

# Cyber Security General Staff Training for Welfare Sector

# Training Agenda – Section1

14:30 – 14:50  
20 Minutes

1

## Ice Breaking

- Cyber Security Basic Concept

14:50 – 15:20  
30 Minutes

2

## Cyber Security Status and Recent Incidents Sharing

- Recent Cyber Incidents Related to NGO and HK
- Protect the Organisation

15:20 – 15:35  
15 Minutes

## Break

15:35 – 16:15  
40 Minutes

3

## External Cyber Threat Analysis and Security Advice

- Social Engineering Scams
- Malware
- Browser and Mobile Security Issues



# Training Agenda – Section2

16:15 – 16:25  
10 Minutes

4

Interactive session

16:25 – 16:40  
15 Minutes

Break

16:40 – 17:20  
40 Minutes

5

Internal Cyber Threat Analysis and Security Advice

- BYOD and WFH Risks
- Data Leakage

17:20 – 17:30  
10 Minutes

6

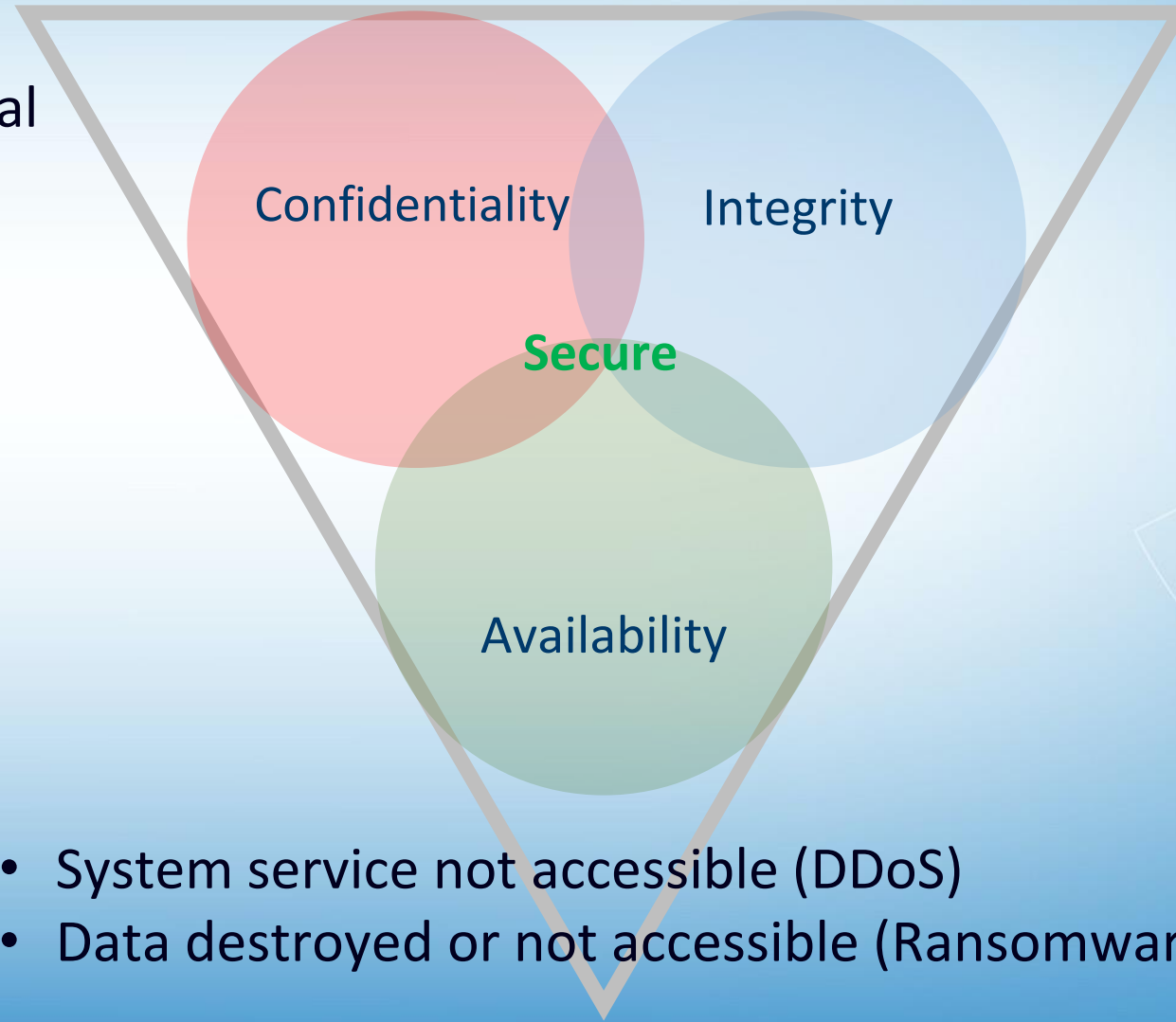
Key Take Away





# Basic Concept: CIA Triad of Cyber Security

- Leaking confidential data



- Data contaminated
- Forged transaction
- System compromised
- Identity spoofed

- System service not accessible (DDoS)
- Data destroyed or not accessible (Ransomware)



# Security 101

威脅

**Threats**

漏洞

**Vulnerabilities**

攻擊

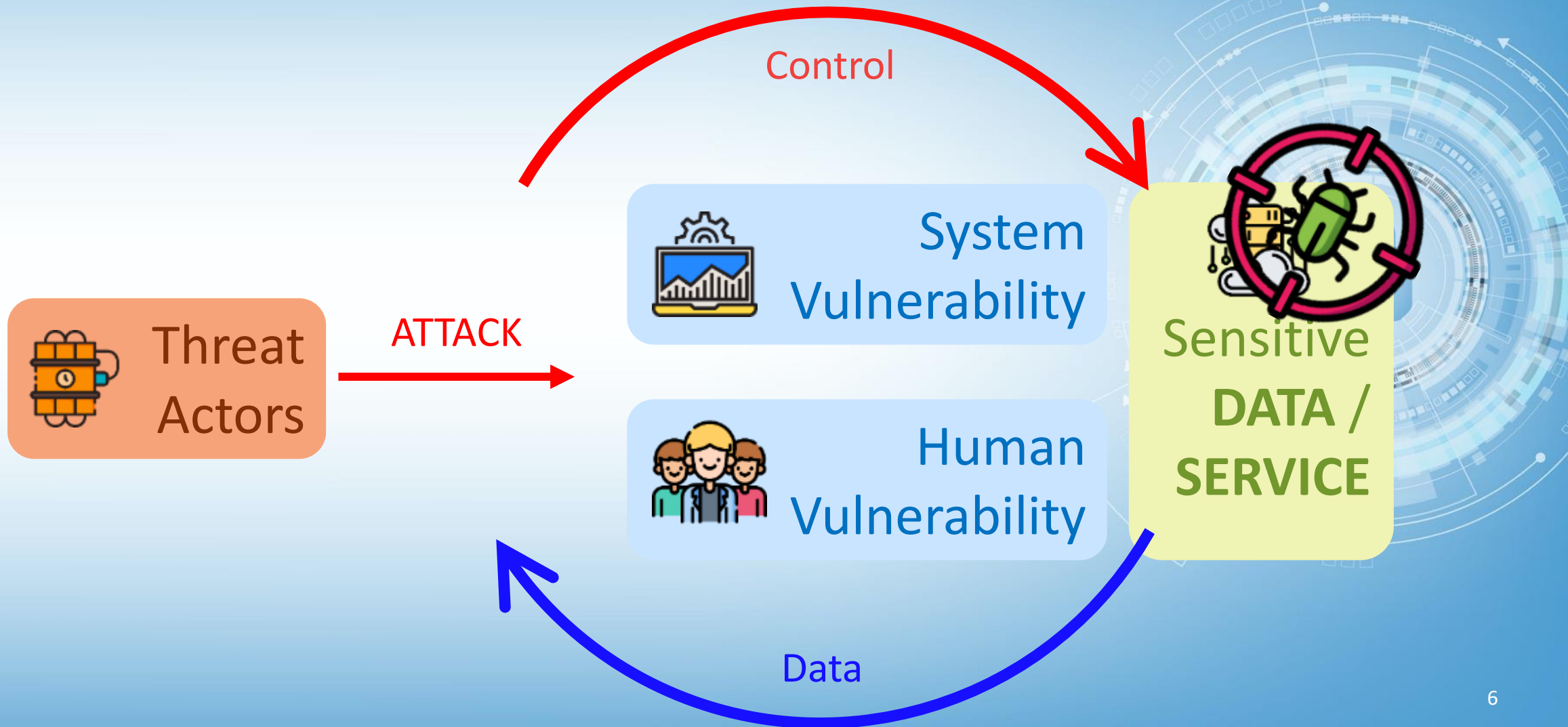
**Attacks**

風險

**Risks**



# Threat, Vulnerability & Attack





2

# Cyber Security Status and Recent Incidents Sharing





## Predicted Global Cybercrime Costs by 2021

### Global Cybercrime Damage Costs:

- **\$6 Trillion USD a Year. \***
- **\$500 Billion a Month.**
- **\$115.4 Billion a Week.**
- **\$16.4 Billion a Day.**
- **\$684.9 Million an Hour.**
- **\$11.4 Million a Minute.**
- **\$190,000 a Second.**



