

# Security Challenges & Prevention for Schools

網絡安全挑戰與防衛

Jan 2020

# Agenda

- About HKIRC
- Company Mission
- Security Challenges & Prevention
  - Phishing attack
  - Ransomware
  - Data Breaches
- Security Measures
- Conclusion

## About HKIRC

- Non-profit member-based organisation
- Set up in December 2001
- Endorsed by the Government of the HKSAR
- Oversee the administration and assignment of the country code top level Internet domain names ending with .hk and .香港.

# Company Mission

## Mission

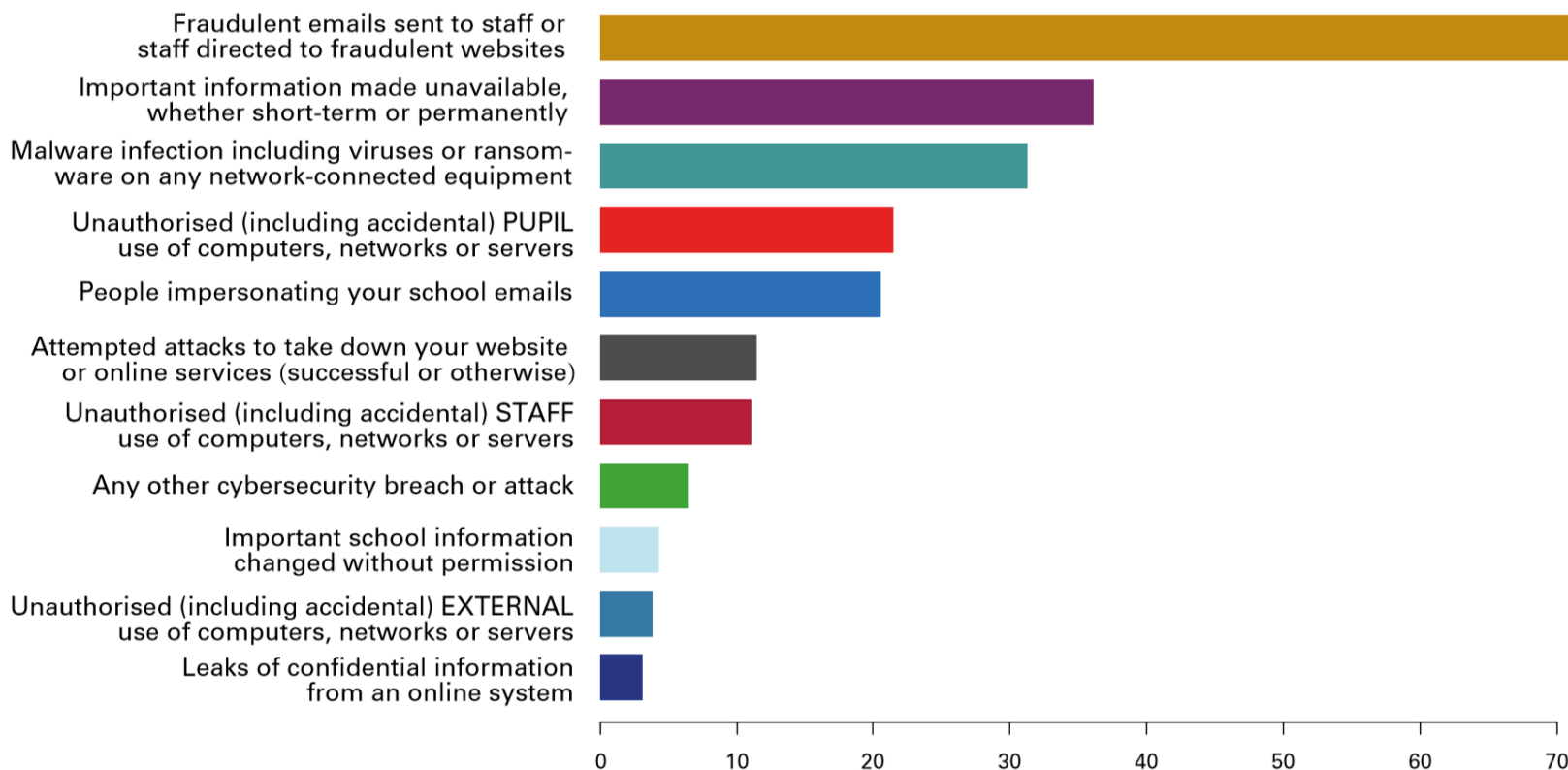
- Providing, and supervising the provision of .hk and .香港 Internet domain names registration, resolution and related services in an uninterrupted, effective, customer-centric and sustainable manner.
- Promotes Hong Kong as an inclusive, secure, innovative and international city for the Internet and encourages the use of Internet and the related technologies.

