Cybersecurity Landscape of Healthcare in 2022 and Preparation for 2023

醫療保健業的網絡安全展望 2022 及迎接 2023

Fuller Yu

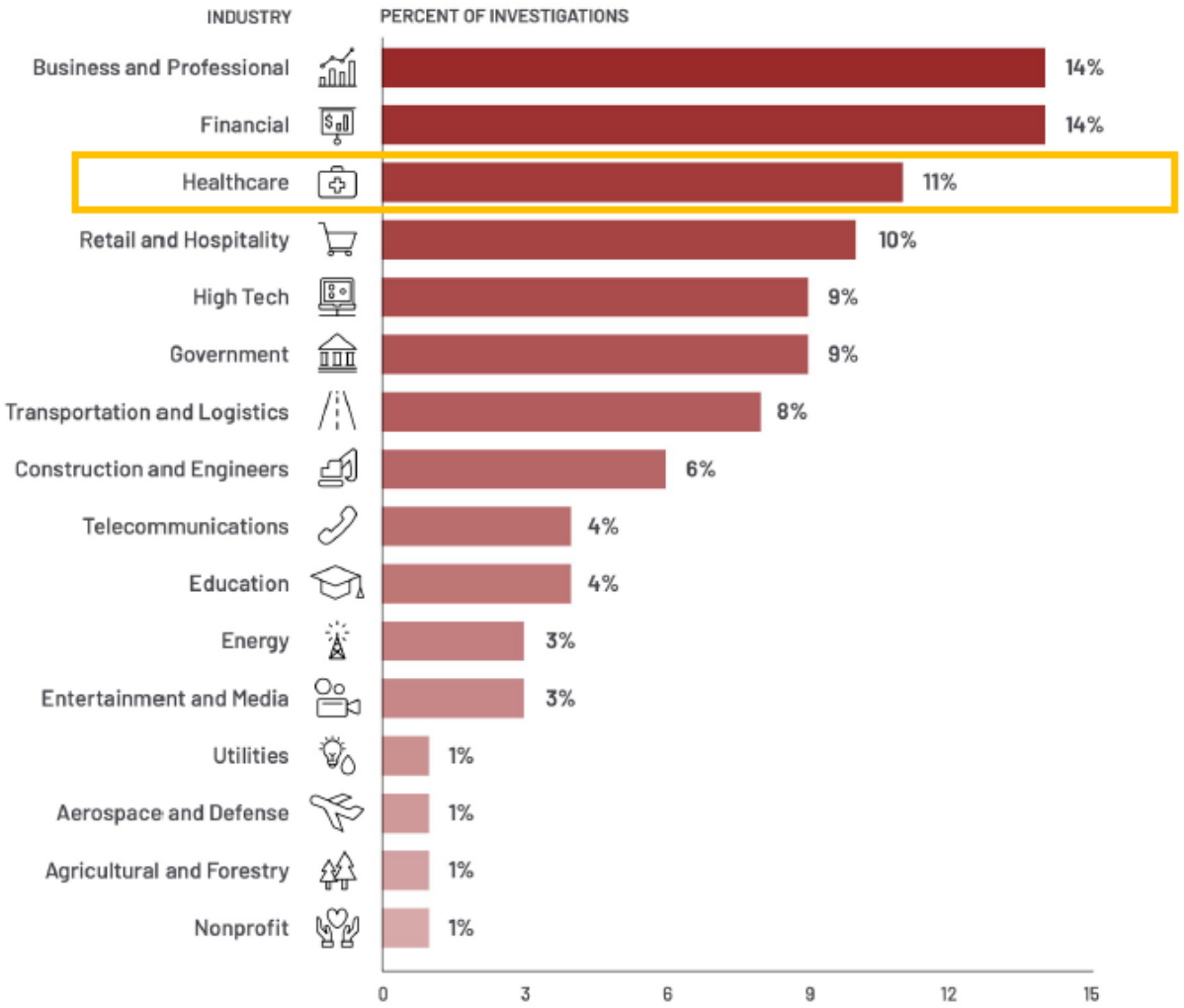
Chief Information Security Officer (CISO), Hospital Authority
Co-Chair of Cyber Security Work Stream, Global Digital Health Partnership
Ex-Co Member of Cybersecurity Specialist Group, HK Computer Society

October 2022


The Cyber Landscape in 2022

Healthcare is one of top 3 most attacked industries globally

Which Industries Are Under Attack?



IT&HI

Ransomware Attacks are prevailing in HK

Over 750,000 ransomware attacks HK firms monthly

Ransomwares like Revil and TrickBot were the usual suspect.

More than 750,000 ransomware attacked organisations in Hong Kong every month on average between April and June 2021, cybersecurity firm, Fortinet, reported.

冒名發欺詐電郵 稅務局籲勿開啟已交警方調查

2022-06-06 19:18 列印 文字大小

稅務局呼籲市民留意聲稱由該局發出一封標題為「Your Annual Tax Refund Is Ready」的欺詐電郵。資料圖片

資安 · 私隱 Biz.IT

思科：港企近七成受勒索軟件攻擊　將夥香港警察守網者推自我檢測

2022-09-06 | Updated: 2022-09-07 分享

hket 香港經濟日報

32°C 香港時間：2022年9月26日 (週一) 16:28 昔日新聞

熱門關鍵字： ATMX 新經濟股 收息 騰訊 阿里巴巴 滙豐 上車盤 退休規劃 專題: 退

即時新聞 財經 理財 科技 中國 國際 商業 回歸25周年 大灣區

【網絡威脅】如何提升終端保安　應對涵蓋勒索軟件的網絡威脅

科技 09:00 2022/08/15 讚好 0

另外，2021年首三季的香港勒索軟件攻擊數量已超越2020年全年，達到等同該年數字的105%。同年亦約有38%經分析的數據外洩事故由勒索軟件引起，數字較2020年上升3%。由此可見，勒索軟件早已遍佈全球，成為不可忽視的網絡威脅。

