2020網絡安全趨勢和安全小貼士

Billy Ngun

Senior Consultant

HKCERT

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**

- Funded by Government
- Operated by Hong Kong Productivity Council

Services

Incident Response

24-hr Hotline: 8105-6060

Monitoring and Early Warning

Free security alerts subscription (hkcert@hkcert.org)

Awareness Promotion and Advices

Cross Border Coordination

Contact HKCERT

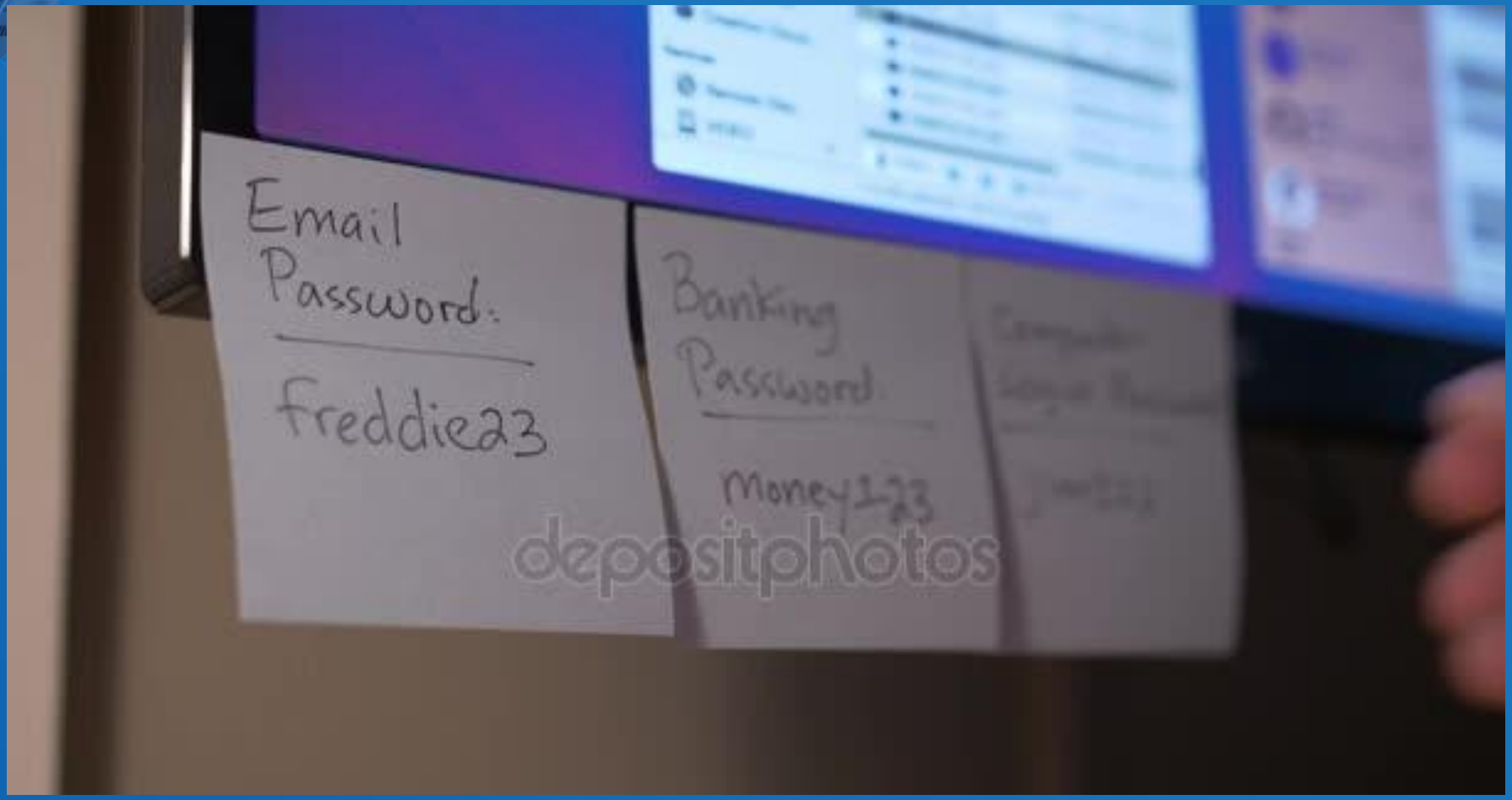
WWW: hkcert.org
Email: hkcert@hkcert.org
Hotline: 8105 6060

Facebook page:
https://www.facebook.com/hkcert

The top 10 most common passwords were:

- 123456
- 123456789
- qwerty
- password
- 111111
- 12345678
- abc123
- 1234567
- password1
- 12345