# Cyber Security Schools Audit 2019 in UK

- LGfL (London Grid for Learning) & NCSC (National Cyber Security Centre, part of GCHQ) carried out a joint audit of cyber security in schools across the UK
- The audit was open from 15 March – 20 April 2019
- 432 schools took part
- Findings were discussed vastly in media
- Issues highlighted in the report may also applicable in schools in HK

# Highlight of Findings

## 83% of schools experienced different levels of cyber-incidents



## Highlight of Findings (Cont')

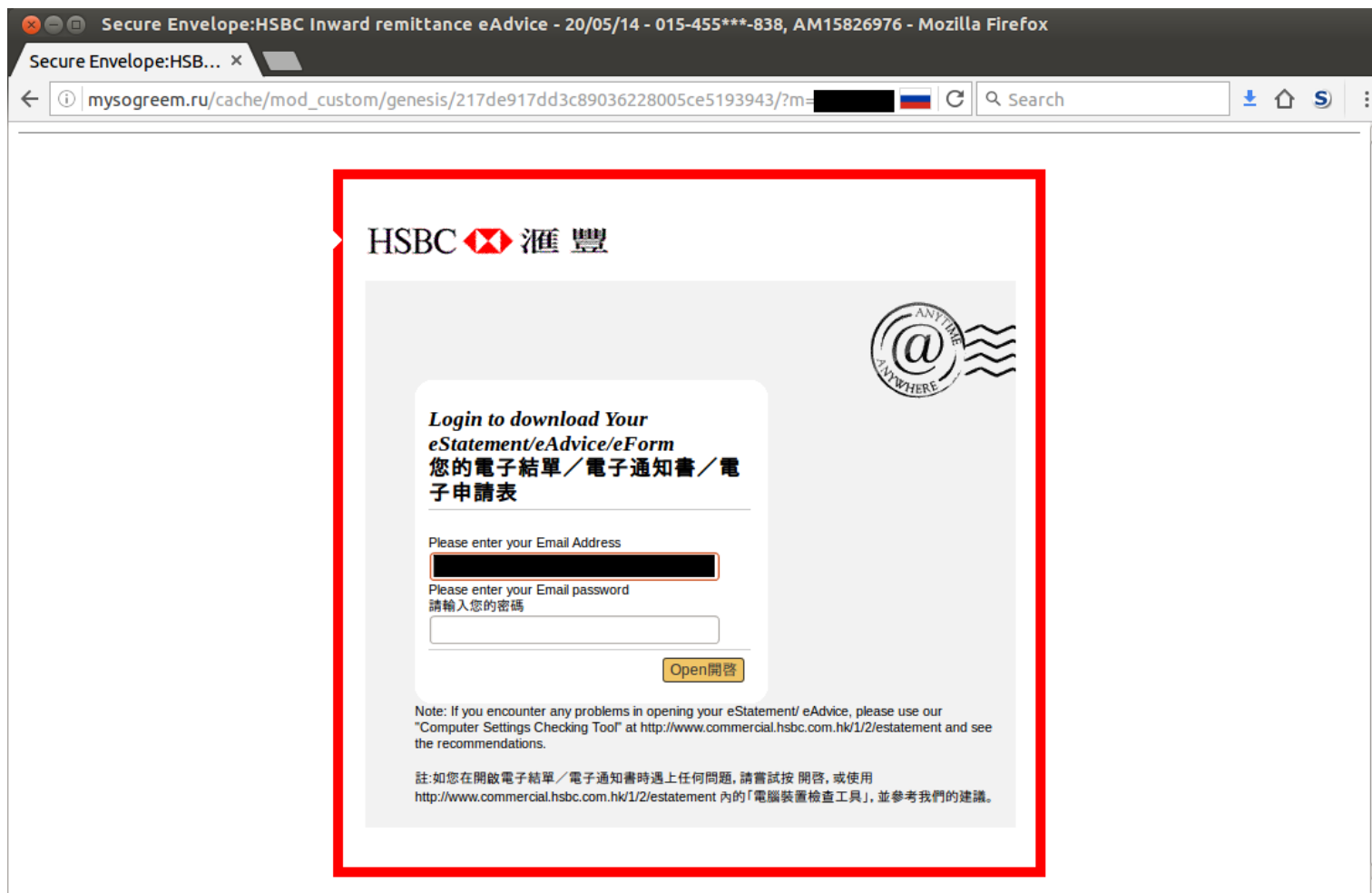
- 98 and 99 percent of schools, respectively, had antivirus and firewall protections
- 85 percent of schools had a cyber security policy or plan, but only 45 percent included core IT services in risk register & only 41 percent had a business continuity plan
- Only around a third of schools (35 percent) train non-IT staff in cybersecurity
- Less than half of schools (49 percent) were confident that they are adequately prepared in the event of a cyberattack
- A focus on support for non-IT staff is a clear need, 92 percent of schools welcome more cybersecurity awareness training for staff

# Common Attack in Schools



# Phishing Attack

# Recent Phishing Attacks



# Recent Phishing Attacks (Cont')



From Inland Revenue Department <taxnfo@ird.gov.hk>☆

Subject **TAX INFORMATION UPDATE.**

To undisclosed-recipients;☆

10:07 AM

**ATTENTION:**

**2018-19 Budget – Tax Measures**

In his 2018-19 Budget, the Financial Secretary proposed a number of tax measures, all of which require legislative amendments before implementation.

Reducing profits tax, salaries tax and tax under personal assessment for the year of assessment 2017/18

Adjusting the tax bands and marginal tax rates.

Increasing allowances and introducing a personal disability allowance.

Raising the deduction ceiling for elderly residential care expenses.

Relaxing the requirement for election of Personal Assessment by married persons.

Kindly update your tax information with the inland revenue department from the attached pdf.

