Cosmos

Is your company adopting to work from home under 5th wave of COVID-19 ?

Over 750,000 ransomware attacks HK firms monthly

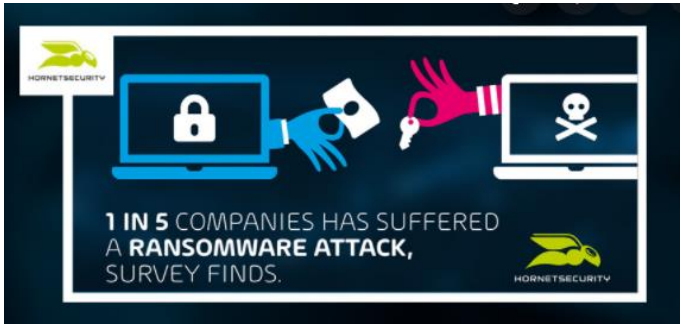
Ransomwares like Revil and TrickBot were the usual suspect.

The threat attack surface expanded as more companies required employees to work from home during the pandemic

https://hongkongbusiness.hk/information-technology/news/over-750000-ransomware-attacks-hk-firms-monthly

Small and Midsize Businesses Face Greater Cyber Security Risks and Challenges because :

- Considering themselves too small to be targeted.
- Arguably fewer resources, smaller budgets and fewer skills available to defend against attacks
- Cybercriminals are well aware of these vulnerabilities and also understand that SMEs can be a useful conduit to bigger, more valuable organisations via the supply chain.



Cyber Security Threat

In the second half of 2020, ransomware attacks increased seven times as the work and school shifted to a remote setup.

Have you experienced any of the Cyber Attacks like…

- **Phishing Email** 82%
- **Ransomware** 42%
- **CEO Scam** 29%
- **DDos** 28%
- **Other Malware Attack incl. Botnet** 21%

Top 5 Cyber Attacks *Incidents among the respondents of the Survey conducted by Hong Kong Productivity Council with no less than 350 enterprises.*

Source: HKT Hong Kong Enterprise Cyber Security Readiness Index HKT 香港企業網絡保安準備指數 2021 (HKPC 生產力局)

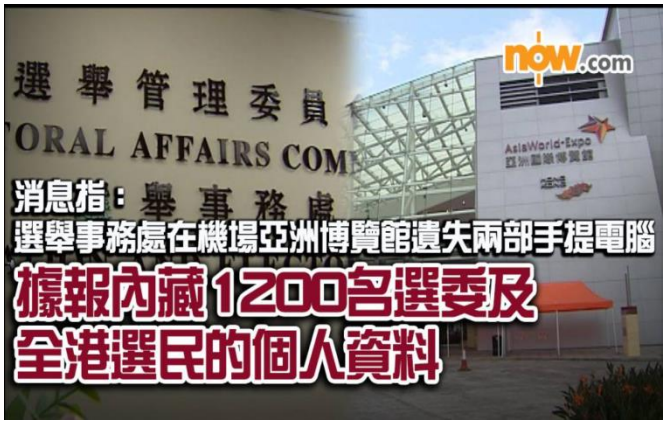
Recent incident in HK

Hong Kong gov't loses computers with personal data of all registered voters.

The Registration and Electoral Office (REO) confirmed on Monday evening that it lost two computers containing the personal data of all 3.7 million registered voters in the city.

The machines were being stored in a locked room at AsiaWorld-Expo, which was used as a backup polling station for Sunday's chief executive election. The REO said the computers also contained the full names of the 1,194 Election Committee members who voted in the election.

The personal data included the names, addresses and identity card numbers of all registered voters in Hong Kong.



Recent incident in HK

HKTVmall's parent company, HKTV, says it detected 'abnormal and suspicious activities' in its computer systems last month

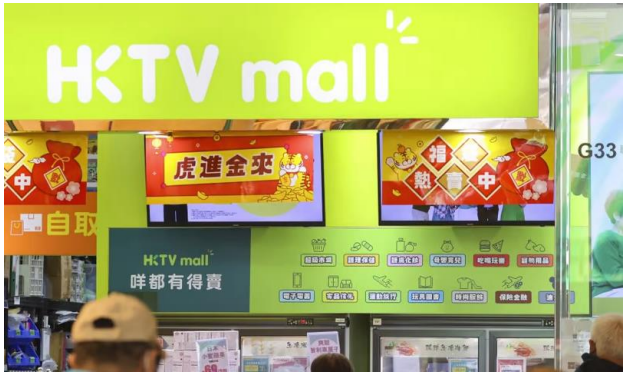
(5 Feb 2022)

A security breach at one of Hong Kong's largest online shopping platforms last month led to the unauthorised access of customer information such as delivery addresses, recipient names and contact numbers.

Based on its investigation, it concluded that the affected customer information might include names of account holders, encrypted and masked login passwords, email addresses, recipients' names, delivery addresses and contact numbers for orders placed between December 2014 and September 2018.

The date of birth, recipients' names and email addresses for HKTVmall accounts linked to Facebook accounts and Apple ID might also have been accessed.

HKTV promised it would take responsibility for any unauthorised purchases made as a result of the data breach.



