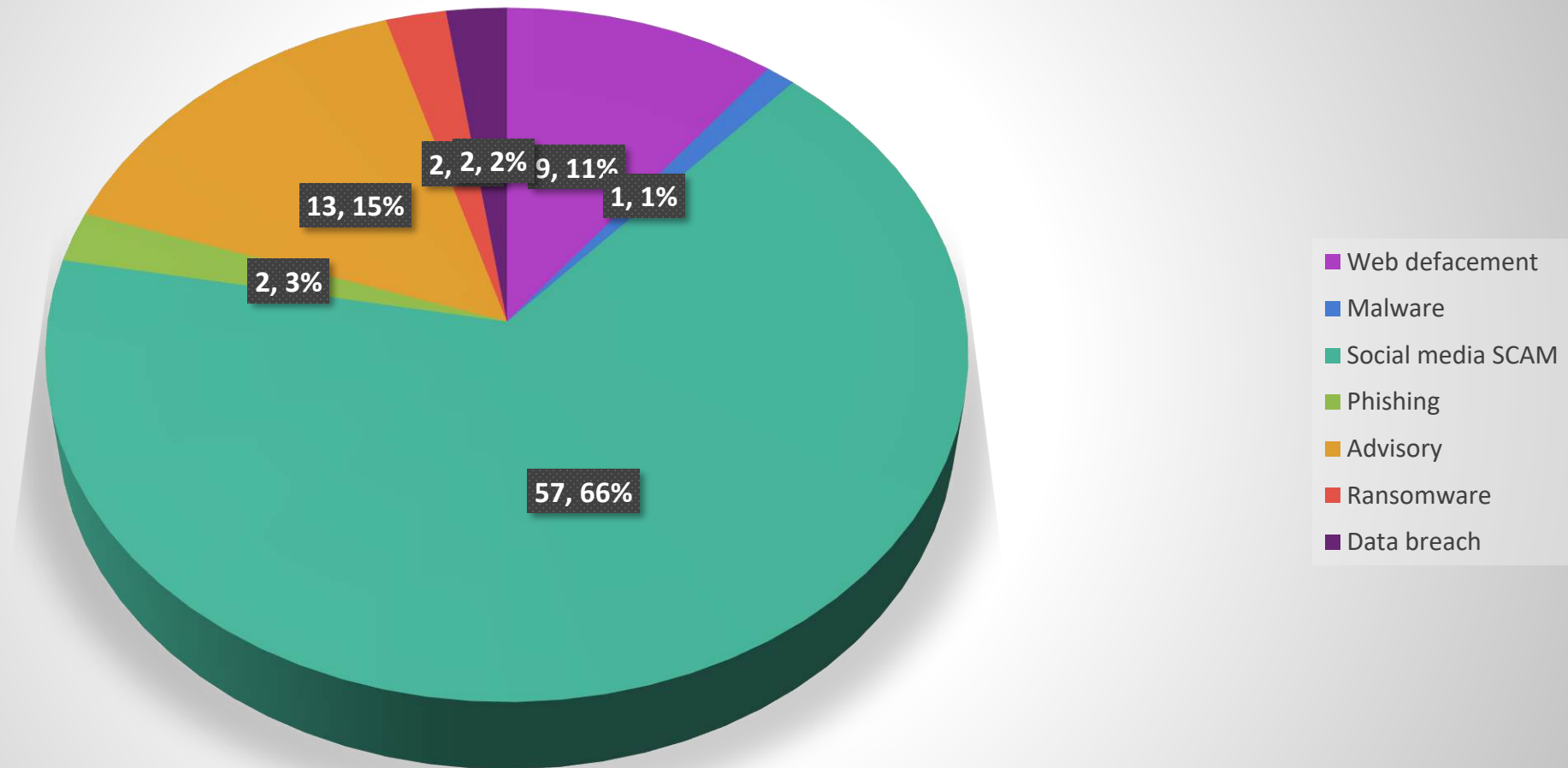


GLOBAL OVERVIEW



ສະຖິຕິການຮັບແຈ້ງເຫດໄພຄຸກຄາມທາງໄຊເບີ

Incident report to LaoCERT Feb-Sep 2023



ສະຖິຕິການນຳໃຊ້ສື່ສັງຄົມອອນລາຍເພສບຸກຄົນ ສປປ ລາວ ປີ 2024

ຈຳນວນບັນຊີຜູ້ໃຊ້

ສະເລ່ຍໃສ່ປະຊາກອນ

ສະເລ່ຍໃສ່ປະຊາກອນ
ເກນອາຍຸ 18+

ເພດຍິງ

ເພດຊາຍ



3.75

MILLION

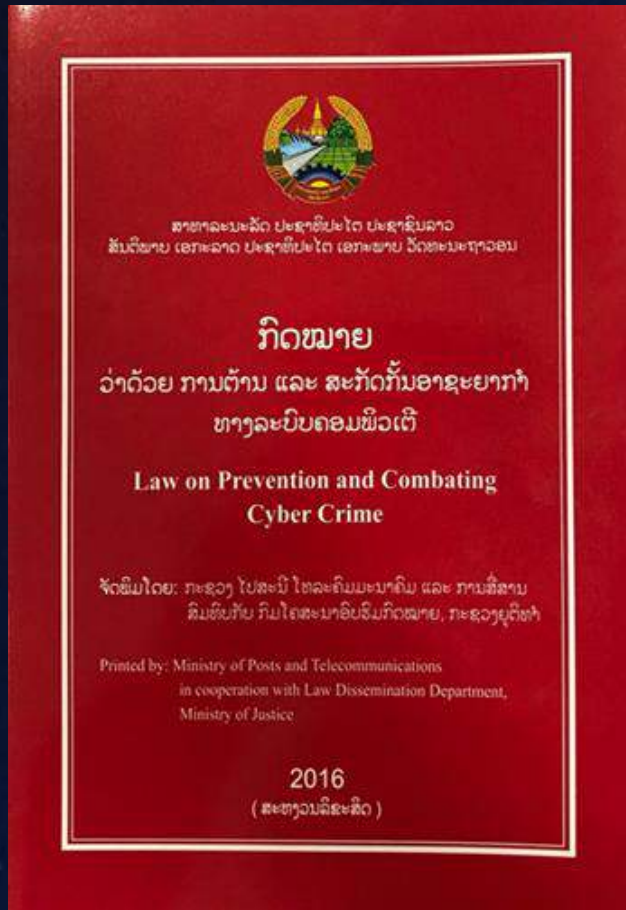
48.8%

75.1%

46.7%

53.3%

ນິຕິກຳ

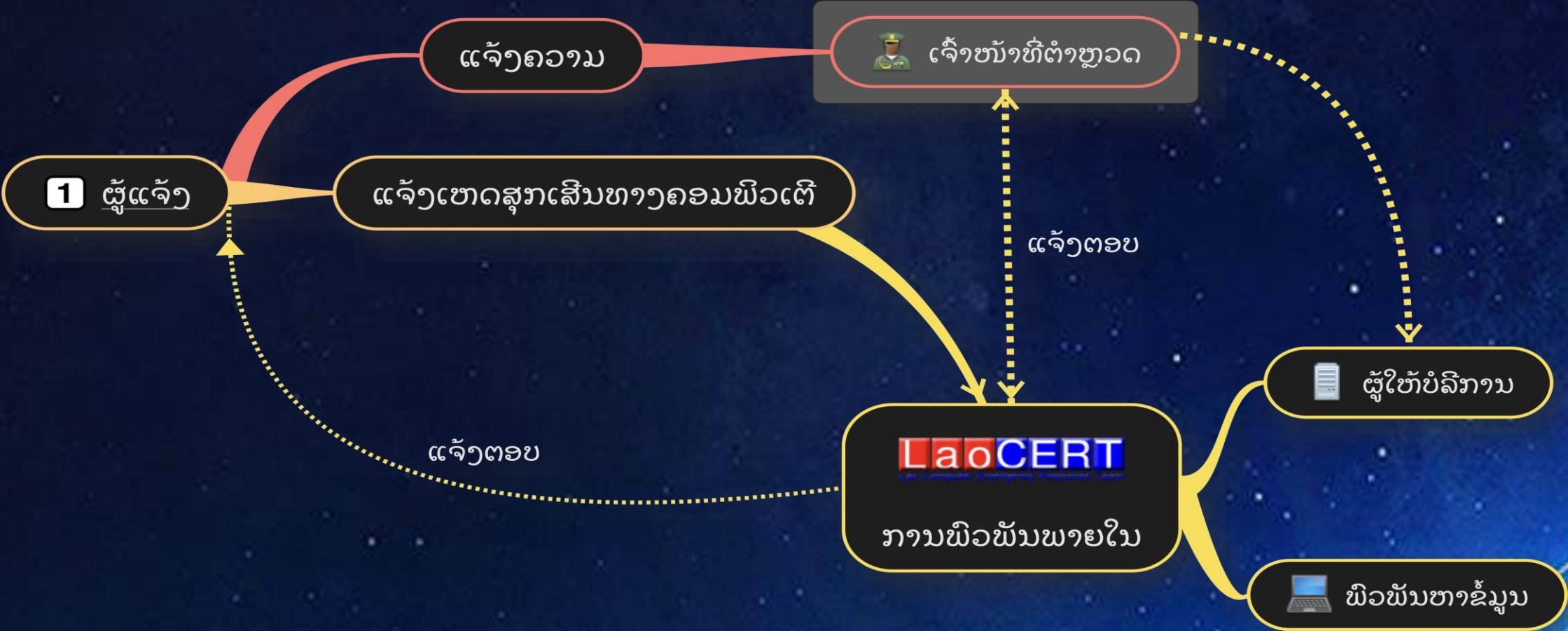


- ກົດໝາຍວ່າດ້ວຍ ການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳ ທາງລະບົບຄອມພິວເຕີ, ສະບັບເລກທີ 012/ສພຊ, ລົງວັນທີ 15 ກໍລະກົດ 2015 ມີທັງໝົດ 8 ພາກ, 64 ມາດຕາ
- ຄຳແນະນຳການຈັດຕັ້ງປະຕິບັດກົດໝາຍວ່າດ້ວຍການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ, ສະບັບ ເລກທີ 2543/ປທສ, ລົງວັນທີ 24 ກັນຍາ 2018 ທັງໝົດມີ IV ຂໍ້ໃຫຍ່.

ນິຕິກຳ



ການແຈ້ງເຫດຫາກົມຄວາມປອດໄພໄຊເປີ (ຄຄອຊ)



ການແກ້ໄຂສິ່ງຄົມອອນລາຍ

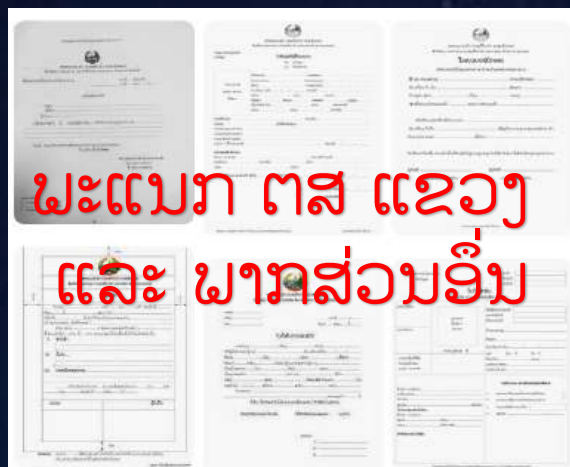


ກະຊວງ ປກສ



ກະຊວງ ເຕັກໂນໂລຊີ ແລະ ການສື່ສານ
ກົມຄວາມປອດໄພໄຊເບີ

LaoCERT
Lao Computer Emergency Response Team



ພະແນກ ຕສ ແຂວງ
ແລະ ພາກສ່ວນອື່ນ

ກໍລະນີຖືກຕາມເງື່ອນໄຂຂອງບໍລິສັດ