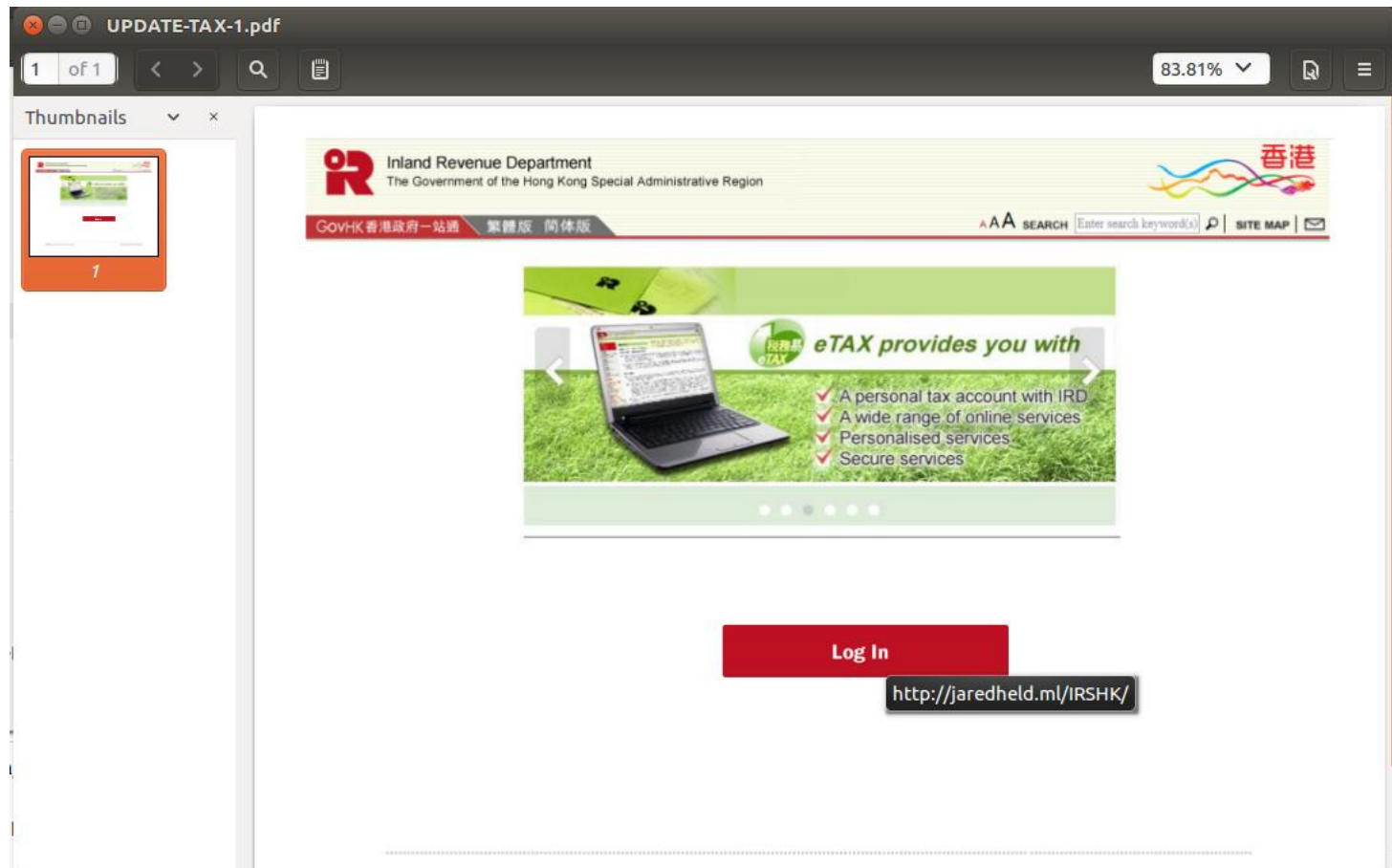
Regards,

Inland Revenue Department

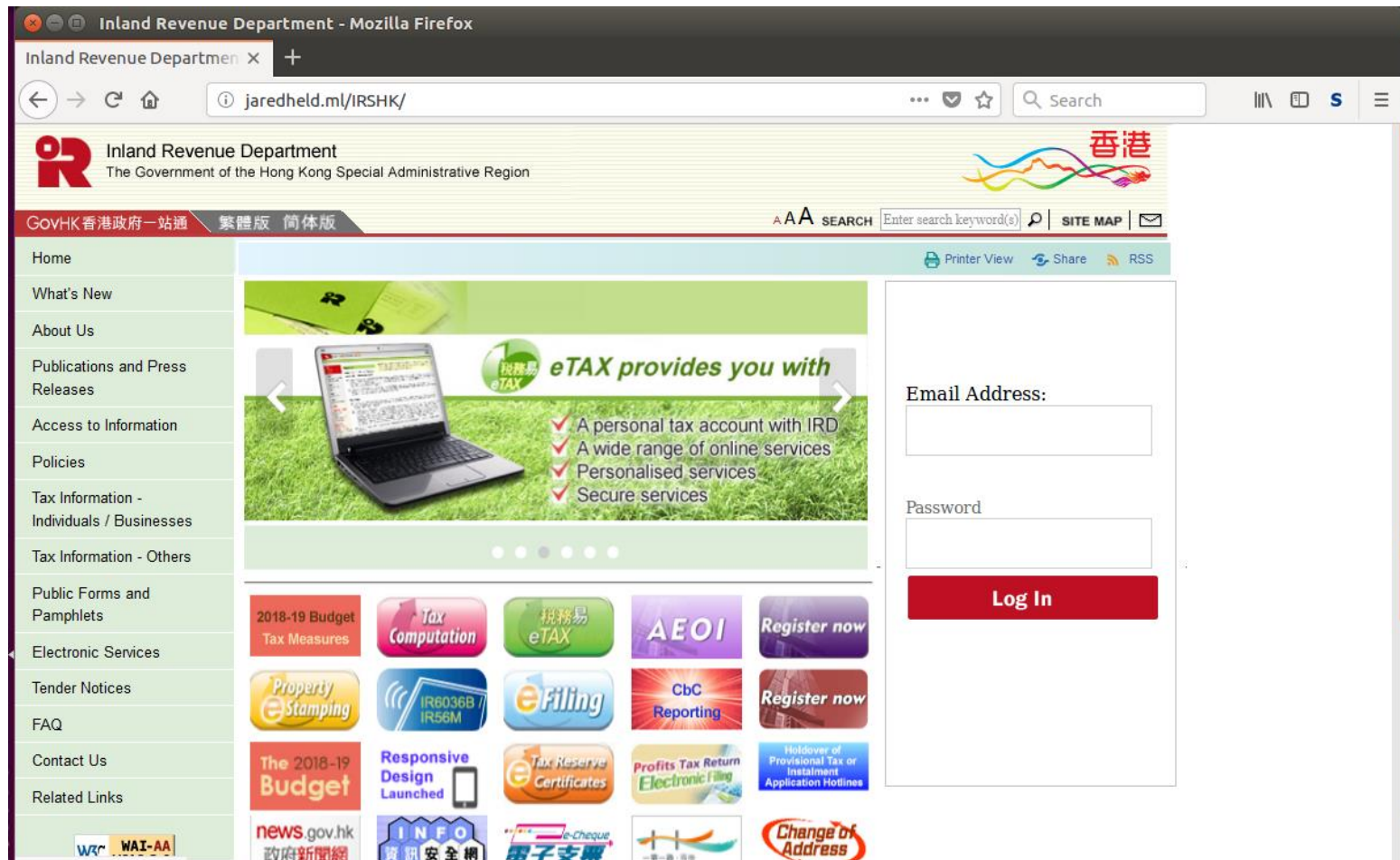
1 attachment: UPDATE-TAX.pdf size unknown

Save

# Recent Phishing Attacks (Cont')



# Recent Phishing Attacks (Cont')



# Recent Phishing Attacks (Cont')




From Inland Revenue Department <egis\_notification@ogcio.gov.hk> ☆  
Subject **Refund Account - 200013364790** Wednesday, February 28, 2018 06:45 AM  
To [REDACTED] ☆

From: "Sent by EGIS on behalf of IRD" <egis\_notification@ogcio.gov.hk> on behalf of "e alert" <alert2@ird.gov.hk>  
Reply To: "e alert" <alert2@ird.gov.hk>

We are sending this email to announce that after the last annual calculation of your fiscal activity ,  
we have determined that you are eligible to receive a tax refund of 1917.35 HKD.

In order to receive your tax return online

 [Click here to follow the steps needed](#)

Inland Revenue Department  
Hong Kong Special Administrative Region

This mail is system-generated, please do not reply to this email account.

## CONFIDENTIALITY

This email message (together with any attachments) is intended solely for the use of the designated recipient. It may contain confidential information that is privileged. If you are not the intended recipient, you should not

# Recent Phishing Attacks (Cont')



Access to Information - Mozilla Firefox

Access to Information x +

www.bupyongshopping.co.kr/board/board/Cust/sol/TaxHK/Access.html

Inland Revenue Department  
The Government of the Hong Kong Special Administrative Region

GovHK 香港政府一站通 繁體版 简体版

SEARCH Enter search keyword(s)