ALL FIGURES ARE  
PREDICTED BY 2021

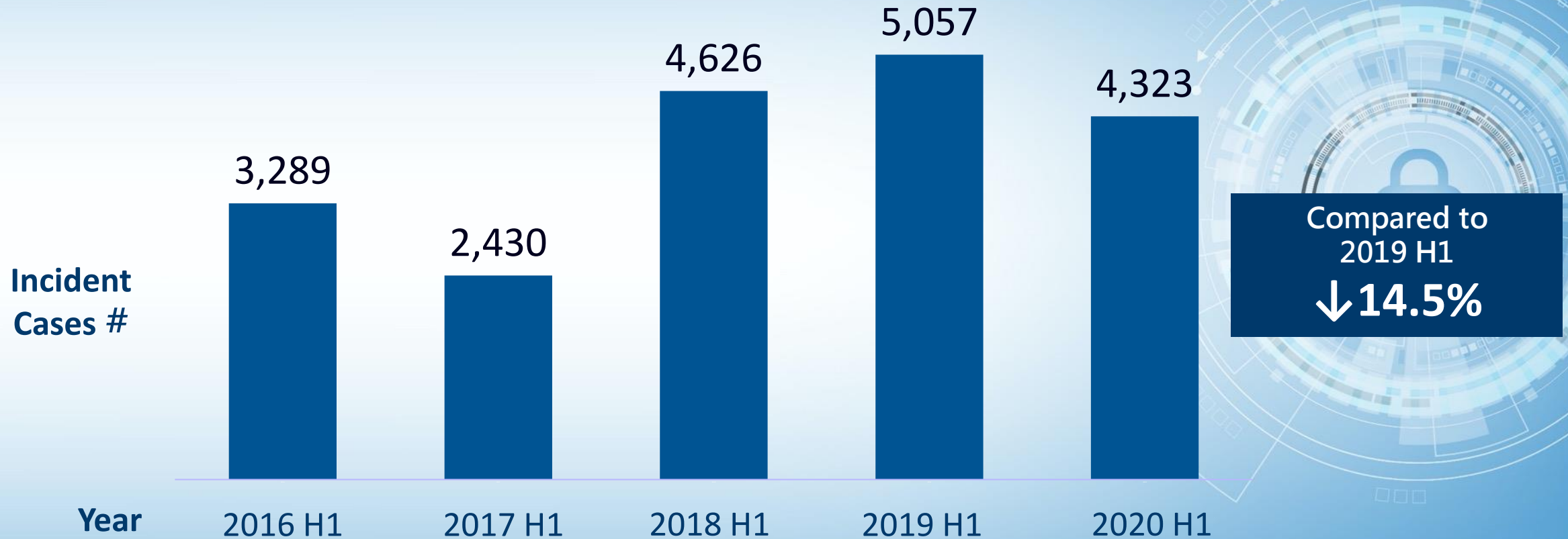
\* SOURCE: CYBERSECURITY VENTURES



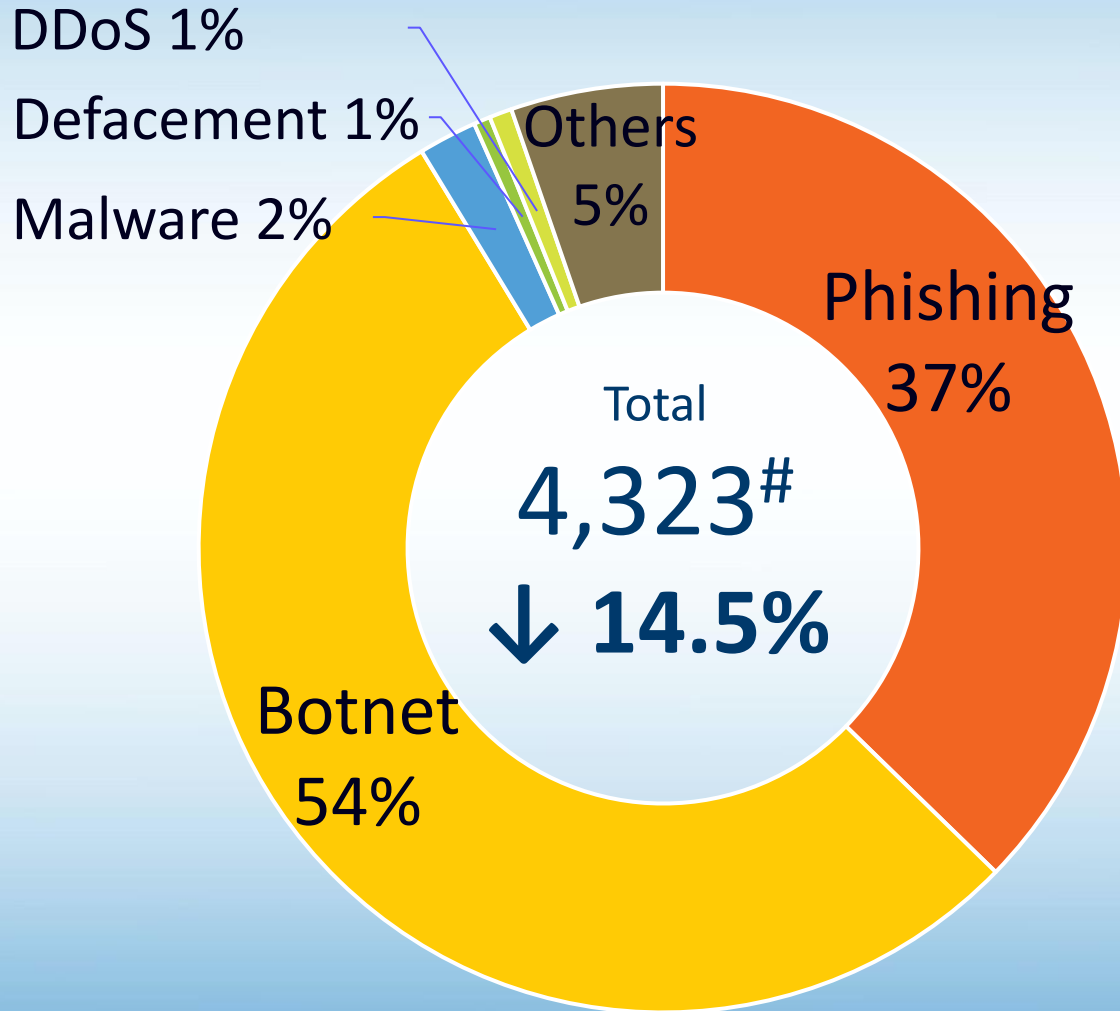
**CYBERSECURITY  
VENTURES**



# HKCERT Incident Reporting of H1 of past 5 years



# HKCERT Security Incident Reports of 2020 H1



## Major Security Incidents

	2019 H1	2020 H1	Change
Botnet	2,365	2,335	↓ 1%
Phishing	1,146	1,612	↑ 41%
Malware	1,141	88	↓ 92%

*Ransomware goes targeting enterprises.*



## Recent Cyber Security Incident Targeting **Organisations**



**Apr 2020** | Unknown activists have posted nearly **25,000 email addresses and passwords** allegedly belonging to the **National Institutes of Health, the World Health Organization, the Gates Foundation** and other groups working to combat the coronavirus pandemic.

# Recent Cyber Security Incident Targeting **Organisations**

## SolarWinds Orion Platform Multiple Vulnerabilities

Last Update Date: 15 Dec 2020 10:55 | Release Date: 15 Dec 2020 | 1205 Views

RISK: High Risk



TYPE: Servers - Network Management



Multiple vulnerabilities were identified in SolarWinds Orion Platform, a remote attacker could exploit some of these vulnerabilities to trigger denial of service, remote code execution and sensitive information disclosure on the targeted system.

**Note: These Vulnerabilities were reported being used in scattered attacks.**

### Impact

- ▶ Denial of Service
- ▶ Remote Code Execution
- ▶ Information Disclosure

**Dec 2020** | Multiple U.S. agencies and private firms were breached by hackers who compromised the software provider **SolarWinds** and exploited their access to **monitor internal operations**.

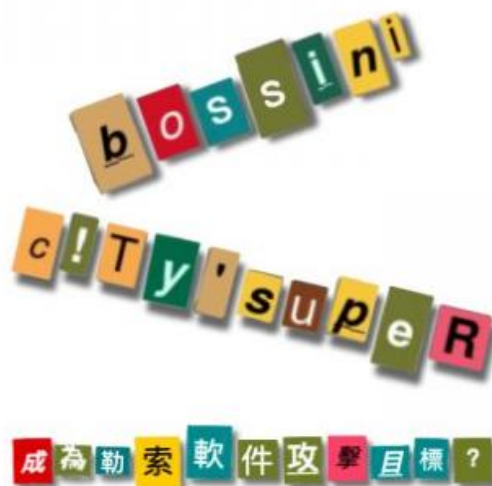


## Recent Cyber Security Incident in Hong Kong

### 【大件事】Bossini、c!ty'super成為勒索軟件攻擊目標？

By WEPRO180 總編 — 最後更新於 Jun 7, 2020

科技傳訊



勒索軟件 (Ransomware) 的確令人聞風喪膽，小編身邊已有唔少朋友嘅公司中咗招，一日唔提高防禦水平，相信受害者將會普遍到總有一個喺左近。就好似最近一個新開張、專門提及有邊啲公司正受到襲擊嘅 Twitter 帳

**Jun 2020** | Hong Kong company **Bossini** and **c!ty'super** were attacked by **ransomware** and reported the **data leak** caused by ransomware groups **Maze** and **Netwalker**.

## Recent Cyber Security Incident in Hong Kong

### 局長都中招！企業手機資訊保安需知

博客論壇 17:33 2020/11/09

👍 44

A+ A- 圖文 關注文章 儲存文章

分享: f d e



香港特區政府通知傳媒，食物及衛生局局長陳肇始的社交媒體《WhatsApp》帳戶被盜用，短暫未能使用。政府未有具體交代該《WhatsApp》帳號如何被盜，只是向傳媒稱說沒有政府相關資料洩漏。

**Oct 2020** | The **WhatsApp** account of the **Secretary for Food and Health, Dr. Sophia Chan** was hacked by others and could not be used for a short time.





## Recent Cyber Security Incident in **Hong Kong**



**Jan 2021** | Massive pan-Asian retail chain operator **Dairy Farm Group** was attacked by the **REvil ransomware** operation. The attackers claim to have demanded a \$30 million ransom.

# Common **Cyber Incidents** in NGO Sector

## Cyber attack targets NGO's Website

- Website Defacement
- Malware Hosting
- Exploit the Vulnerabilities in Open Source Software ( such as WordPress, Django, etc)

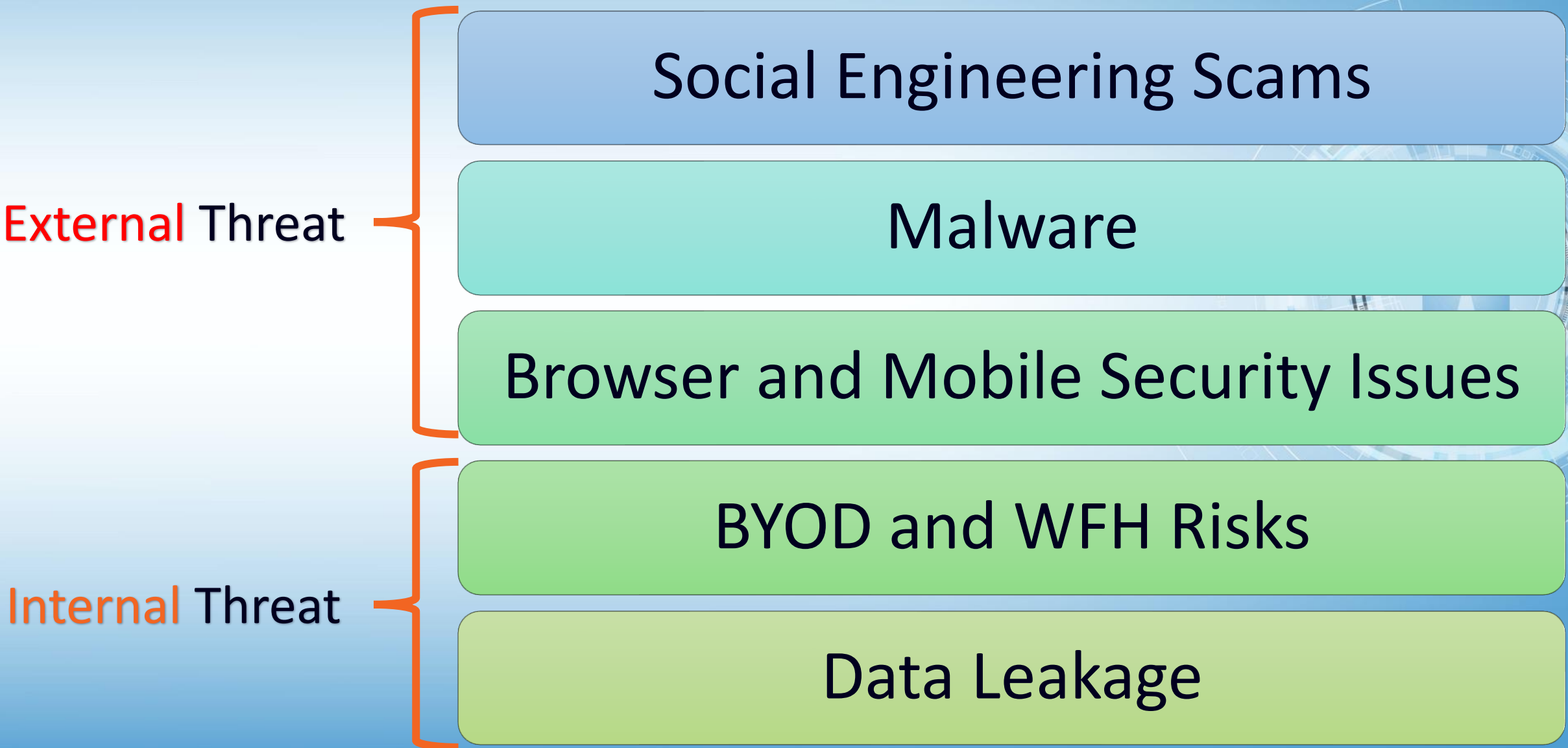
## Online Donation Scams

## Ransomware attack

Laptops and other portable devices (such as tablets, smartphones, USB drives, etc.) are stolen or lost



# Main **Cyber Threats** in NGO Sector



# Protect the Organisation



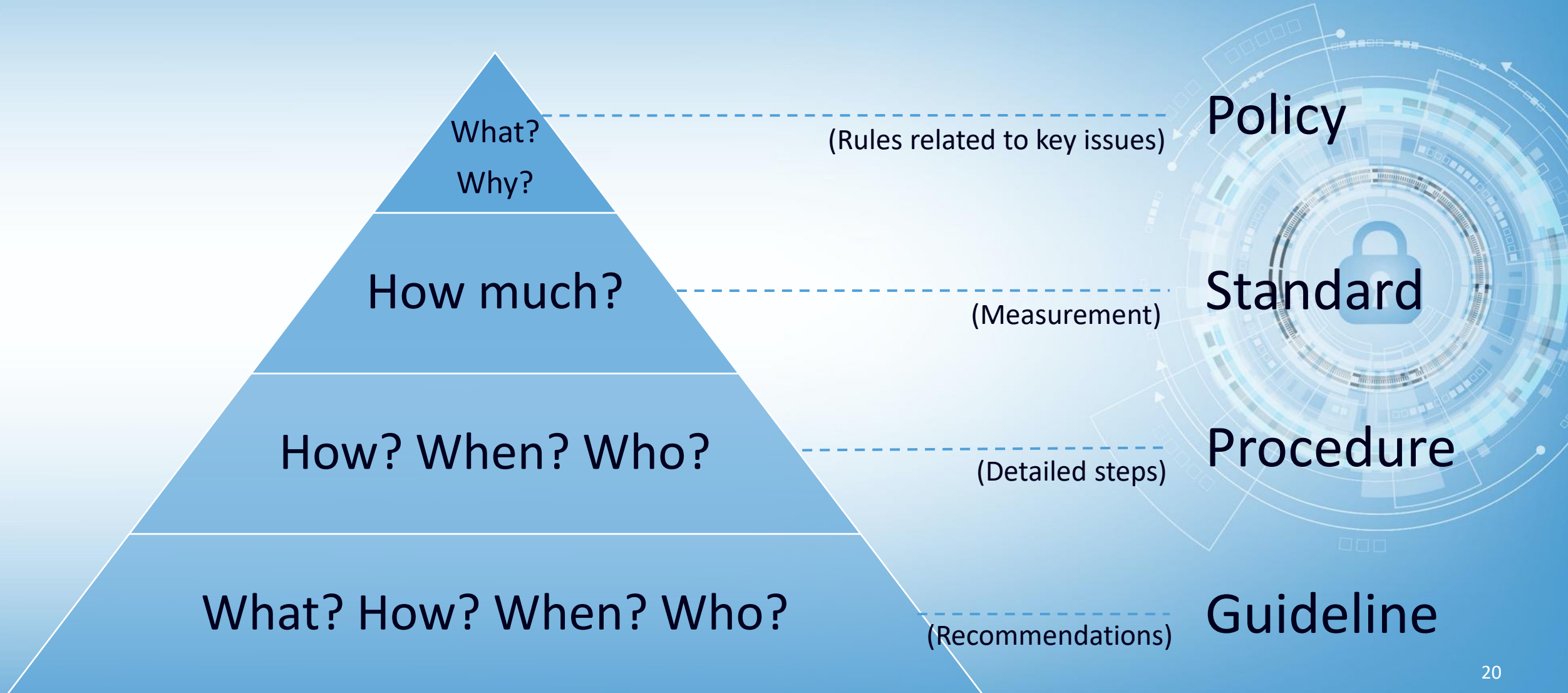


# IT Security Policy

- **Information Security Policies (ISP)** is a set of rules enacted by an organization to ensure that all users within the organization's domain abide by the prescriptions regarding the security of data stored digitally within the boundaries the organization stretches its authority.
- An ISP is **governing the protection of information, which is one of the many assets a corporation needs to protect.** The organization is working off a common understanding of the expectations and a common understanding of terms.



