Latest Cyber Security Threats & Trends

The Ways To Deal With Them

Summm CHAN | Security Consultant | September 2019

Agenda

- Latest Cyber Security Threats & Trends
- Cyber Attack & Defense
- Security Incidents Handling
- Security Advice Round Up

About Us

Hong Kong Computer Emergency Response Team Coordination Centre (香港電腦保安事故協調中心)

Mission:
As the **Centre for coordination** of computer security incident response for local enterprises and Internet Users, and the **International Point-of-Contact**

- Founded in 2001
- Funded by Government
- Operated by Hong Kong Productivity Council

asd

Website: www.hkcert.org
24-hour Hotline: 8105 6060
Email: hkcert@hkcert.org

HKCERT services

01 Security Alert Monitoring and Early Warning

02 Report and Response

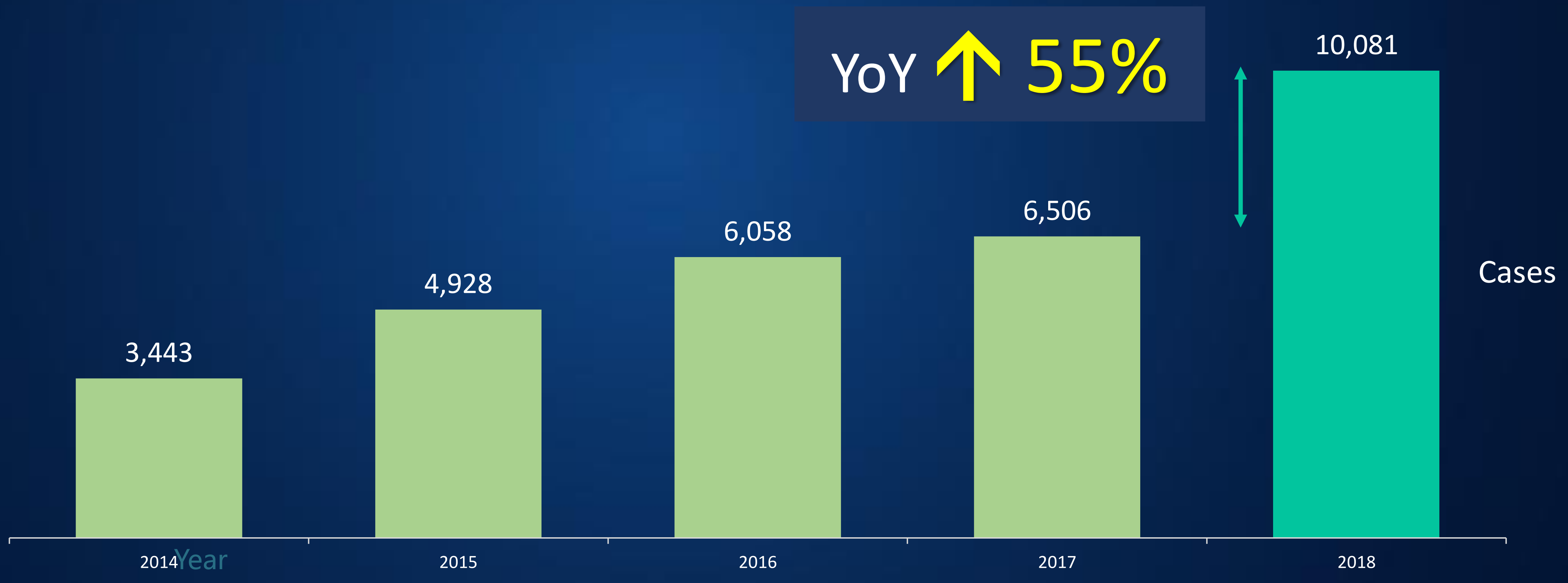
03 Publication of Security Guidelines and Informatior

04 Promotion of Information Security Awareness

Cyber Security

Threats & Trends

Summary of HKCERT Security Incident Reports



YoY ↑ 55%

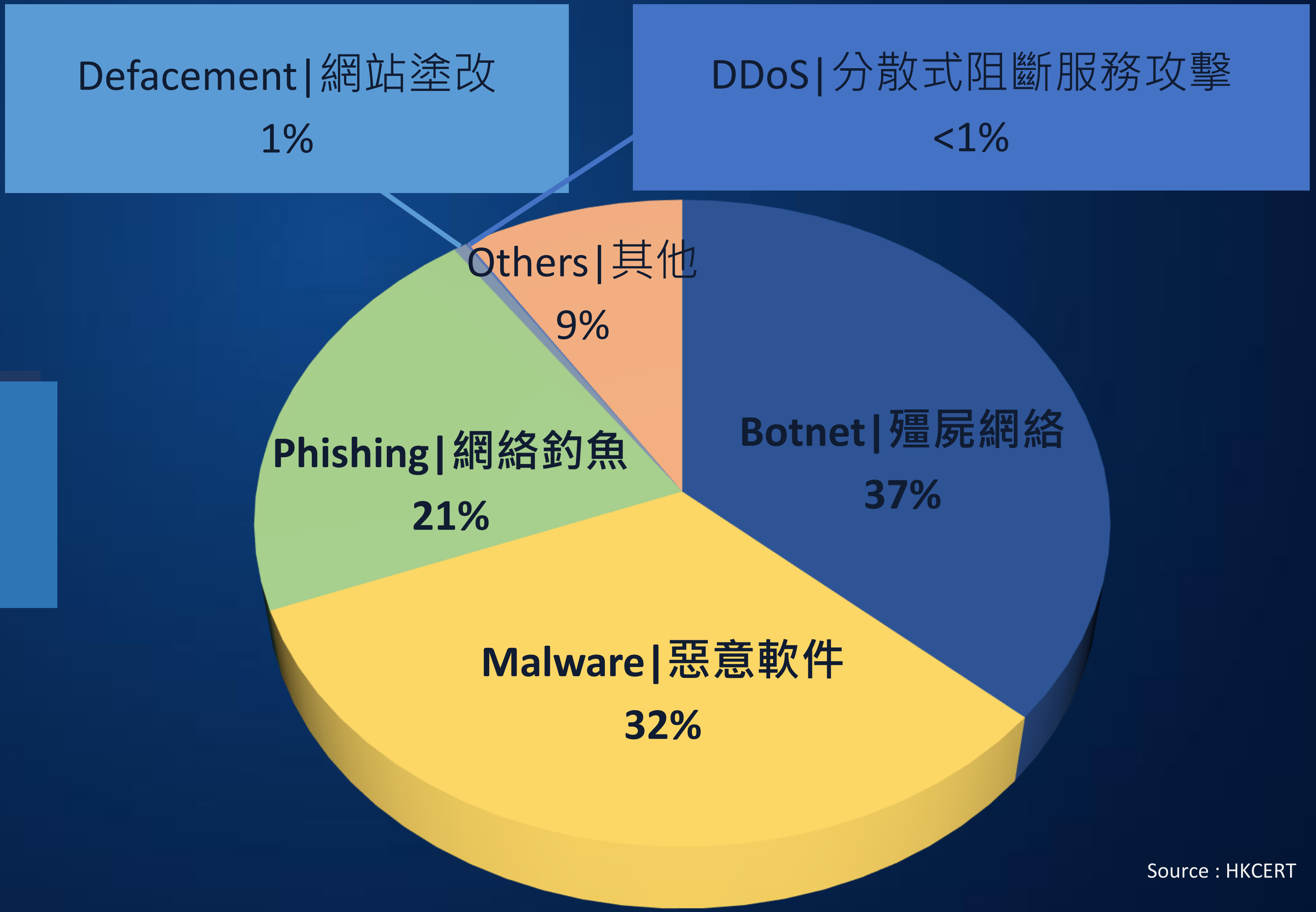
Referred case contributed 95%

Source 來源: HKCERT

Summary of HKCERT Security Incident Reports

Total

↑ 55%



Source : HKCERT

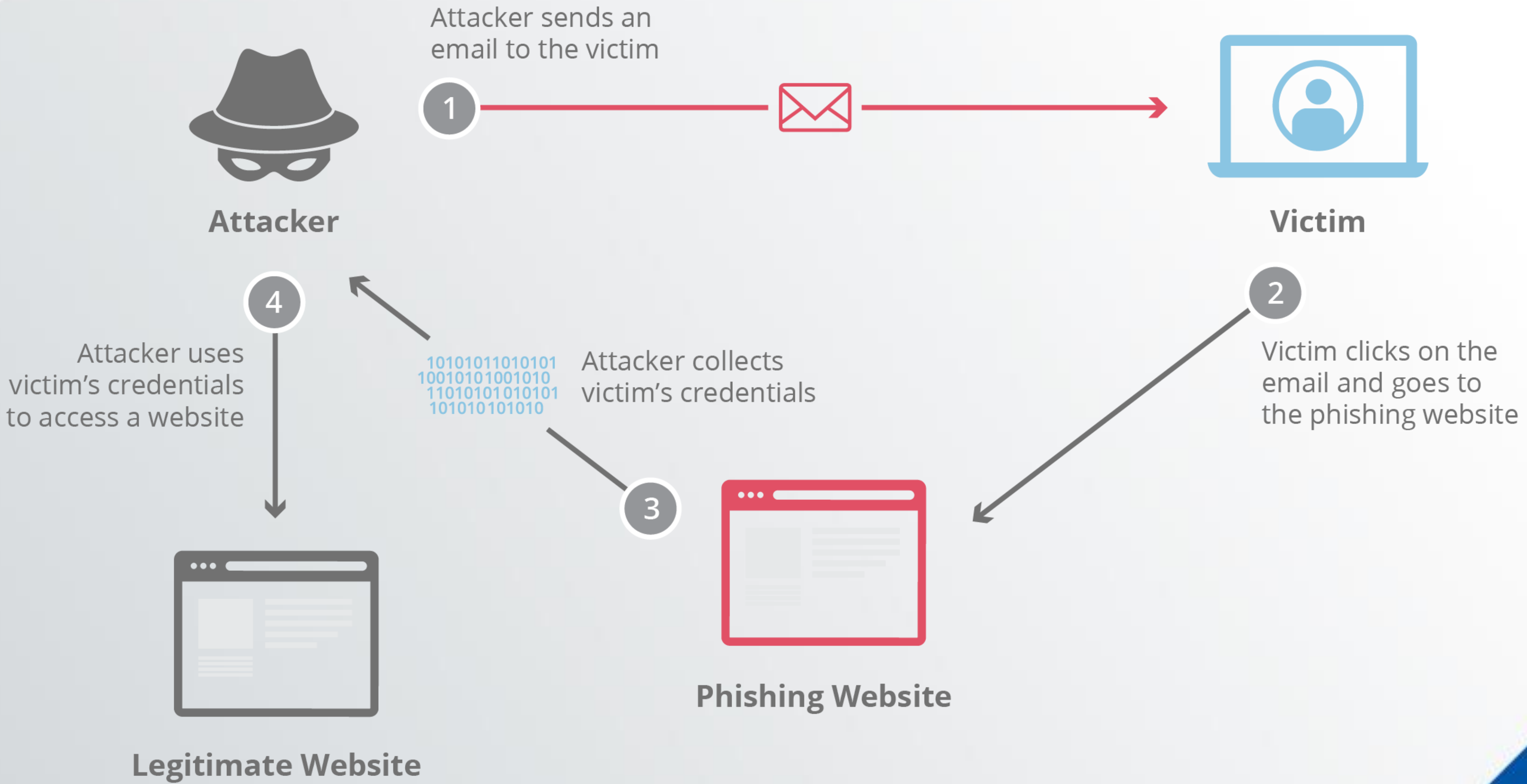
Cyber Attack & Defense

#Cyber_Attacks

Image credit: **https://economictimes.indiatimes.com/tech/internet/69-indian-firms-face-serious-cyber-attack-risk-study/articleshow/69305216.cms**

1
Phishing

What is Phishing?



Attacker sends an email to the victim

Attacker

Victim

Victim clicks on the email and goes to the phishing website

Attacker collects victim's credentials

Attacker uses victim's credentials to access a website

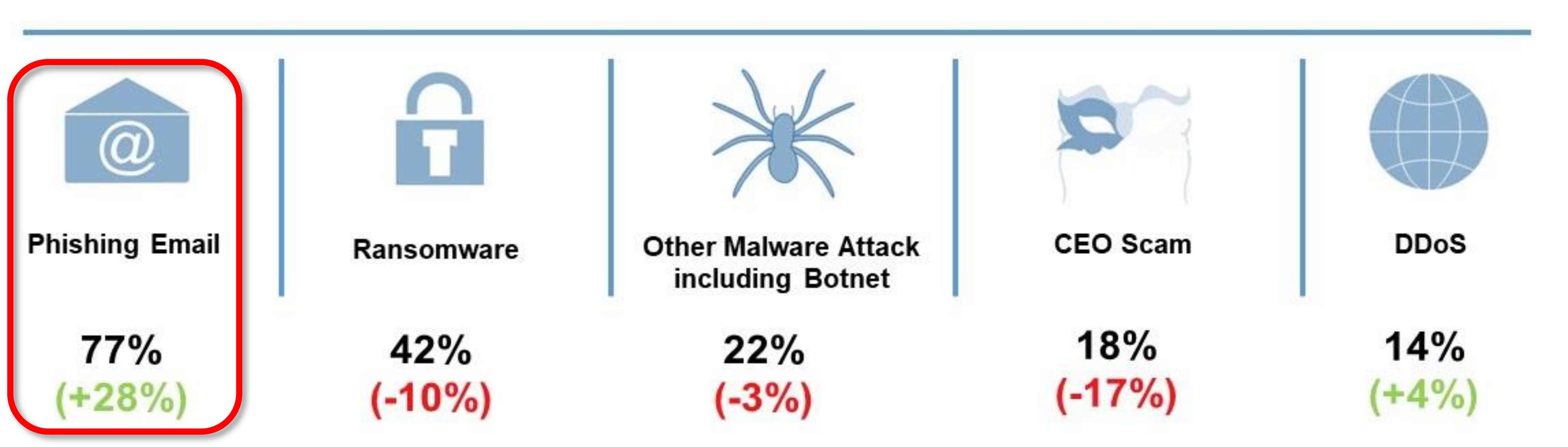
Phishing Website

Legitimate Website

Cyber Security Incidents of Enterprises in Past 12 Months (2019-03)