A Typical Infection Chain of a Ransomware Attack

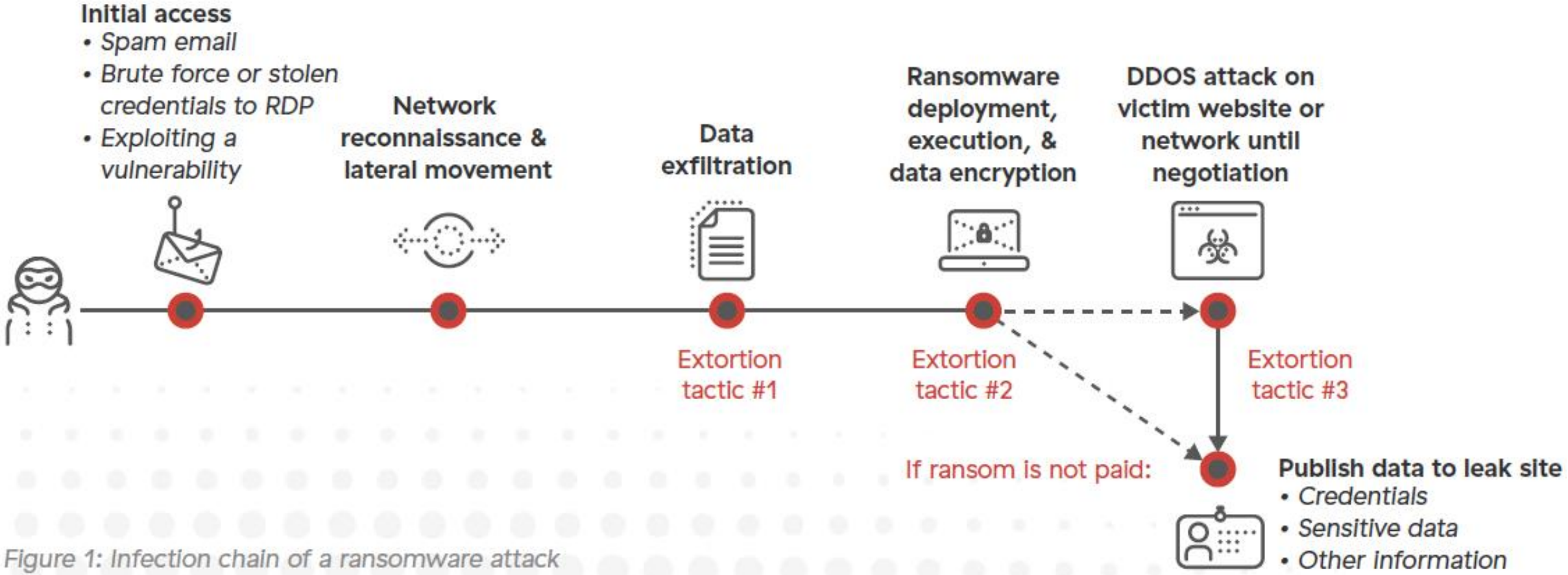
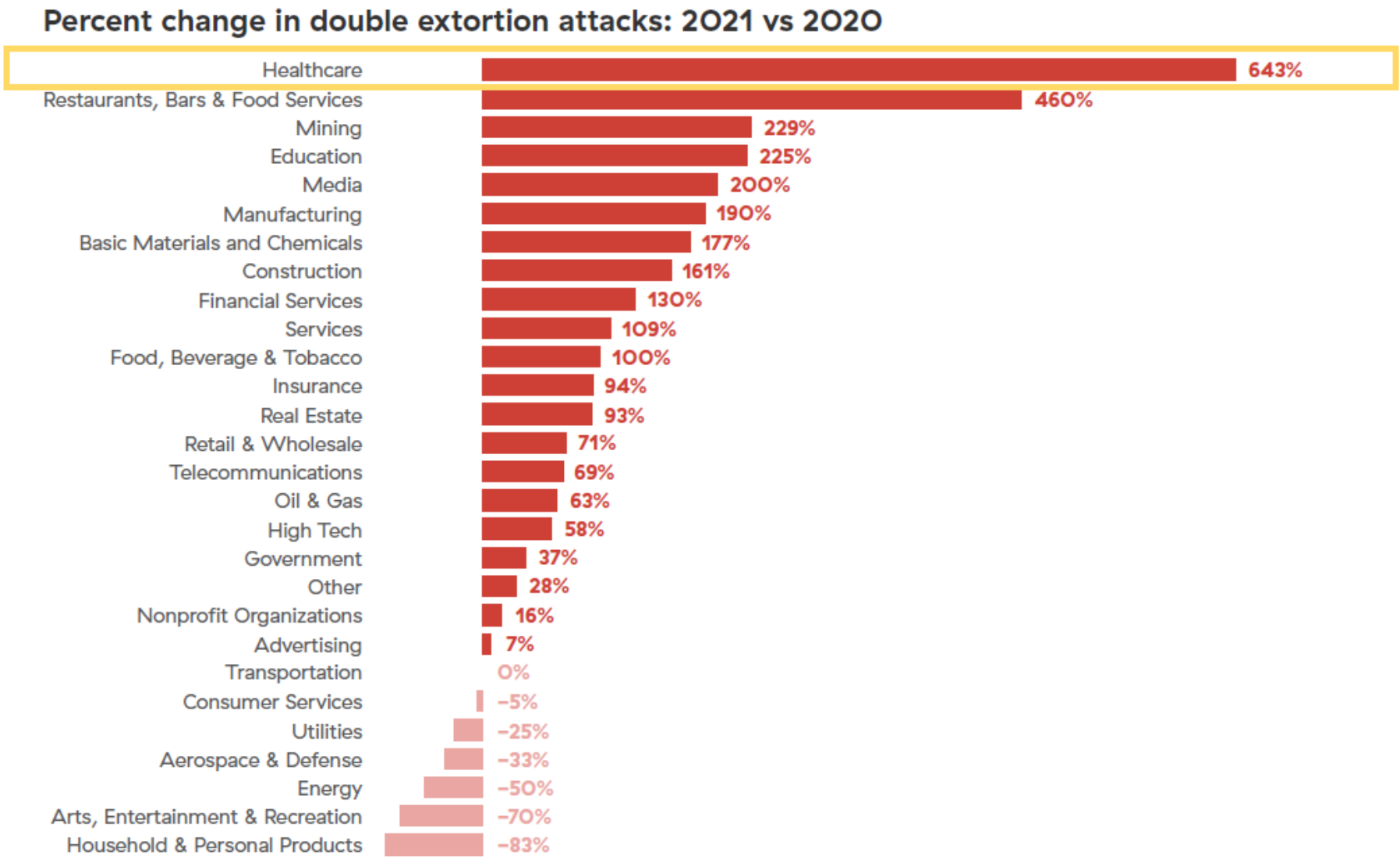