Recent incident in HK

E-mail leaks for hundreds of LeaveHomeSafe enquiries

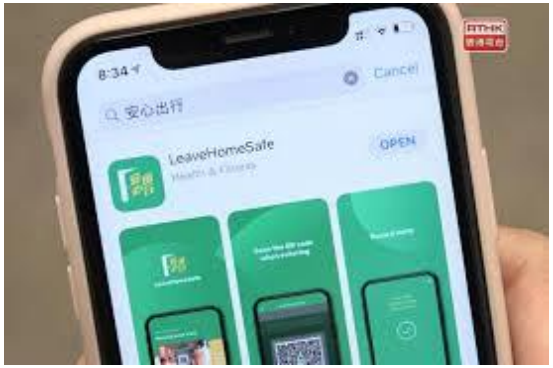
(13 Jun 2021)

The government's IT office said staff employed by a contractor had accidentally leaked hundreds of e-mails from people asking them about the LeaveHomeSafe app.

Apple Daily reported on Sunday that more than 400 emails were sent to one of those who offered opinion through the government hotline, 1823, on the app that helps with Covid-19 contact tracing.

The Office of the Government's Chief Information Office (OGCIO) said the leak took place on 23 May, and it's launched an immediate probe.

"The office immediately notified the Privacy Commissioner
for Personal Data and asked for its advice,
and offered apologies through separate e-mails
to each of those affected the next day,"
it said in response to media enquiries.



Other incident

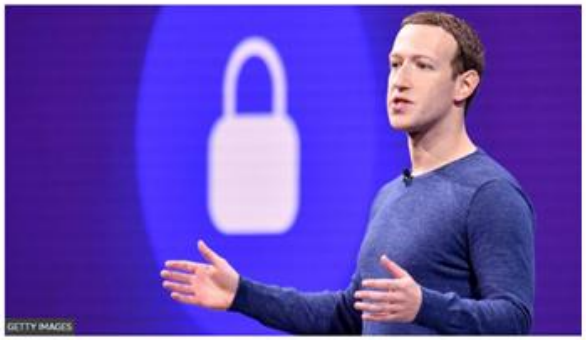
LinkedIn hackers leak 700 million data scrap

September 25, 2021 2 Min Read

- Data from over 500 million LinkedIn users is being sold online to hackers

Facebook faces investigation over data breach

14 April 2021



- 530 million users' personal data was lifted in a breach in August 2019
- User's data are found on hacker forum and for sale purposes
- Facing investigation of The Irish Data Protection Commission for the users' data published online

Fimmick ransomware attack puts over 35,000 people's data at risk

Over 35,000 people's personal data are at risk after digital marketing agency Fimmick had its computer system attacked by ransomware in September.

The Office of the Privacy Commissioner for Personal Data confirmed on Thursday that L'Oreal Hong Kong customers had their personal data leaked, including their name, telephone number, email address, residential address, month of birth, Facebook name, and Facebook email address.

Nine companies are still investigating if their customers are affected. They include Fimmick's corporate clients McDonalds, Coca-Cola China, Bupa (Asia) Limited, Europe Group Holdings, Green Square Marketing, Mentholatum (Asia Pacific), Nestle Hong Kong, Reckitt Benckiser Hong Kong, and Mead Johnson Nutrition (Hong Kong).

The office received data breach notifications from Fimmick in October, which involved the leakage of some of the personal data processed by the agency.

The Privacy Commissioner for Personal Data, Ada Chung Lai-ling, appealed to citizens who have provided personal data to the above companies, including those who have become their fan club members or made online purchases with them, to be vigilant about the potential theft of their personal data.

"If they are in doubt about whether their personal data have been leaked, they may make enquiries with the companies concerned or make enquiries or complaints to the Office," she added.

Cosmos

How to improve Cyber Security Level?

FOUR EASY STEPS!!

1. Know **what kind of data** you have and where it's located
2. Have **multiple backups** that you test regularly
3. Ensure that **email security**, such as DMARC, is implemented
4. Provide regular cyber security **awareness** and security **training**

Measures on Company Level

1. Provide Cyber Security **Training**
1. Compliance to regulations on Cyber Security and Personal Data Protection
2. Cyber Security **Drill** on Simulations
3. Diverse your Risk by **Cyber Insurance**

Contact us to find out more about
Cyber Insurance
coverage as a
Smart Alternative

Cosmos

Please contact Cosmos for more information

We are a subsidiary of ITOCHU Corporation, operating in HK since 1974.

We are handling corporate insurance (G/I) & employee benefit insurance(E/B) :

(G/I) Property All Risk, Marine Cargo, Product Liability, Trade Credit, D&O, etc.

(E/B) Employee Compensation, Group Medical, Travel, Health Check up, etc.

Our professional staff is available to assist with your enquiries.
(Cantonese, English, Japanese)
We will act as your insurance representative and negotiate with insurers.

PIC : Ms. Jacqueline Yeung
Manager - Direct Marketing Division
jacqueline.yeung@coshk.com.hk
Direct Line: 2861 4226

COSMOS Services Co., Ltd.

28th Floor, United Centre, 95 Queensway, Hong Kong