# IT policies, standards, procedures & guidelines





# User Responsibilities

- **Security policies and procedures** should be **accessible to all employees**.
- **Employees at all levels shall read and accept the security policies** to discern how they should act in the best interest of the organization.



# IT Security Practice Guide for the Social Welfare Sector

*Covered 17  
Security Domains*

- 1) IT Security Governance
- 2) Password Control and Authentication
- 3) Websites and Web Applications
- 4) Data Management
- 5) Computer Networks Security
- 6) Email Security
- 7) Cloud Computing Security
- 8) Physical Security
- 9) Mobile Security
- 10) Remote Access/Work from Home
- 11) Security Risk Assessment and Audit
- 12) Insider Threats
- 13) Vendor Management
- 14) Awareness and Training
- 15) Incident Response Management
- 16) Business Continuity Management
- 17) Log Management and Monitoring





# Incident Response Procedure

## Notification

- Report to supervisor
- Report to IT department (email/hotline)

## Record the evidence if possible

- Use mobile phone to take a photo for the abnormal screen
- Forward the phishing email to dedicated mailbox of IT department

## Process and procedure

- Follow the internal handling guideline on loss storage/mobile phone with organisational data





# External Cyber Threat Analysis and Security Advice

010101100110101010101



# Social Engineering Scams



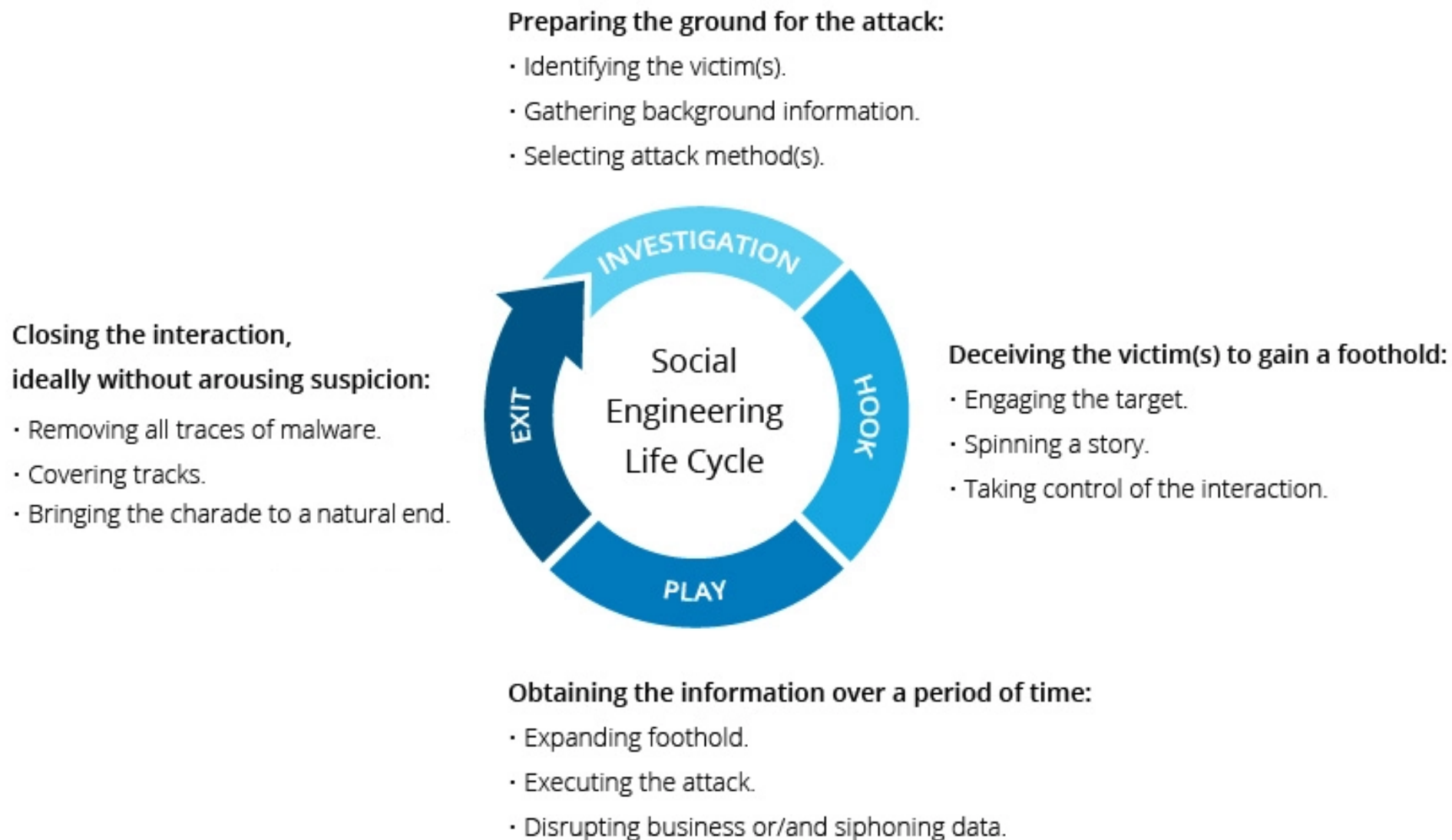
# Social Engineering Scams

**Social engineering** is the term used for a broad range of malicious activities accomplished through **human interactions**. It uses **psychological manipulation** to trick users into making **security mistakes** or giving away **sensitive information**.

- ❖ **98%** of **cyber attacks** rely on social engineering.
- ❖ Social engineering attempts spiked more than **500%** from the first to second quarter of 2018.



# Social Engineering Attack Lifecycle





# Types of Social Engineering Scams

- ❖ **Phishing**
- ❖ Baiting
- ❖ Pretexting
- ❖ Tailgating
- ❖ quid pro quo
- ❖ More others



## Phishing Email



# Phishing Attacks

**Phishing** attackers pretend to be a **trusted institution** or **individual** in an attempt to persuade victims to expose personal data and other valuables.

Phishing ways:

- **Spam** phishing
- **Spear** phishing





# Typical Phishing Methods



Email phishing

Voice phishing  
(vishing)



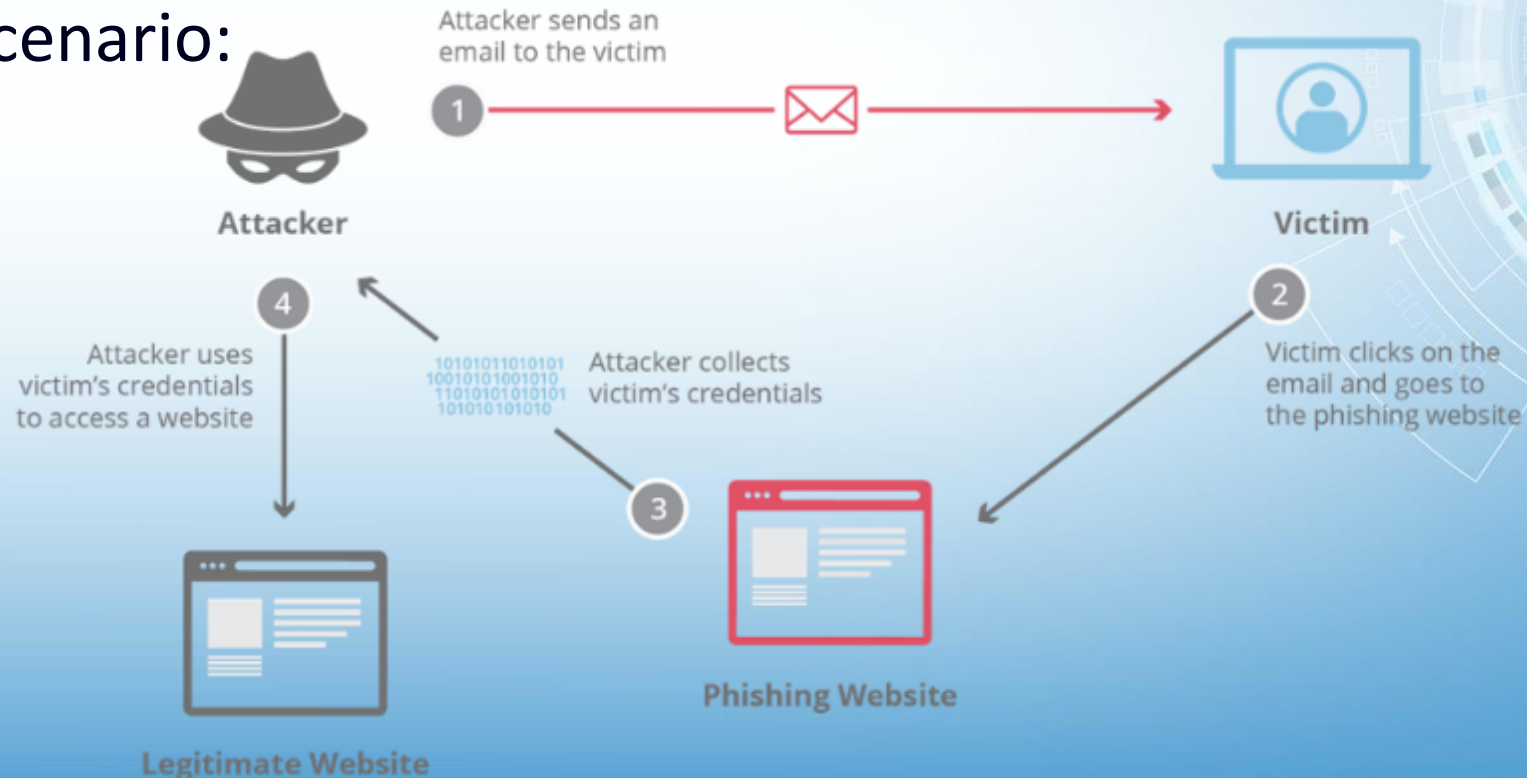
SMS phishing  
(smishing)



# Email Phishing

**Email phishing** is the most traditional means of phishing, using an email urging you to reply or follow-up by other means. Web links, phone numbers, or malware attachments can be used.

Typical scenario:



# Characteristics of a Phishing Email

1. Make **unrealistic** threats or demands
2. The name of the address is **not specified**
3. Sender email address may **be exactly same as** the genuine information of the related organisation
4. Poor **spelling** and **grammar**
5. Appear as an **important notification** from the organisation
6. Include a **mismatched** or **spoofed** hyperlink
7. Request to click the **hyperlink** or open an **attachment** in the email





## Phishing Email Example

你的EMAIL超出最大范围限制。  
[Profile Icon] ( [Email]@ntu.edu.tw) Add contact 2013/3/8 08:31

To:

! This message is High Priority.

You have exceeded your email quota limit of 200MB and you need to expand the e-mail quota before the next 48 hours or your saved mail will be lost and your mailbox closed. If you have not updated your e-mail account in 2013, you must do it now. You can expand to 10GB email quota limit clicking on the hyperlink below to upgrade your account;

[Click Here](#)

URL: <https://docs.google.com/a/blumail.org/spreadsheet/viewform>

Thanks for  
Admin: Copyright © 2013 Webmaster Central Help-desk.