350 Large Enterprises and SMEs interviewed

Top 5 External Attacks



Phishing Email	Ransomware	Other Malware Attack including Botnet	CEO Scam	DDoS
77%	42%	22%	18%	14%
(+28%)	(-10%)	(-3%)	(-17%)	(+4%)

Source: **SSH Hong Kong Enterprise Cyber Security Readiness Index Survey 2019, HKPC**

Cyber Security Incidents of Enterprises in Past 12 Months (2019-03)

Industries Most affected by Island Hopping

Finance	Manufacturing	Retail	Healthcare
47%	42%	32%	21%

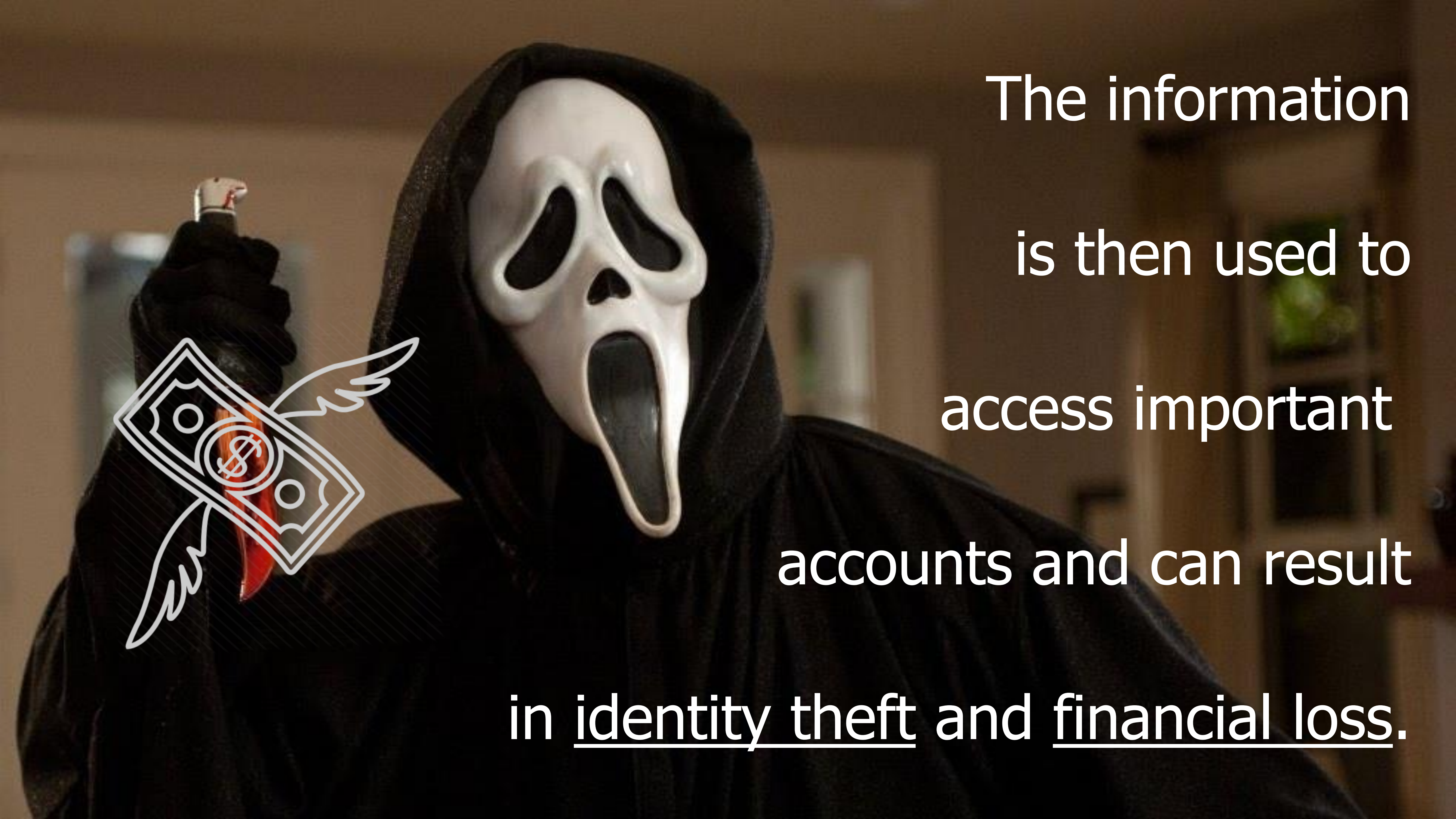
- Hop to connected network (enterprise internal) – lateral movement
- Reverse Business Email Compromise – take over mail server (enterprise internal)
- Website waterhole (trap customers)

Source: **Global Incident Response Threat Report, 2019-Q1, Carbon Black**

PHISHING . . . .

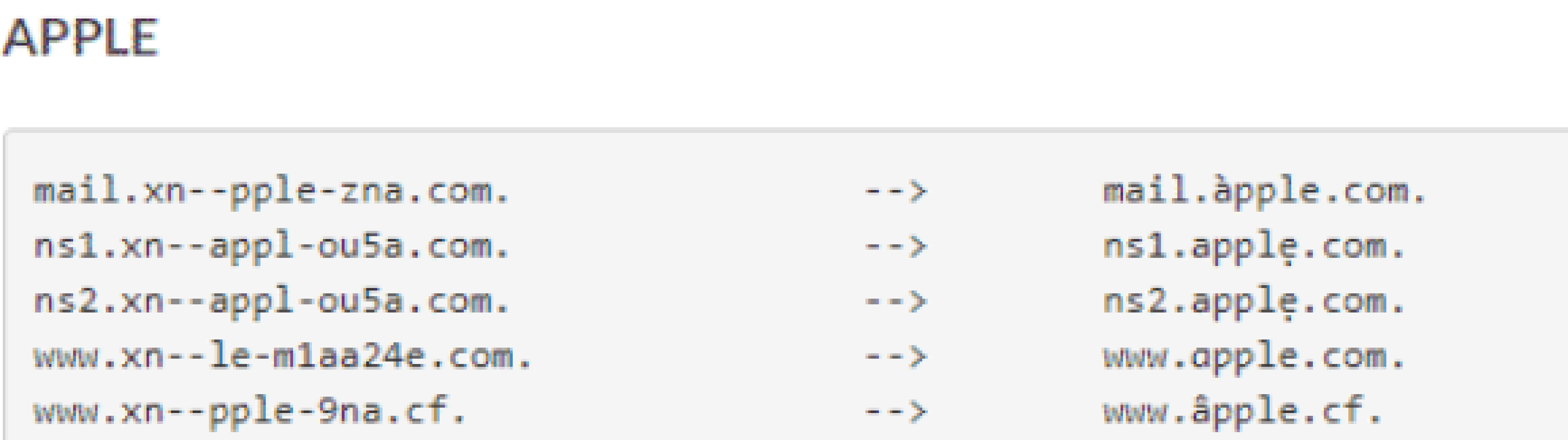
the begin of a cyber attack story

Image credit: **https://people.com/celebrity/beauty-and-the-beast-live-action-movie-with-emma-watson-all-about-disney-film/**



The information is then used to access important accounts and can result in identity theft and financial loss.

Phishing Tactics: New Developments (1)

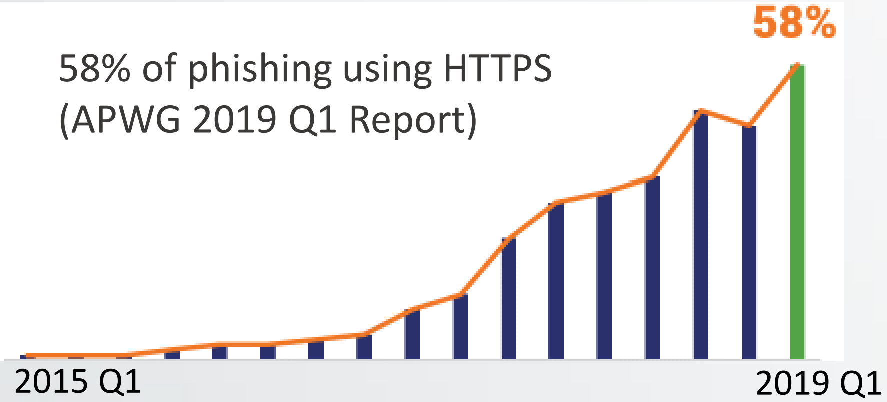


APPLE

```
mail.xn--pple-zna.com.          -->       mail.àpple.com.
ns1.xn--appl-ou5a.com.          -->       ns1.applẹ.com.
ns2.xn--appl-ou5a.com.          -->       ns2.applẹ.com.
www.xn--le-m1aa24e.com.         -->       www.аррle.com.
www.xn--pple-9na.cf.            -->       www.âpple.cf.
```

- **Use of HTTPS**

Let's Encrypt



58% of phishing using HTTPS
(APWG 2019 Q1 Report)

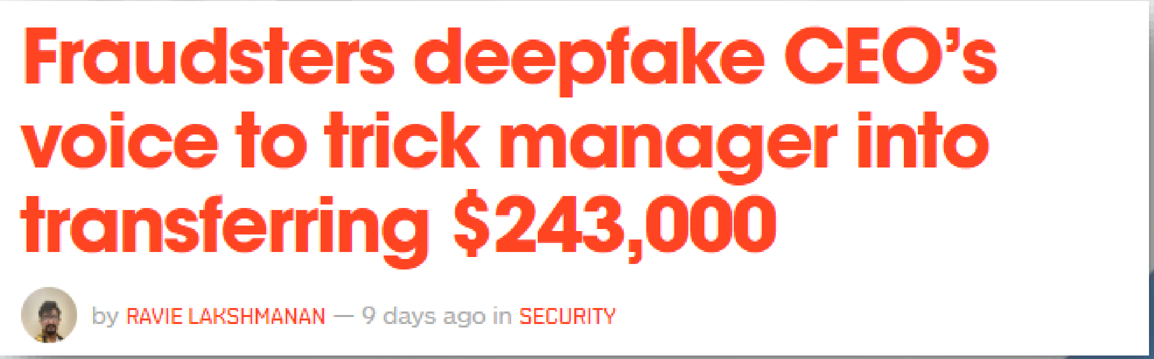
Phishing Tactics: New Developments (2)

Multi-level Social Engineering

- Attacker created a post in LinkedIn and built trust on the post with comments and dialogue with the “friends” for some time.
- Attacker sent email to victim with reference to the post

Evade spam filter by using image

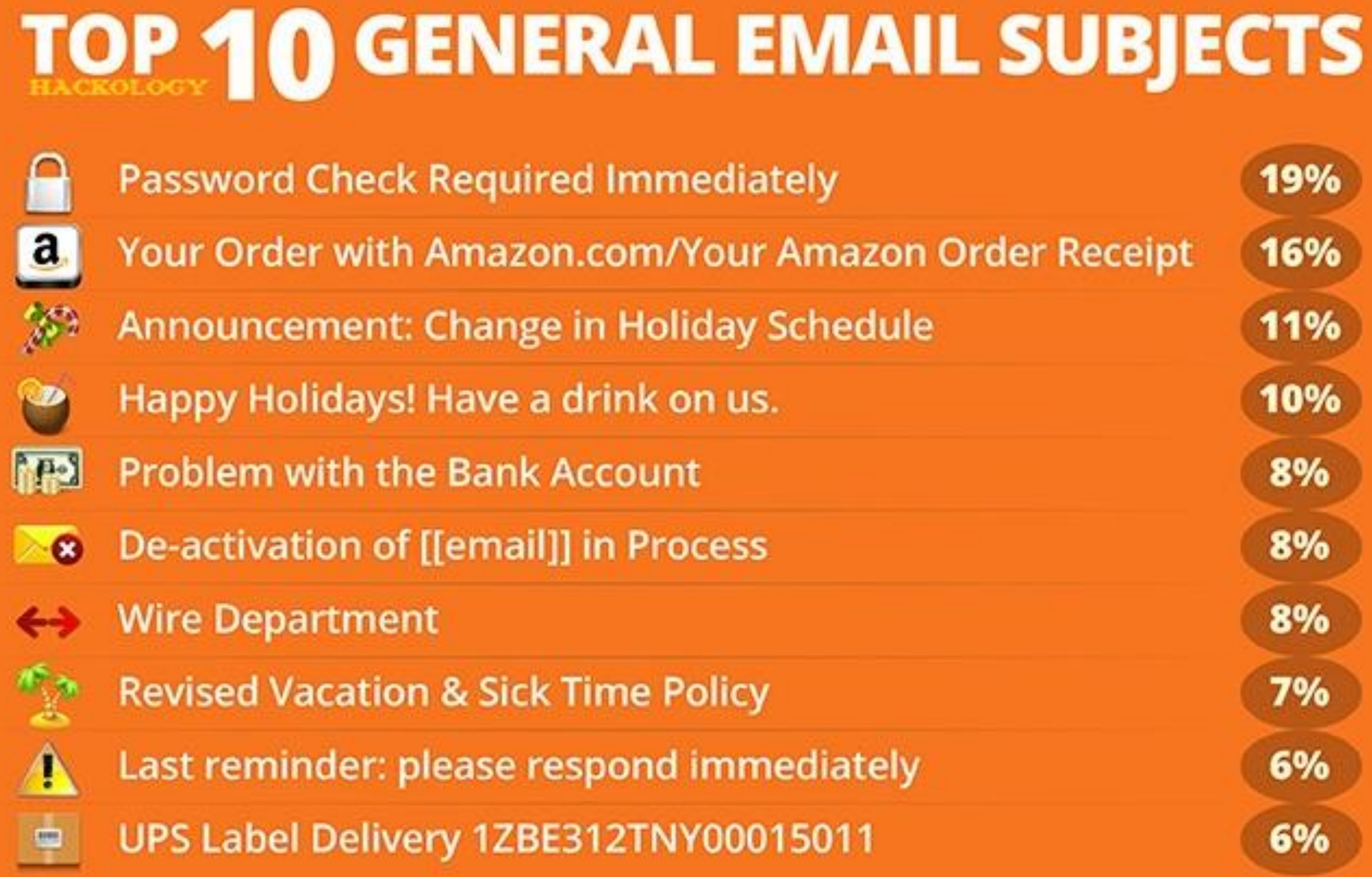
- Ransom email in image
- Payment bitcoin address in QR code