SITE MAP

Home

What's New

About Us

Publications and Press Releases

Access to Information

Policies

Tax Information - Individuals / Businesses

Tax Information - Others

Public Forms and Pamphlets

Electronic Services

Tender Notices

FAQ

Contact Us

Related Links

Home > Access to Information

**Contact Information**

Current Email

Mobile Number

**Contact Information**

First name

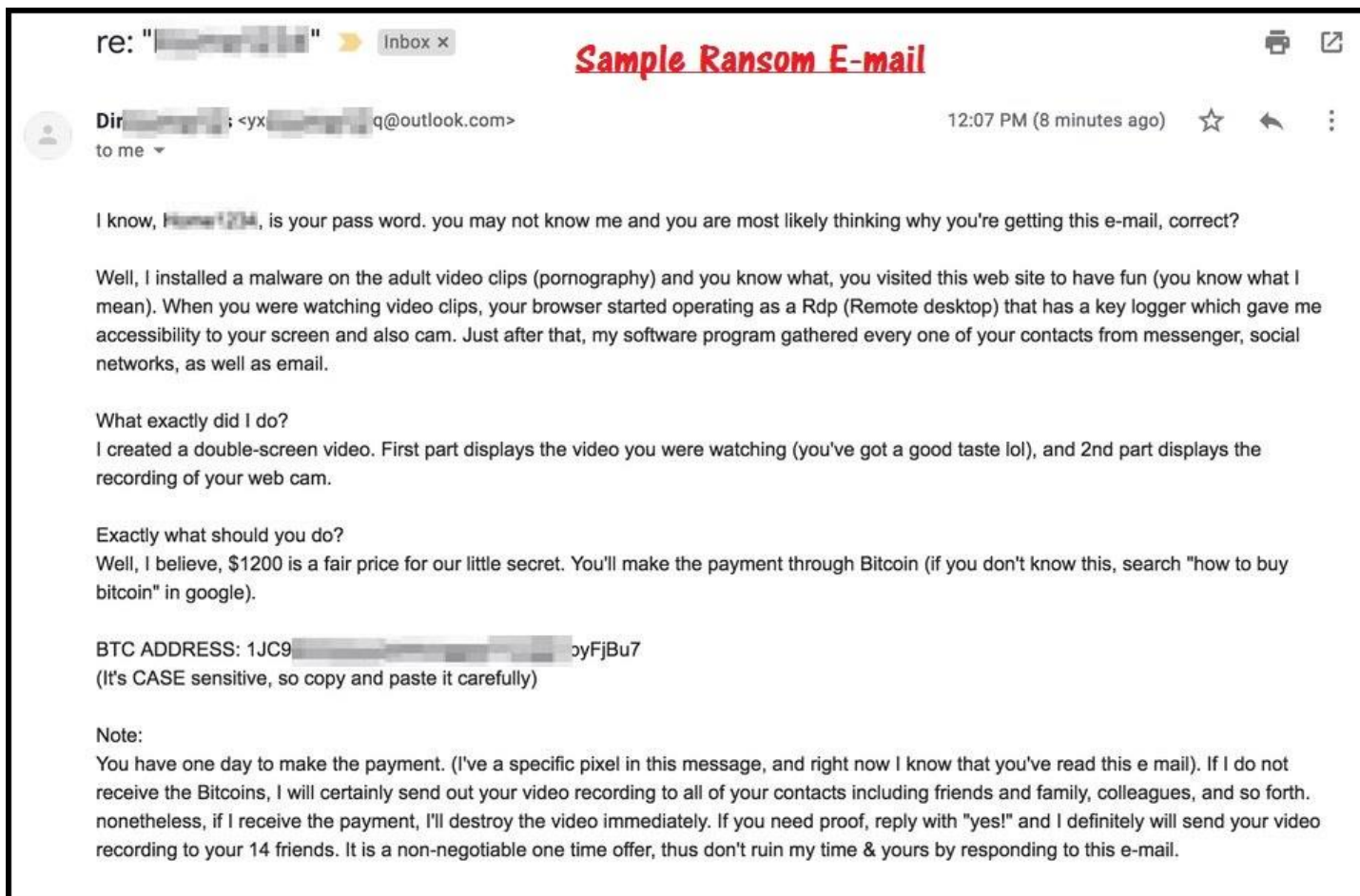
Last name

HK ID

Date of Birth

**Account Information**

# Ransom E-mails





# Tackling Phishing Attack



- Do not open suspicious links in E-mail & Web browser
- Do not key-in user name and passwords from forms open by E-mails
- Make sure system patches and anti-virus software are up-to-date
- Enable Two Factor Authentication (2FA) function wherever it is provided

# Ransomware

# Ransomware



Cybercriminals



Email with  
malicious  
attachment



Open the email and  
execute the attachment



2016 Locky, Zepto, CryptXXX  
2017 WannaCry, NotPetya  
2018 GandCrab, SamSam  
2019 LockerGoga, etc.



Bitcoin blackmail

**Ransomware** is a serious security threat that limits victims to access their files or system functions. It has “data-kidnapping” capabilities.

Cybercriminals tend to threaten victims to pay ransom (bitcoin) in order to regain access to their files or systems.

# Ransomware Evolution



## Crypto Ransomware

- 2013 CryptoLocker (PC)
- 2014 BitCrypt (PC)
- 2014 CyptoDefense (PC)
- 2014 **Synolocker (NAS)**
- 2014 **Simplocker (Mobile)**
- 2014 CryptoGraphic Locker
- 2015 CyptoWall, TeslaCrypt, CTB-Locker
- 2016 Locky, Zepto, CryptXXX
- 2017 WannaCry, NotPetya
- 2018 GandCrab, SamSam
- 2019 LockerGoga, etc.

Expect to continue ...

# Newest Trend of Ransomware



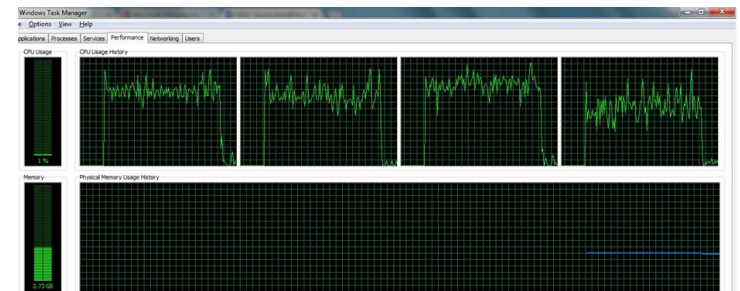
## New Virus Decides If Your Computer Good for Mining or Ransomware