ຕົວຢ່າງ: ແບບຟອມປະກອບຂໍ້ມູນການກູ້ຄືນເຟສບຸກເຟກ (ຕໍ່)

ເນື້ອໃນການຮ້ອງຂໍໃຫ້ເຟສບຸກ ຊ່ວຍກູ້ຄືນບັນຊີເຟສບຸກເຟກອອກຊື່: “.....”

ລຳດັບ (No)	ເນື້ອໃນ (Content)	ລາຍລະອຽດ (Details)
01	ຊື່ເຟສບຸກ (Name of Facebook)	
02	ຄຳອະທິບາຍ (Description)	ເຟສບຸກເຟກອອກຊື່: “.....” ມີໝາຍເລກໄອດີ ແມ່ນ ໄດ້ຖືກຄືນບໍ່ຫວັງດີແຮັກເຂົ້າ ນຳໃຊ້ ແລະ ໄດ້ປິດບັນຊີຜູ້ເບິ່ງແຍງເຟສບຸກເຟກຂອງຫ້ອງການ.....ອອກ ເຮັດໃຫ້ເຈົ້າຂອງເຟສບຸກເຟກ ກໍ່ ຄື ຫ້ອງການ..... ບໍ່ສາມາດເຂົ້າໃຊ້ງານໄດ້, ບໍ່ສາມາດອອກຂ່າວໃຫ້ສັງຄົມໄດ້, ຖືກປ່ຽນແປງຂໍ້ມູນຂ່າວສານ ຊຶ່ງສົ່ງຜົນເສຍຫາຍໃຫ້ກັບຫ້ອງການ ແລະ ປະຊາຊົນລາວຜູ້ທີ່ຕິດຕາມຂໍ້ມູນຂ່າວສານຂອງ.....
03	ຈຸດປະສົງ (Purpose)	ຮ້ອງຂໍທາງເຟສບຸກຊ່ວຍກູ້ຄືນບັນຊີເຟສບຸກເຟກອອກຊື່: “.....” ເພາະບັນຊີດັ່ງກ່າວໄດ້ຖືກ ບຸກຄົນບໍ່ຫວັງດີແຮັກເຂົ້າໃຊ້ງານ.
04	ລິ້ງ (Link)	
05	ເລກໝາຍໄອດີ (ID)	
06	ໜ້າເຟສບຸກເຟກອອກຊື່“.....”	(ແຕັບຮູບໜ້າເຟກໃສ)
07	ອີເມວ ຂອງຜູ້ຄຸ້ມຄອງເຟສບຸກເຟກ (Admin Page)	1.....@..... 2..... 3..... 4.....
08	ເບີໂທ ຂອງຜູ້ຄຸ້ມຄອງເຟສບຸກເຟກ (Admin Page)	1. +856 20 2..... 3..... 4.....
09	ອີເມວສ້າງຂຶ້ນໃໝ່ ເພື່ອກູ້ຄືນເຟສບຸກ ເຟກ ແລະ ເບີໂທລະສັບ (New E- Mail)	@..... ແລະ +856 20