Fraudsters deepfake CEO’s voice to trick manager into transferring $243,000

by RAVIE LAKSHMANAN — 9 days ago in SECURITY

How To Distinguish



TOP 10 GENERAL EMAIL SUBJECTS

Password Check Required Immediately	19%
Your Order with Amazon.com/Your Amazon Order Receipt	16%
Announcement: Change in Holiday Schedule	11%
Happy Holidays! Have a drink on us.	10%
Problem with the Bank Account	8%
De-activation of [[email]] in Process	8%
Wire Department	8%
Revised Vacation & Sick Time Policy	7%
Last reminder: please respond immediately	6%
UPS Label Delivery 1ZBE312TNY00015011	6%

Source: **https://www.securitybrigade.com**

GREED

URGENCY

CURIOSITY

FEAR

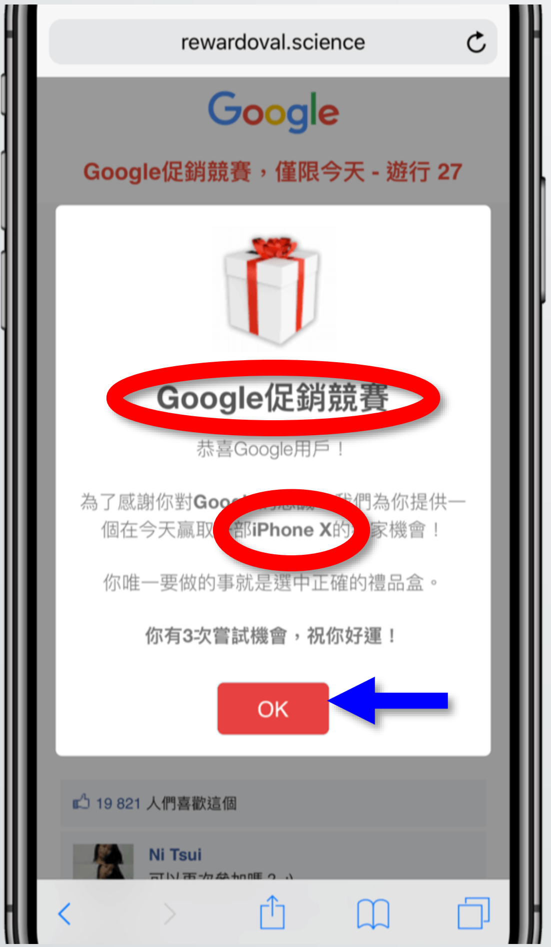
How to distinguish Phishing Scams?

Sample 1

URGENCY

GREED

Lucky Draw & Rewards



rewardoval.science

Google

Google促銷競賽，僅限今天 - 遊行 27

Google促銷競賽

恭喜Google用戶！

為了感謝你對Goo[illegible]我們為你提供一個在今天贏取[illegible]部iPhone X的[illegible]家機會！

你唯一要做的事就是選中正確的禮品盒。

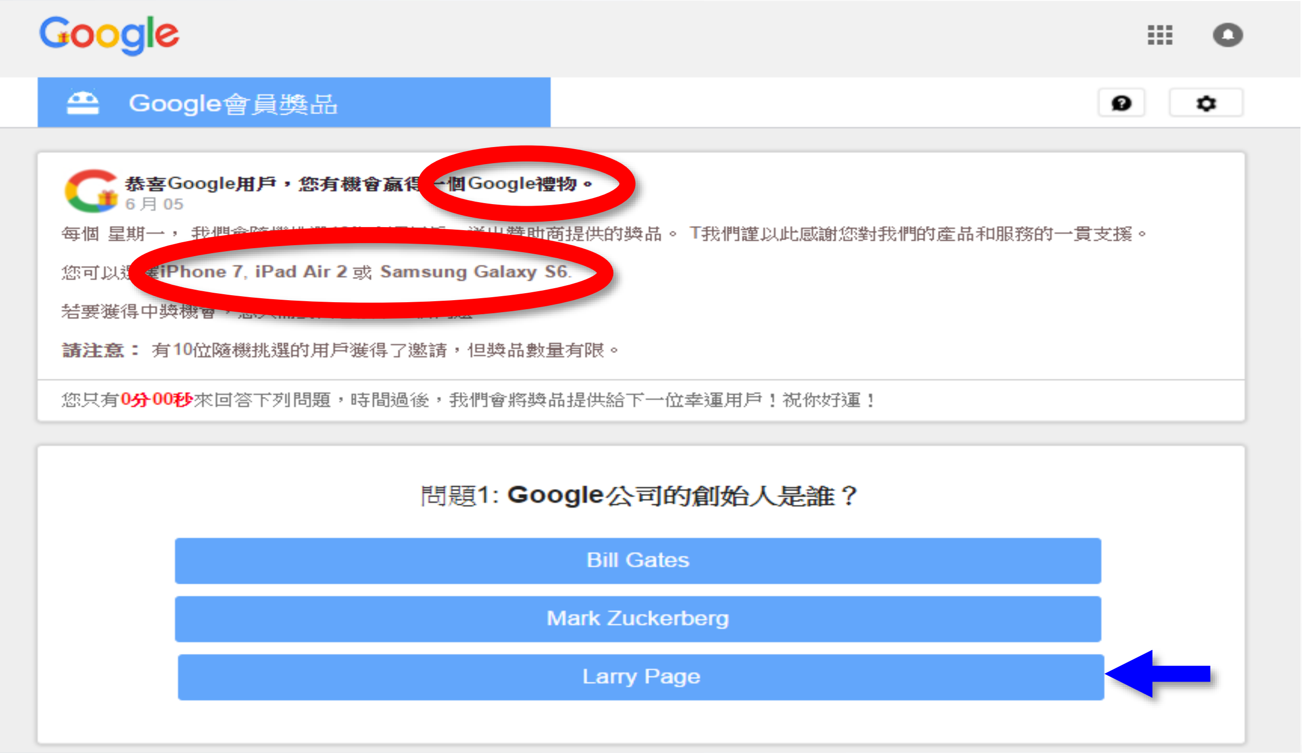
你有3次嘗試機會，祝你好運！

OK

19 821 人們喜歡這個

Ni Tsui

可以再次參加嗎？:)



Google

Google會員獎品

恭喜Google用戶，您有機會贏得一個Google禮物。

6 月 05

每個 星期一， 我們會隨機挑選[illegible]送出贊助商提供的獎品。 T我們謹以此感謝您對我們的產品和服務的一貫支援。

您可以選擇iPhone 7, iPad Air 2 或 Samsung Galaxy S6.

若要獲得中獎機會，[illegible]

請注意： 有10位隨機挑選的用戶獲得了邀請，但獎品數量有限。

您只有**0分 00秒**來回答下列問題，時間過後，我們會將獎品提供給下一位幸運用戶！祝你好運！

問題1: **Google公司的創始人是誰？**

Bill Gates

Mark Zuckerberg

Larry Page

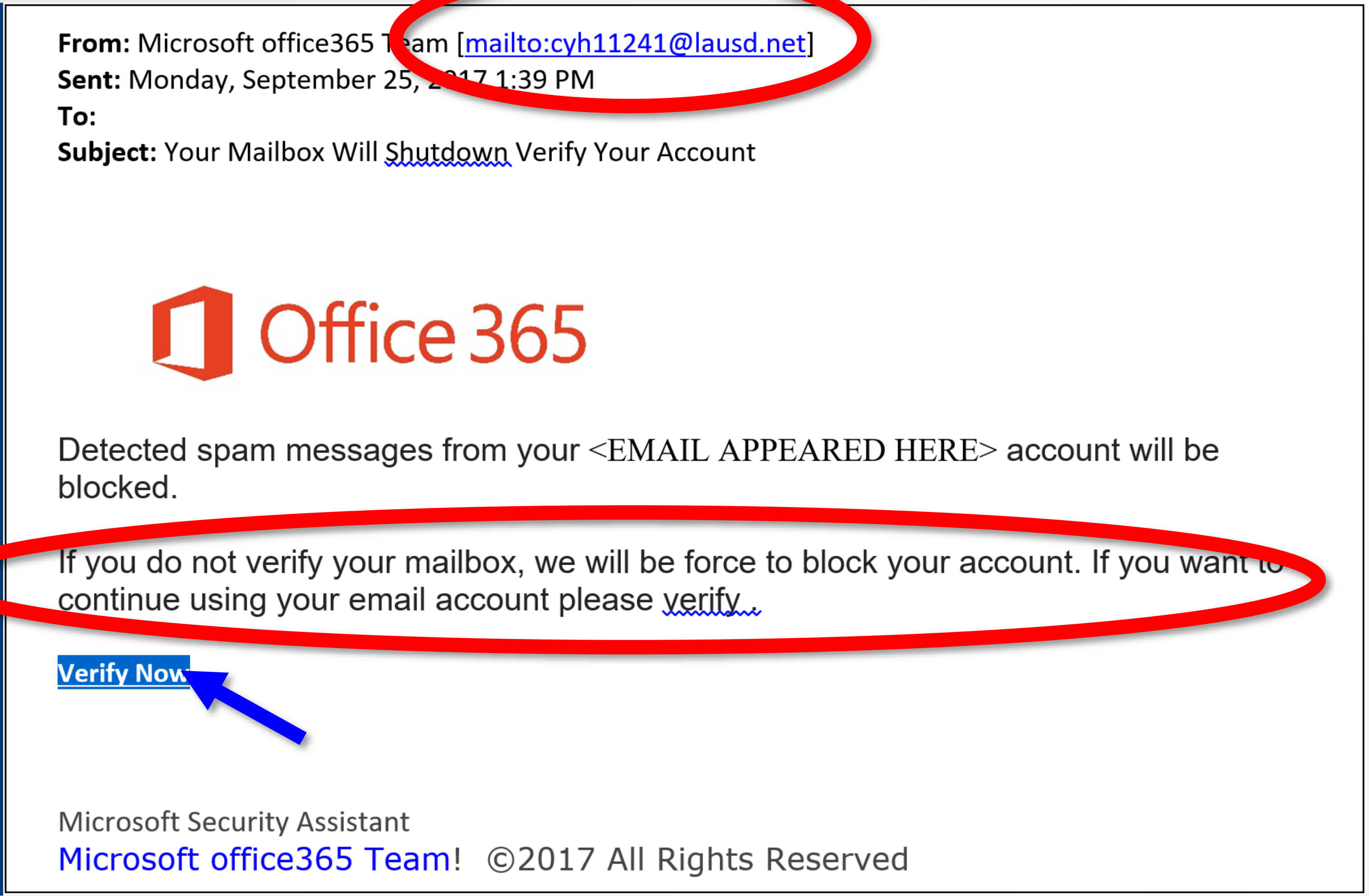
How to distinguish Phishing Scams?

Sample 2

Online Service

URGENCY

FEAR



From: Microsoft office365 Team [mailto:cyh11241@lausd.net]
Sent: Monday, September 25, 2017 1:39 PM
To:
Subject: Your Mailbox Will Shutdown Verify Your Account

Office 365

Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please verify .

Verify Now

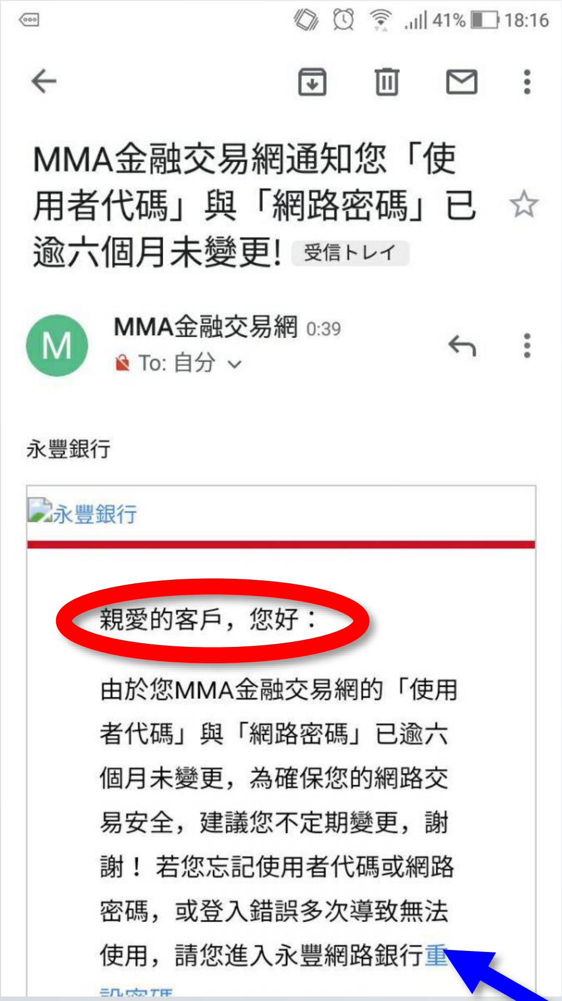
Microsoft Security Assistant
Microsoft office365 Team! ©2017 All Rights Reserved

How to distinguish Phishing Scams?