July 05, 2018 Mohit Kumar



**Cryptojacking** - secret use of your computing device to mine cryptocurrency.

## CPU Surged During Cryptojacking



# Suggestions to Defense Against Ransomware



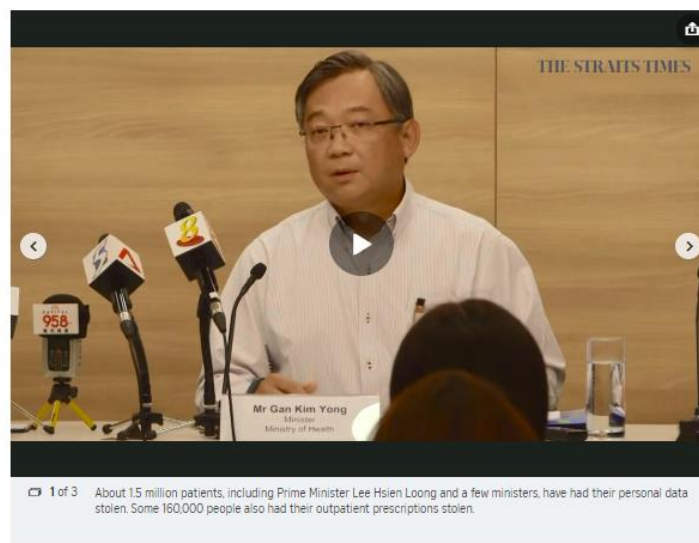
- Do not pay cyber criminals ransom
- Do not open suspicious links in E-mail & Web browser
- Make sure system patches and anti-virus software are up-to-date
- Protect your data – backup your data regularly and put them offline

# Data Breaches

# Data Breaches Cases Surged since 2018...



Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore's worst cyber attack





# Data Breaches Cases Surged since 2018...

## 國泰驚爆940萬乘客資料外洩 5月確認遭攻陷 涉信用卡身份證號碼等

By 信報財經新聞 on October 25, 2018

Like 2 people like this. Be the first of your friends.

原文刊於信報財經新聞



## 5,000 萬用戶數據外洩事件 Facebook 指第三方軟件登入未受影響

讚好此文 讚好 23 分享

十月 4, 2018 • 社交網絡 •

因為 Facebook 的系統漏洞令 5,000 萬名用戶的資料外洩，有網絡保安專家表示，今次黑客可能會藉此入侵那些利用 Facebook 帳號登錄的第三方應用，例如 Instagram、Uber、Venmo、Tinder 等。由於使用 Facebook 帳號登入的第三方軟件和服務不少，當中涉及不少敏感的用户資料，或會令今次事件的嚴重性以幾何級數提高。



# And Even in 2019...

## British Airways faces \$230m fine for data breach

By Adam Satariano New York Times, July 8, 2019, 7:31 p.m.



Poor security at the airline allowed hackers to divert about 500,000 customers visiting the British Airways website last summer to a fraudulent site, UK authorities say. (AAMIR QURESHI/AFP/GETTY IMAGES)

LONDON — British authorities said Monday that they intend to order British Airways to pay a fine of nearly \$230 million for a data breach last year, the largest penalty against a company for privacy lapses under a new European data protection law.

## Hong Kong schools fall victim to cyberattack, raising fears for private data of pupils

South China Morning Post | Danny Mok danny.mok@scmp.com

發布時間 2019年12月7日 17:12



- Police investigating after eight schools are hacked, three of which report data leaks
- Pupil addresses among information stored on administration system targeted by hackers



Three out of eight schools targeted have reported falling victim to data leaks after a government IT system was hacked. Photo: Shutterstock

# Why Data Breaches?



Data Breaches are result of:

- Poor IT operational practices (e.g. late decommission of servers)
- Application vulnerabilities
- Advanced Persistent Threat (APT)
- Deficiency in outsourcing management
- Etc.

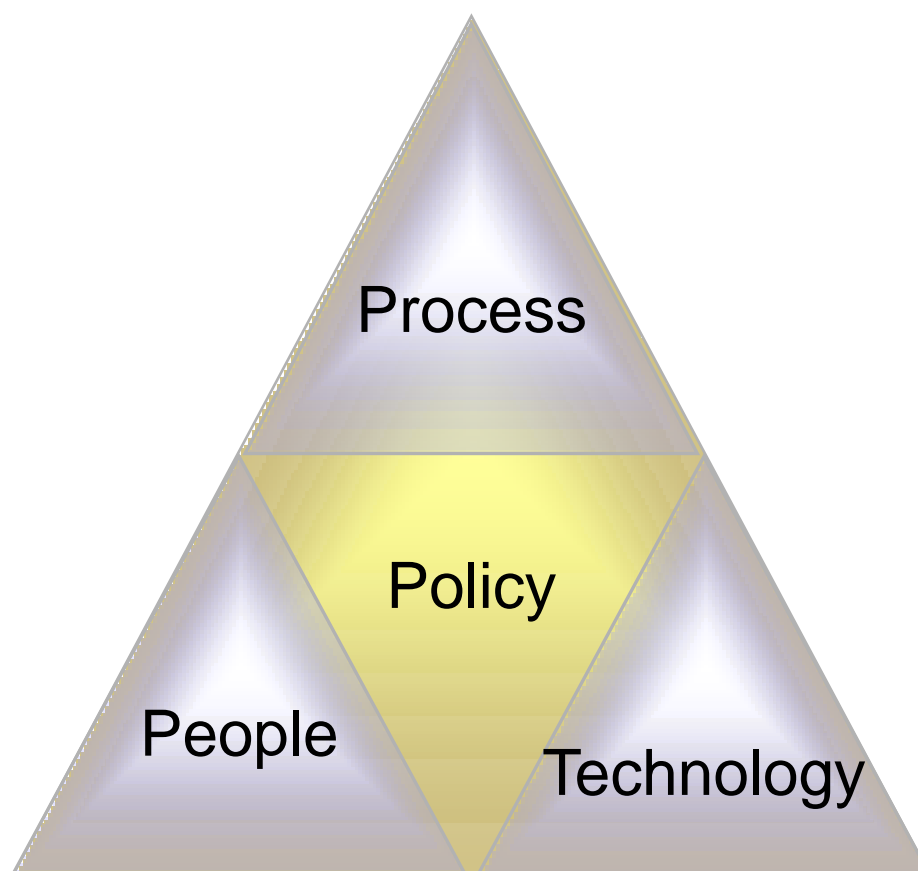
**Organizations need to have a holistic security strategy – combining people, process and technology to reduce exposure to current & future attacks**