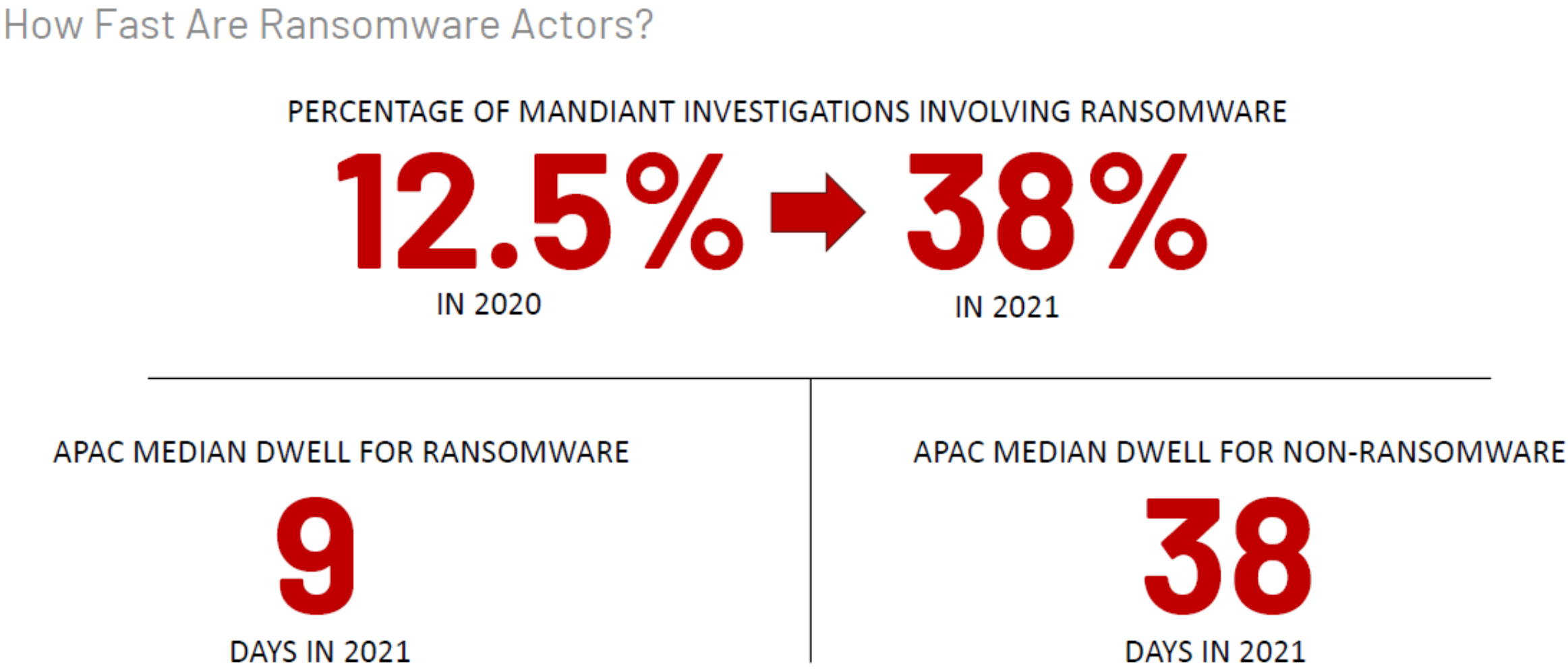
Figure 1: Infection chain of a ransomware attack

Healthcare suffered double extortion attacks the most



IT&HI

Ransomware attacks are more and quicker



Dwell time is the length of time between initial intrusion and detection of an intrusion

IT&HI

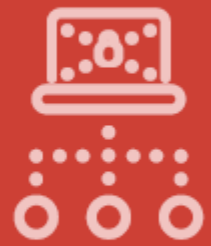
Why Ransomware is so attractive to the cyber criminals?

Supply chain attacks

that exploit trusted vendor relationships to breach organizations and multiply the damage of attacks by enabling threat actors to hit multiple (sometimes hundreds or thousands) of victims at the same time.

Ransomware as a service

that uses affiliate networks to distribute ransomware on a wide scale, allowing hackers who are experts in breaching networks to share profits with the most advanced ransomware groups.