ຕົວຢ່າງ: ການຊອກຫາຂໍ້ມູນໄອດີ ຂອງບັນຊີເຟສບຸກທີ່ເປັນ ເປົ້າໝາຍ “FACEBOOK ID”

The screenshot displays the Lookup-ID.com website interface. The main heading is "Looking for your Facebook profile ID / Group ID / Page ID ...". Below this, it prompts the user to "Type your Facebook profile URL" with an input field containing "https://m.facebook.com/username" and a yellow "Lookup" button. To the right, a smaller browser window shows the "Find your Facebook ID" page, which has a text input field with the URL "https://www.facebook.com/khemmanat.chutinanvinij.7" and a "Find numeric ID" button. Below this, an advertisement is visible. Further down, it asks "What's my personal profile URL?" and provides examples of valid and invalid URLs. At the bottom of the main page, a "Success!" message is displayed, stating "Your Facebook personal numeric ID is:" followed by the ID "100007499011782" in a large red font, and a "Find another" button.

<https://randomtools.io/>

<https://lookup-id.com/>

<https://commentpicker.com/find-facebook-id.php>

<https://www.duplichecker.com/find-facebook-id.php>

ຕົວຢ່າງ: ການແຈ້ງເຟສບຸກບິດເຟສບຸກ

ເນື້ອໃນການຮ້ອງຂໍໃຫ້ເຟສບຸກ ຊ່ວຍປິດບັນຊີຜູ້ໃຊ້ເຟສບຸກອອກຊື່: Joseph Akaravong (ປທ ໄຈ)

(The content asks Facebook for assistance in blocking the account of a Facebook user called Joseph Akaravong (Pt. Jo).

ລຳດັບ (No)	ເນື້ອໃນ (Content)	ລາຍລະອຽດ (Details)
01	ຊື່ເຟສບຸກ (Name of Facebook)	Joseph Akaravong (ປທ ໄຈ)
02	ຄຳອະທິບາຍ (Description)	ເຟສບຸກອອກຊື່: Joseph Akaravong (ປທ ໄຈ) ໄດ້ມີການນຳໃຊ້ເຜີຍແຜ່ໂຄສະນາຄື: ໃສ່ຄ້າຍປ້າຍສີ, ໝິ່ນປະມາດ, ສ້າງຂໍ້ມູນເທັດ, ສ້າງຂໍ້ມູນຫຼອກຫຼວງ, ສ້າງຂໍ້ມູນທີ່ບໍ່ເປັນຄວາມຈິງ, ຊວນເຊື່ອ, ຍຸຍົງ ແລະ ສິ່ງເສີມໃຫ້ປະຊາຊົນຕໍ່ຕ້ານລັດຖະບານແຫ່ງ ສປປ ລາວ ຊຶ່ງເປັນການທຳລາຍຄວາມໝັ້ນຄົງຂອງຊາດຊາດ, ຄວາມສະຫງົບ, ຄວາມເປັນລະບຽບຮຽບຮ້ອຍຂອງສັງຄົມ, ວັດທະນະທຳ ແລະ ຂີດຄອງປະເພນີອັນດີງາມຂອງ ສປປ ລາວ ແລະ ກໍ່ຜິດລະບຽບຂອງບໍລິສັດເຟສບຸກເອງ ພ້ອມທັງຜິດກົດໝາຍ ຂອງ ສປປ ລາວໃນກົດໝາຍວ່າດ້ວຍ: ການຕ້ານ ແລະ ສະກັດກັ້ນອາຊະຍາກຳທາງລະບົບຄອມພິວເຕີ ຢູ່ໃນ ມາດຕາ 11: ການຕັດຕໍ່ເນື້ອໃນ, ຮູບ, ຜາປະຕິມາ, ສຽງ ແລະ ວິດີໂອ ໂດຍບໍ່ໄດ້ຮັບອະນຸຍາດ ແລະ ມາດຕາ 13: ການສ້າງຄວາມເສຍຫາຍຜ່ານສື່ສັງຄົມອອນລາຍ. Currently on Facebook, under the name of Joseph Akaravong (Pt. Jo), he has been publishing advertisements such as slander, blaspheming, creating fake information, creating false information, persuading, inciting, and encouraging people to oppose the government of the Lao PDR, which is to destroy the stability of the nation, peace, national culture, and fine traditions of the nation, breaking Facebook rules of the Facebook company and the Law of Lao PDR in Article 11: Unauthorized editing of pictures, audio, and videos; and article 13: Creating damage via online social media.
03	ຈຸດປະສົງ (Purpose)	ຮ້ອງຂໍທາງເຟສບຸກຊ່ວຍປິດບັນຊີເຟສບຸກອອກຊື່: Joseph Akaravong (ປທ ໄຈ) ເພາະບັນຊີດັ່ງກ່າວໄດ້ກະທຳຜິດຕໍ່ກົດໝາຍຂອງ ສປປ ລາວ ແລະ ລະບຽບຂອງເຟສບຸກເອງ. (Request to Facebook to assist in blocking the Facebook account named Joseph Akaravong (Pt. Jo) since the account has violated Lao PDR laws and Facebook policies.)
04	ລິ້ງ (Link)	https://www.facebook.com/profile.php?id=100008068268130
05	ເລກໝາຍໄອດີ (ID)	100008068268130
06	ໜ້າເຟສບຸກເພກ (Facebook Page)	