# Security Measures

# Security Measures



- Security Measures can be classified into 3 categories: **Technology**, **Process** and **People**



# Information Security Protection via Technology

## **Well planned Security Architecture needed:**

- Anti-malware
- Firewall
- Network Access Control
- Encryption
- Patches update
- A lot more...

# Information Security Protection via **Process**.hk

## **Well planned processes and procedures needed:**

- IT and Security Policy
- Information Classification
- Risk Assessment
- A lot more...

# Information Security Protection via **People**.hk

**People is the weakest link in cybersecurity, need more emphasis:**

- Minimum Privilege and Accountability
- Password Management
- Security Awareness – avoid phishing & social engineering
- A lot more...



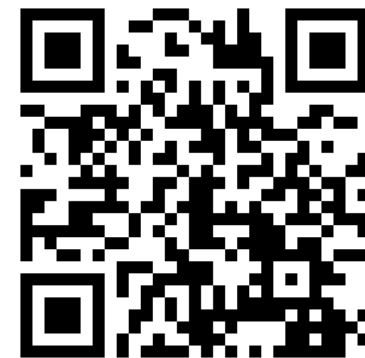
# Conclusion



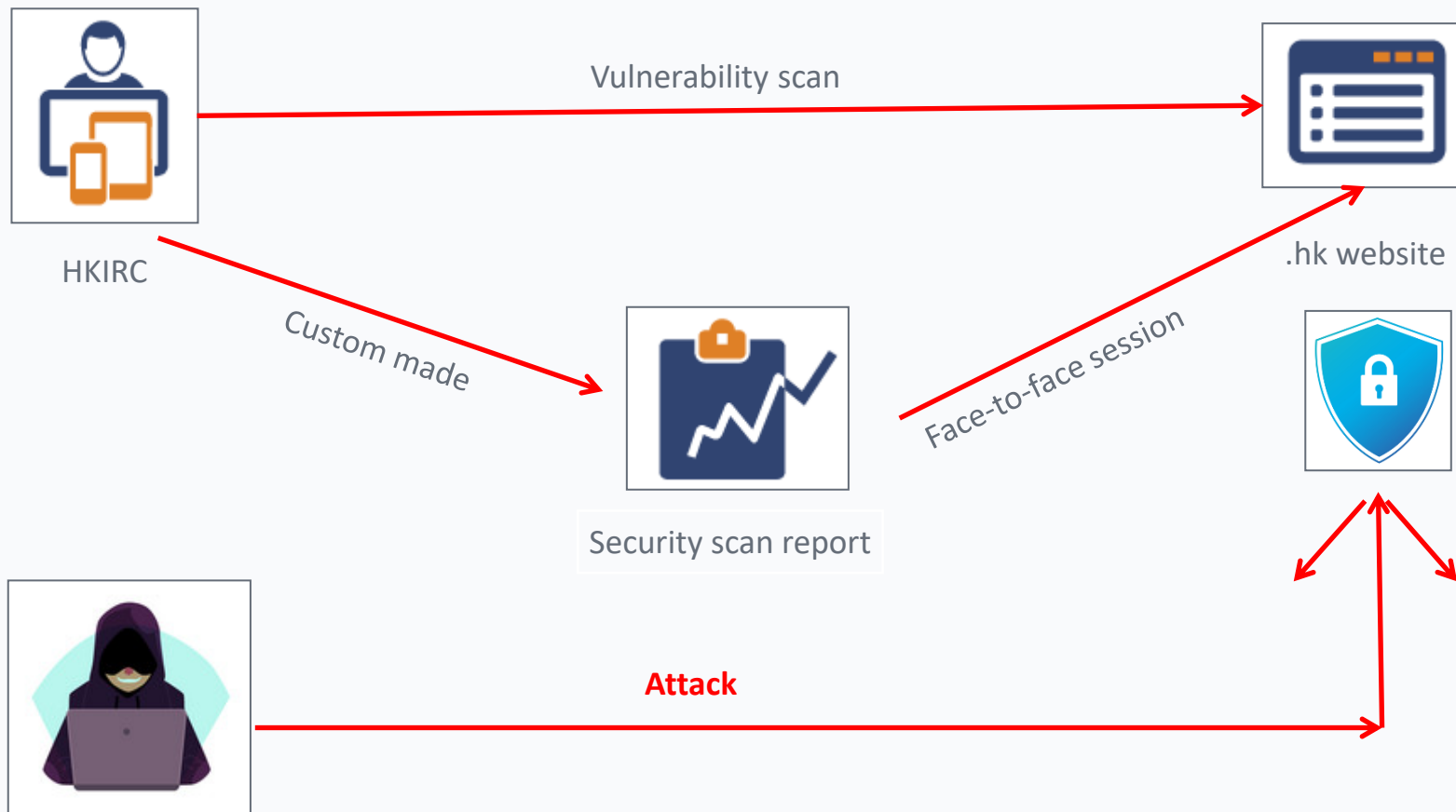
- Everyone relies on the cyber World to conduct business nowadays
- However, the cyber world is full of cybersecurity challenges
- We discussed some security challenges here:
  - Phishing Attack
  - Ransomware
  - Data Breaches
- To deal with these challenges, we need a holistic security strategy combining **people**, **process** and **technology**.
- Among these 3 aspects, **people** is the weakest link. More awareness effort needed.