- Jan_pw$!
- Feb_pw$!
- Mar_pw$!
- Apr_pw$!
- #$Ax!48


Email
Password:
Freddie23
Banking
Password
Money123
depositphotos

Secure Passwords

Strong Password
Don’t use “same” password

NIST 800-63 Password Guidelines 2019

- 8 character minimum when a human sets it
- 6 character minimum when set by a system/service
- Support at least 64 characters maximum length
- All ASCII characters (including space) should be supported
- Truncation of the secret (password) shall not be performed when processed
- Check chosen password with known password dictionaries
- Allow at least 10 password attempts before lockout
- No complexity requirements
- No password expiration period
- No password hints
- No knowledge-based authentication
- No SMS for 2FA

Source: https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

Passphrase and password manager

- “My favourite sport is tabletennis!” is extremely easy to remember but very difficult for computers to crack due to its length
- Consider using a password manager. All you need to remember is one single passphrase.

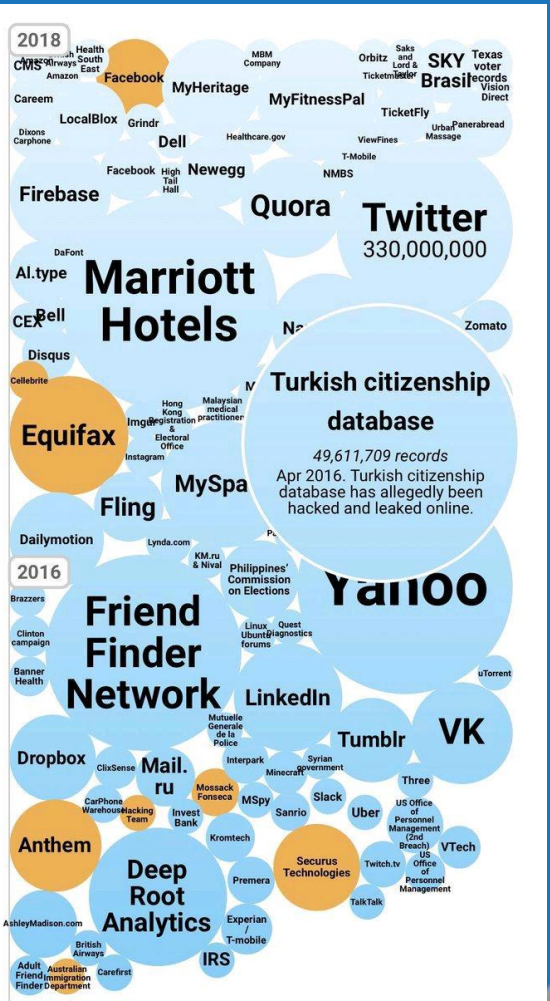
Cyber Security Incidents

HACKER COMBAT COMMUNITY

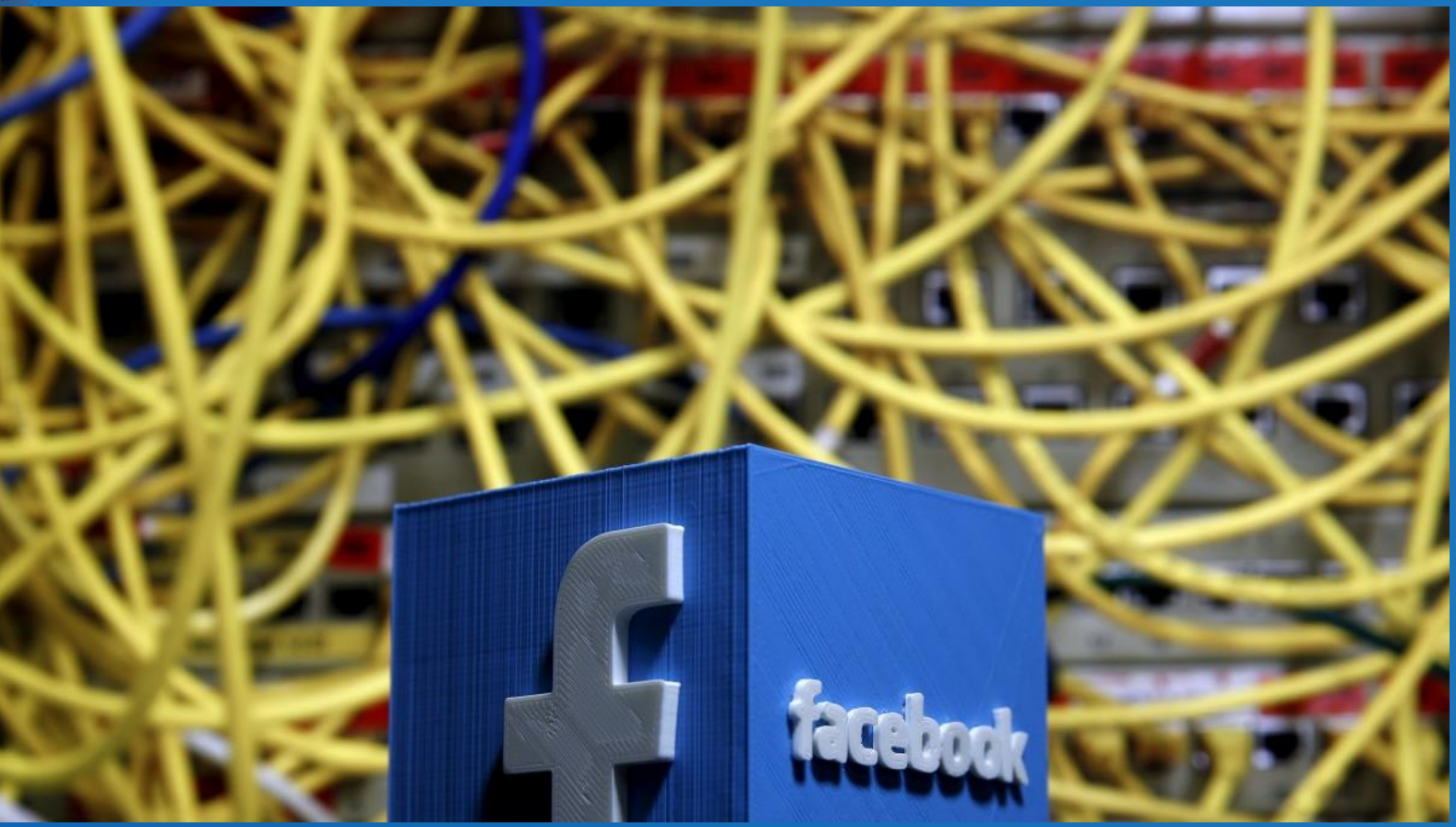
10 Biggest Data Breaches of All Time

Yahoo – 3 billion (2013)
Marriott – 500 million (2014-2018)
Adult FriendFinder – 412 million (2016)
MySpace – 360 million (2016)
Under Armor – 150 million (2018)
Equifax – 145.5 million (2017)
eBay – 145 million (2014)
Target – 110 million (2013)
Heartland Payment Systems – 100+ million (2018)
LinkedIn – 100 million (2012)

Source: Quartz



Number of records affected: 540 million
Year: 2019



Number of records affected: 885 million
Year: 2019

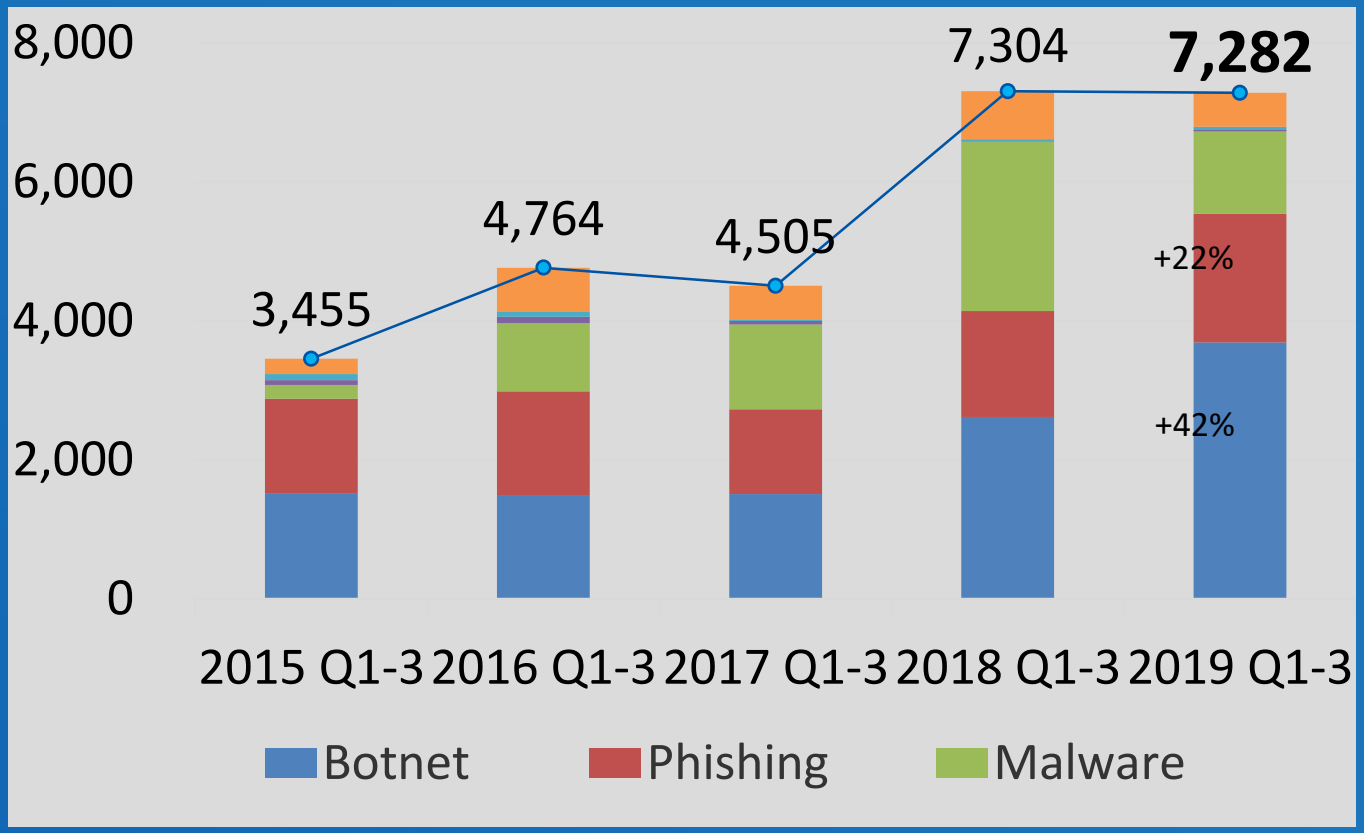
Number of records affected: 106 million
Year: 2019