您已超过电子邮件配额限制为200MB，并在未来48小时内或已保存的邮件之前，您需要扩展的e-mail配额将会丢失，并且关闭您的邮箱。如果你还没有更新您的e-mail帐号在2013年，你必须现在就做。升级您的帐户，您可以扩展到10GB点击以下超链接的电子邮件配额限制；

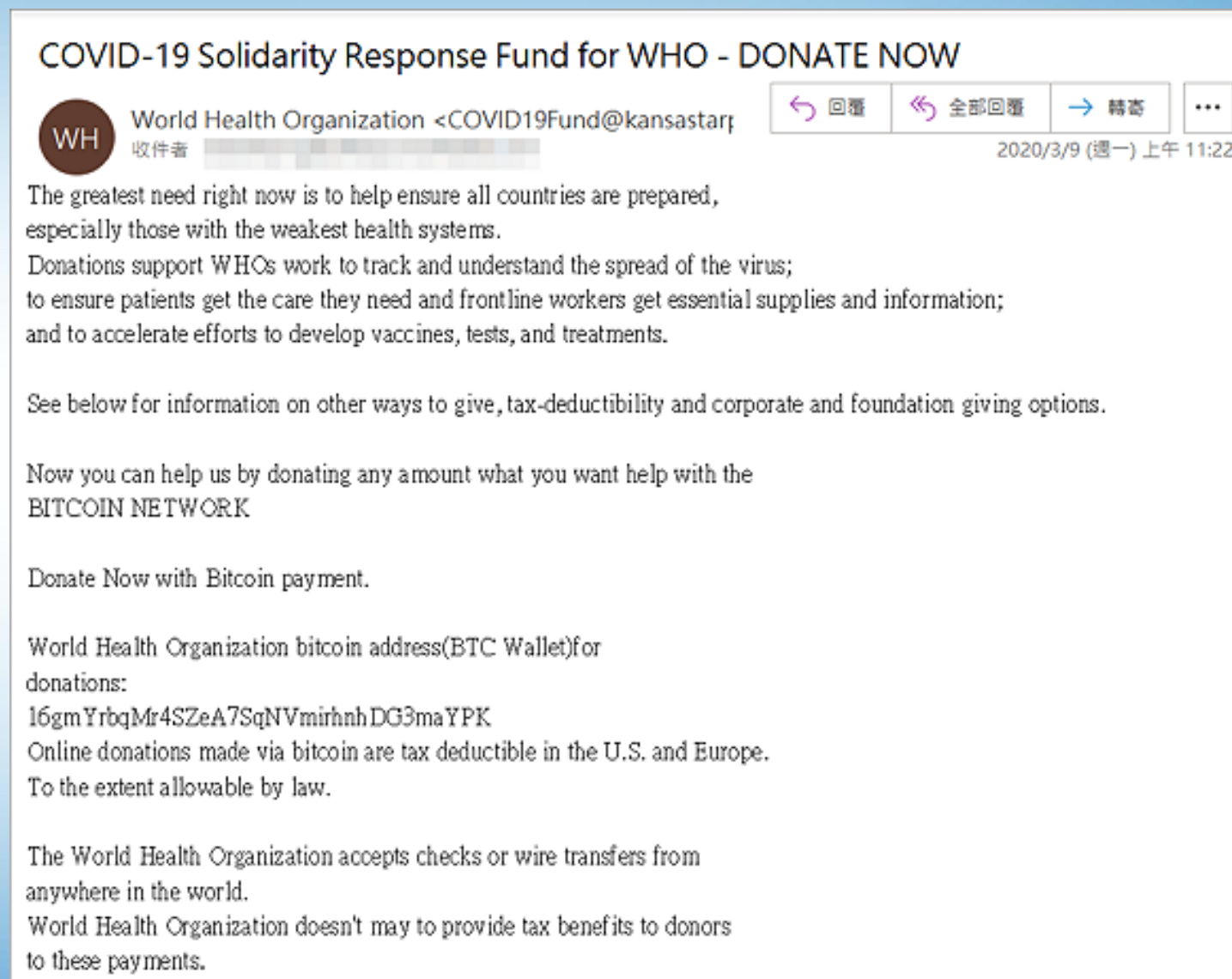
[点击这里](#)

感谢您的  
URL: <https://docs.google.com/a/blumail.org/spreadsheet/viewform>

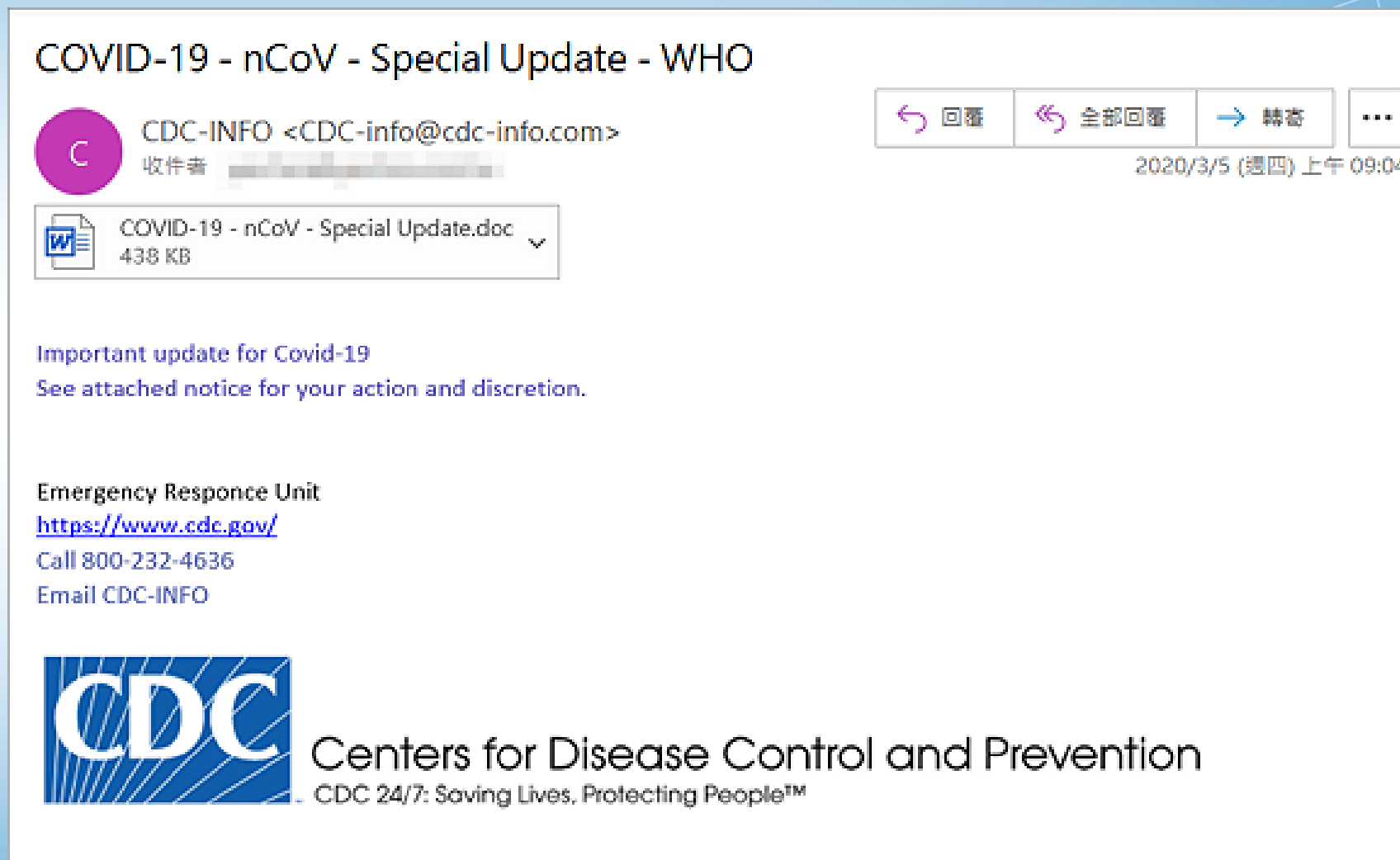
管理员：©2013网站管理员中心帮助台。



## Donation Scam Phishing Email Example

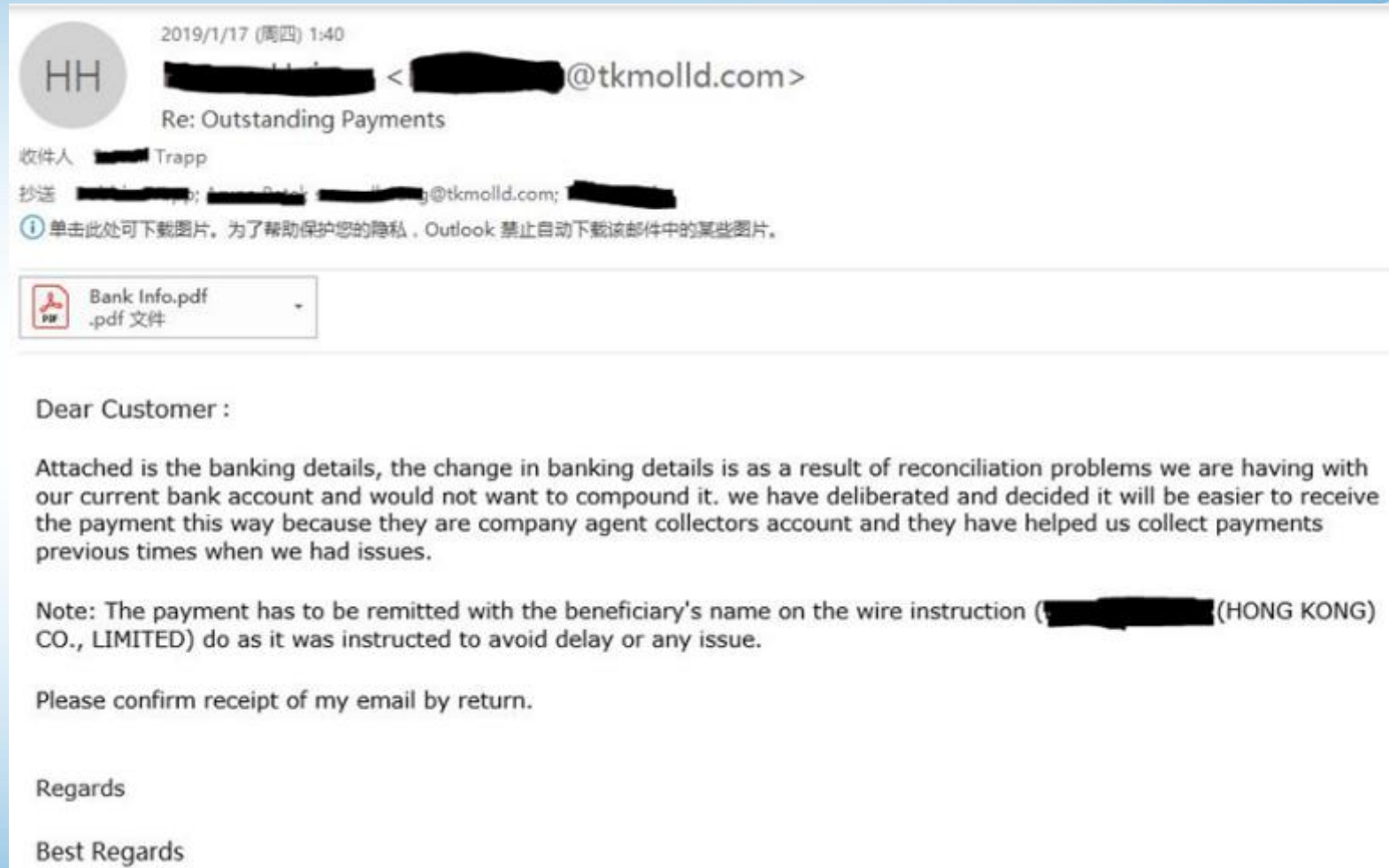


# COVID-19 Related Malware Phishing Email Example












## Business Email Compromise Scam Example



## Ransom Email Scam Example

re: "[redacted]"  **Sample Ransom E-mail**  

 **Dir [redacted]**; <yx[redacted]q@outlook.com> 12:07 PM (8 minutes ago)   

to me ▾

I know, **Home1234**, is your pass word. you may not know me and you are most likely thinking why you're getting this e-mail, correct?

Well, I installed a malware on the adult video clips (pornography) and you know what, you visited this web site to have fun (you know what I mean). When you were watching video clips, your browser started operating as a Rdp (Remote desktop) that has a key logger which gave me accessibility to your screen and also cam. Just after that, my software program gathered every one of your contacts from messenger, social networks, as well as email.

What exactly did I do?

I created a double-screen video. First part displays the video you were watching (you've got a good taste lol), and 2nd part displays the recording of your web cam.

Exactly what should you do?

Well, I believe, \$1200 is a fair price for our little secret. You'll make the payment through Bitcoin (if you don't know this, search "how to buy bitcoin" in google).

**BTC ADDRESS:** 1JC9[redacted]yFjBu7  
(It's CASE sensitive, so copy and paste it carefully)

**Note:**

You have one day to make the payment. (I've a specific pixel in this message, and right now I know that you've read this e mail). If I do not receive the Bitcoins, I will certainly send out your video recording to all of your contacts including friends and family, colleagues, and so forth. nonetheless, if I receive the payment, I'll destroy the video immediately. If you need proof, reply with "yes!" and I definitely will send your video recording to your 14 friends. It is a non-negotiable one time offer, thus don't ruin my time & yours by responding to this e-mail.



# Phishing Email Quiz

## Can You Spot All of the Errors in This Phishing Email?

Payment Declined -- Update Required Immediately!

From: **ApplePay Support** <customer\_support\_ref\_@apple.com>

Dear Apple User,

It has come to our attention that you're recent payment was declined. An update is required immediately..

To make this change, visit the support section at the link below.