## Free In-Depth Website Security Scan

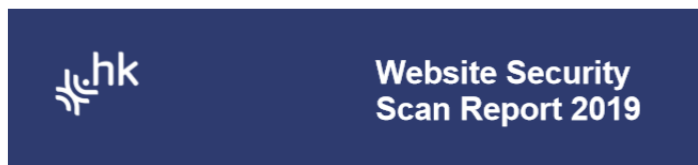
- In-Depth Website Security Scan now open for application
- All .hk users and HK SMEs can apply for the free service
- HKIRC will provide:
  - Remote black-box vulnerability scan for web server
  - Organized report for identified issues & mitigation actions
  - A consultation session for briefing report
  - Referral to appropriate solution vendors if needed
- Application form: <https://www.hkirc.hk/upload/blog/6/self/5df2ebec9c9e7.pdf>
- Any inquiry, please call HKIRC hotline 2319 2030 or E-mail to [sme-security-scan@hkirc.hk](mailto:sme-security-scan@hkirc.hk)



# In-depth Webscan for SME



# Sample Report



Site Name : <http://xyz.com.hk>  
IP Address : 111.222.333.444  
Session : 5 July 2019 10:00am-12:00am

HKIRC Reference No. : 07xxx  
Status : Success

## Overall Risk Level

High

## Risk Ratings

High: 2  
Medium: 1  
Low: 3

## Background

A remote web vulnerability assessment was conducted by HKIRC against the web-interfaced system. The purpose of this assessment was to remotely identify and quantify vulnerabilities or potential threats in the web-interfaced system before they are exploited by attackers. This report is provided as it is and HKIRC cannot guarantee all vulnerabilities of the system are identified in this remote security scanning.

## Executive Summary

This security scan identified **2 High severity issues**, **1 Medium severity issue** and **4 Low severity issues**. Most issues can be rectified by modifying configurations of web server. Others may need a review on application logic.

See below for analysis of these items. For technical details, please refer to the Appendix Section.

## Findings and Recommendations

### Findings

- The system seemed to be a shared web hosting. So only web application contents are scanned in this assessment, instead of running a full security scan on the server.
- The major issue of the website is that user input is not filtered properly. It is possible to inject scripts and even SQL statements in user input variables and cause it executed by the server.
- Other issues are related to configuration of web server

### Recommendations

- Filter user input properly. Remove special characters like "<", ">", "@", "\$", "%", "#", "&" and other special characters from user input
- Configure web server to enable security related headers and settings

## Technical Summary

Section	Risk Level	CVSS*	Issue	Summary of issue	Solution
	High		SQL Injection	SQL Injection may be possible	Modify program logic to filter user input properly
	High		Cross Site Scripting (Reflected)	Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client.	Modify program logic to filter user input properly
	Medium		X-Frame-Options Header Not Set	X-Frame-Options header is not included in the HTTP response to protect against 'Clickjacking' attacks.	Ensure web server sets the Content-Type header appropriately, and X-Content-Type-Options header set to 'nosniff' for all web pages
	Low		Web Browser XSS Protection Not Enabled	Web Browser XSS Protection is not enabled by configuration of the 'X-XSS-Protection' HTTP response header	Turn X-XSS-Protection HTTP response header to '1'
	Low		X-Content-Type-Options Header Missing	The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows some older versions of browsers to perform MIME-sniffing on the response body.	Ensure web server sets the Content-Type header appropriately, and X-Content-Type-Options header set to 'nosniff' for all web pages
	Low		Absence of Anti-CSRF Tokens	No Anti-CSRF tokens were found in a HTML submission form	Generate unique nonce for each form
	Low		Cookie No HttpOnly Flag	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible	Ensure HttpOnly flag is set for cookies

### Disclaimer

A remote web vulnerability assessment was conducted by HKIRC against the web-interfaced system. The purpose of this assessment was to remotely identify and quantify vulnerabilities or potential threats in the web-interfaced system before they are exploited by attackers. This report is provided as it is. The scanning was done using industry recognized security scanning tools but HKIRC cannot guarantee all vulnerabilities are identified in this remote security scanning.

\* The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of vulnerability and produce a numerical score reflecting its severity. CVSS is a published standard used by organizations worldwide, and the SIG's mission is to continue to improve it.

# Q & A