Sample 3

URGENCY

Banking & Finance



MMA金融交易網通知您「使用者代碼」與「網路密碼」已逾六個月未變更! 受信トレイ

MMA金融交易網 0:39

To: 自分

永豐銀行

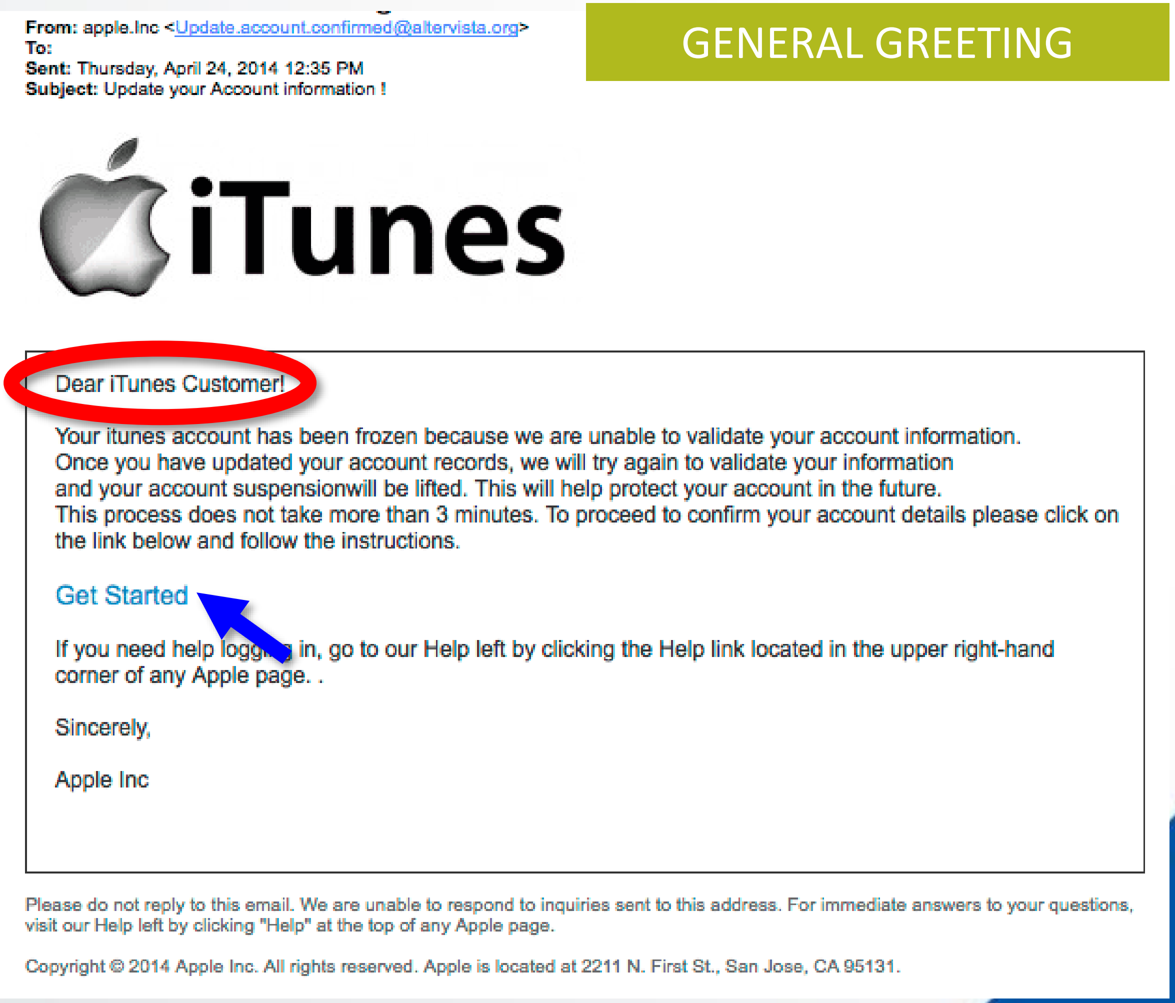
永豐銀行

親愛的客戶，您好：

由於您MMA金融交易網的「使用者代碼」與「網路密碼」已逾六個月未變更，為確保您的網路交易安全，建議您不定期變更，謝謝！若您忘記使用者代碼或網路密碼，或登入錯誤多次導致無法使用，請您進入永豐網路銀行重設密碼

Retail

GENERAL GREETING



From: apple.Inc <Update.account.confirmed@altervista.org>
To:
Sent: Thursday, April 24, 2014 12:35 PM
Subject: Update your Account information !

iTunes

Dear iTunes Customer!

Your itunes account has been frozen because we are unable to validate your account information. Once you have updated your account records, we will try again to validate your information and your account suspensionwill be lifted. This will help protect your account in the future. This process does not take more than 3 minutes. To proceed to confirm your account details please click on the link below and follow the instructions.

Get Started

If you need help logging in, go to our Help left by clicking the Help link located in the upper right-hand corner of any Apple page. .

Sincerely,

Apple Inc

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help left by clicking "Help" at the top of any Apple page.

Copyright © 2014 Apple Inc. All rights reserved. Apple is located at 2211 N. First St., San Jose, CA 95131.

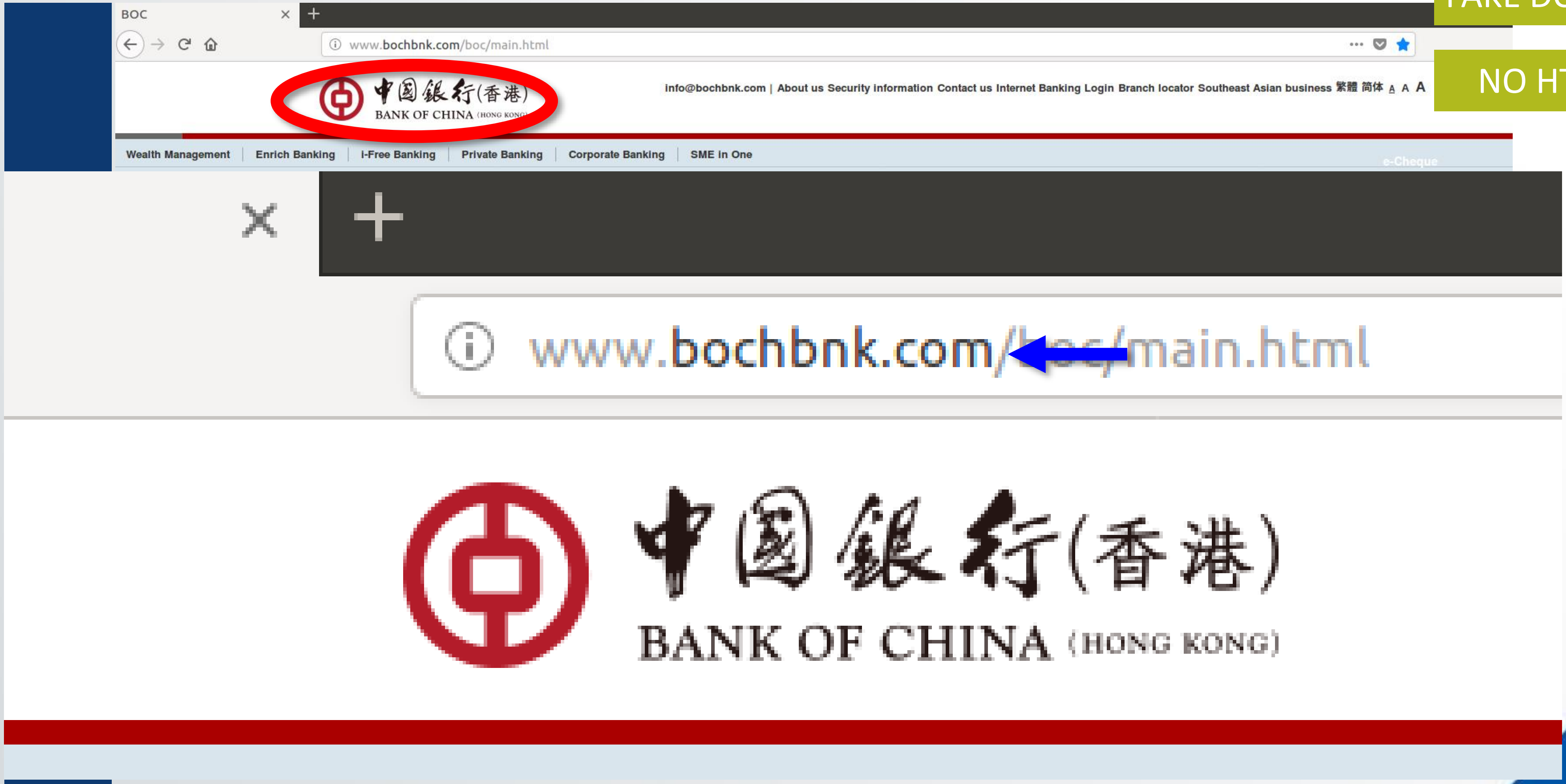
How to distinguish Phishing Scams?

Sample 4

URGENCY

FAKE DOMAIN

NO HTTPS



BOC

www.bochbnk.com/boc/main.html

中國銀行(香港) BANK OF CHINA (HONG KONG)

info@bochbnk.com | About us Security information Contact us Internet Banking Login Branch locator Southeast Asian business 繁體 簡体 A A A

Wealth Management | Enrich Banking | i-Free Banking | Private Banking | Corporate Banking | SME in One

e-Cheque

www.bochbnk.com/boc/main.html

中國銀行(香港)

BANK OF CHINA (HONG KONG)

How to distinguish Phishing Scams?

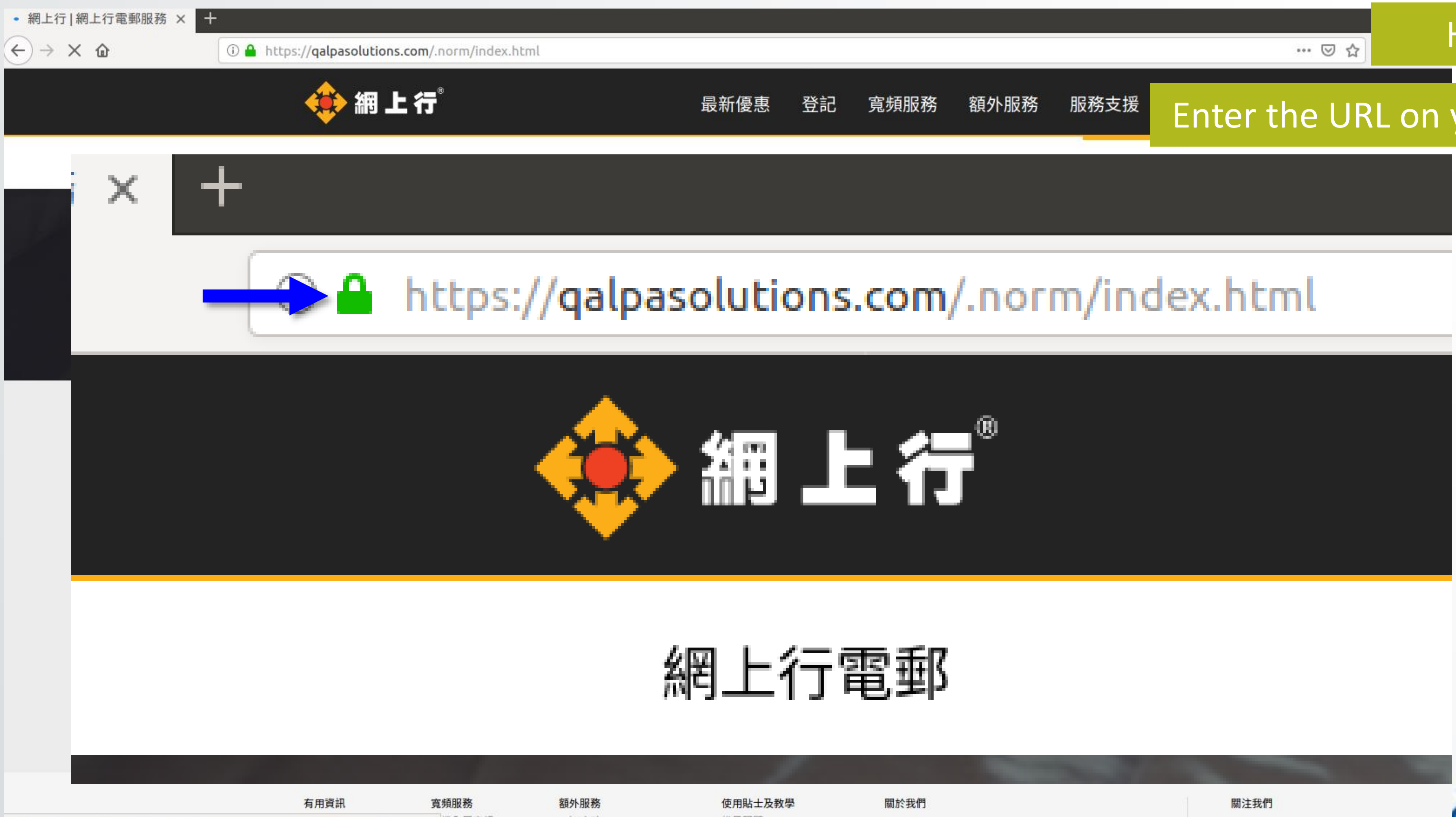
Sample 5

Internet Service Provider

FEAR

HTTPS

Enter the URL on your own



網上行 | 網上行電郵服務

https://qalpasolutions.com/.norm/index.html

https://qalpasolutions.com/.norm/index.html

網上行電郵

How to distinguish Phishing Scams?

