

Cyber Security

UPDATE 2019

ปีติกร เตังตระกูล

30 ตุลาคม 2561

กรมการพัฒนาชุมชน

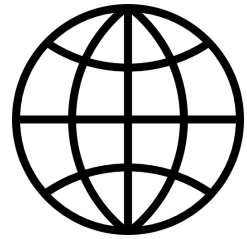


Kahoot!

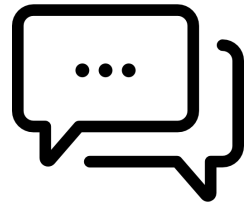
Game PIN

Enter

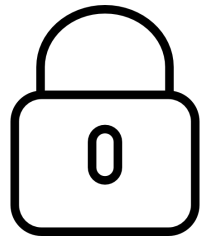
Agenda



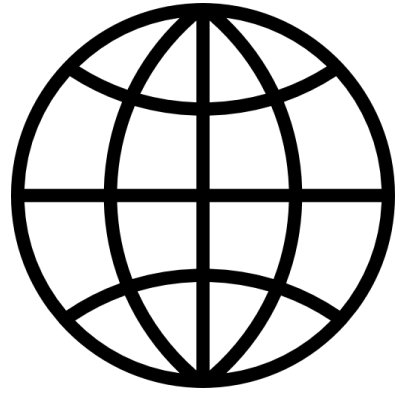
Threat



Trend



Take care



Threat

Threat

- Security report: 2018
- Social network
- Two factors authentication
- Cryptojacking
- Major incidents