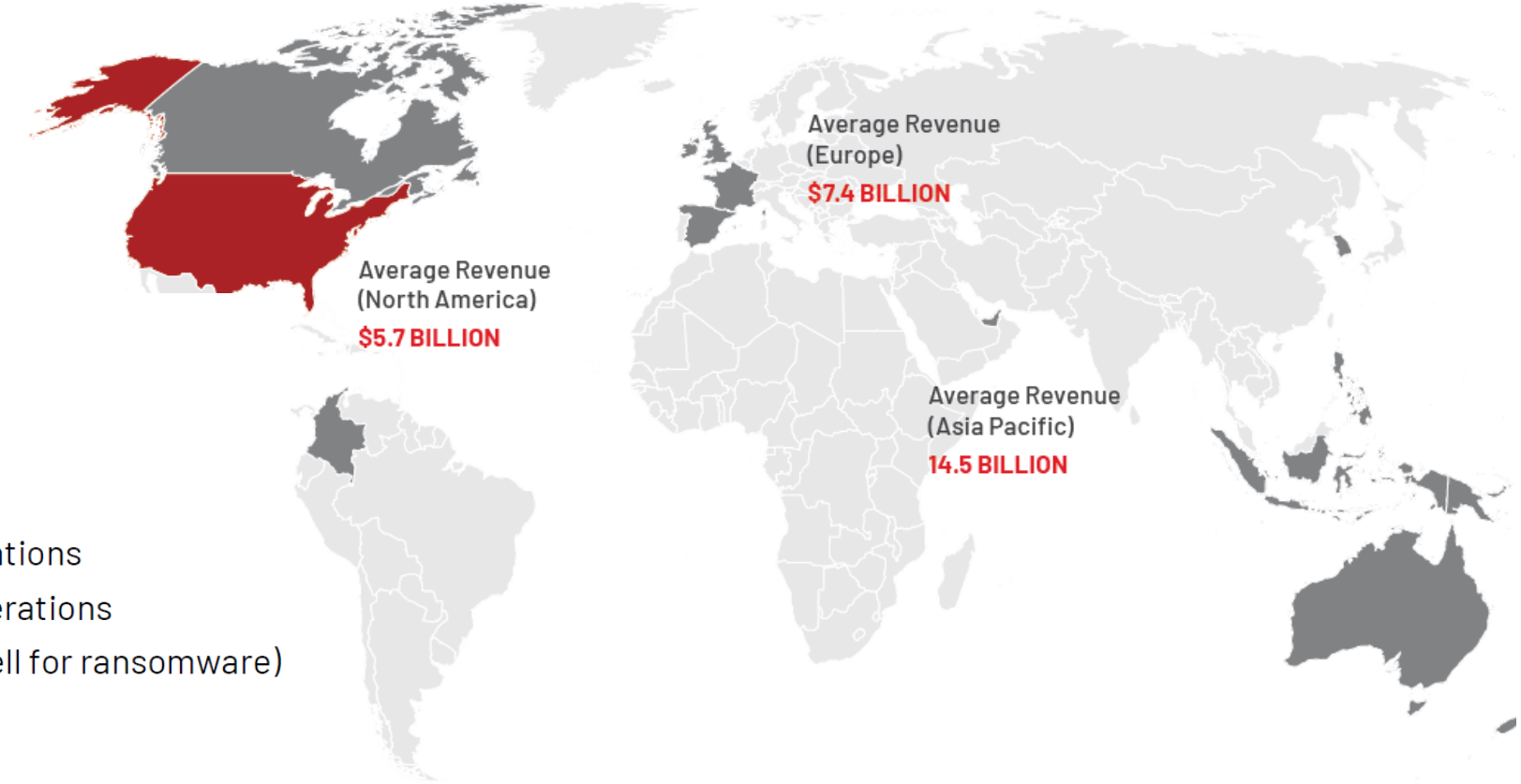


Multiple-extortion attacks

that utilize data theft, distributed denial of service (DDoS) attacks, customer communications, and more as layered extortion tactics to increase ransom payouts.

FIN12 RYUK Ransomware

FIN12 VICTIMOLOGY OVERVIEW



FIN12

Who is FIN12?

Attacking : Since At least 2018

Aligned to : RYUK Ransomware

Volume : 20% of Mandiant's Ransomware Investigations

Notable : Prioritizes on Speed, lacks data theft operations

Median Dwell Time : <2 Days (vs 5-day average dwell for ransomware)

Targets: Healthcare is one of the target industries

PRIVATE SECTOR 83%

PUBLIC SECTOR 17%

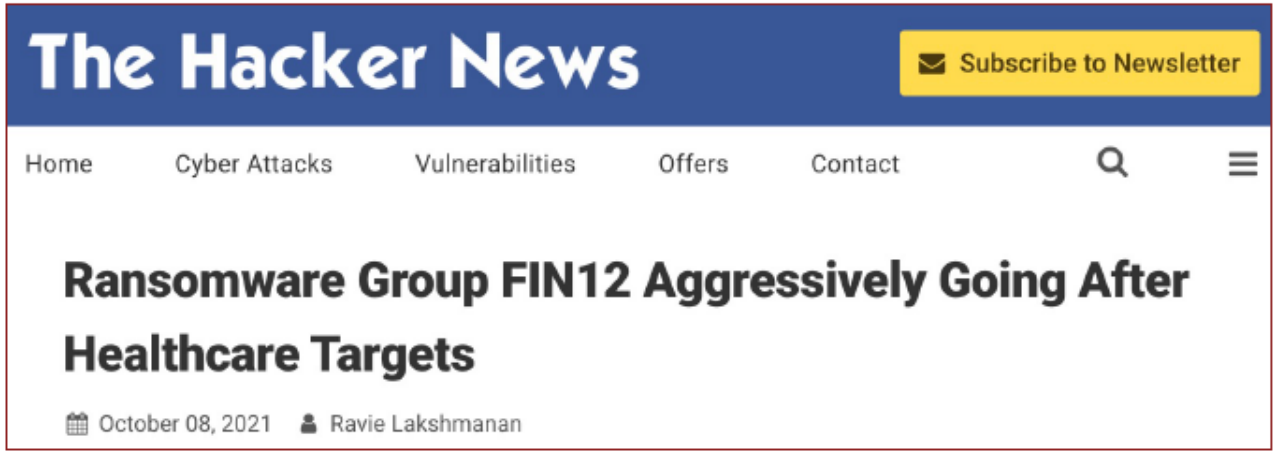
MOST FREQUENTLY TARGETED INDUSTRIES

- HEALTHCARE
- MANUFACTURING
- EDUCATION
- TECHNOLOGY
- FINANCIAL

IT&HI

FIN12 is targeting Healthcare Industry

Who is FIN12?



2022-2023 Predictions on Cyber Landscape

- Ransomware as a service will continue to increase
- Changing ransomware models will lead to changing targets
- Dwell time will continue to decrease
- Supply chain attacks will increase as adversaries compromise partner and supplier ecosystems
- Ransomware will be used as a wiper to destroy data in the increasing geopolitical tensions