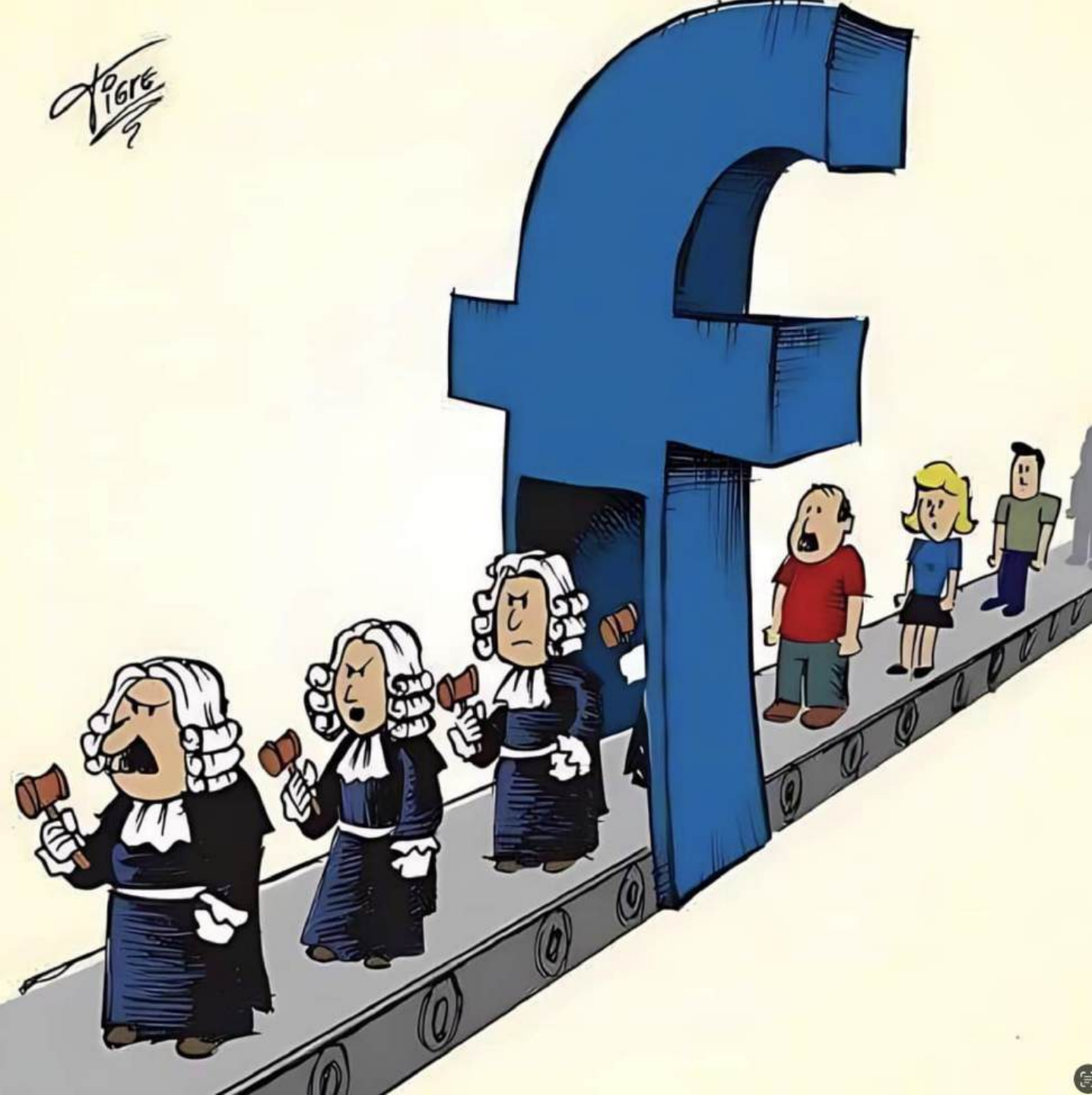
		
07	ລິ້ງກົດໝາຍ (Link of Law)	https://na.gov.la/wp-content/uploads/2021/11/95-Law-on-cyber-crime28-8-2015.pdf

		reveal without any authorization causing damage to state, person, legal entity, organization and society. Article 10. Unauthorized Computer Access Unauthorized computer access is an offence applying an electronic equipment or device to access any computer having specific computer access prevention measure or any commercial, financial data and information as well as secret confidence, other related information of person, legal entity and organization. Article 11. Unauthorized Editing Picture, Animation, Audio and Video Unauthorized Editing Picture, Animation, Audio and Video is an offence of editing picture or image, adding or modifying the original version by means of electronic process or other means in order to disseminate the outcome through computer system causing damage to state, person, legal entity and organization concerned. Article 12. Unauthorized Interception of Computer's Data and Information Unauthorized interception of Computer's Data and Information is an offence of interception of Computer's Data and Information by means of applying any electronic equipment or device while the receiver is receiving, or the sender is sending, data and information via computer system. Article 13. Causing Damages via Online Social Media Causing Damages via Online Social Media are offences in the actions of following: 1. Posting of computer's data and information containing of content on slandering, blaspheming, using impolite words through computer system; 2. Applying of violence, false, misleading and deception information into computer system; 3. Bringing the computer's data and information destroying national security, peace, order in society, national culture and fine tradition of the nation to apply into computer system; 4. Bringing the computer's data and information containing of aspects of conveying, persuading and encouraging people to resist the government or separate the national solidarity; 5. Advertising of drug, weapon of war, chemical weapon selling as well as human, prostitute, prostitution trafficking and other illegal products concerned; 6. Disseminating and sending of computer's data and information prescribed in Article 11 and 14 of this law including the title number 1, 2, 3, 4 and 5 in this Article. Article 14. Dissemination of Pornography Pornography is data and information containing of content clearly appearing in physical aspects such as picture and image, animation, audio, video relating to sexual organs and sexual activities of human. Dissemination of Pornography is an offence of selling, buying, distributing, transferring, introducing and disseminating of above prescribed in this Article. Article 15. Computer System Interference Computer System Interferences are offences in the actions of following: 1. Using of computer program, virus or other tools to interrupt or destroy the performance of computing; 2. Sending of computer system data and information or electronic mail or message with concealing of address, source of sender to disturb and/or destroy the performance of computing. Article 16. Computer's Data and Information Forgery Computer's Data and Information Forgery is an offence of using the computer, computer system and electronic equipment or device by means of action of following: 1.1 forgery of any computer original data
--	--	---

ຕົວຢ່າງ: ການກູ້ຄືນເຟສບຸກເຟກຜ່ານມາ



Page 9



THE
BADBOY
CLUB



THE DANGER OF

 / THEBADBOY_CLUB_



ONE SIDED STORY.

ຕົວຢ່າງການເກັບຂໍ້ມູນຂອງ Google App



ຕົວຢ່າງການເກັບຂໍ້ມູນຕົນເອງທີ່ເຄີຍລົງໃນອິນເຕີເນັດ



The image shows a white, rounded rectangular interface for the Webmii search engine. At the top, the logo "Webmii" is displayed in a bold blue font, with the tagline "People search engine" in a smaller, grey font directly below it. Below the logo is a long, thin search input field with a light grey border. Inside the field, the placeholder text "first and last name..." is written in a light grey, italicized font. To the right of the input field is a small grey square button with a white plus sign. Below the input field is a prominent blue button with rounded corners and the word "Search" written in white text.