59%



OF COMPANIES CONSIDER
RANSOMWARE TO BE THEIR
BIGGEST THREAT₄

24%



OF COMPANIES
HAVE EXPERIENCED A DDOS
ATTACK IN THE PAST YEAR₆

OVER

300



APPS IN THE GOOGLE PLAY
STORE CONTAINED MALWARE
AND WERE DOWNLOADED BY
OVER 106 MILLION USERS₇

64%



OF ORGANIZATIONS HAVE
EXPERIENCED A PHISHING
ATTACK IN THE PAST YEAR₂

1 in 3 

RETAILERS HAVE
ALREADY BEEN HIT BY
A CYBER ATTACK¹⁷

82% 

OF MANUFACTURERS
HAVE EXPERIENCED A
PHISHING ATTACK IN
THE PAST YEAR¹⁸

100% 

OF ALL BUSINESSES HAVE
HAD A MOBILE MALWARE
ATTACK⁸

32% 

OF GOVERNMENT
OFFICES WERE VICTIM
TO A DATA BREACH IN
THE PAST YEAR²⁰

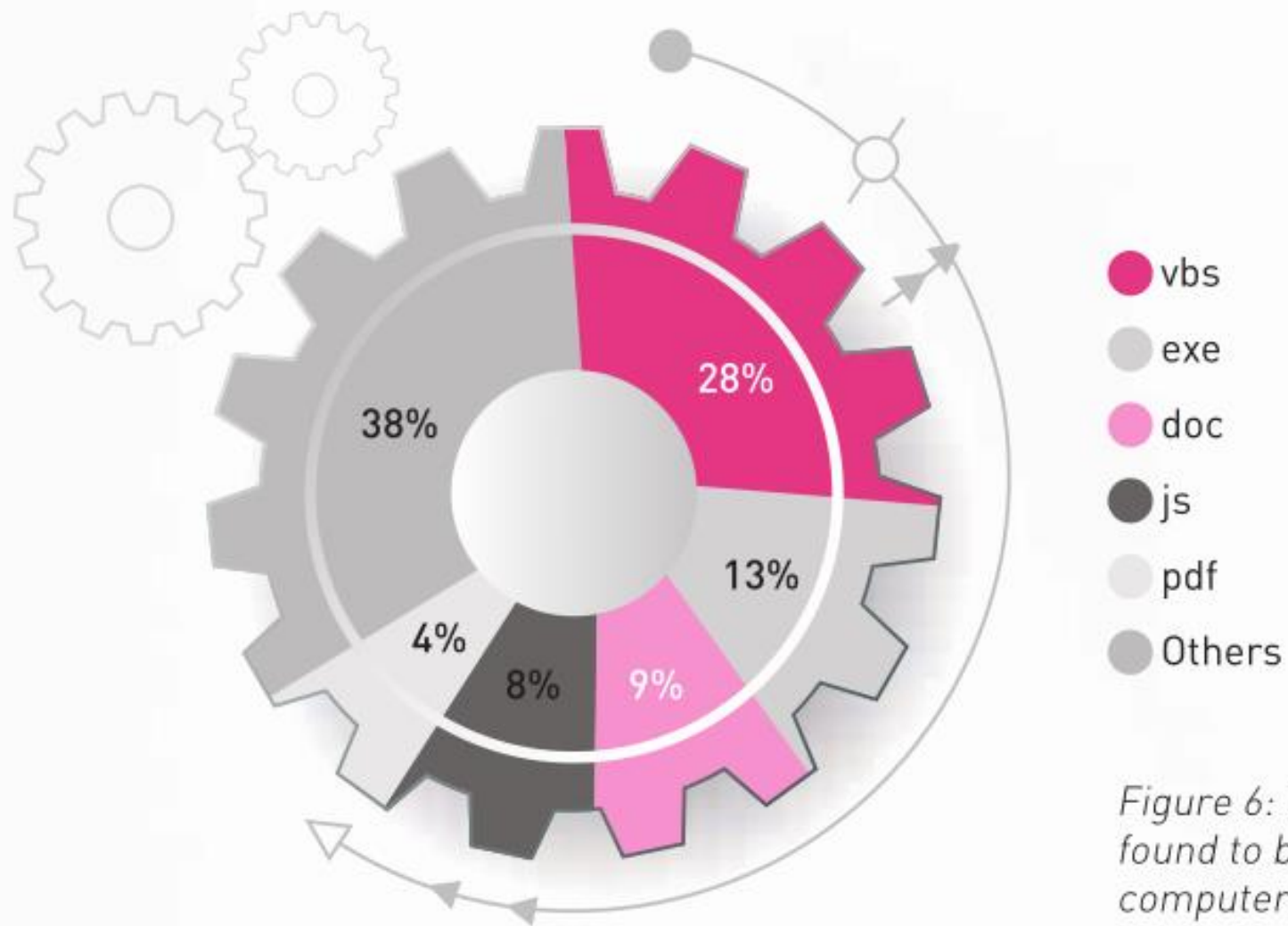


Figure 6: The top malicious file types found to be used to infect users' computers. ¹⁹

Social network: Google+

- March 2018
 - Bug in API – App developers
 - User profile data
 - Since 2015 (Hidden)
- Shut down in 2019
 - Avoid Reputation damage
 - Possible \$\$\$ Fine





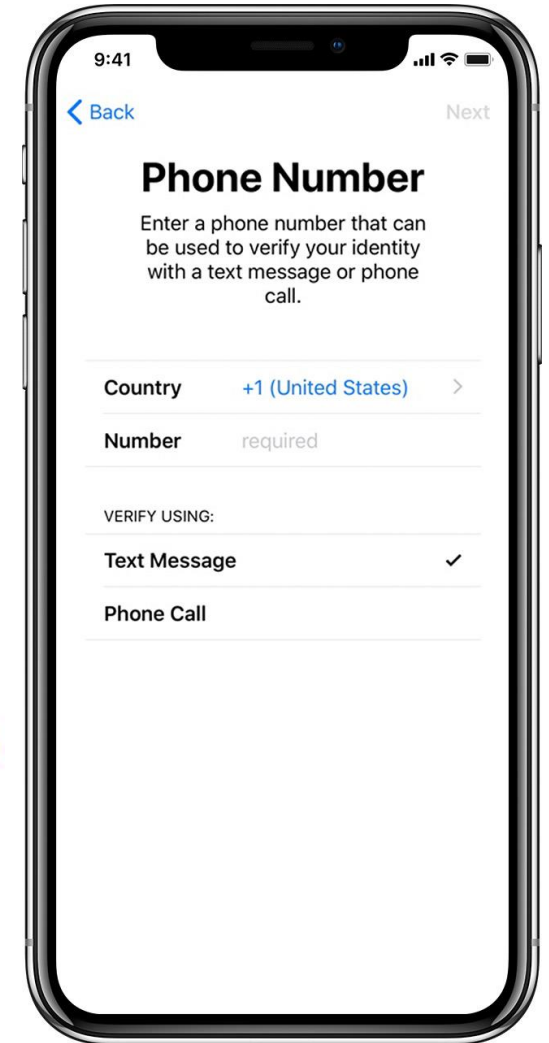
Social network: Facebook

- Cambridge Analytica
 - Disclose: March 2018
 - 90 millions profile/ timeline
 - 2015 - Presidential election
- “View As”
 - Disclose: September 2018
 - 90 millions accounts
 - (\$ 1.5 Billion Fine)
 - Account setting → Security and Login
→ Where you’re logged in



Two factors authentication (2FA)

- Something you -
 - Know = Password, Security question
 - Have = Mobile, Access card, Keys
 - Are = Finger print, Facial, Retina
- SMS Hijacking
 - Thailand: Fraud identity
 - Intercept SMS
 - Signaling System No.7 (SS7)
 - \$ 500 on Dark web



SERVICES

(Contact me at interconnect0r@protonmail.com to purchase)

CELL PHONE REPORTS

A cell phone report contains network information, such as MCC, MNC, IMSI, TMSI and location information(real-time) - You can also request encryption keys, call status.

1 MONTH: \$150

CELL PHONE INTERCEPTION

This service is simple and easy, after purchase, you will receive an access key, which you can use for the web panel. These prices are for 1 month of unlimited usage, and the ability to change the target any time.