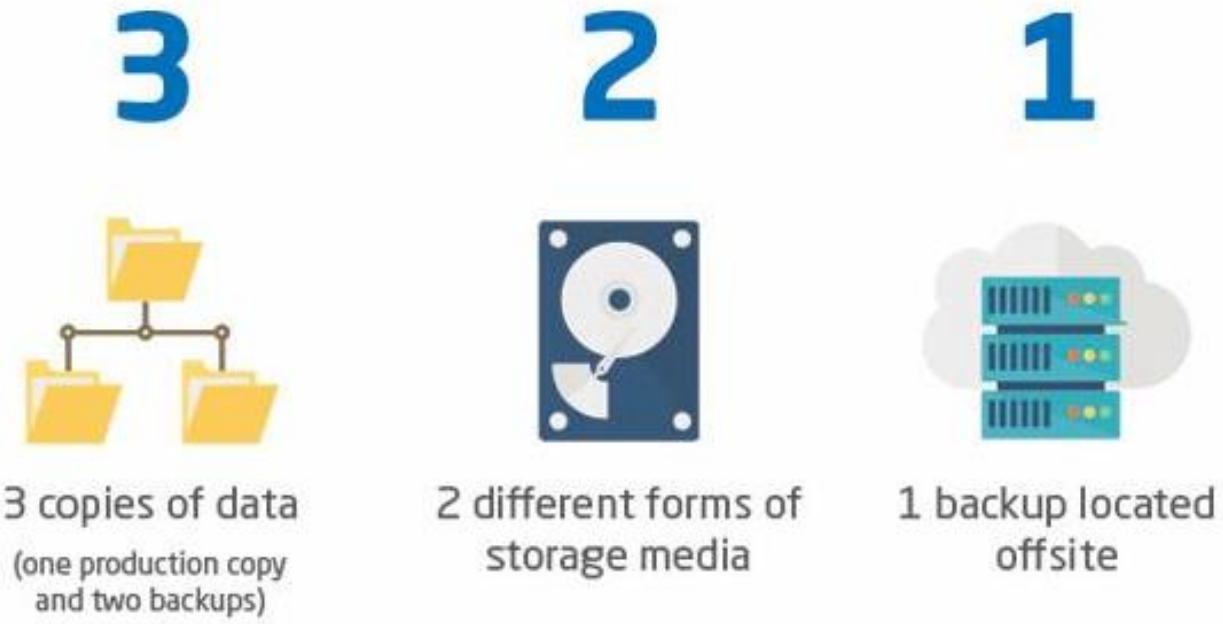
Prepare for 2023

Get the basic right to avoid being low hanging fruit

Source: HKCert.org

Prepare for the worst – Backup, Backup, and Backup

- Implement 3-2-1 Backup Strategy
- 3 copies on 2 different media with 1 at offsite
- Restore your backup regular to ensure it is working
- Establish, test and update the recovery plan with business and users



IT&HI

90% of all cyber attacks begin with a phishing email

Tips to Spot Phishing Email 網路釣魚 全攻略

Tips to spot Phishing Email 網路釣魚 全攻略

Greed
邊有咁大隻
蛤蜊隨街跳

Urgency
十萬火急
幫緊你

Curiosity
開心些牙

Fear
怯 你就輸成世

Greed 邊有咁大隻蛤蟆隨街跳

Greed 邊有咁大隻蛤蜊隨街跳

CONGRATULATIONS!!

Your Email was selected in Powerball Lottery Draw with the sum of 1.5million dollars. Kindly send your Full Name, Address and Phone Number for claims.

Yours Sincerely
Mr. James Hodges
Head Of Operations

BETTER PART TIME JOB OFFER FOR STUDENT AND STAFF

Avila Rebecca <avilaword7272@gmail.com>
to Susanhancock002

Hello,

Would you love to work as a Mystery Shopper in your location for $400? Your job is to sit down at service tables. Pay is $400 per assignment, and each assignment requires 20-30 minutes of your time at a store plus time to write up your post visit reports. CliKk the link below for registration:
https://form.myjotform.com/82564185981569

Regards
susanhancock
Richfeild Evaluation Co.

Urgency 十萬火急 幫緊你

Urgency 十萬火急 幫緊你

DHL Express,

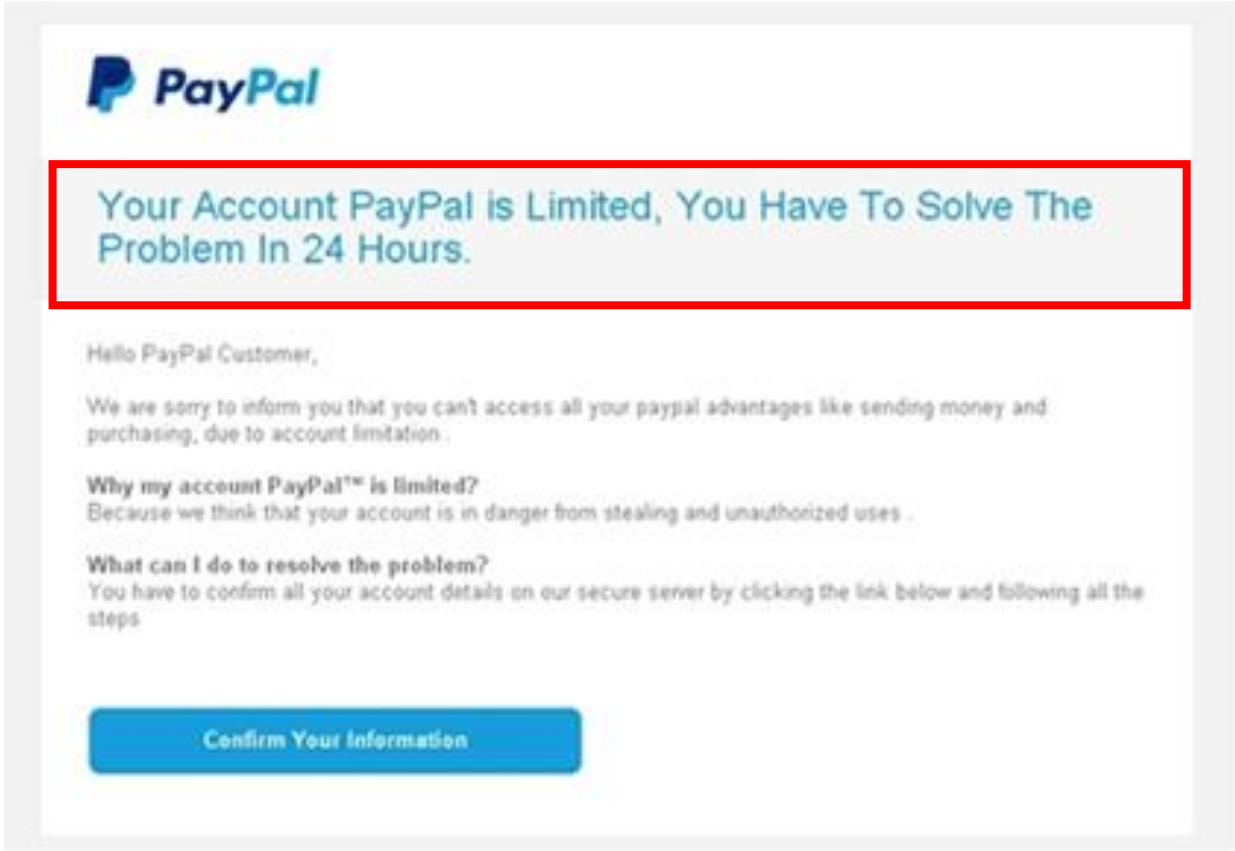
Dear Customer,

you have a package pending delivery in Terminal 1! due to the unpaid shipping cost.

Please complete the shipping transaction

Confirm the payment 2.99 AUD of the shipment to be able to deliver it

Note: the package will be returned within 48 hours if no action has been taken.