ປະເພດໄພຄຸກຄາມທາງໄຊເບີ

Types of Cyber Attack

1. Viruses

2. Malware
Attack

3. Phishing
Attack

4. Password
Attacks

5. Vishing
Attacks

6. Man in the
Middle Attacks

7. Dos/ DDoS

8. Brute Force
Attack

9. Spyware &
Keylogger

10. Cross Site
Scripting

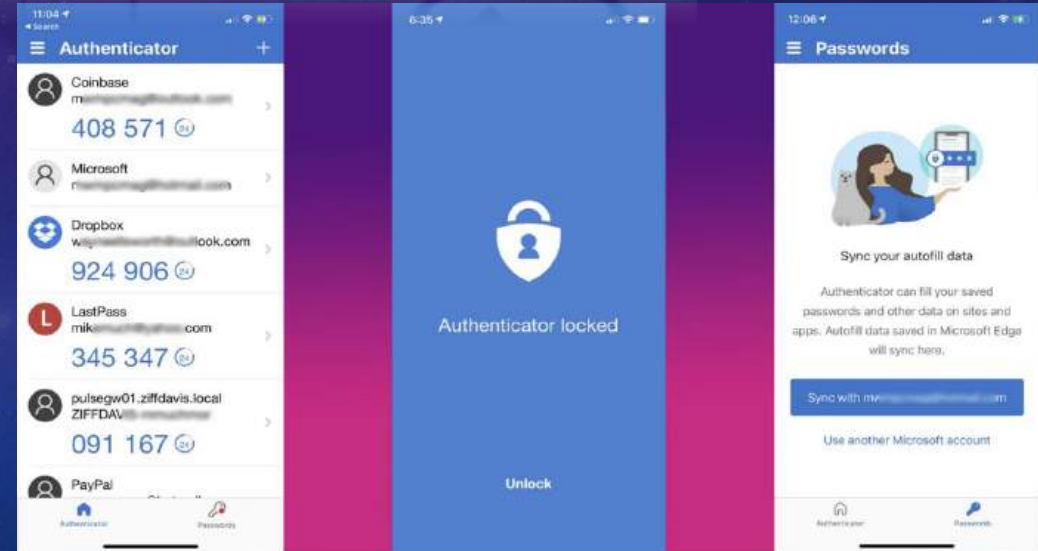
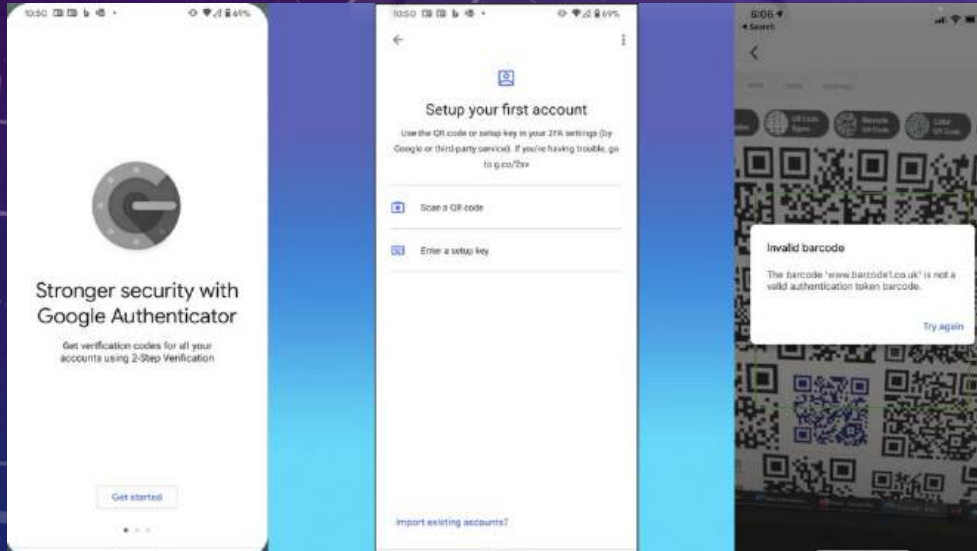
11. SQL
Injection

3. Phishing Attack

ປະເພດໄພຄຸກຄາມທາງໄຊເບີ



ໂປແກມທີ່ໃຊ້ໃນການຢັ້ງຢືນຕົວຕົນສອງຂັ້ນໂດຍທົ່ວໄປ (ຕໍ່)



ການບໍລິຫານຈັດການລະຫັດ

Create strong passwords with Password Generator

te-rlw*E8exe



Copy Password

✓ Strong password

Use the slider, and select from the options, below, to lengthen your password and strengthen your security.

Password Length (4-64)

12

☒ Letters ☒ Mixed case ☒ Punctuation ☒ Numbers



Secure Password Generator

English ▾

Password Length:

16 ▾

Include Symbols:

☒ (e.g. @\$%)

Include Numbers:

☒ (e.g. 123456)

Include Lowercase Characters:

☒ (e.g. abcdefgh)

Include Uppercase Characters:

☒ (e.g. ABCDEFGH)

Exclude Similar Characters:

☒ (e.g. i, l, 1, L, o, 0, O)

Exclude Ambiguous Characters:

☒ ({ } [] () \ ' " ~ , ; . < >)

Generate On Your Device:

☒ (do NOT send across the Internet)

Auto-Select:

☐ (select the password automatically)

Save My Preference:

☐ (save all the settings above for later use)

Load My Settings Anywhere:

URL to load my settings on other computers quickly

Generate Password

Copy

Advanced(Free)

Your New Password:

cU%#-3yvTX_%BGc8

Copy

Remember your password:

coffee USA % # - 3 yelp visa TOKYO XBOX _ % BESTBUY GOLF coffee 8

ລະຫັດທີ່ບໍ່ຄວນນຳໃຊ້

1	123456	26	ubnt
2	admin	27	abc123
3	12345678	28	Aa@123456
4	123456789	29	abcd1234
5	1234	30	1q2w3e4r
6	12345	31	123321
7	password	32	qwertyuiop
8	123	33	87654321
9	Aa123456	34	987654321
10	1234567890	35	Eliska81
11	1234567	36	123123123
12	123123	37	11223344
13	111111	38	0987654321
14	Password	39	demo
15	12345678910	40	12341234
16	000000	41	qwerty123
17	admin123	42	Admin@123
18	1111	43	1q2w3e4r5t
19	P@ssw0rd	44	11111111
20	root	45	pass
21	654321	46	Demo@123
22	qwerty	47	azerty
23	Pass@123	48	admintelecom
24	112233	49	Admin
25	102030	50	123meklozed

ການກວດວ່າລະຫັດທີ່ໄດ້ຕັ້ງຢູ່ໃນເກນໃດ

Password Check

Can you tell if a password has been compromised?

This site was set up to demonstrate that a **STRONG PASSWORD** isn't necessarily a **SAFE PASSWORD**.

Although many passwords meet typical algorithmic strength requirements, they may still be unsafe if they exist in password cracking dictionaries used by cybercriminals.

Start your password check. Enter a password below to see both its strength and if it is among the billions that have been compromised. Consider these examples:

sk8erboy | pha69Htm | punkforlife | correct horse battery staple | 2bon2btitq | Hunter@2 | minecrafter1521 | oscarshi1998

[Learn more about this site →](#)

The password will be sent securely to our server to check if it is compromised. We will not store the password.

Strong

ການກວດລະຫັດມີການຮົ່ວໄຫຼໃນອິນເຕີເນັດ

haveibeenzuckered.com

anling ສູ່ທຸກອິນເຕີເນັດ ທຸກ... 037HDMovie.com... ສູ່ທຸກອິນເຕີເນັດ ສູ່ທ... Login Brute Forcin... cPanel - Tools Zone-Xsec - Sear... SingCERT Cyber I... FireHOL IP Lists | I... https://scite.ai/ All Book

Facebook Data Breach Checker

A large dataset containing 533 million Facebook accounts was made available for download. The data was obtained by exploiting a vulnerability that was, according to Facebook, corrected in August 2019.

Check if your telephone number is present within the Facebook data breach.

We have finalised ingesting the dataset, and we currently have processed **502 769 112** records from **106** different countries. This tool does not store user-provided input and uses k-anonymity to ensure privacy.