CALLS: \$250

SMS MESSAGES: \$250

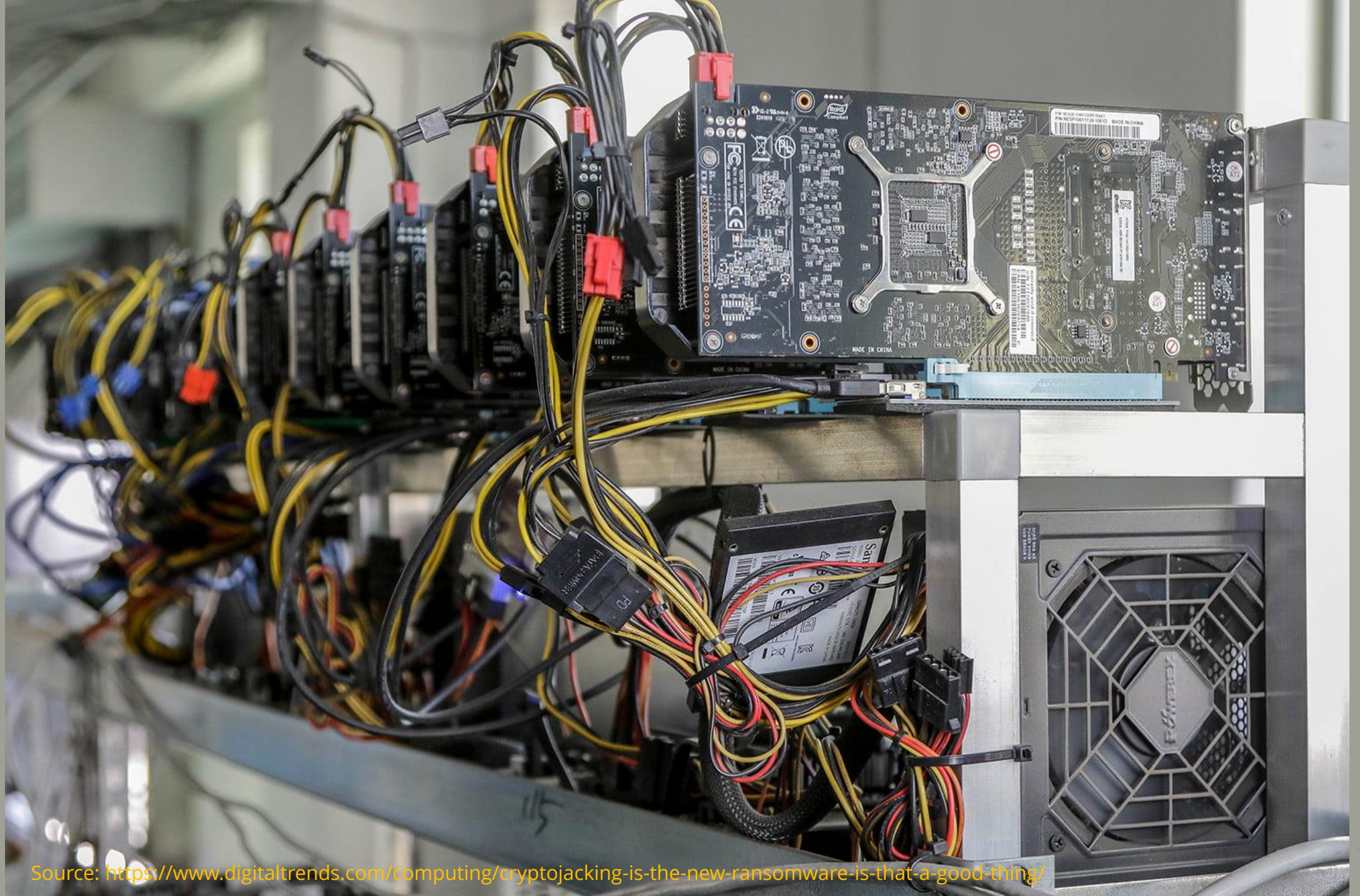
PANEL PREVIEW

FULL ACCESS

With this, you can do everything I can, by connecting to a user-friendly SSH terminal. API Access includes the following: Tracking, subscription modifying, jamming, intercepting, SMS/Call Spoofing.

1 MONTH: \$500

3 MONTHS: \$1000



Source: <https://www.digitaltrends.com/computing/cryptojacking-is-the-new-ransomware-is-that-a-good-thing/>

Cryptojacking

- Crypto-Mining code
 - Run on background
 - For \$ Bitcoin
- Infection
 - Computer: Botnet, Malware
 - Browser: Script on websites
- Kits available for only \$ 30 on Dark web
 - \$ 30 vs. \$ 600/card (buy own Graphic card)



Major incidents: 2018

- Cathay Pacific



- Oct 2018: All 9 million passengers
- Passport, Email, Credit card

- Uber

- Sep 2018: 60 million customers + drivers
- Paid \$100 K to hacker to silent --> \$133 M Fine