Fear 怯 你就輸成世

Fear 怯 你就輸成世

From

Subject: **Your devices have been hacked! including this account:** 16/4/20, 4:38 am

To

Hi, stranger!

I hacked your device, because I sent you this message from your account.
If you have already changed your password, my malware will be intercepts it every time.

You may not know me, and you are most likely wondering why you are receiving this email, right?
In fact, I posted a malicious program on adults (pornography) of some websites, and you know that you visited these websites to enjoy
(you know what I mean).

While you were watching video clips,
my trojan started working as a RDP (remote desktop) with a keylogger that gave me access to your screen as well as a webcam.

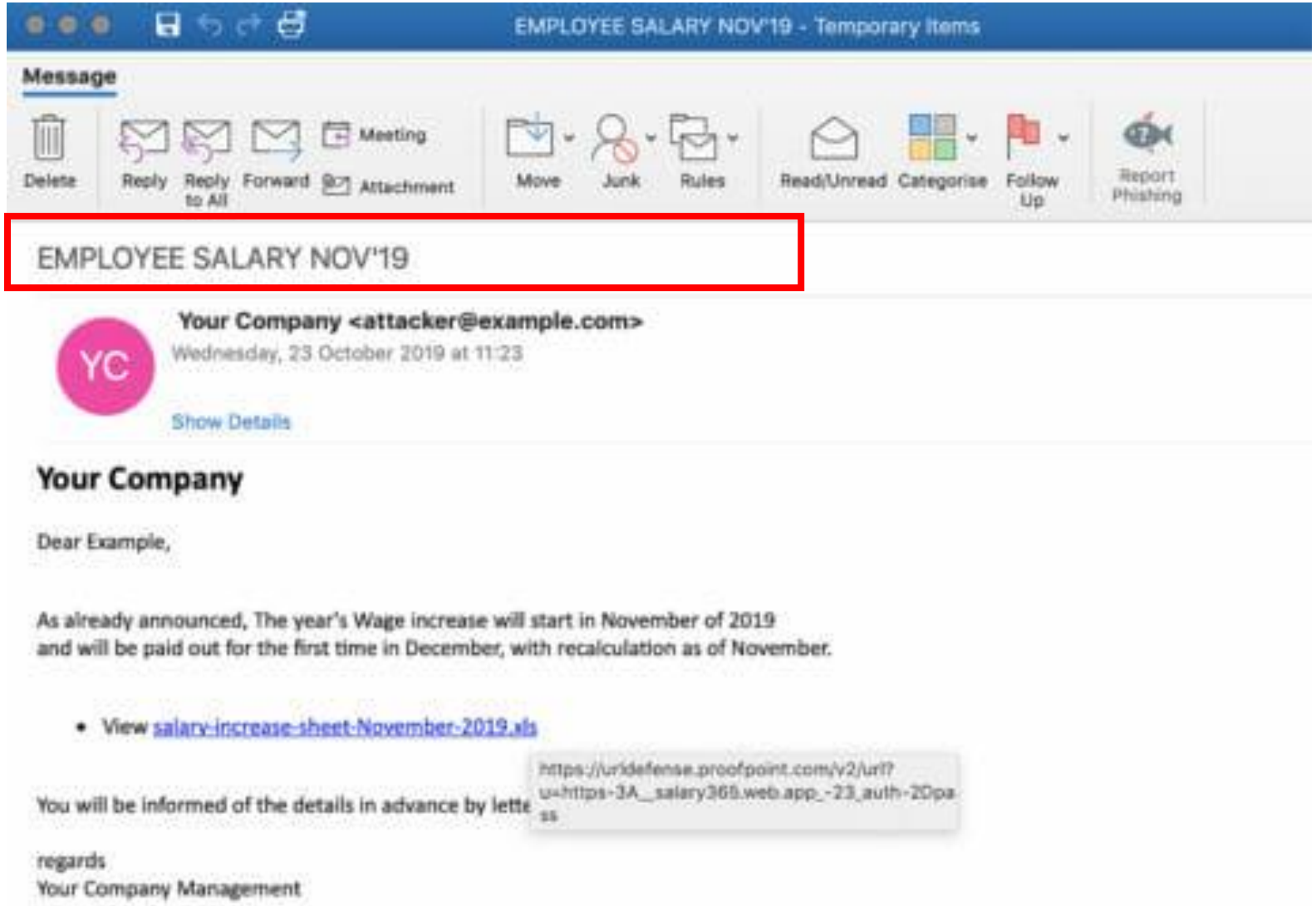
Immediately after this, my program gathered all your contacts from messenger, social networks, and also by e-mail.

What I've done?
I made a double screen video.
The first part shows the video you watched (you have good taste, yes ... but strange for me and other normal people),
and the second part shows the recording of your webcam.