<https://www.applepay.com/subscriptions/payment-update>  
<http://944.535.32/index/apple.html>

**If you do not update your payment information in the next 24 hours, your account will be deactivated.**

Regards  
ApplePay Support

—  
Copyright © 2012 Apple Inc.  
All rights reserved  
3 Loop, Madisonville KY 42001


 apple-invoice.zip [Download](#)





# Phishing Email Quiz

## Can You Spot All of the Errors in This Phishing Email?

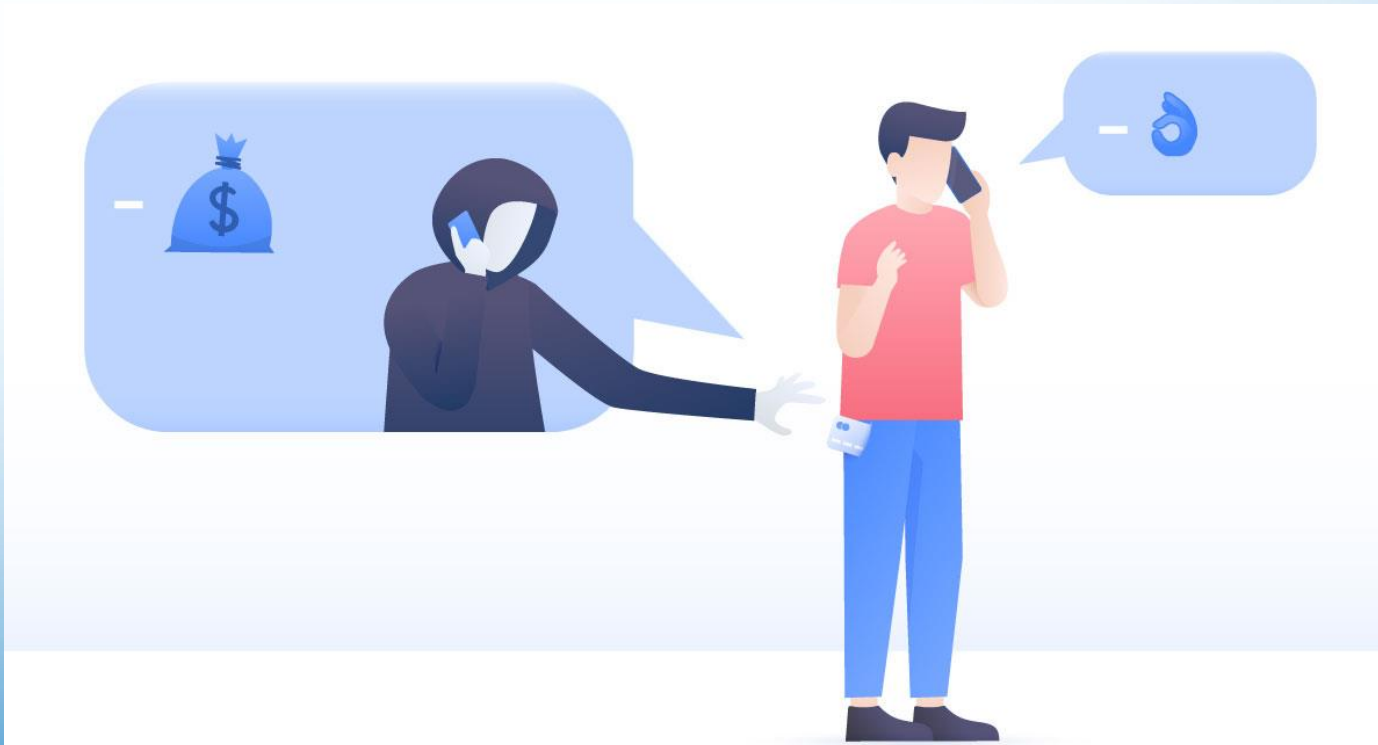
- 1 Payment Declined -- Update Required Immediately!
- 2 From: **ApplePay Support** <customer\_support\_ref\_@apple.com>
- 3 Dear Apple User,
- 4 It has come to our attention that you're recent payment was declined. An update is required immediately..
- 5 To make this change, visit the support section at the link below.  
<https://www.applepay.com/subscriptions/payment-update>  
<http://944.535.32/index/apple.html>
- 6 If you do not update your payment information in the next 24 hours, your account will be deactivated.
- 7 Regards  
ApplePay Support
- 8 Copyright © 2012 Apple Inc.  
All rights reserved  
3 Loop, Madisonville KY 42001
- 9  apple-invoice.zip [Download](#)

- 1 Sense of urgency  
Fear tactics
- 2 Imitating known brand  
Fake email address
- 3 Impersonal
- 4 Urgency  
Punctuation and grammar mistakes
- 5 Rollover shows malicious link
- 6 Scare tactics
- 7 Impersonal  
Not real customer service
- 8 Copyright date is incorrect  
Location is incorrect
- 9 ZIP file



# Voice Phishing

**Voice phishing** (vishing) phone calls may be **automated message systems** recording all your inputs. Sometimes, a **live person** might speak with you to increase trust and urgency.



# Common Vishing Examples

- **Telemarketing or enterprise fraud**
- **Government fraud**
- **Tech support fraud**
- **Bank or other financial institutions fraud**
- **Relationship fraud**



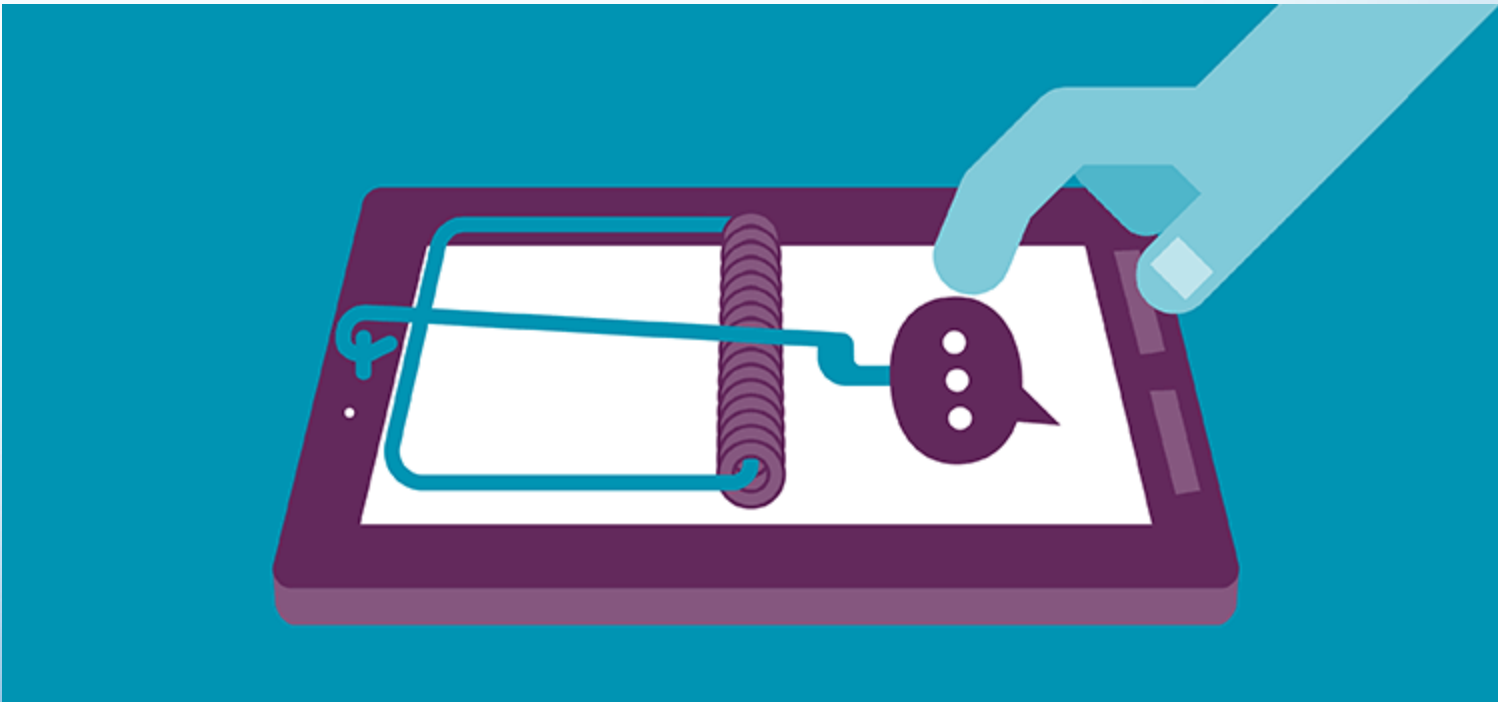


## Vishing

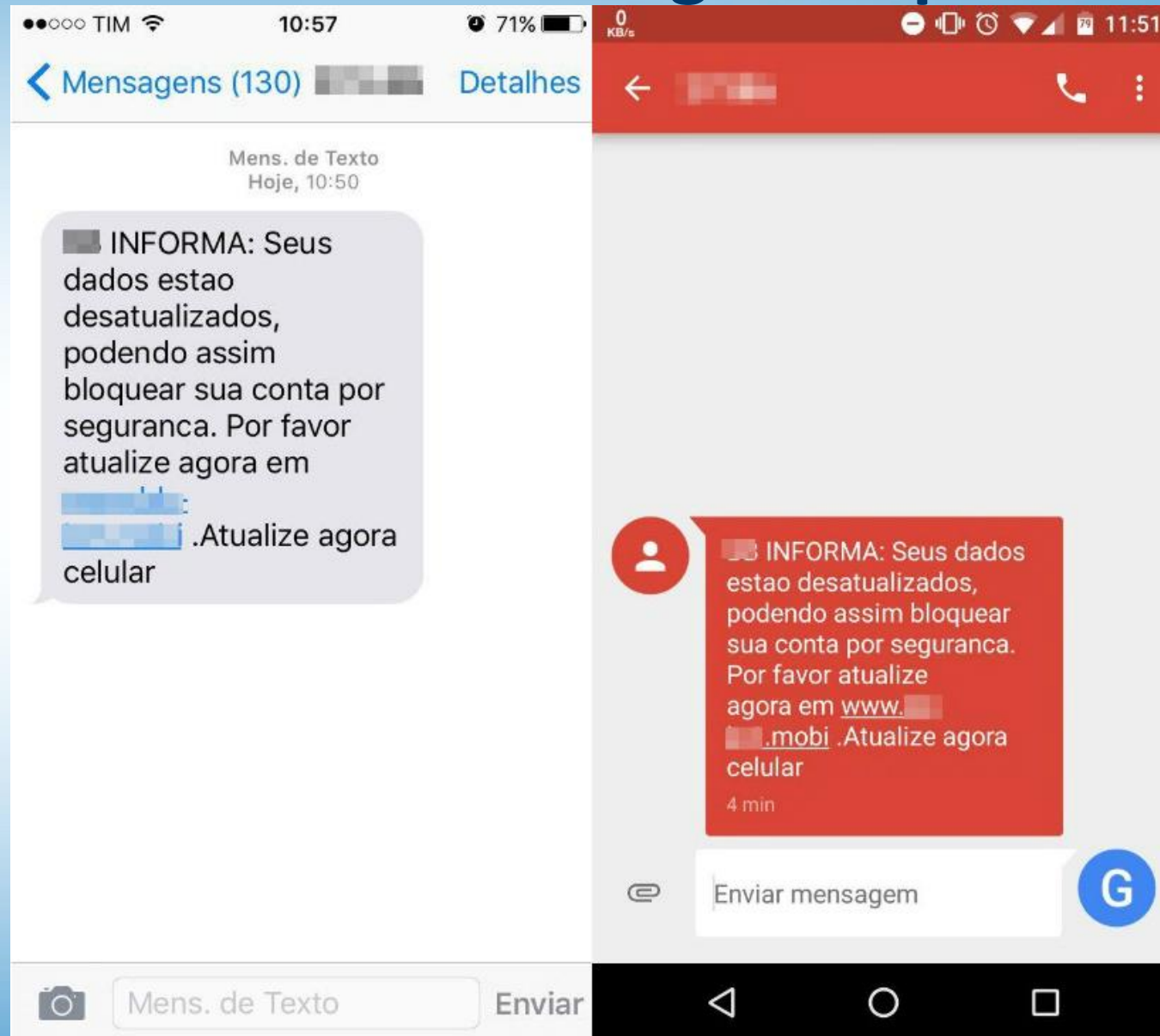


# SMS Phishing

**SMS phishing** (smishing) **texts** or **mobile app messages** might include a web link or a prompt to follow-up via a fraudulent email or phone number.



## SMS Phishing Example





## Social Media Phishing Example



## Social Media Phishing Example

上水15歲青年疑墮裸聊陷阱遭拍片 被勒索損失3,000元





# Security Advice for General Users

- **Keep calm**
- **Verify** the sender's identity
- **Contact** the legitimate sender via **other method** for **double confirmation**
- **Confirm** the URL is legitimate before clicking
- **Do not** open suspicious attachments or links
- **Do not** leave devices, such as mobile or laptop connected to organisation networks, unattended in public areas
- **Report** to your organisation when receiving suspicious social engineering attack





# Malware



# Malware

**Malware**, short for malicious software, is a blanket term for viruses, worms, trojans and other harmful computer programs hackers use to **wreak destruction** and **gain access** to sensitive information.



# Types of Malware

## ❖ Ransomware

- ❖ Viruses
- ❖ Worms
- ❖ Trojans
- ❖ Spyware
- ❖ Cryptojacking
- ❖ Adware
- ❖ Rootkit
- ❖ Botnet





# Ransomware

**Ransomware** is a type of malware that threatens to **publish the victim's data** or perpetually **block access** to it unless a **ransom** is paid.