Major causes of data breaches

- System Misconfiguration For example, cloud infrastructure
- Business logic vulnerability
- Web application vulnerabilities
- Old, unpatched security vulnerabilities
- Human error
- Malware

Cyber Security Trend

HKCERT Incident Reports Q1-Q3



Source 來源: HKCERT

Highlight of top incident reports in 2019 Q1-3

- Botnet 3,690 (+42%)
  - Top 3 botnets: Avalanche (1,651), Necurs (640), Ramnit (501)
  - Top 2 IoT botnets: Mirai (401), VPNFilter (132) **[+46%]**
  - **Impacts: financial loss, loss of control of device**
- Phishing 1,853 (+22%)
  - Top 3 targeted brands: China Construction Bank, Apple, Amazon
  - **Impacts: financial loss, data breach**

Source 來源: HKCERT

Hong Kong Police Technology Crimes Statistics

	# of Cases		Financial Loss (HK$ million)	
	2018 H1	2019 H1	2018 H1	2019 H1
Internet Deception	2,794	2,610	1,057.5	1,306.2
Email Scam *	**404**	**401**	**759.6**	**1,127.5 (+48.4%)**
Social media deception	1,003	930	155.4	142.4
Online Biz Fraud	1,107	1,154	20.4	14.8
E-banking fraud	0	0	0	0
Misc. fraud	280	125	122.1	21.5
Internet blackmail	184	177	0.9	0.6
Misuse of Computer	126	40	92.2	0.6
Others	395	261	2.1	1.3
TOTAL	3,499	3,088 (-11.7%)	1,152.7	1,308.7 (+13.5%)

* Email scam (malware + social engineering) -- attacker sending spoof emails on behalf of a senior staff (CEO or similar) or a trusted customer with an aim to trigger a payment or release of confidential data.

Protection against Phishing Attacks

- User: Think before click; Verify by phone
- Provide 2FA to customer accounts
- Corporate Brand Protection
- Adopt Email Defense Technology and DMARC
- User Training (never trust always verify)
- Phishing Drill Exercises

Cybersecurity in the IoT devices

- IoT security vulnerabilities
  - Use of hardcoded credentials
  - Use of default credentials
  - Exposure of sensitive user information
    - Unprotected cloud storage
    - Device Theft scenarios
    - Security defects in Command & Control
  - Firmware comes with known vulnerabilities
    - Unpatched device
    - A device that no longer receives security updates

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

AI & Machine Learning for Cyber Attack

https://www.youtube.com/watch?v=5iZuffHPDAw

AI & Machine Learning for Cyber Attack

https://www.youtube.com/watch?v=5iZuffHPDAw

Fraudster used AI to Deepfake the boss' voice - manage to trick to transfer $243K

- Victim believed he was talking to his German boss.
  - the voice carried the German boss' subtle accent and his pace.

Reference:

- https://thenextweb.com/security/2019/09/02/fraudsters-deepfake-ceos-voice-to-trick-manager-into-transferring-243000/

Security Issues arising from the End of Support (EOS) of Technologies

- Microsoft Win 7, Win Server 2008/2008R2 reach EOS in Jan 2020. No more security updates.

Key takeaway

- Information Security is Everybody's Business
- Prepare for upgrade/ migration of EOS systems
- IoT devices have their share of security vulnerabilities
- Prevention is always better than cure
- Protection via People, Process and Technology
- Report incident and Know where to get Assistance

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號生產力大廈
+852 2788 5678 www.hkpc.org