 +856 >



<https://haveibeenzuckered.com/>

ການກວດລະຫັດມີການຮົ່ວໄຫຼໃນອິນເຕີເນັດ

haveibeenpwned.com

VMware Training -... vXpress: VSPHERE P2V ADMIN ISO :... support.ge-ip.co... Check Username... Domain Name List... DuckDuckGo Goo... ສູ້ກັບ Zpanel ສູ້ກັບເນັດ... IS...

Home Notify me Domain search Who's been pwned Passwords API About Donate

';--have i been pwned?

Check if your email or phone is in a data breach

email address pwned?

672	12,496,783,237	115,744	227,329,839
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

Recently added breaches

177,554	CityJerks accounts
8,227	MEO accounts
2,075,625	Terravision accounts
529,020	OGUsers (2022 breach) accounts
400,635	The Kodi Foundation accounts
8,000,000	Genesis Market accounts
274,461	Sundry Files accounts
114,907	Leaked Reality accounts

<https://haveibeenpwned.com/>

Home Proxy Server List Port Scanner Proxy Checker Tools More

Search the world's largest dataset of leaked passwords

In February of 2021, the largest dataset of leaked credentials (emails, usernames, and passwords) named COMB (Combination Of Many Breaches) was leaked to the public. It was the largest data leak of all time, containing over 3.2 billion credentials combined across from various other data breaches over the years from services such as Netflix, LinkedIn and many others. The purpose of this tool is to make that massive dataset of leaked usernames and passwords easily searchable, and to encourage better security practices by giving people an ability to check if their credentials were leaked and thus exposed to hackers.

If you find yourself on this list - **change your password immediately**, and always enable two factor authentication whenever possible. Your searches are not logged nor ever stored on our servers.

search by email, username or password ... Search

ລິ້ງເຂົ້າເວັບໄຊ

Has your password been leaked?

Password hacking compromised more than 237,215,238 accounts these past 6 months!
Find out if a password hack has exposed your password to the world.

..... Test password

Password has been leaked!

This password has been seen 388,412 times before.

<https://leakedpassword.com>



Create new

Dashboard

Links

QR Codes **NEW!**

Link-in-bio

Campaigns

Custom links

Settings

ການກວດກາຟາຍ, ທີ່ຢູ່ລຶ້ງ

bit.ly/3LPEBHY

0 clicks

↳ https://drive.google.com/file/d/0B2J3twGqr5igc2hXaEZhN2JZUzg/view?usp=share_link... 🔒 Redire

QR Code



Create QR Code

Link-in-bio ?



Create a Link-in-bio



<https://bitly.com>

ການກວດກາຟາຍ, ທີ່ຢູ່ລຶ້ງ



<https://bit.ly/3LPEBHY>



<https://getlinkinfo.com>

GetLinkInfo.com

Get Link Info

Enter any URL, for example: <http://tinyurl.com/2unsh>, <http://bit.ly/1dNVPaw>

<https://checkshorturl.com/>

<https://checkshorturl.com/>

<https://www.urlchecker.com/>

<https://getlinkinfo.com/>

<https://urlex.org/>

<https://urlex.org>

URLEX

<https://bit.ly/3LPEBHY> <https://drive.google.com/file/d/0B2J3t...>

<https://www.urlchecker.com/url/https://bit.ly/3LPEBHY>

Expand URLs. Stay safe...

Your result is here.

URL Destination	Trust Score
https://drive.google.com/file/d/0B2J3t.../view?usp=share_link&resourcekey=0-b2Jp4Deos7U8aB10vS_w	85%