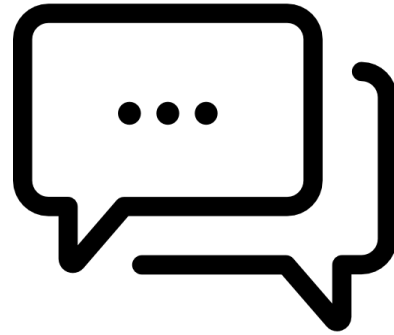
- Reddit

- Aug 2018: Undisclosed scale



Note

- Security breach = Late report
 - Keep secret, Stay silent
 - Disclose months (years) later
- Dark web = Accelerator / Facilitator
- Same old methods
 - Malware
 - Spear phishing
 - Brute force



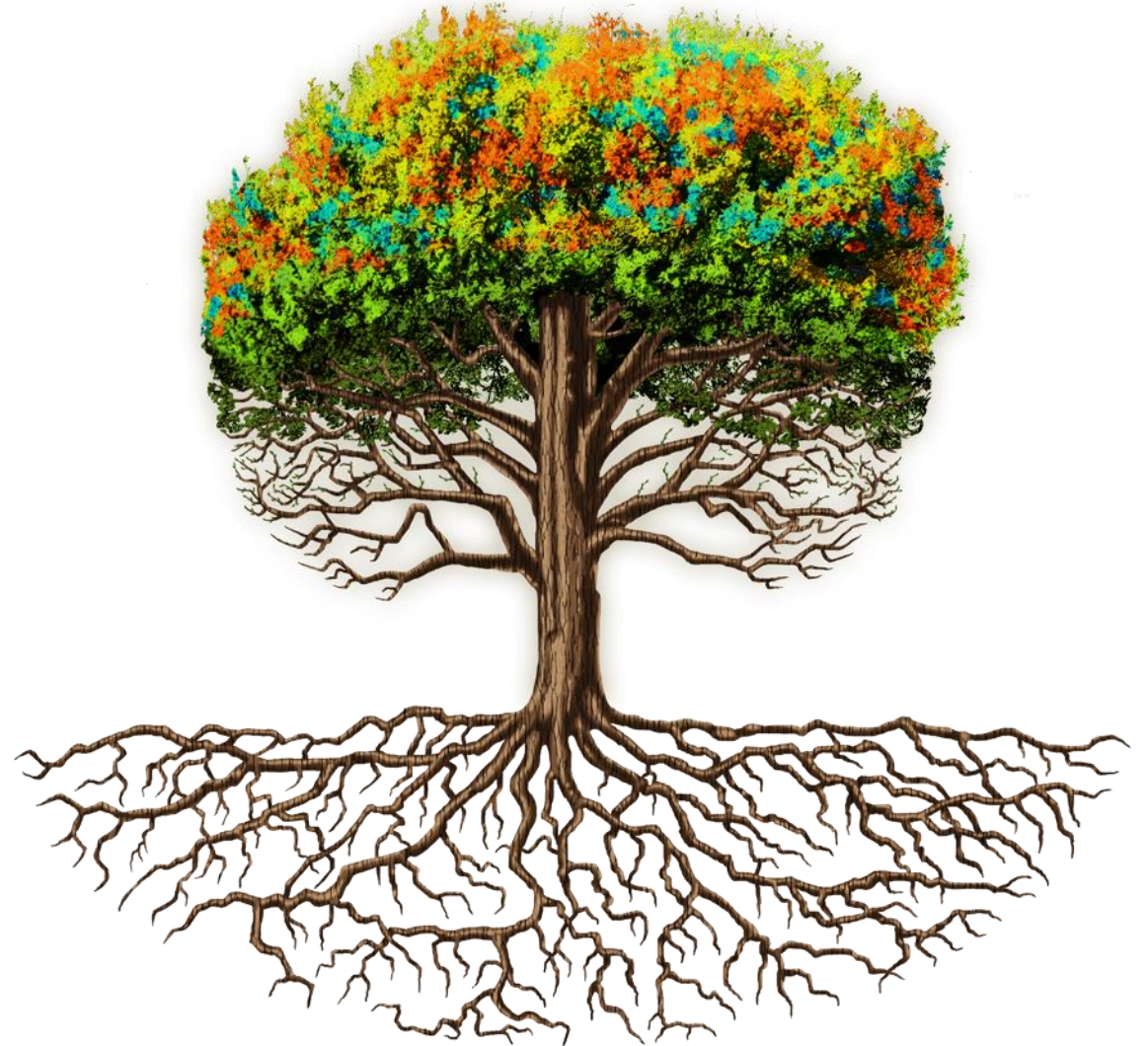
Trend

Trend

- Facilitating technology
- Blockchain
- Edge computing
- AR / VR
- GDPR

Facilitating technology

- Cloud
- IoT
- Big data
- Artificial Intelligence (AI)
- 5G



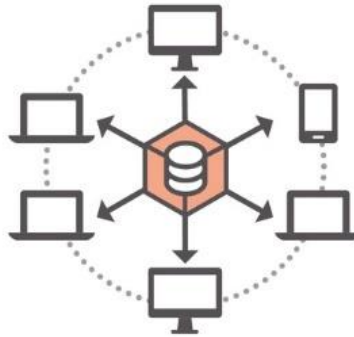
Blockchain



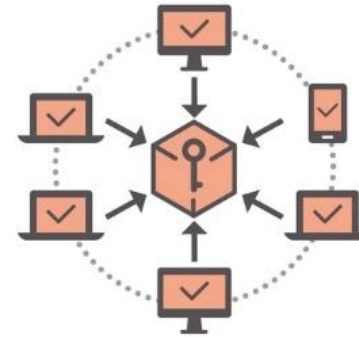
A transaction is requested



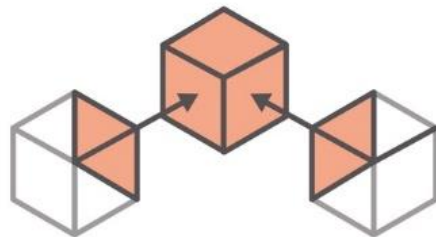
The transaction is broadcasted to a network of nodes



The network validates the transaction using known algorithms



The transaction is unified with other transactions as a block of data.



The new block is added to the blockchain in a transparent and unalterable way.