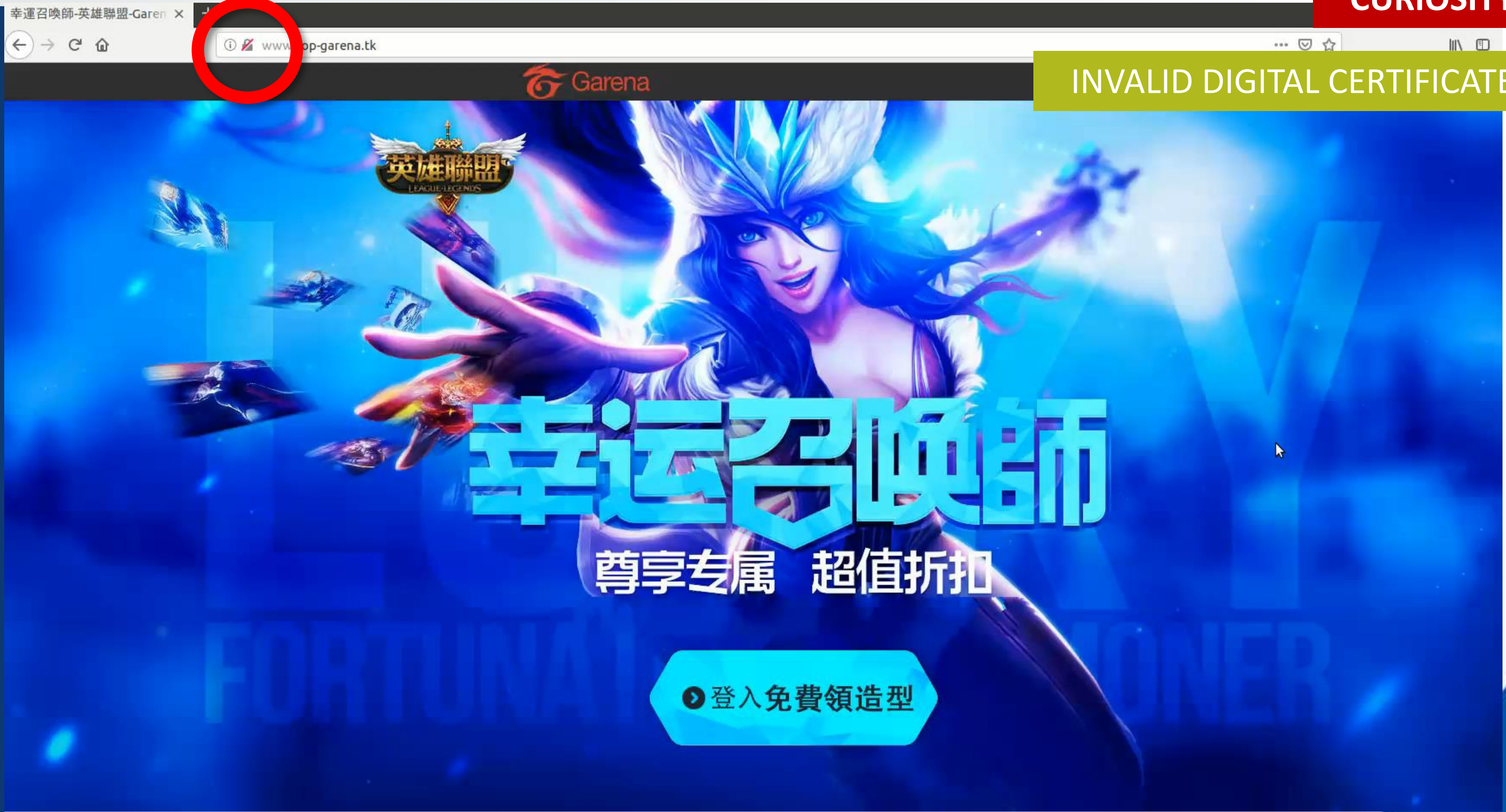
Sample 6

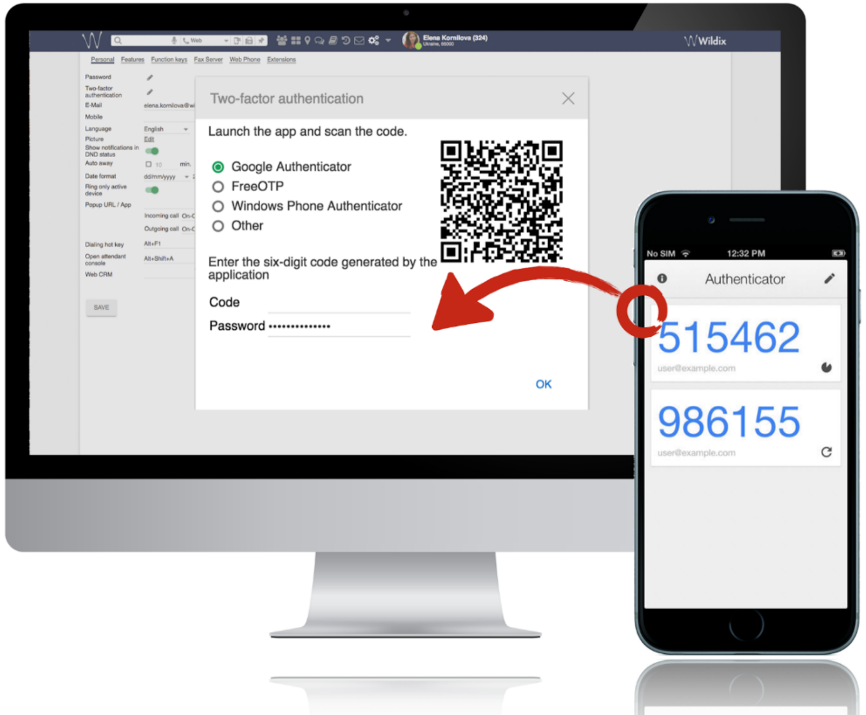
GREED

CURIOSITY

INVALID DIGITAL CERTIFICATE

Electronic Sports





Two-factor authentication

Launch the app and scan the code.

● Google Authenticator
○ FreeOTP
○ Windows Phone Authenticator
○ Other

Enter the six-digit code generated by the application

Code

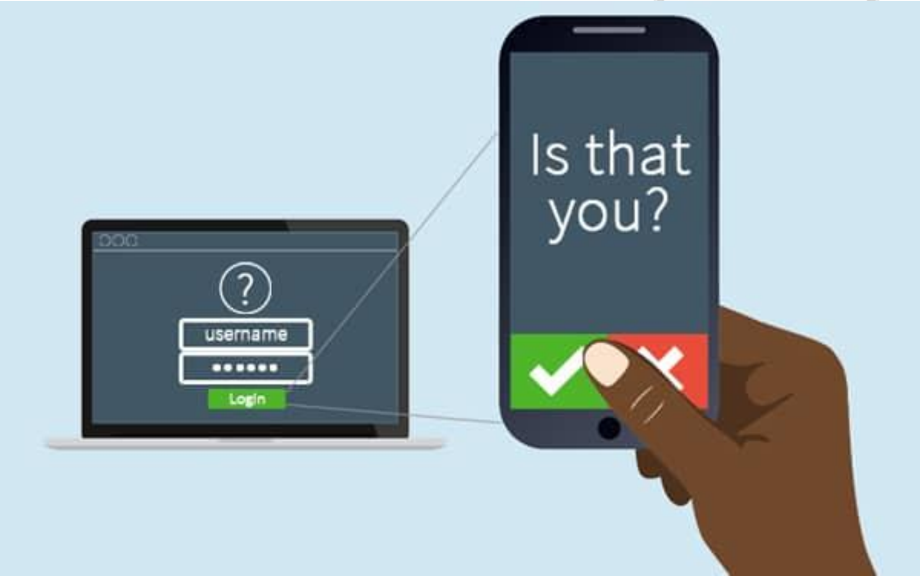
Password ••••••••••••••

OK

Authenticator

515462
user@example.com

986155
user@example.com



- Think before you click
- Pick up the phone to verify
- Use two-factor authentication (2FA) across all accounts
- Use different passwords for different services
- Use email filtering technology & make sure the technique is up-to-dated
- Conduct phishing drill exercises for all general staff

MALWARE & BOTNET

Image credit: **Rawpixel.com**

Malware | *Propagation Channels*

Executable

- Fake security software / mobile app
- Fake video player codec

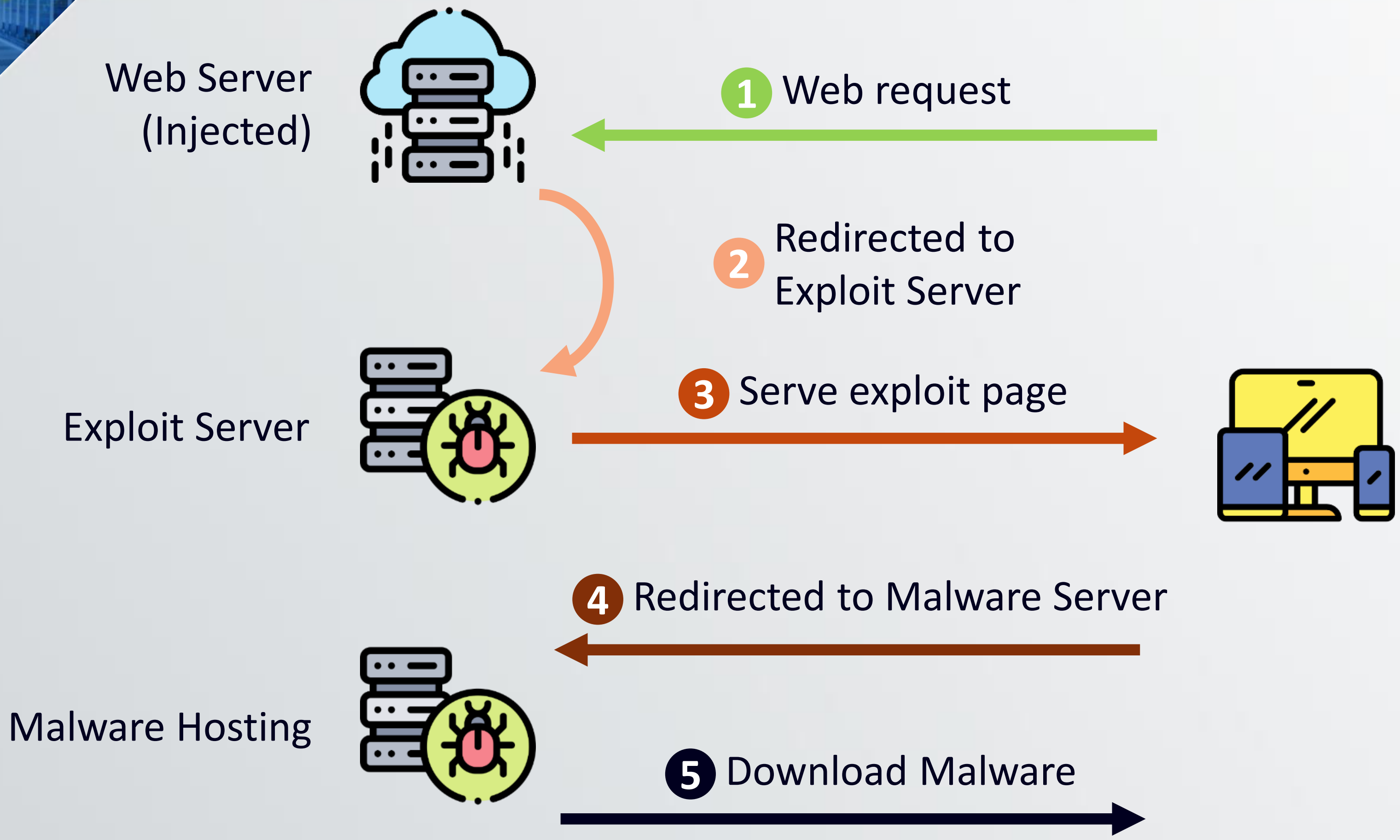
Document Malware ★

- Embedded malware in PDF or Office files
- Botnet served PDF malware

Website ★★

- Legitimate and trusted websites compromised
- Web admin incapable to detect and mitigate the risks

Multi-Stage Malware Infection | *Drive-by Download*

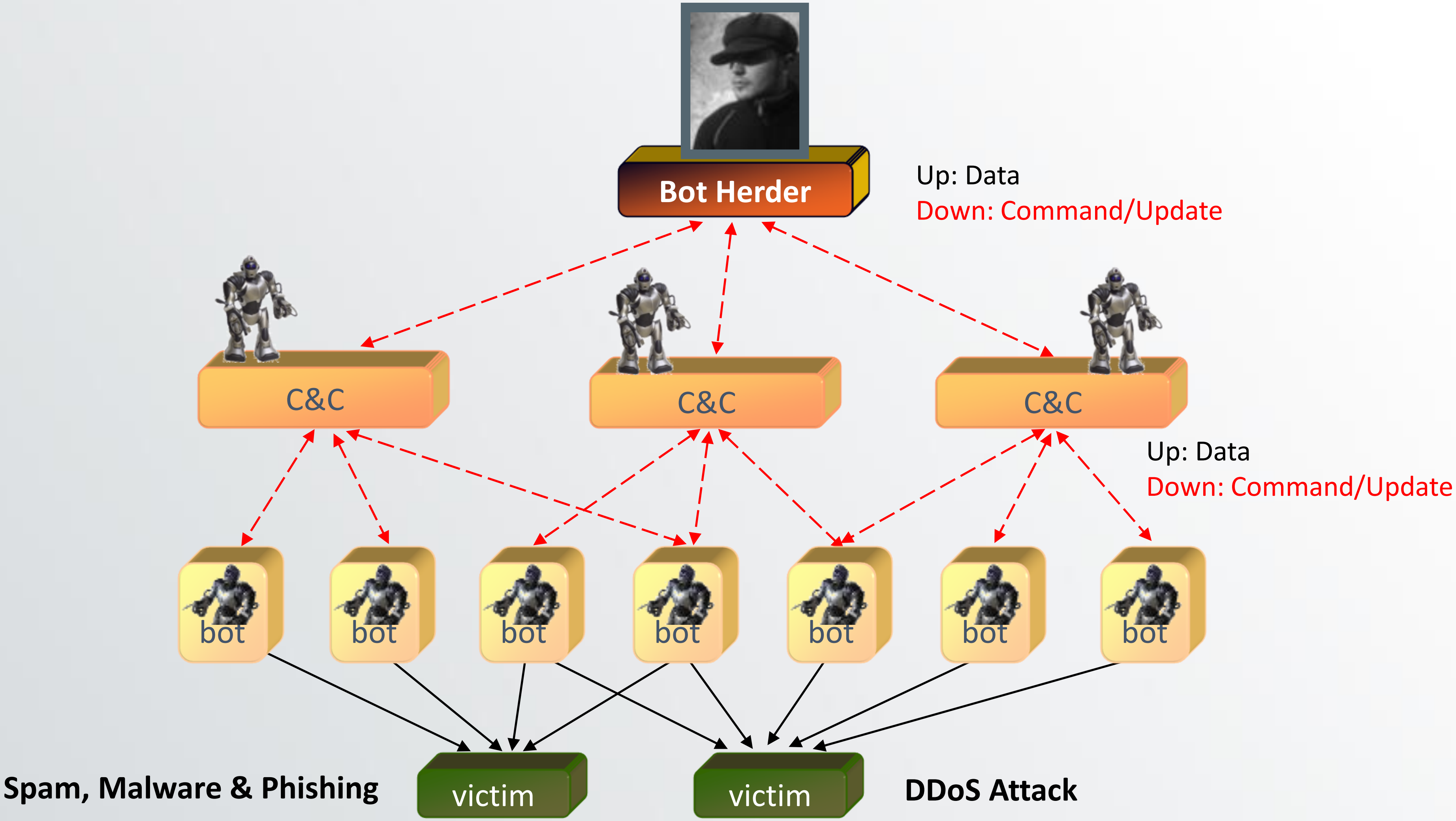


- Exploits imported from other servers via iframes, redirects
- When compromised, dropper download and install the actual bot malware