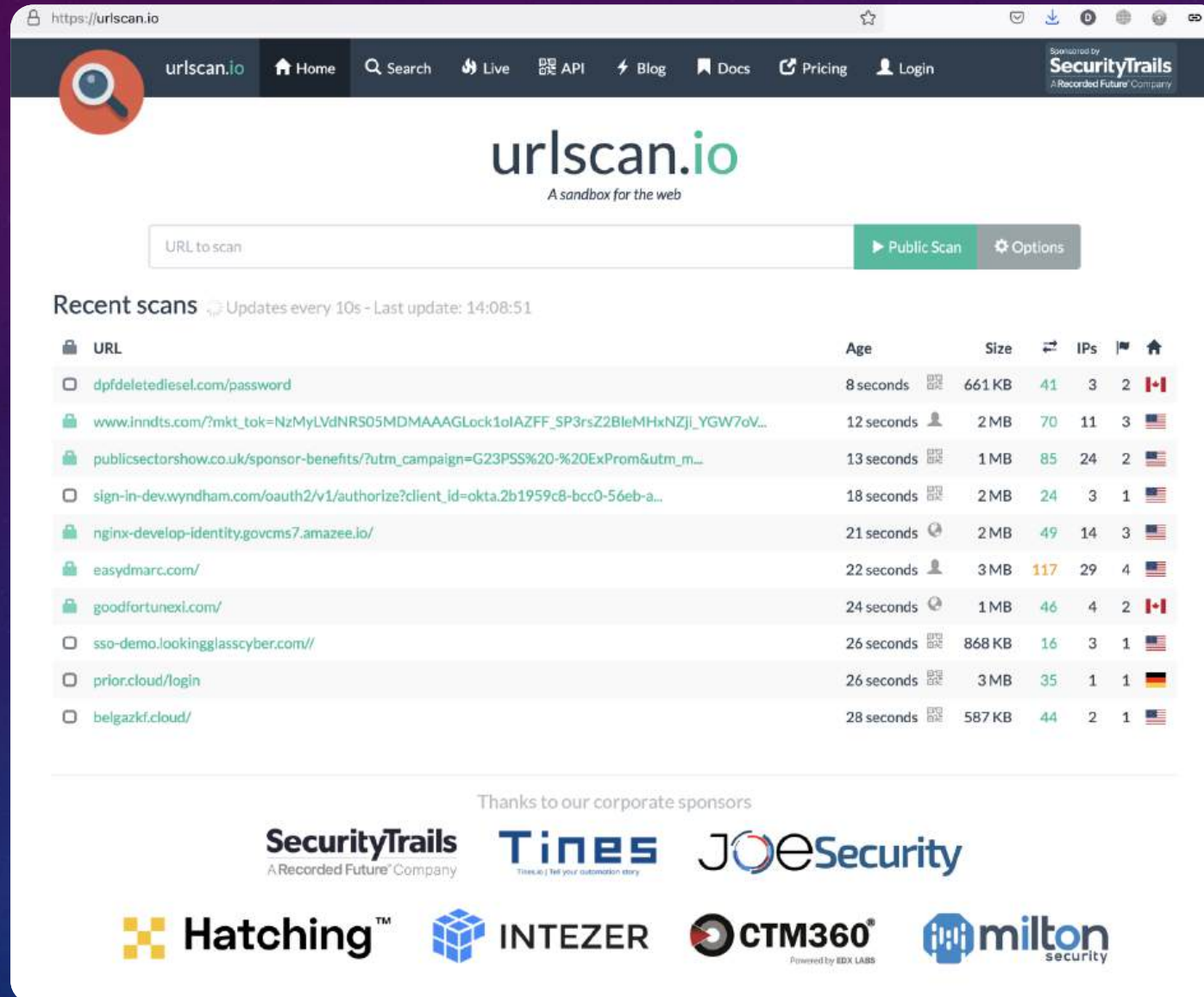
ການປ້ອງກັນໃຫ້ມີຖືມີຄວາມປອດໄພ

ສິ່ງທີ່ເຮົາຄວນຈະເຮັດເພື່ອໃຫ້ມີຖືທີ່ນຳໃຊ້ມີຄວາມປອດໄພ

- ນຳໃຊ້ລະຫັດຜ່ານທີ່ຄາດເດົາໄດ້ຍາກ
- ໃຊ້ການຍັງຢືນຕົວຕົນ 2 ຂັ້ນ ຫຼື ຫຼາຍກ່ວາ
- ປັບປຸງດ້ານຄວາມປອດໄພຂອງມືຖືເປັນປະຈຳ
- ລຶບຂໍ້ມູນທີ່ມີການບັນທຶກໄວ້
- ນຳໃຊ້ຊັອບແວທີ່ປ້ອງກັນໂປແກມປະສົງຮ້າຍ
- ນຳໃຊ້ລະບົບທີ່ມີການເຂົ້າລະຫັດ



ການກວດຄວາມປອດໄພຂອງຟາຍ ຫຼື ໂປແກຼມ



The screenshot shows the urlscan.io website interface. At the top, there's a navigation bar with links for Home, Search, Live, API, Blog, Docs, Pricing, and Login. The main header features the urlscan.io logo and the tagline "A sandbox for the web". Below this is a search bar labeled "URL to scan" with buttons for "Public Scan" and "Options".

The "Recent scans" section displays a table of scan results. The table has columns for URL, Age, Size, and a set of icons representing various metrics. The scans are listed in descending order of age.

URL	Age	Size	Icons
dpfdeletediesel.com/password	8 seconds	661 KB	41, 3, 2, Canada flag
www.inndts.com/?mkt_tok=NzMyLVdNR505MDMAAGLock1olAZFF_SP3rsZ2BleMHxNZjl_YGW7oV...	12 seconds	2 MB	70, 11, 3, US flag
publicsectorshow.co.uk/sponsor-benefits/?utm_campaign=G23PSS%20-%20ExProm&utm_m...	13 seconds	1 MB	85, 24, 2, US flag
sign-in-dev.wyndham.com/oauth2/v1/authorize?client_id=okta.2b1959c8-bcc0-56eb-a...	18 seconds	2 MB	24, 3, 1, US flag
nginx-develop-identity.govcms7.amazee.io/	21 seconds	2 MB	49, 14, 3, US flag
easydmarc.com/	22 seconds	3 MB	117, 29, 4, US flag
goodfortunexi.com/	24 seconds	1 MB	46, 4, 2, Canada flag
sso-demo.lookingglasscyber.com//	26 seconds	868 KB	16, 3, 1, US flag
prior.cloud/login	26 seconds	3 MB	35, 1, 1, Germany flag
belgazkf.cloud/	28 seconds	587 KB	44, 2, 1, US flag

Below the table, there's a section titled "Thanks to our corporate sponsors" featuring logos for SecurityTrails, Tines, JOE Security, Hatching, INTEZER, CTM360, and milton security.

<https://urlscan.io/>

ການກວດຄວາມປອດໄພຂອງຟາຍ ຫຼື ໂປແກຼມ

https://www.virustotal.com/gui/file/8c00a52be5cc69d94e7a227d8cbde38c3bdbc51c3f9d5145816f61fe8af8112b

52be5cc69d94e7a227d8cbde38c3bdbc51c3f9d5145816f61fe8af8112b

24 / 60

24 security vendors and no sandboxes flagged this file as malicious

8c00a52be5cc69d94e7a227d8cbde38c3bdbc51c3f9d5145816f61fe8af8112b

Cheat.Engine.7.5_Rus.rar

2.19 MB
Size

2023-05-09 17:48:44 UTC
13 hours ago

rar

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label **trojan.offercore/bundler**

Threat categories trojan adware virus

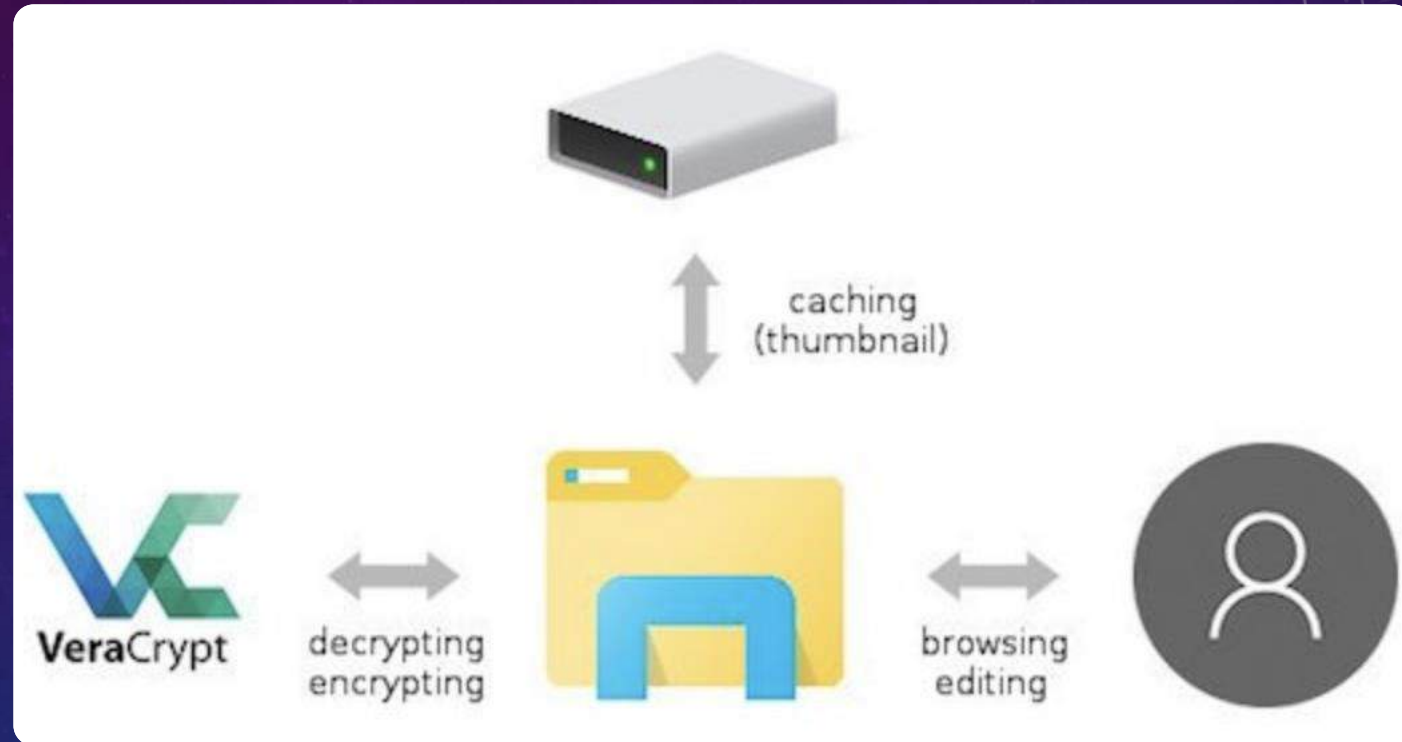
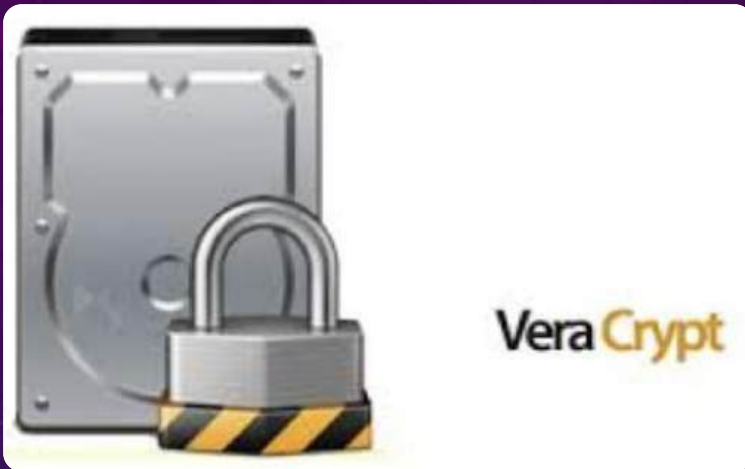
Family labels offercore bundler instalcor