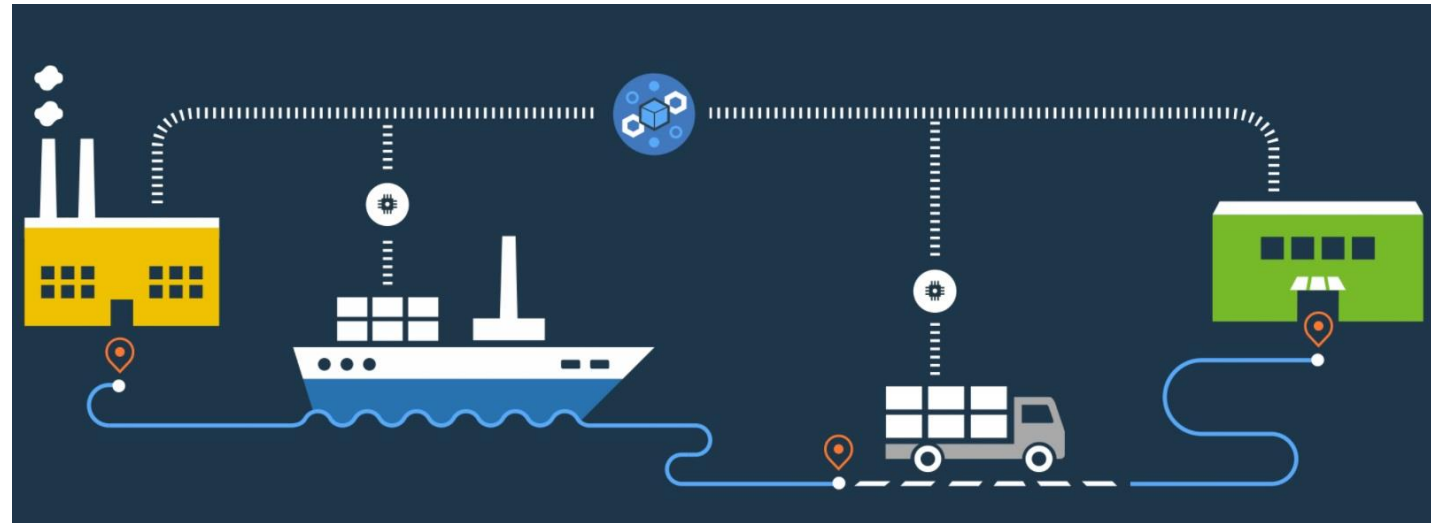


The transaction is complete

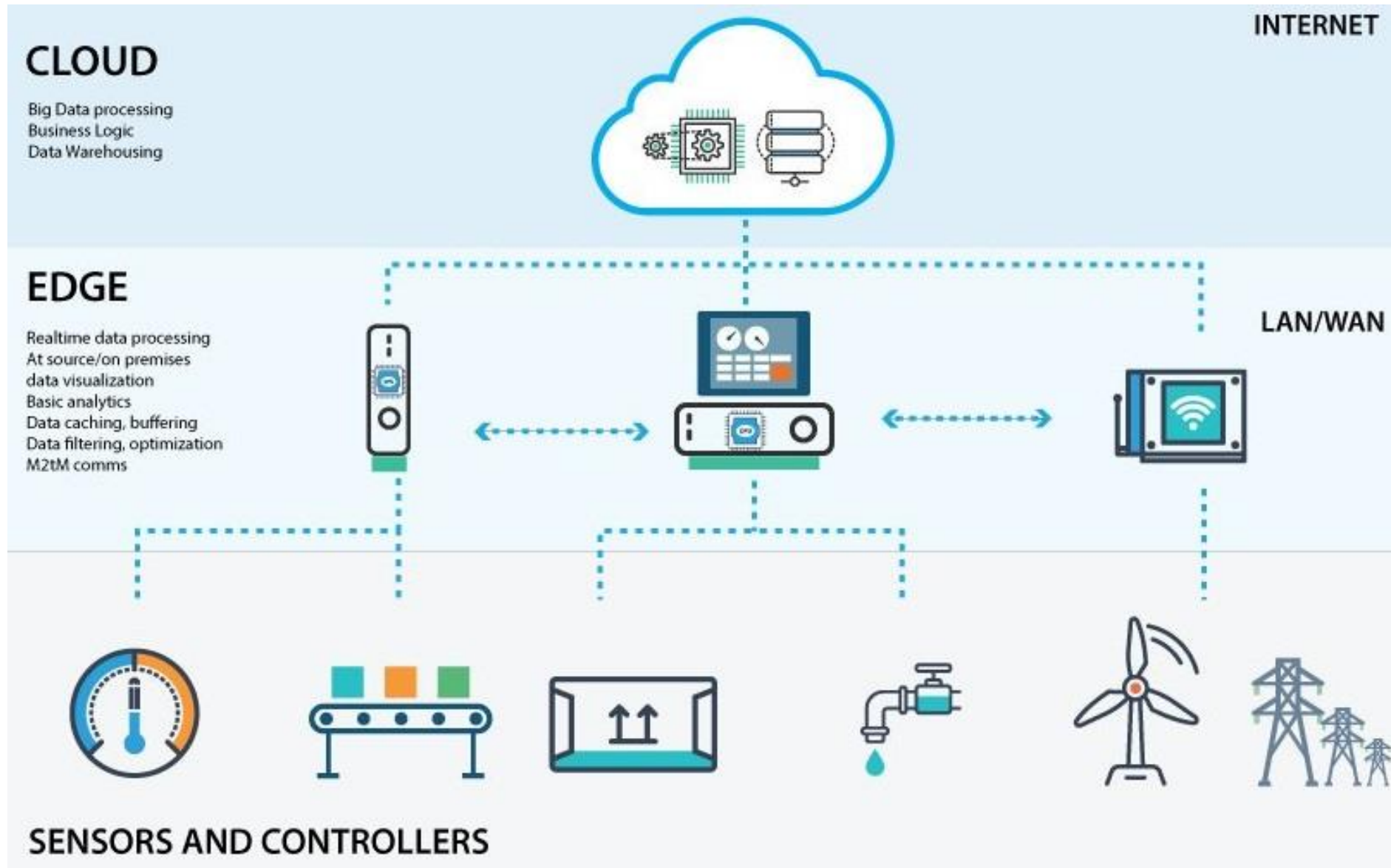


Blockchain

- Properties
 - Decentralized database (Ledger)
 - Immutable
 - Transparent + chain
 - Smart contracts (rules)
- Applications
 - Transactions
 - Foods/Goods tracking
 - Any supply chains