Image credit: **Flaticon.com**

Botnet (roBot Network)

Infrastructure of Controlled Victim Computers (BOTs)



Up: Data
Down: Command/Update

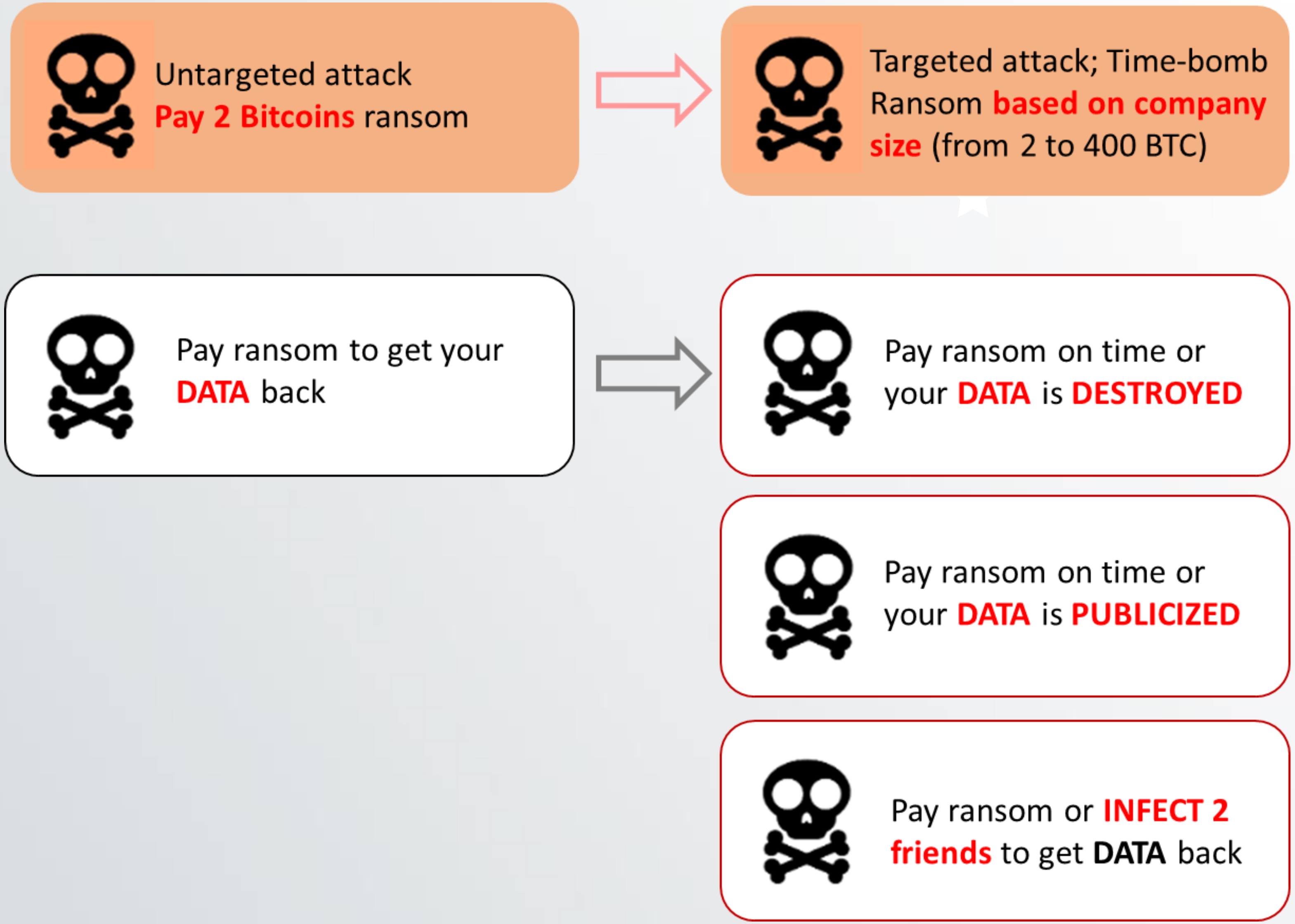
Up: Data
Down: Command/Update

Spam, Malware & Phishing

DDoS Attack

Image credit: **https://www.kratikal.com/blog/ransomware-attacks-shook-world/**

Ransomware



Untargeted attack
Pay 2 Bitcoins ransom

→

Targeted attack; Time-bomb
Ransom **based on company size** (from 2 to 400 BTC)

Pay ransom to get your **DATA** back

→

Pay ransom on time or your **DATA** is **DESTROYED**

Jigsaw

Pay ransom on time or your **DATA** is **PUBLICIZED**

Doxware

Pay ransom or **INFECT 2 friends** to get **DATA** back

Popcorn time

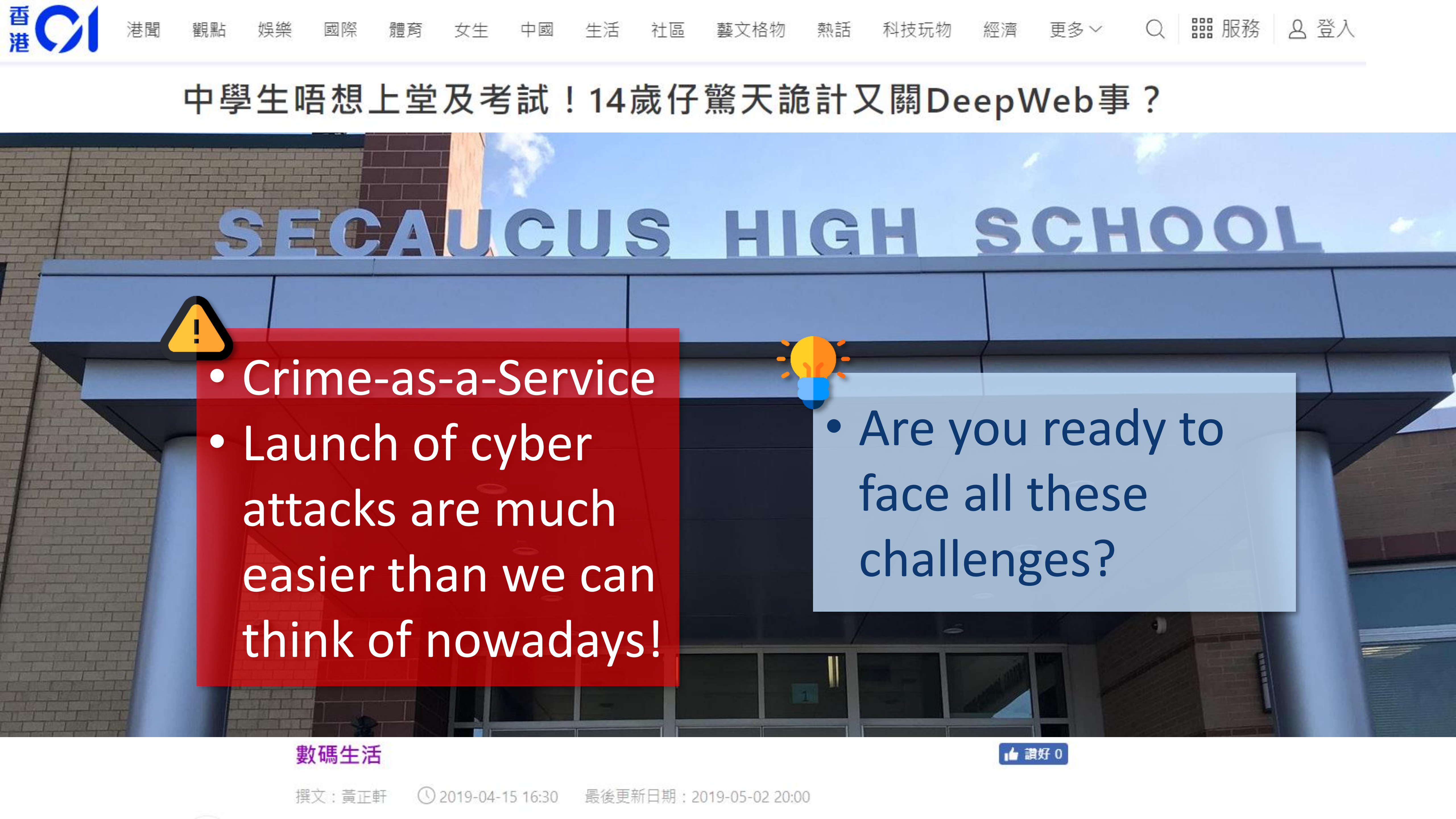
Protection against Ransomware

- Isolate infected computer immediately
- Do NOT pay ransom nor contact attacker
- Perform regular backups on important data and keep an **offline** copy
- Ensure that OS, software and anti-virus signatures are kept updated regularly
- Do NOT open suspicious email attachments and website links

Canon DSLR Camera Infected with Ransomware Over the Air

ANYTHING Can Be Targeted [video]

Source: **https://www.bleepingcomputer.com/news/security/canon-dslr-camera-infected-with-ransomware-over-the-air/**



中學生唔想上堂及考試！14歲仔驚天詭計又關DeepWeb事？

- Crime-as-a-Service
- Launch of cyber attacks are much easier than we can think of nowadays!

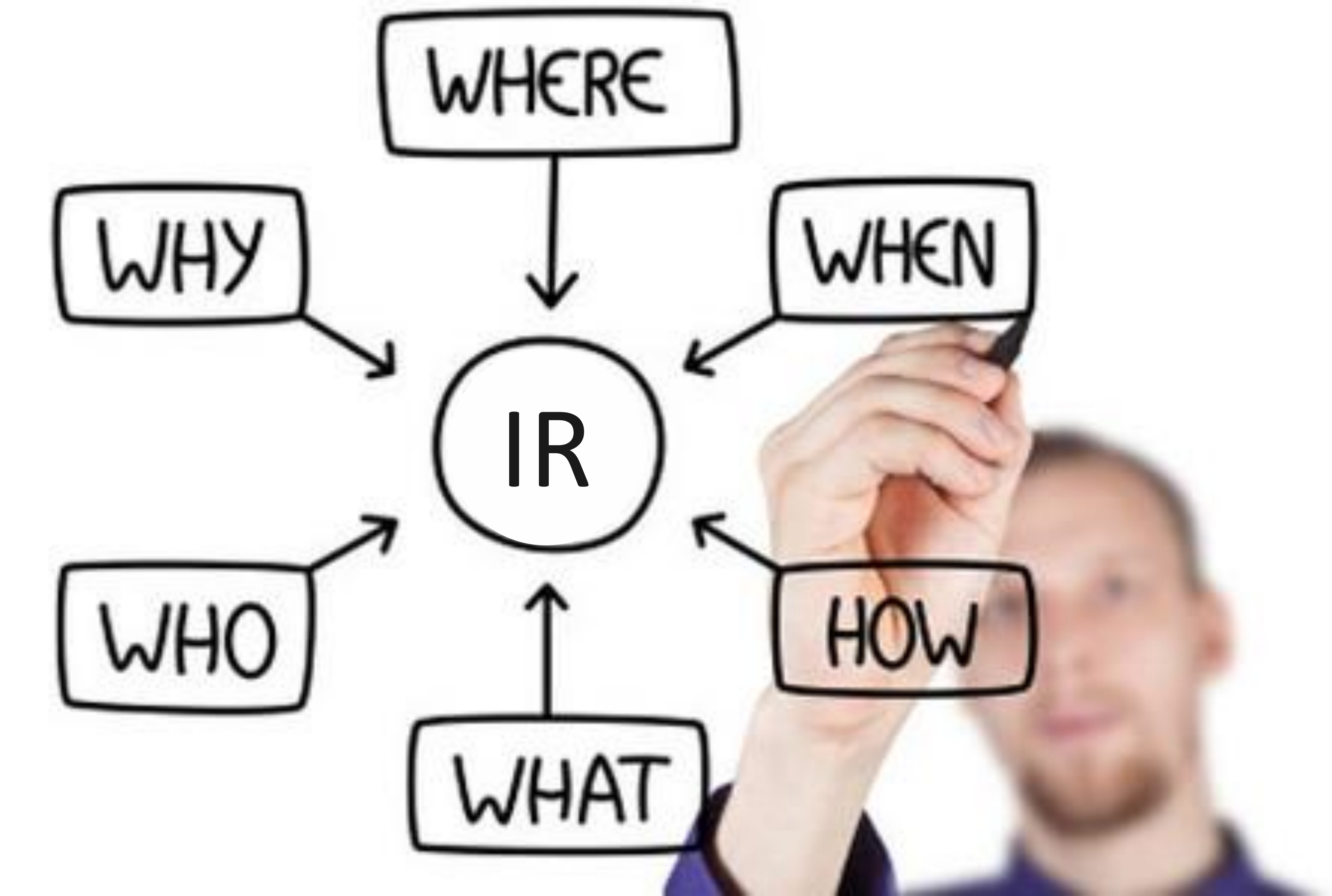
- Are you ready to face all these challenges?