Security vendors' analysis

Avira (no cloud)	PUA/OfferCore.Gen	Cynet	Malicious (score: 99)
Cyren	W32/ABRisk.UXVL-4804	DeepInstinct	MALICIOUS
DrWeb	Trojan.InstallCore.4077	ESET-NOD32	Win32/OfferCore.C Potentially Unwanted
F-Secure	PotentialRisk.PUA/OfferCore.Gen	Fortinet	Riskware/OfferCore
Google	Detected	Gridinsoft (no cloud)	PUP.OfferCore.ddlc
Ikarus	PUA.OfferCore	K7AntiVirus	Adware (00595a211)
K7GW	Adware (00595a211)	Kaspersky	Not-a-virus:Downloader.Win32.Bundle
Lionic	Riskware.ZIP.Bundler.1fc	Malwarebytes	PUP.Optional.OfferCore
MaxSecure	Trojan.Malware.121086327.susgen	McAfee-GW-Edition	Artemis
Microsoft	PUADManager.Win32/OfferCore	Rising	Adware.OfferCore!1.DF2E (CLASSIC)
Sophos	Mal/Generic-S	VBA32	Trojan.InstallCore
VirIT	Deceptor.CheatEng.DWG	ZoneAlarm by Check Point	Not-a-virus:Downloader.Win32.Bundle

<https://www.virustotal.com/gui/home/search>

ການເຂົ້າລະຫັດເອກະສານ



ໂປແກມປ້ອງກັນໄວຣັດ

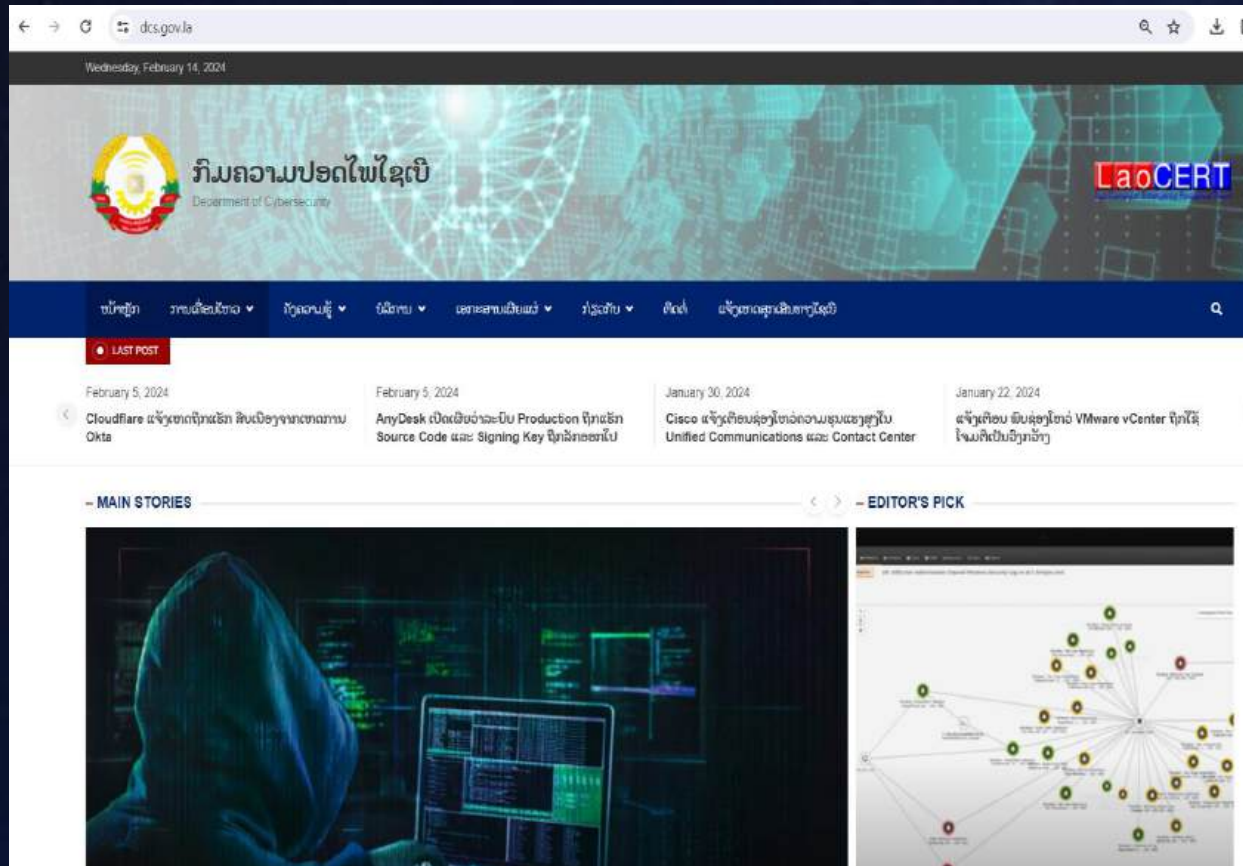
- #1 Bitdefender
- #2 Norton
- #3 Kaspersky
- #4 ESET
- #5 Webroot
- #5 Avast
- #5 McAfee
- #5 Trend Micro
- #5 Avira
- #10 AVG Technologies
- #11 Malwarebytes
- #12 Sophos



ບາງຫົວຂໍ້ທີ່ທາງກົມໄດ້ເຜີຍແຜ່ຜ່ານ



<https://www.dcs.gov.la/>



<https://laocert.gov.la/>



ຂໍຂອບໃຈ



www.dcs.gov.la

www.laocert.gov.la



report@laocert.gov.la



+ 856 20 5786 9628



ບ້ານ ສາຍລົມ, ເມືອງຈັນທະບຸລີ
ນະຄອນຫຼວງວຽງຈັນ