IT&HI

Curiosity 開心些牙

Curiosity 開心些牙



Tips to spot Phishing Email 網路釣魚 全攻略

Greed
邊有咁大隻
蛤蜊隨街跳

Urgency
十萬火急
幫緊你

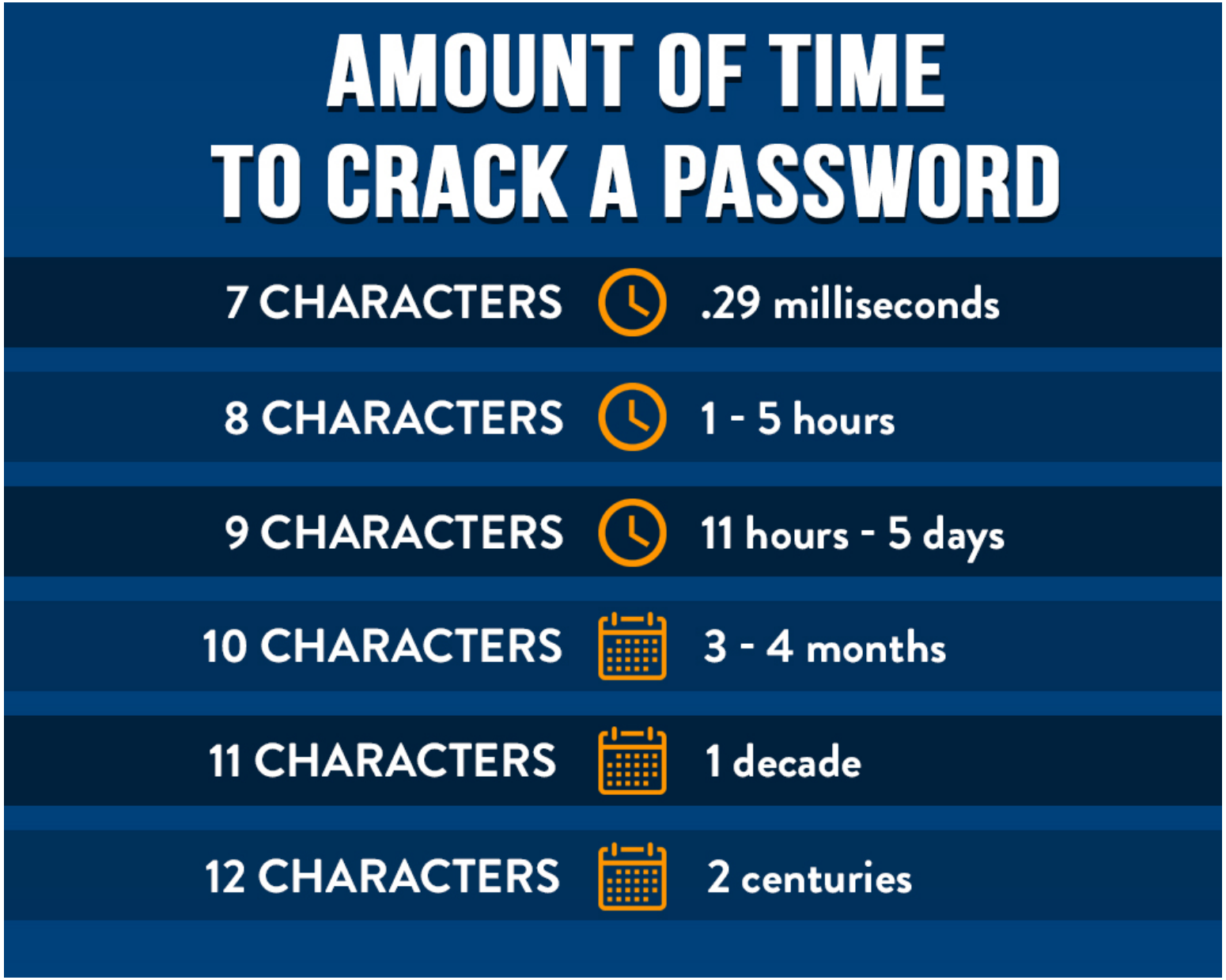
Curiosity
開心些牙

Fear
怯 你就輸成世

Don't click when in doubt – 6-sec Rule

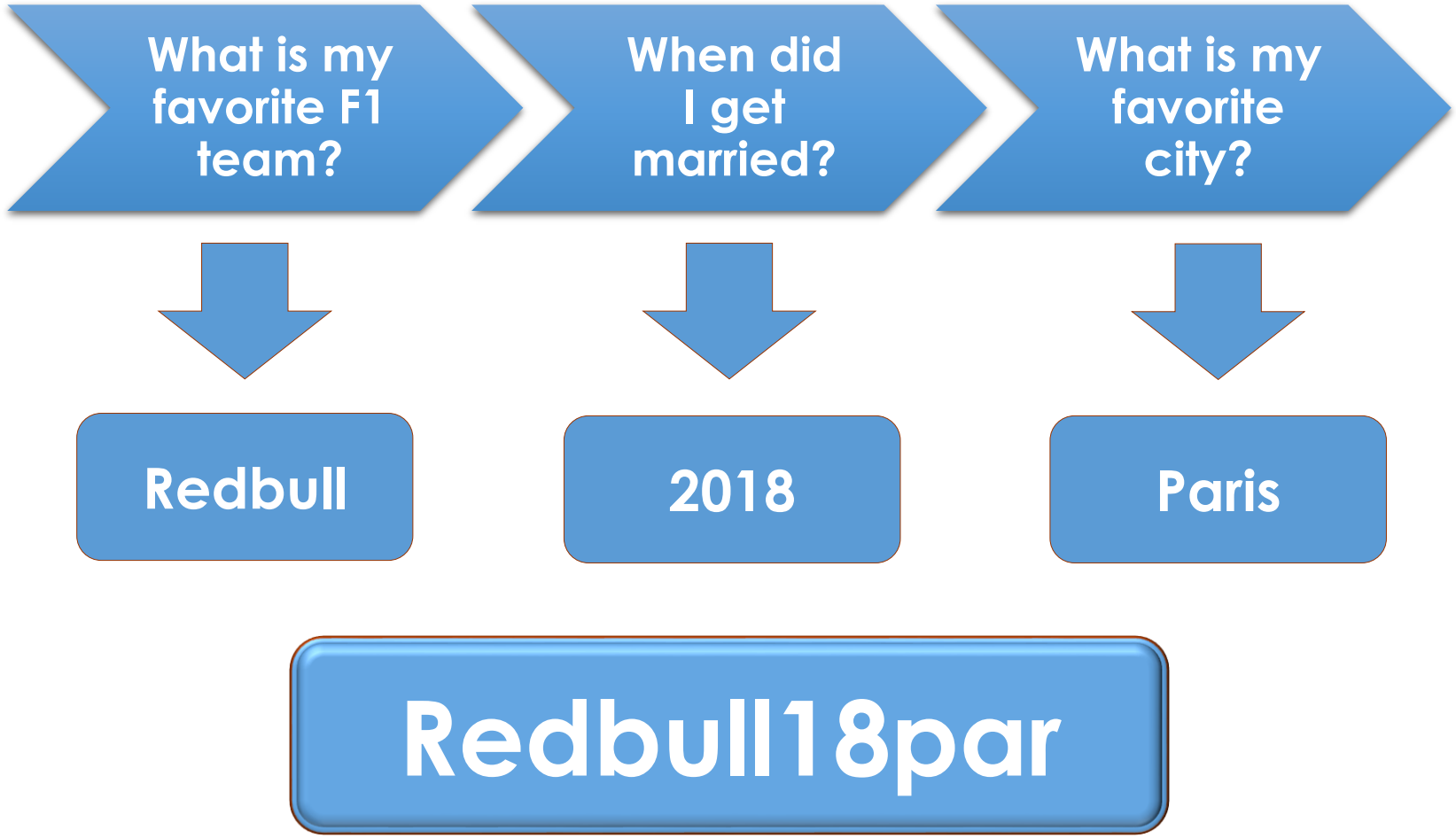
- Waiting for 6 seconds for your clear brain, then ask yourself
- What is the email trying to get me to do?
- How is it trying to get me to do it?