數碼生活

撰文：黃正軒　2019-04-15 16:30　最後更新日期：2019-05-02 20:00

Security Incidents Handling

5W1H



Incident Reporting Basics (1)

- What actually happened?
- What the incident might mean for the organization?
- What is the impact?
- What system affected?
- What service affected?
- What actions had been taken?
- and etc.

WHAT

- Threat actor / IP address
- Attack source
- Hacking group
- Attack target
- Owner of targeted system
- Owner of involved business function
- Customers affected
- Parties involved
  - ➢ Internal
  - ➢ External
- and etc.

WHO

Incident Reporting Basics (2)

- When the incident happened?
- When the incident being detected?
- Incident duration
- Incident timeline
  - ➢ Actions
  - ➢ Decisions
  - ➢ Information collected
- and etc.

WHEN

- Where is the attacks originated from?
- Attack paths
- Lateral movement
- Logical
  - Network zone
- Physical
  - Cloud
  - On-premises
- and etc.

WHERE

Incident Reporting Basics (3)

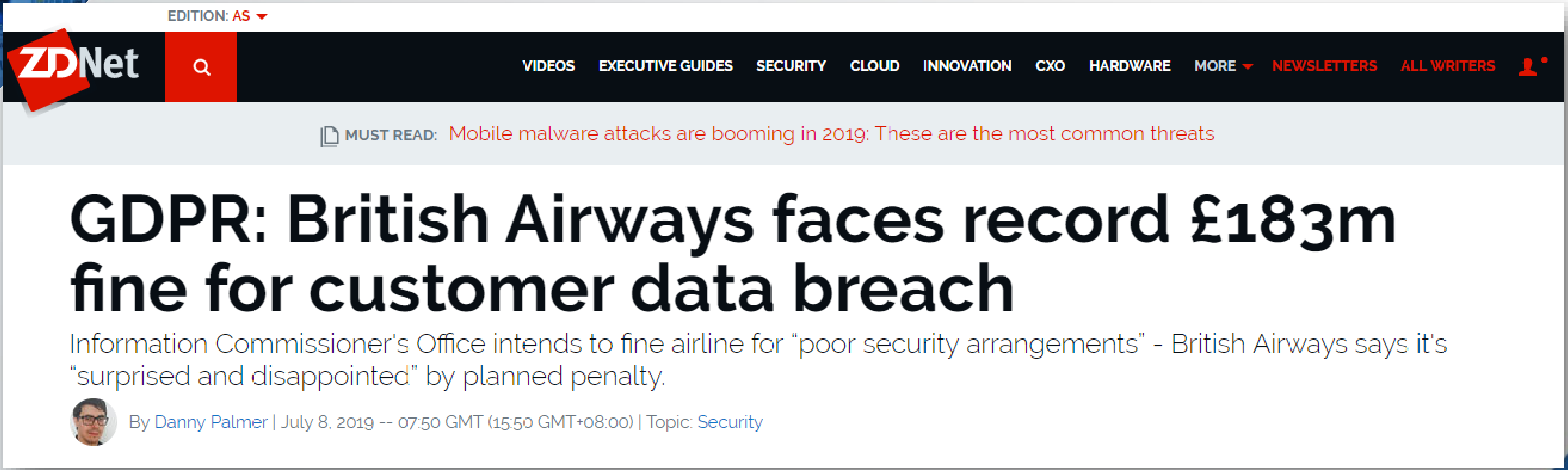
- How does it happened?
- How the systems infected?
- What vulnerabilities exploited?
- Attack method
- Intrusion method
- Command and control
- Evade detection
- Obfuscation
- and etc.

HOW

- Why does it happened?
- Root cause
- and etc.

WHY

Case Study | **British Airways Data Breach Incident**



MUST READ: Mobile malware attacks are booming in 2019: These are the most common threats

GDPR: British Airways faces record £183m fine for customer data breach

Information Commissioner's Office intends to fine airline for "poor security arrangements" - British Airways says it's "surprised and disappointed" by planned penalty.

By Danny Palmer | July 8, 2019 -- 07:50 GMT (15:50 GMT+08:00) | Topic: Security

Case Study | **British Airways Data Breach Incident**

□ **What affected?**

- *Online booking website and the mobile app*

□ **What data had been stolen?**

- *Customer's personal data (Names, billing address, email address)*
- *Credit card or debit card details*

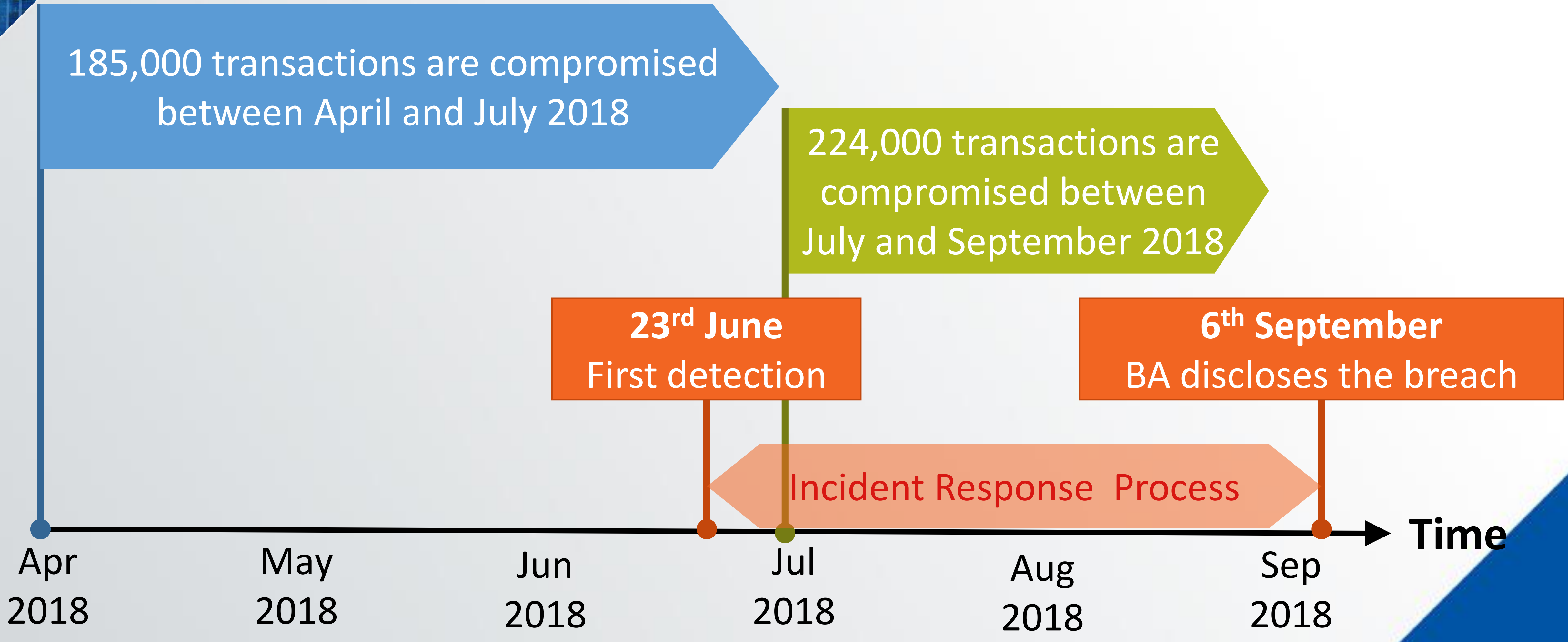
□ **How was it happened?**

- *Breaching by hiding JavaScript code known as Magecart*
- *Customer booking data was sent to malicious site on submission*

□ **Why was it happened?**

- *Vulnerabilities being exploited that cause JavaScript injection on Modernizr module*

Case Study | **British Airways Data Breach Incident**



185,000 transactions are compromised between April and July 2018

224,000 transactions are compromised between July and September 2018

23rd June
First detection

6th September
BA discloses the breach

Incident Response Process

Time

Apr 2018

May 2018

Jun 2018

Jul 2018

Aug 2018

Sep 2018

Security Advice

Round Up

Being HACKED!?

What to do next???

If you have provided **login credentials** in suspicious website, please **reset password** and review the security settings in the related online service accounts

If you have provided **financial information**, such as credit card number, and incur financial loss, please **contact your bank immediately**

You should **report to nearby police station** if any **financial loss** is incurred

If someone **spoofs your identity** to send email to your family, friends and business partners, you should **alert them by other trusted communication channels**.

Contact your

IT Department immediately!

if you have one…

電腦資訊保安

小錦囊

HKCERT Hotline

81056060

www.hkcert.org

HKCERT

Not being hack . . .

just YET !!!

Image credit: **http://www.damazine.com/fishing-a-good-way-of-relaxing/**

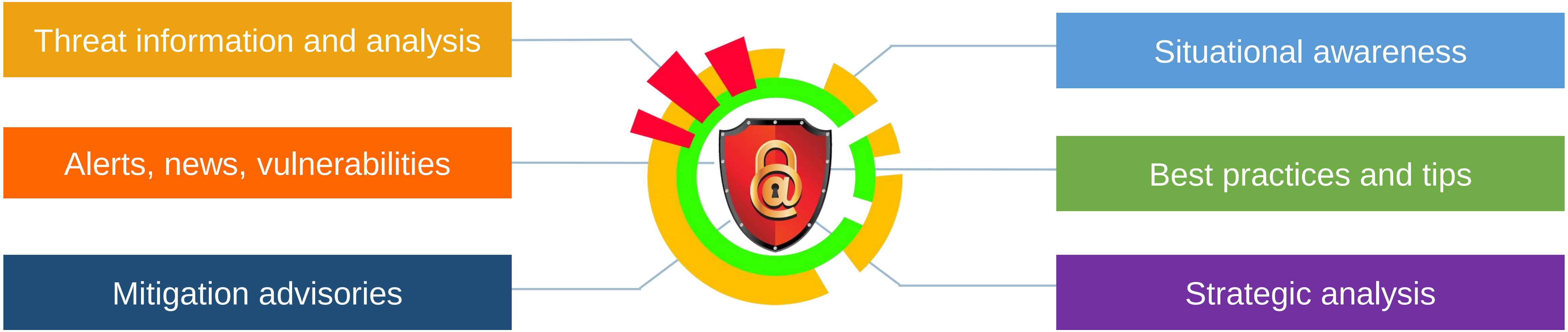
Cybersec Infohub

Sharing

Trust

Collaboration

Cybersec Infohub



Threat information and analysis

Alerts, news, vulnerabilities

Mitigation advisories

Situational awareness

Best practices and tips

Strategic analysis

Key participants

- ISPs
- Critical Infrastructure
- Critical Internet Infrastructure
- IT & Security Vendors
- Researcher
- GovCERT.HK HKCERT Local CERTs