Edge computing



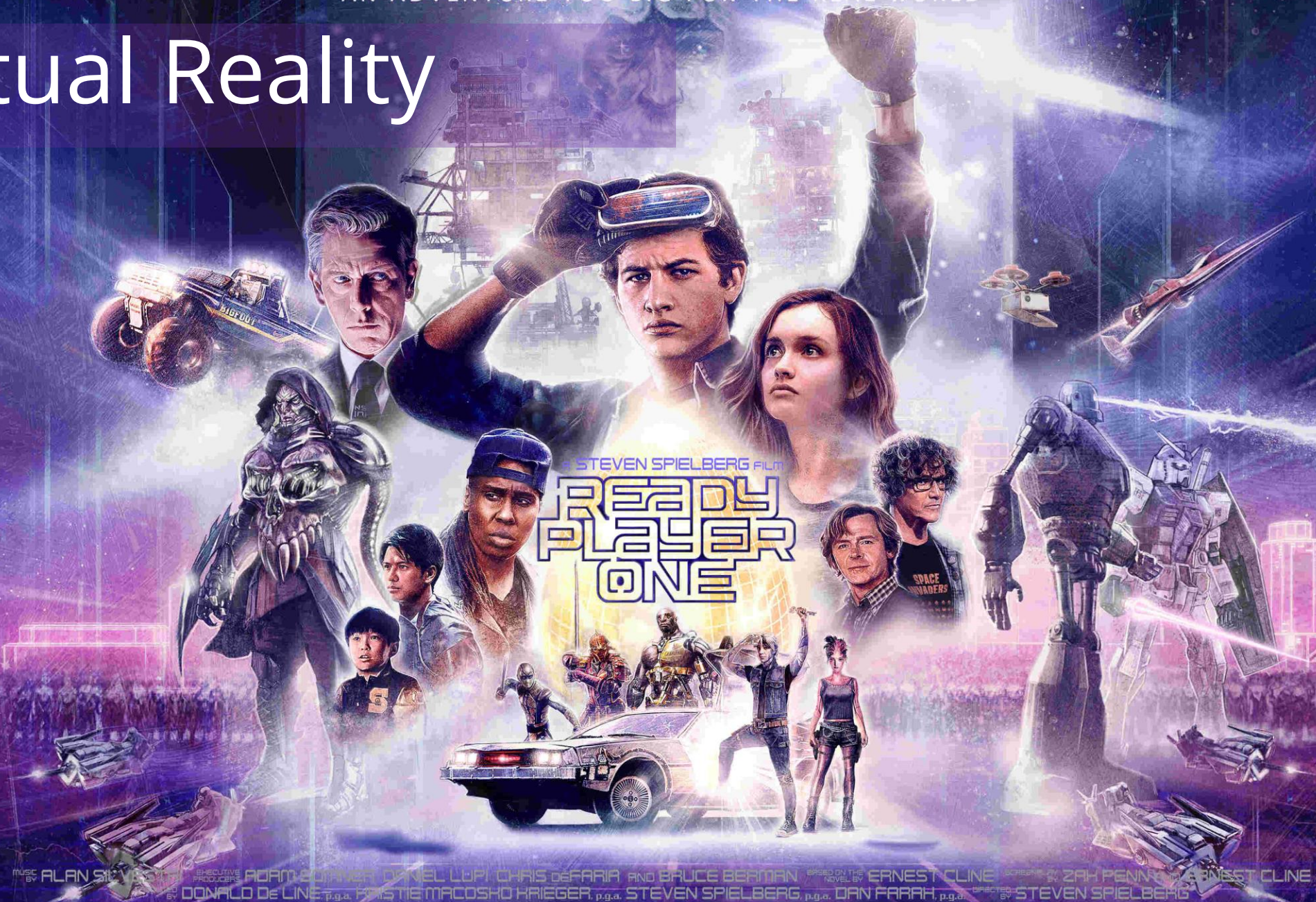
Augmented Reality



Source: <https://www.forbes.com/sites/bernardmarr/2018/07/30/9-powerful-real-world-applications-of-augmented-reality-ar-today>

AN ADVENTURE TOO BIG FOR THE REAL WORLD

Virtual Reality



PRODUCED BY ALAN SILVERMAN
EXECUTIVE PRODUCERS ADAM BOYNER, DANIEL LUPI, CHRIS DEFARIA AND BRUCE BERMAN
BASED ON THE NOVEL BY ERNEST CLINE
SCREENPLAY BY ZAH PENN
DIRECTED BY STEVEN SPIELBERG
CASTING BY DONALD DE LINE
P.G.A. FORSTIE MACOSKO KRIEGER, P.G.A. STEVEN SPIELBERG, P.G.A. DAN FARAH, P.G.A.

GDPR

- General Data Protection Regulation
 - European countries
 - Effective June 2018
- Inspiration of ...
 - Personal Data Protection Act (Thailand)



GDPR... 2018 IN 1 MINUTE

The EU GDPR will increase privacy for individuals and give regulatory authorities greater powers to take action against businesses that breach the new laws.

HERE'S WHAT IT MEANS FOR YOUR BUSINESS:

TOUGH PENALTIES

FINES OF UP TO

4%

OR

**€20
MILLION**

OF ANNUAL
GLOBAL REVENUE



→ €€€€€€

WHICH EVER
IS GREATER

NON-EU COMPANIES

The regulation also applies to **non-EU companies** that process personal data of individuals in the EU.



The **international transfer of data** will continue to be governed under EU GDPR rules.

DEFINITION OF PERSONAL DATA

THE DEFINITION OF PERSONAL DATA IS NOW BROADER AND INCLUDES IDENTIFIERS SUCH AS



GENETIC



MENTAL



CULTURAL



ECONOMIC



SOCIAL
IDENTITY

OBTAINING CONSENT

OBTAINING CONSENT FOR PROCESSING PERSONAL DATA MUST BE CLEAR, AND MUST SEEK AN AFFIRMATIVE RESPONSE.



Data subjects have the Right to be forgotten and **erased from records**



Parental consent is required for the processing of **personal data of children** under age 16



Users may request a copy of personal data in a **portable format**

Controllers must report a data breach no later than

 **72 HOURS**

after becoming aware of the breach, unless the breach has a low risk to the individuals rights

The appointment of a **data protection officer (DPO)** will be mandatory for companies processing high volumes of personal data and good practice for others.



Controllers must have a **legal basis for processing** and collecting personal data.

Data processors can be held **directly liable** for the security of personal data.

Products systems and processes must consider privacy-by-design concepts during development

GDPR IS COMING. WILL YOU BE READY?



Privacy risk impact assessments will be required for projects where privacy risks are high



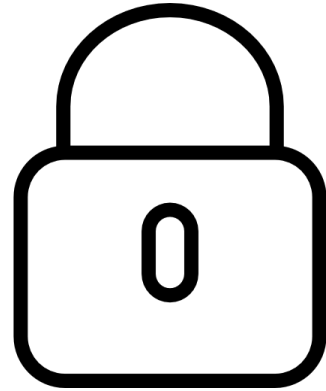
ONE-STOP-SHOP: international companies will only have to deal with one supervisory data protection authority

ISO 27001



ISO 27001 and other certifications will help demonstrate '**adequate technical and organisational measures**' to protect persons data and systems.