Main types:

- **Crypto** ransomware
- **Locker** ransomware



# Ransomware Chain



# Ransomware Typical Infection Vector

Spam email

Compromised websites

Malvertising

Vulnerability exploitation

Remote access

Self-propagation





# New Trends of Ransomware

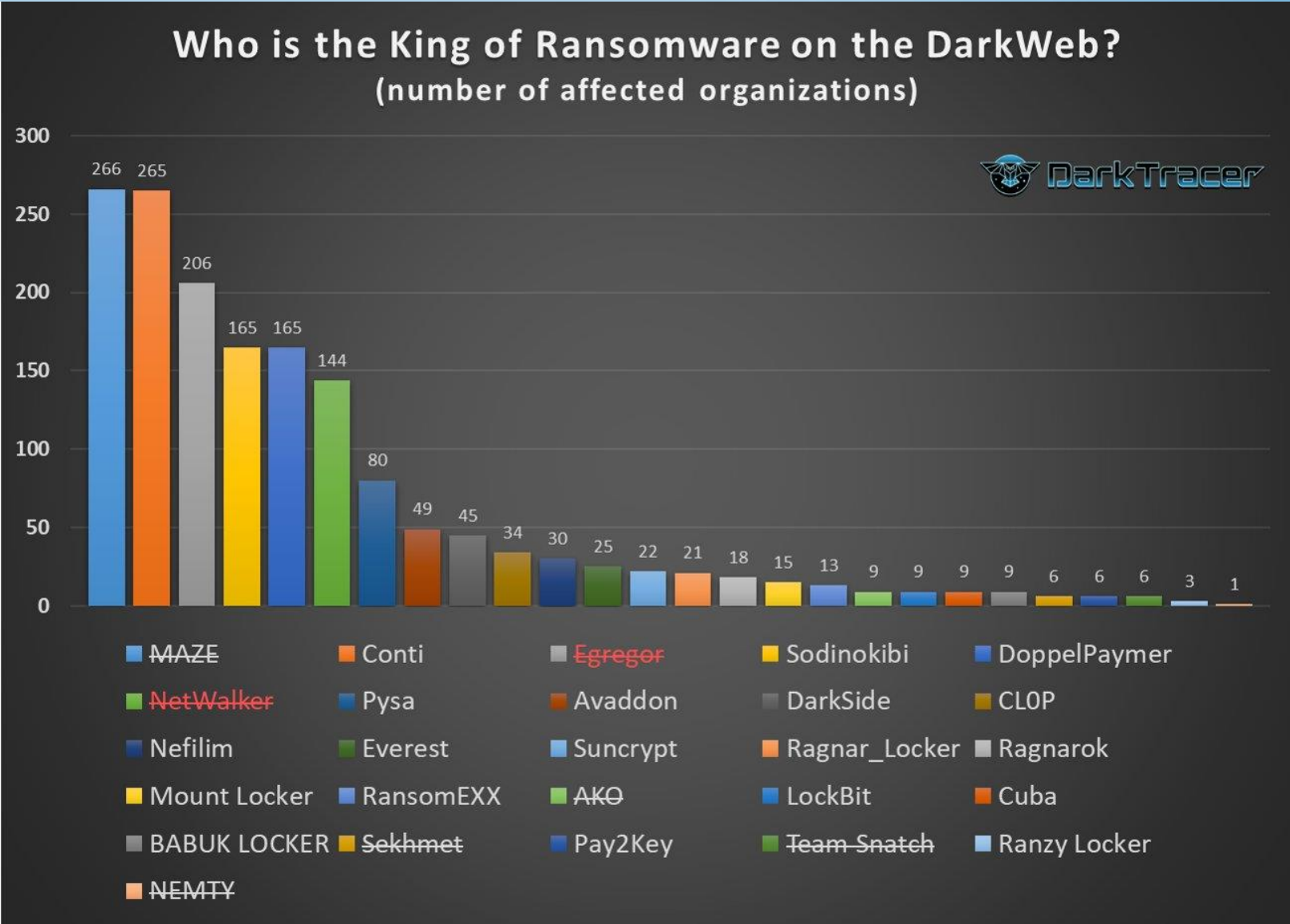
**Ransomware Evolved: Double Extortion and Fake Decryptor**

**Ransomware: Double Extortion Attacks Continued - Intrusion via Exploiting VPN Gateway Vulnerability**

**Some ransomware gangs are going after top execs to pressure companies into paying**

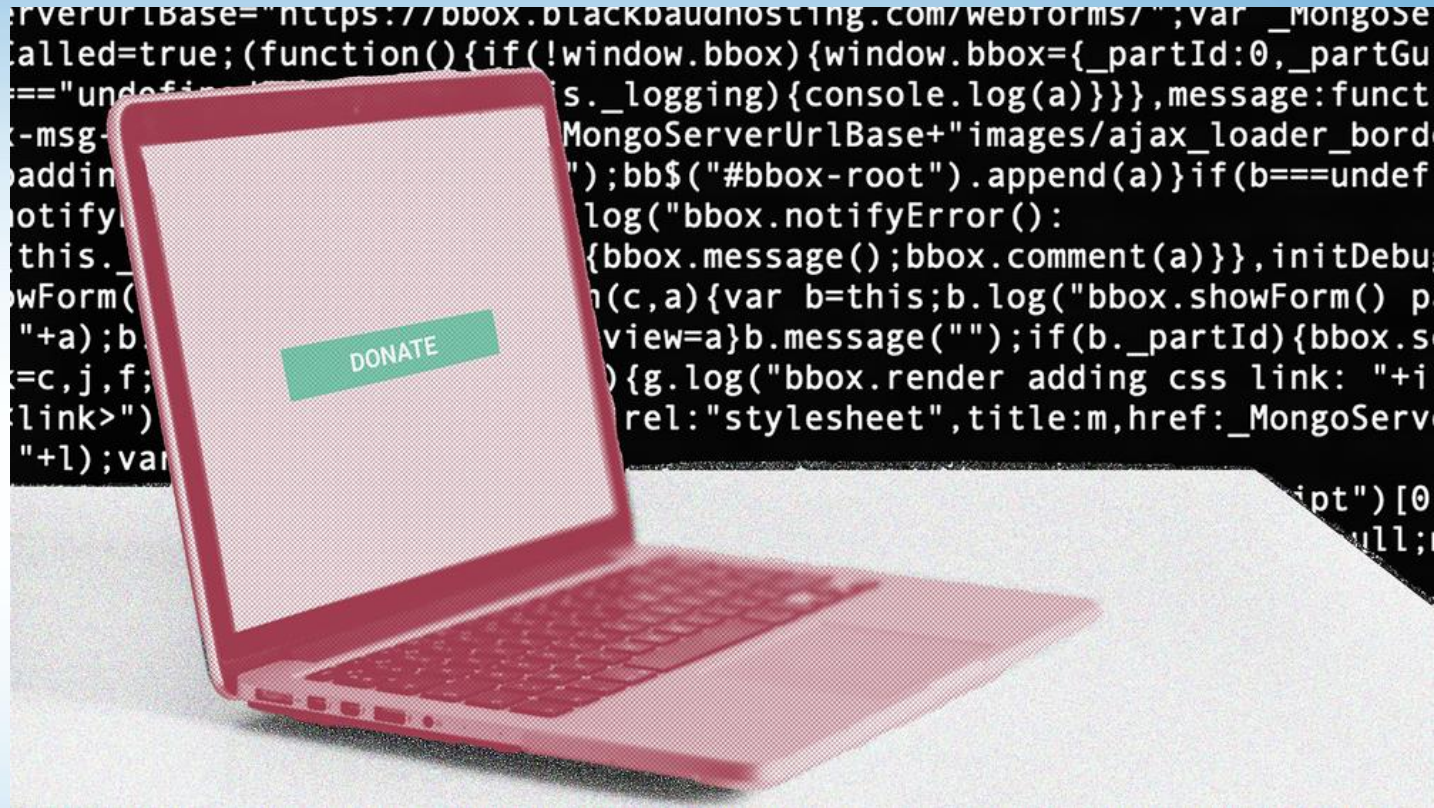
Ransomware gangs are prioritizing stealing data from workstations used by executives in the hopes of finding and using valuable information to use in the extortion process.

# Statistics of Ransomware on the DarkWeb





## Ransomware Attacks on NGOs

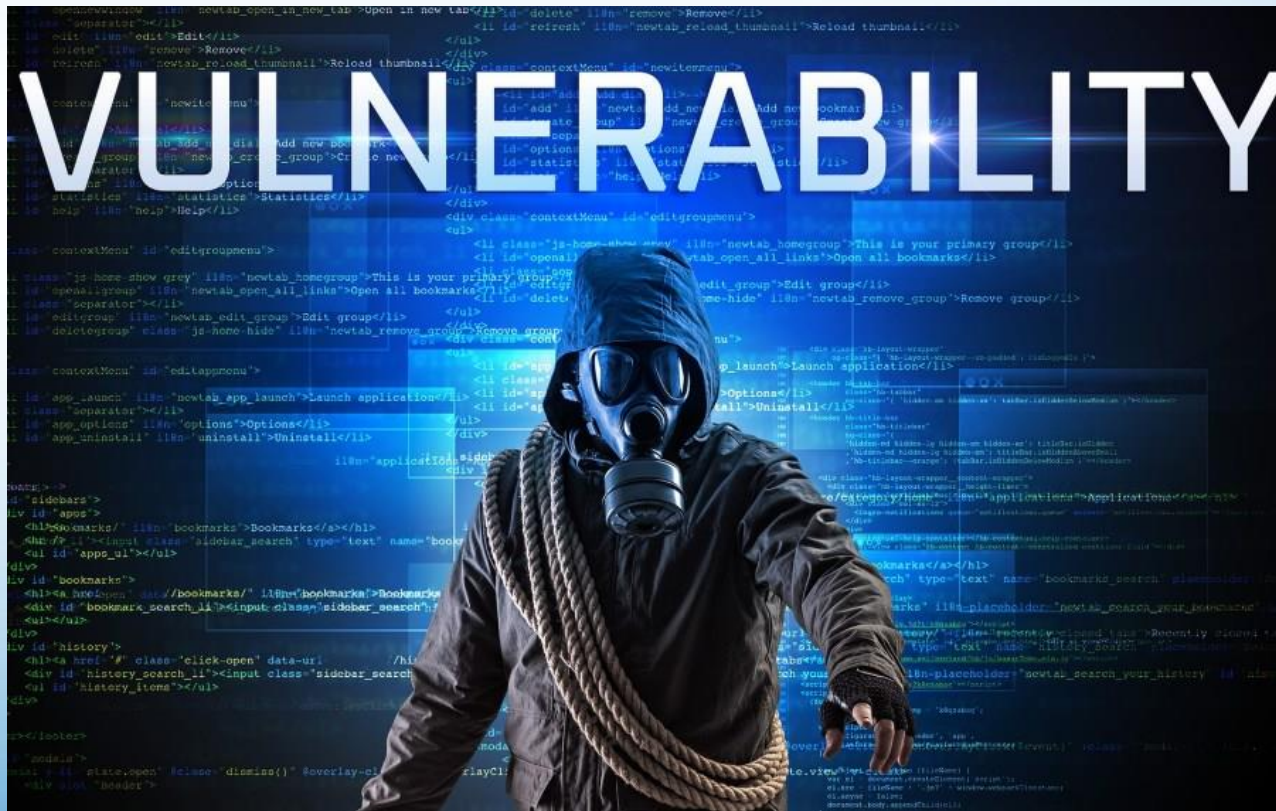


**A major ransomware attack has affected dozens of international NGOs and their records of private donations, but details of the hit on a US fundraising platform are scarce, and two weeks after being warned some aid groups are yet to notify their donors or the public.**



# Vulnerability

In computer security, a **vulnerability** is a weakness which can be exploited by a threat actor, such as an attacker.



# Zero-day

A **zero-day** (also known as 0-day) vulnerability is a computer-software vulnerability that is unknown to those who should be interested in mitigating the vulnerability (including the vendor of the target software).



## Microsoft Exchange Server Zero-day Vulnerabilities

### **Microsoft rushes out fixes for four zero-day flaws in Exchange Server**

At least one vulnerability is being exploited by multiple cyberespionage groups to attacks targets mainly in the US, per ESET telemetry



## Ransomware Attacks with Highest Ransom

### Computer giant Acer hit by \$50 million ransomware attack

By [Lawrence Abrams](#)



March 19, 2021



11:11 AM



0



# Security Advice for General Users

- **Follow** the security policy of your organisation
- **Install** an **anti-malware** program to protect your computer
- **Install** and **enable computer firewall**
- **Ensure** your computer has the **latest security patches**
- **Schedule** a daily full **scan** to check for malwares
- **Check** all removable disks and files downloaded from the Internet
- **Stop** all activities on a computer if it becomes infected by malware
- Before installing any software, do **verify** its integrity
- **Backup** your programs and data regularly and keep the backup copies **disconnected** from the computer
- Constantly **aware** of any **suspicious activities**
- **Contact** your organisation IT staff for **support**
- **Report suspicious activities** to your organisation



# Security Advice about Malware Infection

- **Isolate** and **disconnect** infected machine immediately
- **Contact** the organisation IT staff for help to clean the malware
- **Restore** the files and data from the backup
- If no backup was done previously, we suggest **not restoring** the system to avoid losing information required for decryptions
- **Report** the incident to your **organisation** and **HKCERT**





# Browser and Mobile Security



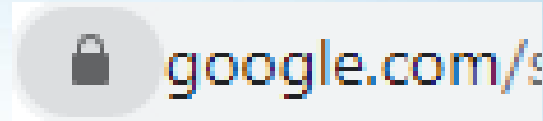
# Browser Security

- Beware of malicious plugin
- Use trusted browser

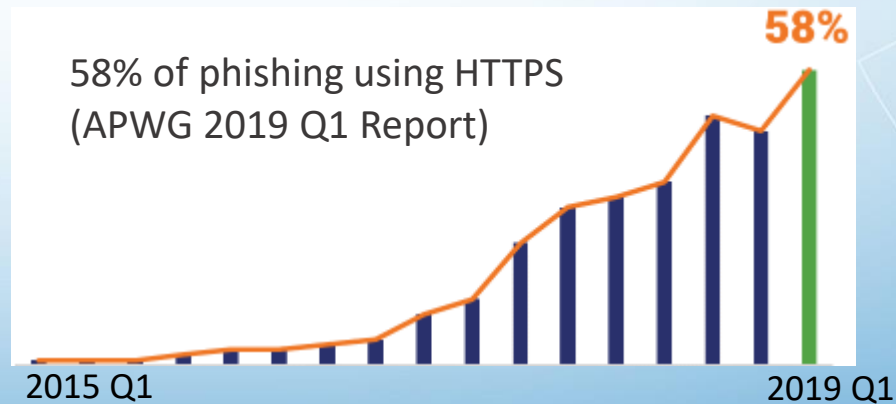


# Browser Security

- Traditionally, the “lock” symbol shows on the web browser can tell you if the connection is protected by SSL/TLS



- Is the SSL/TLS certificate and Certificate Authority trustworthy ?