Methods of Exchange

- Via the Platform
- Industry Event
- Tele-conference
- Webinar
- Working Group

Cybersechub.hk | Public Zone

Alerts

Advisories

Insights

CERT Publications

Cybersechub.hk | Members Zone

Traffic Light Protocol

User Anonymity

Export IOCs for Operation

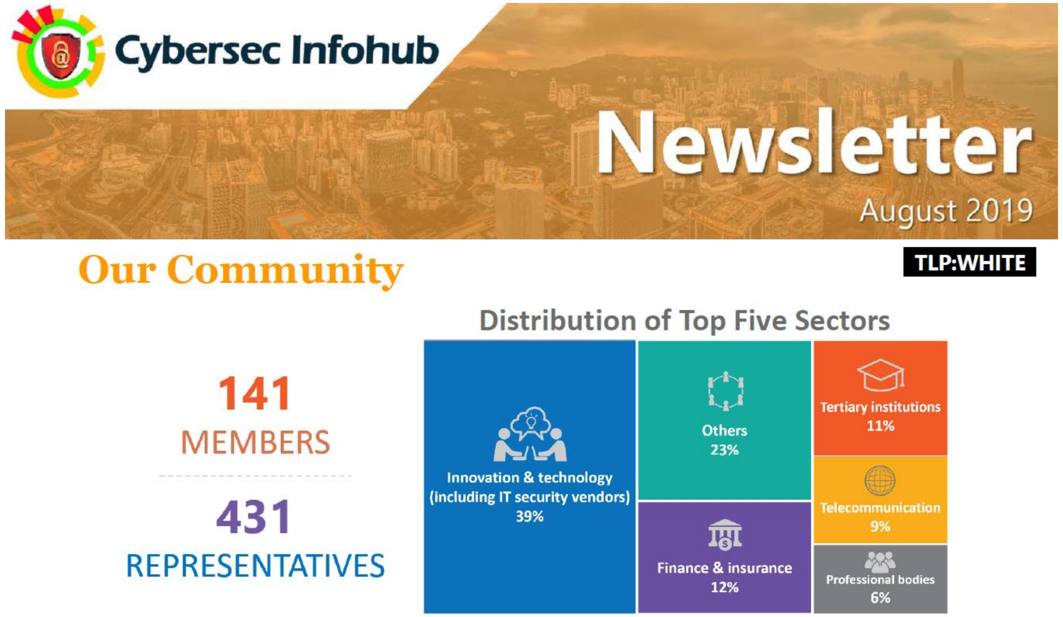
Social Media “Like” Feature

“KOL” of Cybersechub.hk

Trusted Groups Discussion

Private Messaging

Directory for Connections



Cybersec Infohub

Newsletter

August 2019

TLP:WHITE

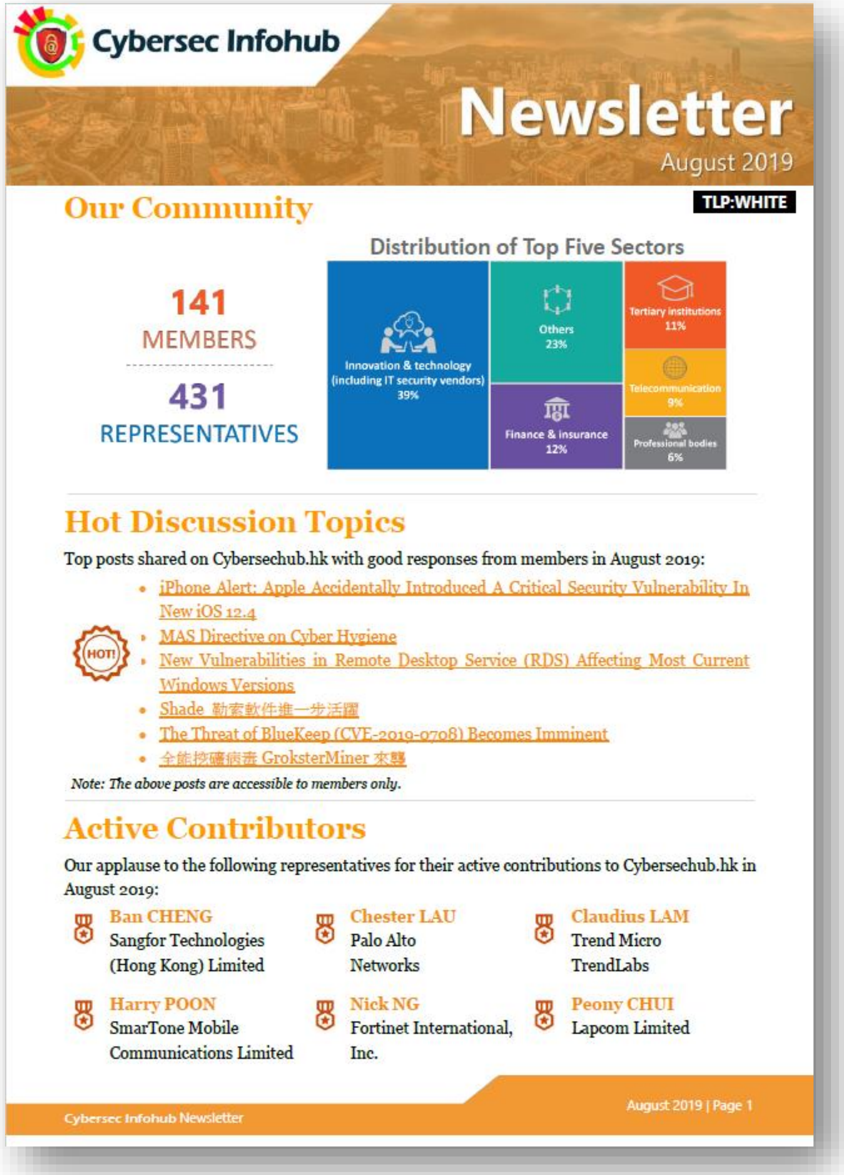
Our Community

Distribution of Top Five Sectors

141
MEMBERS

431
REPRESENTATIVES

Innovation & technology (including IT security vendors) 39%
Others 23%
Tertiary institutions 11%
Telecommunication 9%
Finance & insurance 12%
Professional bodies 6%



Cybersec Infohub

Newsletter

August 2019

TLP:WHITE

Our Community

Distribution of Top Five Sectors

141
MEMBERS

431
REPRESENTATIVES

Innovation & technology (including IT security vendors) 39%
Others 23%
Tertiary institutions 11%
Telecommunication 9%
Finance & insurance 12%
Professional bodies 6%

Hot Discussion Topics

Top posts shared on Cybersechub.hk with good responses from members in August 2019:

- iPhone Alert: Apple Accidentally Introduced A Critical Security Vulnerability In New iOS 12.4
- MAS Directive on Cyber Hygiene
- New Vulnerabilities in Remote Desktop Service (RDS) Affecting Most Current Windows Versions
- Shade 勒索軟件進一步活躍
- The Threat of BlueKeep (CVE-2019-0708) Becomes Imminent
- 全能挖礦病毒 GroksterMiner 來襲

Note: The above posts are accessible to members only.

Active Contributors

Our applause to the following representatives for their active contributions to Cybersechub.hk in August 2019:

Ban CHENG
Sangfor Technologies
(Hong Kong) Limited

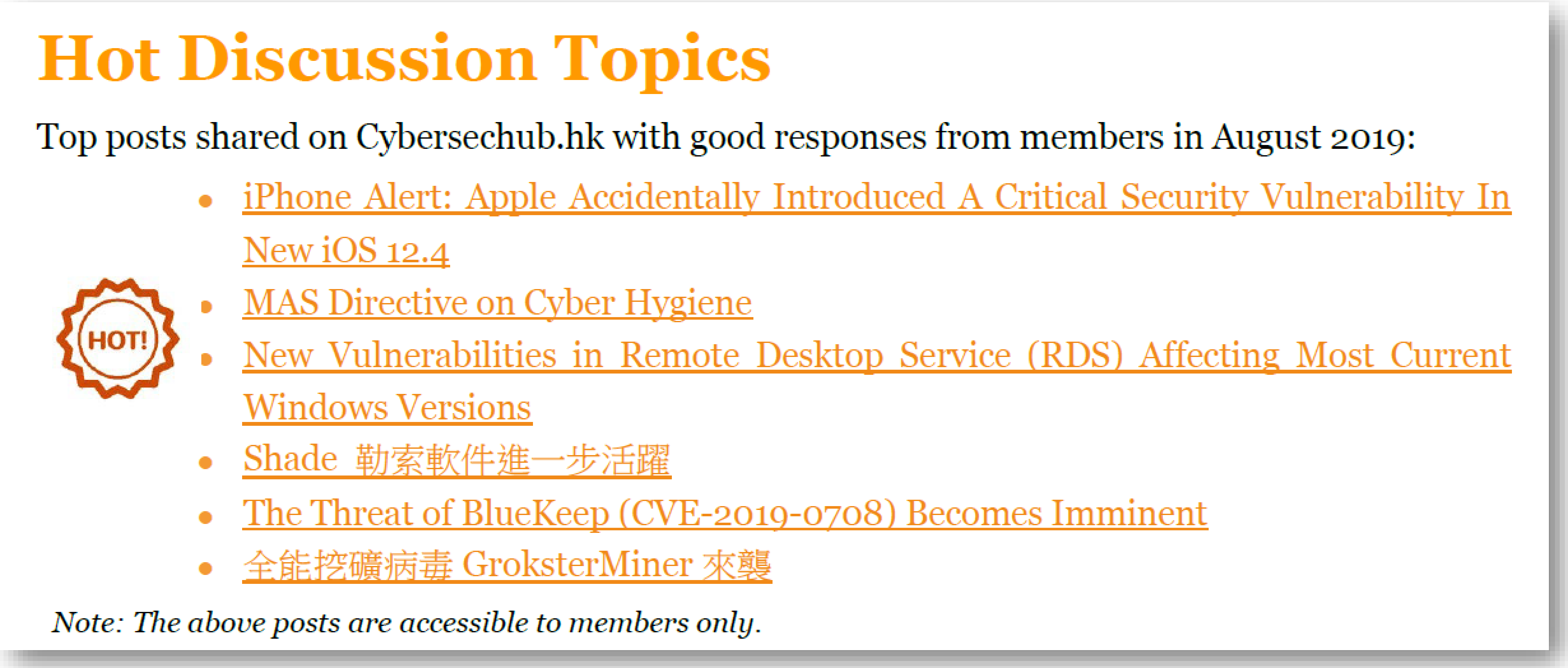
Chester LAU
Palo Alto
Networks

Claudius LAM
Trend Micro
TrendLabs

Harry POON
SmarTone Mobile
Communications Limited

Nick NG
Fortinet International,
Inc.

Peony CHUI
Lapcom Limited

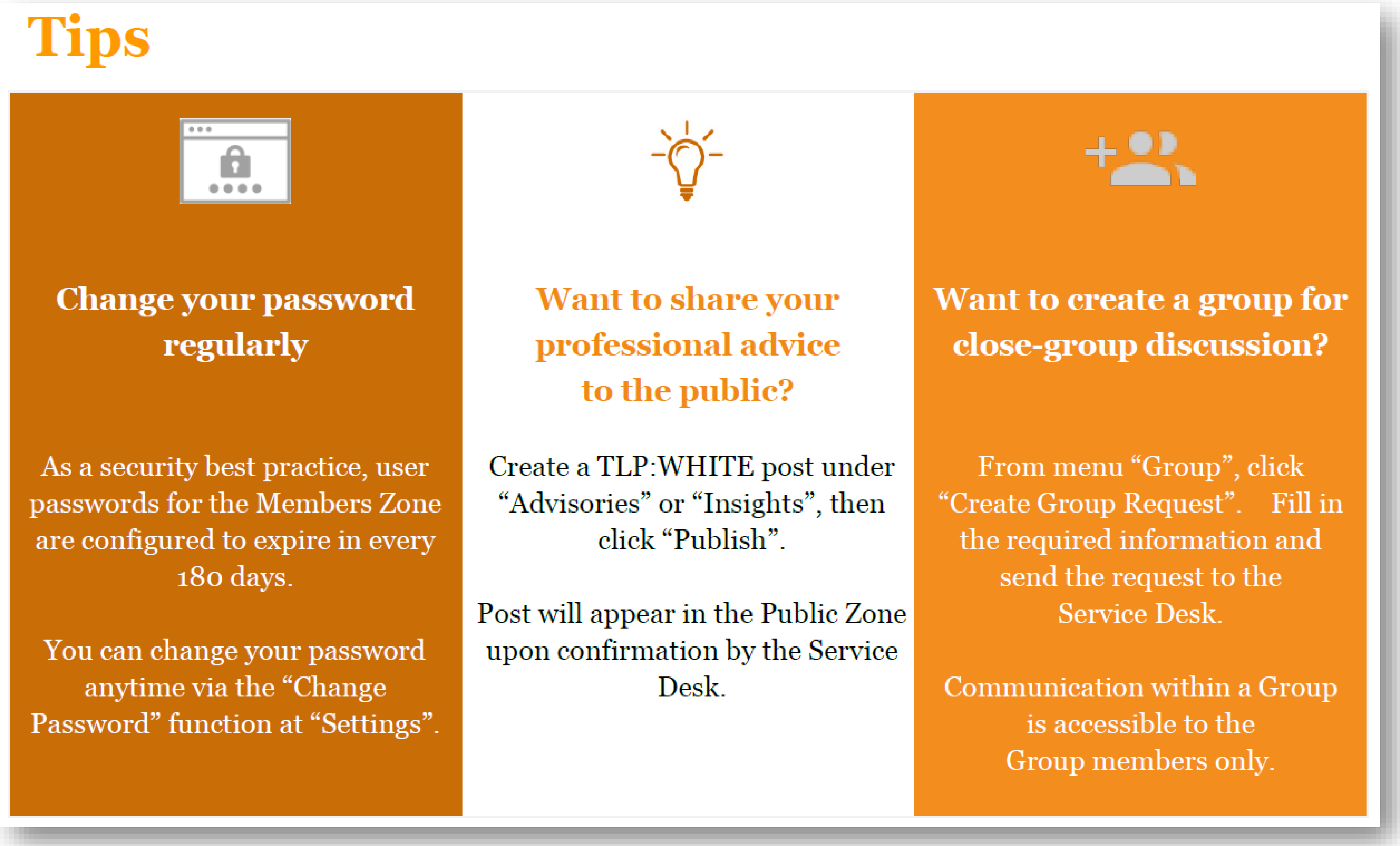


Hot Discussion Topics

Top posts shared on Cybersechub.hk with good responses from members in August 2019:

- iPhone Alert: Apple Accidentally Introduced A Critical Security Vulnerability In New iOS 12.4
- MAS Directive on Cyber Hygiene
- New Vulnerabilities in Remote Desktop Service (RDS) Affecting Most Current Windows Versions
- Shade 勒索軟件進一步活躍
- The Threat of BlueKeep (CVE-2019-0708) Becomes Imminent
- 全能挖礦病毒 GroksterMiner 來襲

Note: The above posts are accessible to members only.



Tips

Change your password regularly

As a security best practice, user passwords for the Members Zone are configured to expire in every 180 days.

You can change your password anytime via the “Change Password” function at “Settings”.

Want to share your professional advice to the public?

Create a TLP:WHITE post under “Advisories” or “Insights”, then click “Publish”.

Post will appear in the Public Zone upon confirmation by the Service Desk.

Want to create a group for close-group discussion?

From menu “Group”, click “Create Group Request”. Fill in the required information and send the request to the Service Desk.

Communication within a Group is accessible to the Group members only.

TLP:WHITE

Events

Our first Cybersec Infohub Webinar –"Threat Intelligence and Exchange from Past to Future" on 16 August 2019

On 16 August 2019, the first Cybersec Infohub webinar was held successfully, as a new channel to shore up our collaborative network. Thank you all the participants for joining the webinar, and we hope it was a fruitful one for everybody.

Can't wait for the next webinar?　Stay tuned!

If you have missed the valuable sharing, you may find the presentation slides, video recording and follow-up discussions in the Members Zone. (https://www.cybersechub.hk/platform/threat/620?nav=informationSharing:General%20Discussion)

Cybersec Infohub

cybersechub.hk

Bring these messages back to your school……

1. Everyone can be targeted, even you are just a **small potato** in your organization!!!!!!!!!!!!!!!!!
2. Set a **strong password** & enable **2FA** whenever possible
3. Make sure your software / App are **up-to-date** & only download from reliable sources
4. Do the **SAME** to your **home PC/laptop/mobile devices**
5. Build your own **Human Firewall**

Question?

Thank You

Hong Kong Productivity Council
香港生產力促進局

HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong
香港九龍達之路78號生產力大樓
+852 2788 6168 www.hkpc.org