GDPR



Take care

Take care

- General guideline
- Workshop
 - **Good** password
- CDD Information Security Policy

General guideline

- 1) Good password
- 2) Two factors authentication
 - 1) 2FA applications
 - 2) 2FA hardware
- 3) Backup
- 4) Awareness



Main sources of being **Hacked !**

- Unpatched / Pirate software
- Trojan horse program
- Responding to FAKE phishing emails
- Weak / Universal Email passwords

12 Signs that you've been **Hacked !**

- 1) Ransom message
- 2) Fake antivirus warnings
- 3) Unwanted browser toolbars
- 4) Redirected Internet searches
- 5) Random popups
- 6) Unintended social media invitation to friends
- 7) Online password is not working

12 Signs that you've been **Hacked !**

- 8) Unexpected software installed
- 9) Mouse pointer moves like a ghost
- 10) Cannot start Antivirus, Task manager, Registry Editor
- 11) Money is missing from Bank account
- 12) Get notification to pay for shipped goods

What to do if Email is **Hacked !**

- 1) Change password
- 2) Let your contacts know
- 3) Change security questions
- 4) Use multi-factor authentication
- 5) Double check “suspicious” email setting (fwd, signature, address book)
- 6) Repeat 1-5) for other associated email accounts
- 7) Scan computers for Malware / Viruses

Workshop : **Good** Password

- 1) Good password necessary ?
- 2) Good password = ?
- 3) Your passwords = Good ?
- 4) How to improve ?

Sign In ×

 Continue With Facebook

 Continue With Google

or with email

Email

Password

Show

☒ Remember me

Sign In

Lab 1: **Good** password is necessary ?

- Database of hacked emails
- Check yourself
 - haveibeenpwned.com

Worst Passwords from 2011 - 2017

	2011	2012	2013	2014	2015	2016	2017
1	password	password	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty
5	abc123	qwerty	abc123	qwerty	12345	football	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789
7	1234567	letmein	111111	1234	football	1234567890	letmein
8	letmein	dragon	1234567	baseball	1234	1234567	1234567
9	trustnot	111111	iloveyou	dragon	1234567	princess	football
10	dragon	baseball	adobe123	football	baseball	1234	iloveyou

Source: <https://www.digitaltrends.com/computing/worst-password-2017-remains-123456/>

Good Password

- Old guideline = c4tlo^eR
- Special characters + Upper case + Numbers
- Long (12 chars) > Complexity
- Uncommon phrase --> *I will always love you*
- Random insert “special characters” in places
- Pick 1st letter from each sentence
- Use “Password manager” software

Why **Good** password ?

Password Length	All Characters	Only Lowercase
3 characters	0.86 seconds	0.02 seconds
4 characters	1.36 minutes	.046 seconds
5 characters	2.15 hours	11.9 seconds
6 characters	8.51 days	5.15 minutes
7 characters	2.21 years	2.23 hours
8 characters	2.10 centuries	2.42 days
9 characters	20 millennia	2.07 months
10 characters	1,899 millennia	4.48 years
11 characters	180,365 millennia	1.16 centuries
12 characters	17,184,705 millennia	3.03 millennia
13 characters	1,627,797,068 millennia	78.7 millennia
14 characters	154,640,721,434 millennia	2,046 millennia

Good Password practices

- Use 2-factors authentication
- Add recovery phone or email
- Never “reuse” password --> Yahoo
- Do not “remember my password” in browser
- STOP using “security questions”, or use FAKE answer
- **STOP changing passwords every 90 days ?**

Lab 2: How **Good** is my password ?

- Test “concept”
- Website = How secure is my password

HOW SECURE IS MY PASSWORD?

ENTER PASSWORD

Lab 3: How to improve my password ?

- Test “concept”
- Password meters = cups.cs.cmu.edu/meter

Create Your Password

Username

Password

Show Password ☐

Continue

Don't reuse a password from another account! [\(Why?\)](#)

Your password must:

☐ Contain 8+ characters

[How to make strong passwords](#)

Creating a password

cabbage

Sorry, the password must be more than 8 characters.

boiled cabbage

Sorry, the password must contain 1 numerical character.

1 boiled cabbage

Sorry, the password cannot have blank spaces.

50fuckingboiledcabbages

Sorry, the password must contain at least one upper case character.

50FUCKINGboiledcabbages

Sorry, the password cannot use more than one upper case character consecutively.

50FuckingBoiledCabbagesShovedUpYourArse.IfYouDo
n'tGiveMeAccessImmediately

Sorry, the password cannot contain punctuation.

NowIAmGettingReallyPissedOff50FuckingBoiledCabbag
esShovedUpYourArselfYou
DontGiveMeAccessImmediately

Sorry, that password is already in use!

CDD Information Security Policy

- ***NO*** Heavy download during “Conference”
 - Bit torrent
 - Streaming (both up / down)
 - Software update
- EMAIL ***@mail.cdd.go.th***
- Antivirus on ***EVERY*** computers



Thank you