## Phishing Website Example



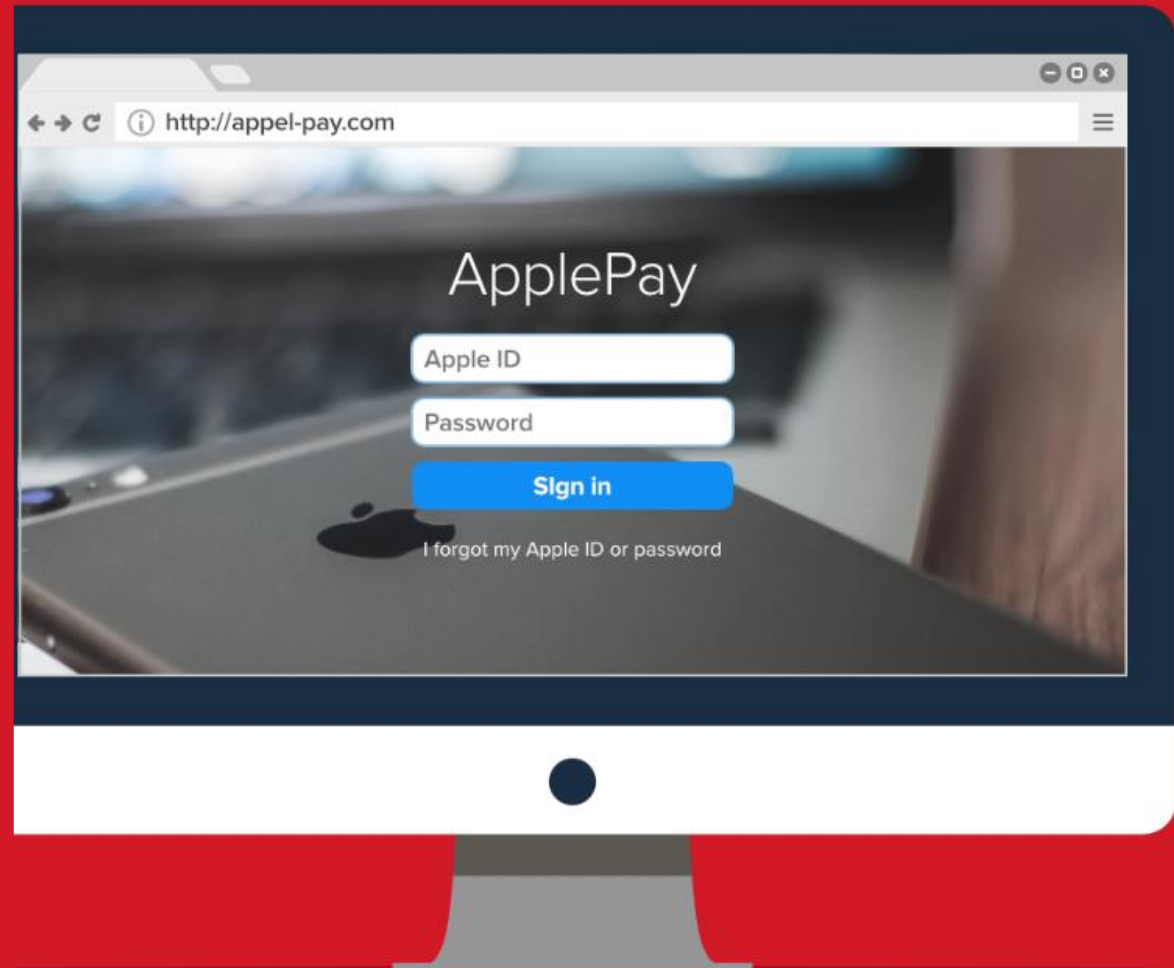
## Defacement Website Example



Hacked by MrAxxCT  
MR-AXXCT-ID18@MMMDK.COM

# Spot Malicious Website

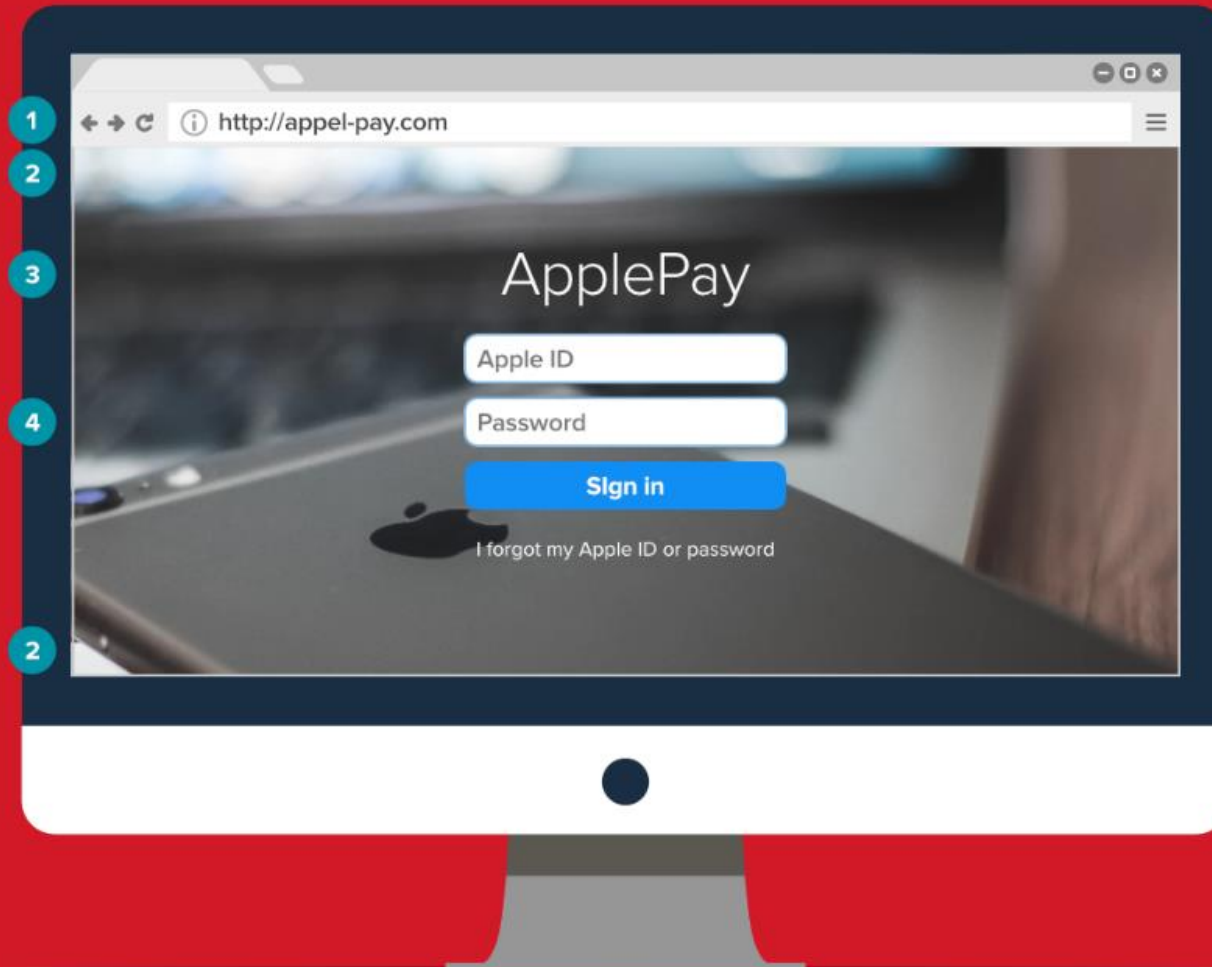
## How to Spot a Malicious Landing Page





# Spot Malicious Website

## How to Spot a Malicious Landing Page



1  
Not a legitimate  
Apple website  
address

2  
Missing  
navigation bar  
and footer

3  
"Apple Pay"  
is misspelled

4  
Apple ID  
homepage doesn't  
require password

## App Permission



- What's the permission(s) the App try to grant? (e.g. Why a Calculator App need to access your phonebook?)
- How the developer going to use your data / info provided?



- Always read carefully on the permission(s) that the App is trying to grant before install it
- Read the T & C on how your data collected will be used for and how to revoke it once uninstall the app

## App Permission

The screenshot shows a ZDNet article with the headline "Two-thirds of all Android antivirus apps are frauds". The sub-headline reads: "Only 23 Android antivirus apps had a 100 percent detection rate with no false positives." The byline is "By Catalin Cimpanu for Zero Day | March 14, 2019 -- 20:24 GMT (04:24 GMT+08:00) | Topic: Security". The article features a large image of a hand holding a tablet displaying a shield with a green checkmark. A red box with a yellow warning icon and the text "Is the App coming with the functionality it claimed for?" is overlaid on the left side of the image. To the right, a blue box contains the text "Study the trustworthiness of software developer before you install". The article text below the image states: "An organization specialized in testing antivirus products concluded in a report published this week that roughly two-thirds of all Android antivirus apps are a sham and don't work as advertised."

**Is the App coming with the functionality it claimed for?**

**Study the trustworthiness of software developer before you install**



## Trust Source

The screenshot shows a ZDNet article from July 4, 2019, about a fake Samsung firmware update app. The article title is 'Fake Samsung firmware update app tricks more than 10 million Android users'. The sub-headline reads: '\*Updates for Samsung\* app promises firmware updates but only shows ads and wants money for (working) downloads.' The author is Catalin Cimpanu. Below the article, there are social media sharing buttons and a section titled 'MORE FROM CATALIN CIMANU' with links to other security-related articles. A red box with a warning icon and a blue box with a lightbulb icon are overlaid on the screenshot, containing text about downloading apps from official sources.

**Fake Samsung firmware update app tricks more than 10 million Android users**

\*Updates for Samsung\* app promises firmware updates but only shows ads and wants money for (working) downloads.

By Catalin Cimpanu for Zero Day | July 4, 2019 -- 17:34 GMT (01:34 GMT+08:00) | Topic: Security

**Always download the App from official App Store / official website**

- Samsung Phone users were using 3<sup>rd</sup> party Update App for OS / firmware update purpose

# Mobile Security Risks

- **Store sensitive information** to the mobile device
- **Sending sensitive information via IM Instant messaging** (IM) e.g. WhatsApp
- Repair the personal mobile **contains organization data** without secure remove the data
- **Lose** the mobile phone
- Mobile phone **without screen lock**



# Security Advice for General Users

- **Do not store sensitive information** to the mobile if unnecessary
- **Protect your IM accounts** (enable 2 factor authentication)
- **Secure remove the data** before sending it to repair
- **Protect** the mobile **physically**
- **Enable** screen lock
- **Avoid** using **public Wi-Fi**
- **Report** to IT department and management if you **lose the mobile which contains organization information**





5

# Internal Cyber Threat Analysis and Security Advice



# BYOD and WFH Risks



# BYOD and WFH





# Major BYOD and WFH Cyber Security Risks

Third-party network flaws

Rooted and jailbroken devices

Malformed content

Lost or stolen gadgets

OS-related vulnerabilities

Malicious apps

Online meeting attack



## BYOD Risks

### 从BYOD到BYOIT，物联网风险骤增

在新冠疫情爆发之前，BYOD始终是困扰企业安全主管的影子IT问题，2020年上半年新冠疫情的爆发，导致企业远程办公人数激增，BYOIT成了新的问题。所谓BYOIT就是员工使用家庭设备（不仅限于手机和PC），还包括个人应用，例如文件共享和视频会议，以及个人网络和存储设备，例如家庭NAS和WiFi路由器，甚至智能家居设备，例如智能音箱和摄像头。

BYOIT极大地增加了企业的攻击面和资产暴露面，同时也成为网络犯罪分子和黑客的热门目标。在11月举行的东京Pwn20wn 2020黑客大会上，消费级路由器和NAS成为参赛漏洞赏金猎人的主要收入来源，这也说明家庭WiFi路由器、NAS存储设备和智能电视等智能家居相关设备存在大量漏洞并且容易得手。



## Zoom-Bombing Attacks

### FBI Warns of Ongoing Zoom-Bombing Attacks on Video Meetings

By [Sergiu Gatlan](#)

March 30, 2020 05:30 PM 0



The US Federal Bureau of Investigation (FBI) warned today of hijackers who join Zoom video conferences used for online lessons and business meetings with the end goal of disrupting them or for pulling pranks that could be later shared on social media platforms.

"The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language," the warning published by FBI's Boston Division says.