Strong Password 強化密碼 全攻略


AMOUNT OF TIME
TO CRACK A PASSWORD
7 CHARACTERS
.29 milliseconds
8 CHARACTERS
1 - 5 hours
9 CHARACTERS
11 hours - 5 days
10 CHARACTERS
3 - 4 months
11 CHARACTERS
1 decade
12 CHARACTERS
2 centuries

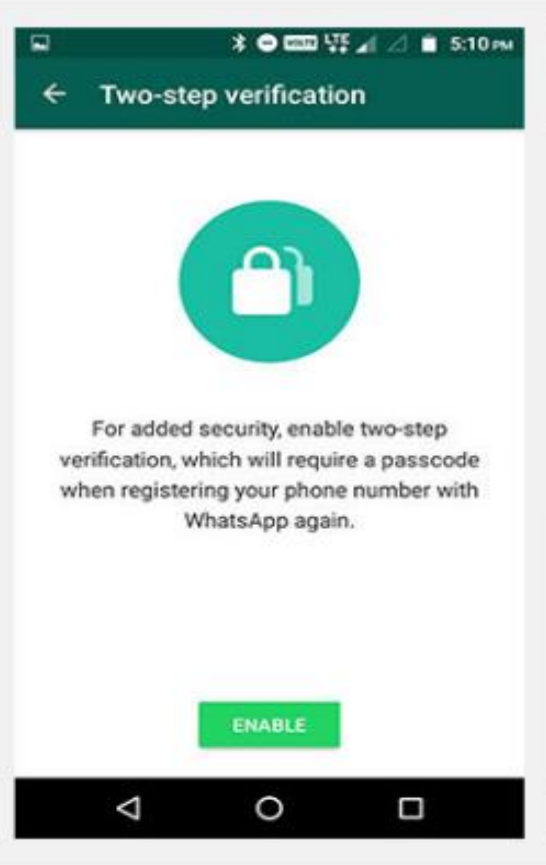
Create a Strong but East-to-remember Password

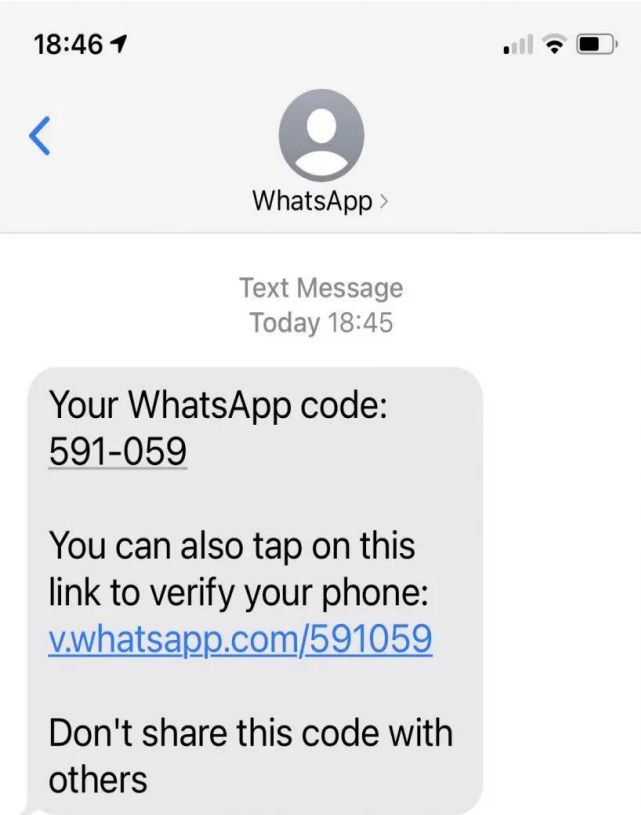
Think a few personal questions which only can be answered by YOURSELF

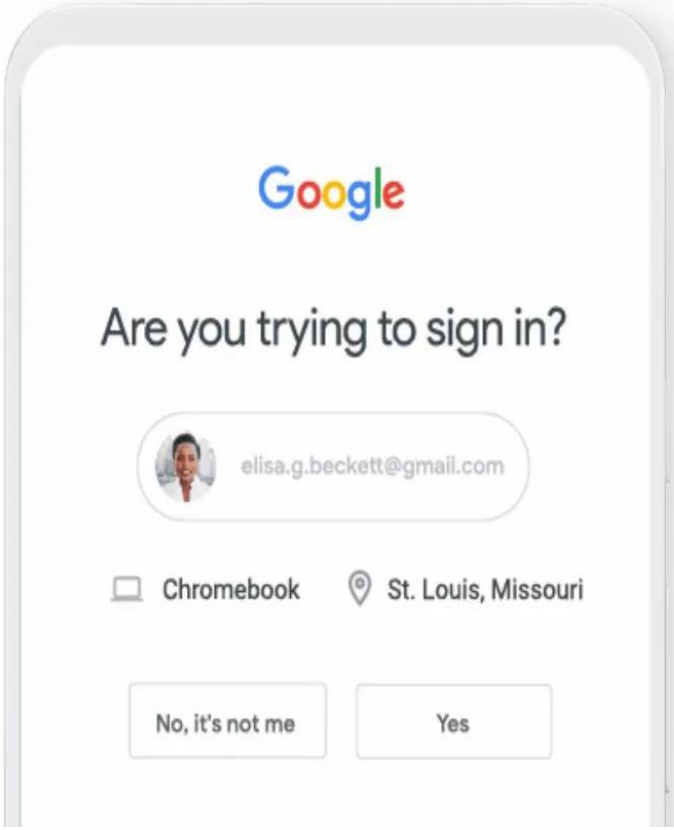


Enable 2-Factor Authentication

… and never disclose your OTP to anyone!







OTP is One Time Passcode

IT&HI

Collaboration with your trusted partners

Health Bureau
The Government of the Hong Kong Special Administrative Region of the People's Republic of China

香港警務處
網絡安全及科技罪案調查科
Hong Kong Police Force
Cyber Security and Technology Crime Bureau

香港個人資料私隱專員公署
Office of the Privacy Commissioner for Personal Data, Hong Kong

醫院管理局
HOSPITAL AUTHORITY

醫健通
ehealth
香港特別行政區政府 HKSAR GOVT

Thank you!