## Remote Work and Video Conferencing



# Security Advice for General Users on BYOD and WFH

- **Keep** software and device **up-to-date**
- **Do not** root and jailbreak your devices
- **Install** anti-malware and set up **auto-update**
- Always **update** the remote access software to latest version
- **Keep** your remote access devices securely
- **Report** to your organisation immediately for any **loss** and **theft**
- **Pay attention** to latest cyber vulnerability information



# Security Advice for General Users on Video Conferencing

- **Use** the latest version of video conferencing application and security software
- **Beware of** any Universal Naming Convention (UNC) links shared by unknown participants
- **Do not** share confidential information during the meeting
- **Use** a meaningful display name
- **Protect** video conferencing account and monitor suspicious activities





# Security Advice for Video Conferencing Hosts

- Make meetings **private** and **deny** trespassers
- **Monitor** your own meeting
- **Pay attention** to security and privacy of meeting recording
- **Keep** your Personal Meeting ID private
- Set up **security policy** for web meetings



# Data Leakage



# Data Values in the Underground Market

Rank	Item	Percentage	Range of Prices
1	Credit cards	28%	\$1 - \$30
2	Bank accounts	24%	\$10 - \$125
3	Email accounts	8%	\$5 - \$12
4	Email addresses	5%	\$5 - \$10 per MB
5	Credit card dumps	4%	No specified prices
6	R57 & C99 shells	3%	\$2 - \$5
7	Full identity	3%	\$3 - \$20
8	Mailers	3%	\$1 - \$5
9	Attack toolkits	3%	\$5 - \$20 or \$120 per month
10	Cash-out services	2%	\$200 - 100 or 50% - 70%



## Data Leakage Incident

### 明愛向晴軒遺失載有理大學生資料USB

2020年9月17日 23:25



【Now新聞台】明愛向晴軒有社工，遺失載有理大學生資料的USB，121名學生受影響。

向晴軒指一名社工在本月四日，意外遺失載有121名理大學生基本資料的USB，指事件是個別人為疏忽，會紀律處分有關社工，並成立專責小組全面檢討問題，對受影響學生致歉。

理大就表示，接獲向晴軒通知事件。指據了解，遺失的USB大部分資料已加密，但有幾名同學的資料無加密。私隱專員公署指已收到通報，表示關注事件，並會展開循規調查。

**Sep 2020** | A support centre run by the **NGO Caritas Hong Kong** has issued an apology after a social worker lost a **USB flash drive** containing personal information on 121 POLYU students.

# Data Leakage Incident

港大法律學院洩漏2500學生資料 有人收簡體字黑客勒索比特幣電郵



社會新聞

👍 讚好 182

撰文：鄧穎琳 胡家欣 ⌚ 2020-06-18 18:19 最後更新日期：2020-10-27 20:16

港大法律學院昨日因操作程序出錯，誤將逾2500位學生個人資料外洩。《香港01》今（18日）接獲一位受影響學生投訴指，與至少兩位同學收到自稱「黑客」的勒索電郵，內文以簡體字撰寫，威脅她們須在24小時內，繳付價值1,250美元比特幣，即相等於約9,688港元，否則會將涉及她們私隱的影片公開。該學生心黑客電郵只屬「冰山一角」，未來會變本加厲，又斥學院未曾提供協助。





## Data Leakage Incident

天文台政府天氣資訊系統被入侵 370多個用戶電郵地址外洩



社會新聞

👍 讚好 7

撰文：王潔恩    ⌚ 2020-11-02 20:25    最後更新日期：2020-11-02 23:33

天文台表示，供傳媒使用的政府天氣資訊系統伺服器，最近曾被不明人士入侵。該伺服器內儲存了非敏感的天氣數據，以及12間傳媒和370多名用戶的註冊電郵名單。天文台向受影響用戶發電郵，並就事件致歉。





## Twitter Scam Incident

### Major US Twitter accounts hacked in Bitcoin scam

🕒 16 July 2020



Kim Kardashian West, Kanye West, Elon Musk, Bill Gates and Barack Obama were all 'hacked'

Billionaires Elon Musk, Jeff Bezos and Bill Gates are among many prominent US figures targeted by hackers on Twitter in an apparent Bitcoin scam.

## Facebook Data Leakage Incident



HKCERT

4月4日 21:17 · 🌐



### 【3百萬個香港Facebook帳戶資料外洩】

黑客剛剛公開咗全球共5億3 千3百萬個Facebook帳戶資料，包括手機號碼、用戶名稱、性別及工作地點等，當中有近3百萬個係屬於香港帳戶，即係話大家嘅手機號碼即使 set 左不公開，但宜家都被黑客偷晒出嚟任人睇。

黑客其實早於2019年已偷咗相關資料，販賣完結後先喺呢兩日對外公開，其他罪犯可能利用資料進行新一波釣魚詐騙，Facebook 帳戶被入侵還可能影響其他經Facebook 登入的服務。HKCERT提醒大家提防詐騙電話，sms/WhatsApp等短訊及帳戶被盜。

請緊記六招應對黑客：

1. 提防利用個人資料進行嘅釣魚詐騙電話及短訊
2. 切勿點擊可疑電郵、短信、連結或附件
3. 更改帳戶密碼及啟用雙重認證，以減低密碼被盜影響
4. 定期檢閱帳戶有否可疑的登入紀錄
5. 檢查及移除不再需要使用 Facebook 登入的網上服務
6. 參閱網絡帳戶的私穩設定，盡量減少個人資料的公開程度

參考連結：

<https://www.bleepingcomputer.com/.../533-million.../>

<https://therecord.media/phone-numbers-for-533-million.../>

#數據外洩 #DataLeakage





# Password Protection

## The Most Popular Passwords Around the World

Most popular passwords appearing in leaks 2018/2019

	2019	change from previous year		2018	change from previous year
1.	123456*	0		123456*	0
2.	qwerty	+3		password	0
3.	password	-1		111111	new
4.	iloveyou	+2		sunshine	+51
5.	111111	-2		qwerty	-2
6.	123123	+6		iloveyou	0
7.	abc123	+4		princess	new
8.	querty123	+12		admin	-1

\* or variation

Source: SplashData

Source: Hive Systems

## TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years



## Cloud Data Security



# Security Advice for General Users

- **Follow** organization's security policy e.g. Data retention
- **Enable 2FA/ MFA**
- Use **long** and **complex** password
- **Encrypt** file(s) contain sensitive information
- **Protect** the USB and cloud storage properly
- **Grant** permission by need
- **Review** configuration, settings and permission regularly
- **Backup** your data





6

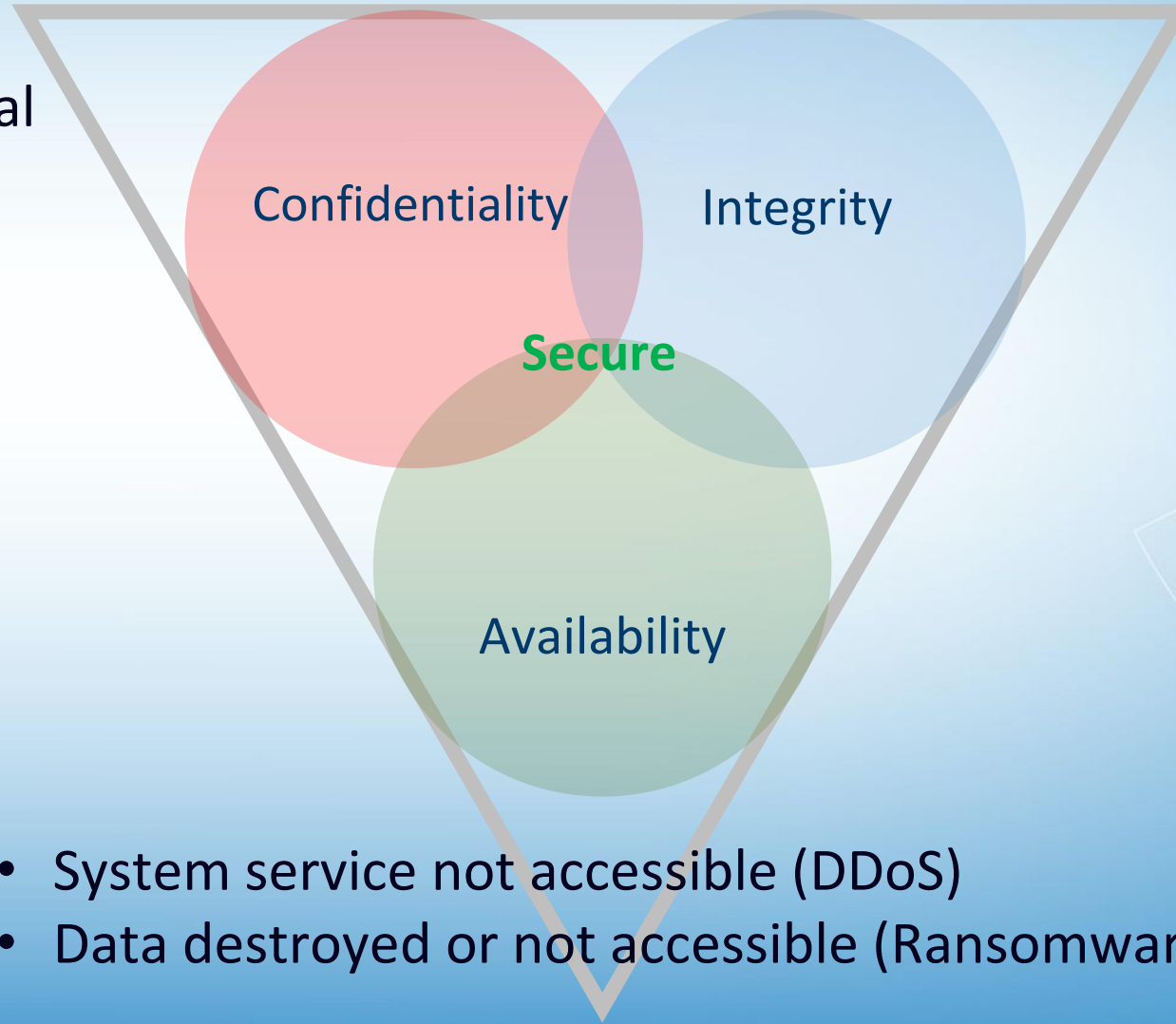
# Key Take Away





# Basic Concept: CIA Triad of Cyber Security

- Leaking confidential data

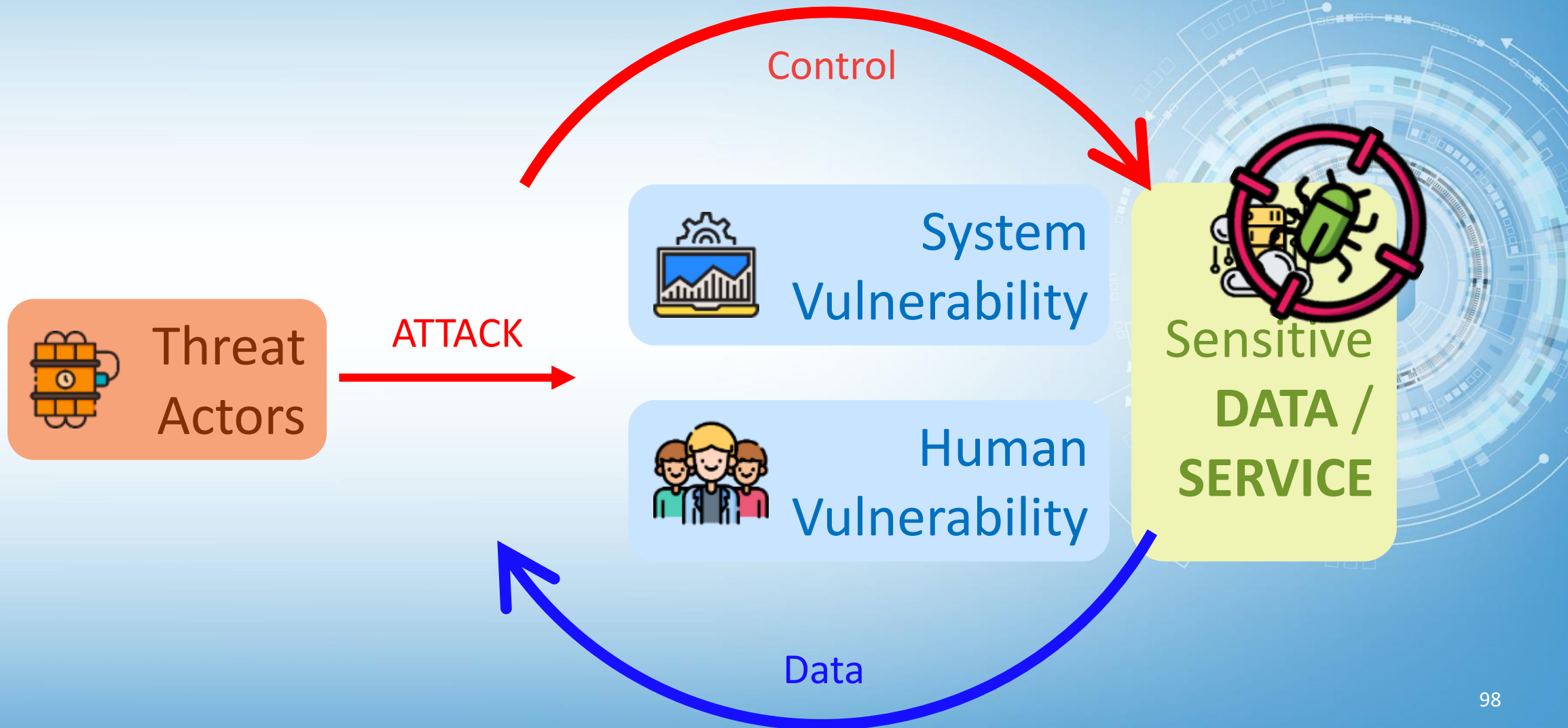


- Data contaminated
- Forged transaction
- System compromised
- Identity spoofed

- System service not accessible (DDoS)
- Data destroyed or not accessible (Ransomware)



# Threat, Vulnerability & Attack



# Incident Response Procedure

## Notification

- Report to supervisor
- Report to IT department (email/hotline)

## Record the evidence if possible

- Use mobile phone to take a photo for the abnormal screen
- Forward the phishing email to dedicated mailbox of IT department

## Process and procedure

- Follow the internal handling guideline on loss storage/mobile phone with organisational data







**Thank you!**