Understand fake technologies,
Spot fraud and disinformation
認識"虛假"技術　助你發現欺詐和謠言

Mr. Frankie Wong, PISA

Intro to PISA

PISA - Professional Information Security Association（專業資訊保安協會）

- is an **independent** and **not-for-profit** organization for information security professionals, with the primary objective of promoting information security awareness and best practice.
    - to facilitate knowledge and information sharing among the PISA members,
    - to promote the highest quality of technical and ethical standards to the information security profession,
    - to promote best-practices in information security control,
    - to promote security awareness to the IT industry and general public in Hong Kong,
    - to be the de facto representative body of local information security professionals

Ref: https://pisa.org.hk/about-us/

Agenda

- Phishing Attack (釣魚攻擊)
- Deepfake Tech (深偽技術)
- Security Tips
- Report & Feedback

Phishing Attack (釣魚攻擊)

Phishing Email

Categories

- Scam email (純詐騙電郵)
- Email with malicious link(s)
- Email with malicious attachment(s)
- Email with mixed malicious links and attachments

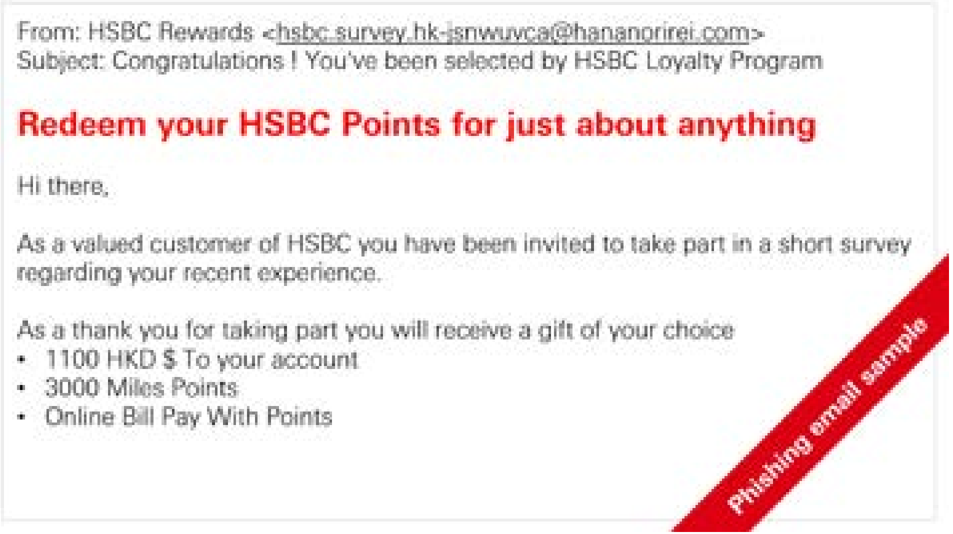
Attack Vector - Understand information/cyber security

- Social Engineering, Phishing Attack

Phishing Email - Scam email

Scam email #1

- Basic scam email
- Spoofing email sender
- “Fake” email address
- Email subject with attractive theme or notification/alert
- Aim:
  - Lure user to have a further communication



From: HSBC Rewards <hsbc.survey.hk-jsnwuvca@hananorirei.com>
Subject: Congratulations ! You've been selected by HSBC Loyalty Program

Redeem your HSBC Points for just about anything

Hi there,

As a valued customer of HSBC you have been invited to take part in a short survey regarding your recent experience.

As a thank you for taking part you will receive a gift of your choice

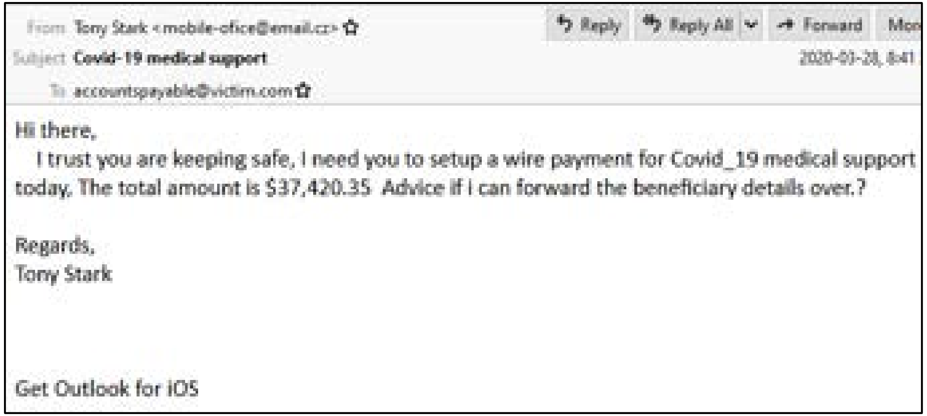
- 1100 HKD $ To your account
- 3000 Miles Points
- Online Bill Pay With Points

Ref: https://www.hsbc.com.hk/help/cybersecurity-and-fraud/phishing/

Phishing Email - Scam email

Scam email #2

- Specific targeted scam email
- [Possibly] Email account or email content was compromised.
- Spoofing email sender
- Use an email subject of existing conversation
- Aim:
  - Requesting financial action, e.g. Change wire transfer account
- Aka Spear-phishing, BEC (business email compromise)



From Tony Stark <mobile-ofice@email.cz> ☆

Subject **Covid-19 medical support** 2020-03-28, 8:41

To accountspayable@victim.com ☆

Hi there,

I trust you are keeping safe, I need you to setup a wire payment for Covid_19 medical support today. The total amount is $37,420.35 Advice if i can forward the beneficiary details over.?

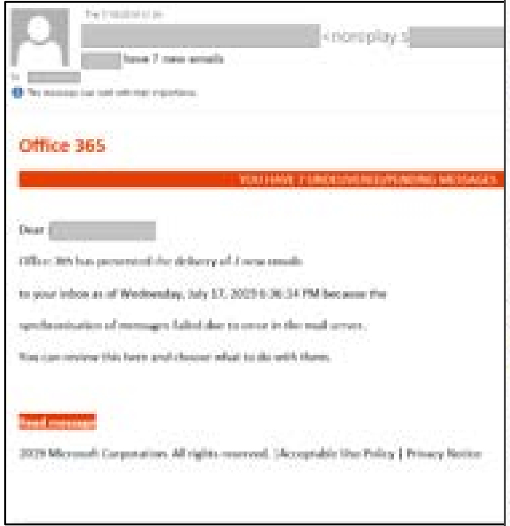
Regards,
Tony Stark

Get Outlook for iOS

Phishing Email - with malicious link/attachment

With malicious link/attachment

- Spoofing email sender
- “Fake” email address
- Includes link(s)/attachment(s)
- Aim:
  - Redirect user to a phishing page, and lure user to input credential
  - Lure user to open the malicious file, and inject malicious code/malware
  - Network/System intrusion, Steal information



[redacted] <noreply@[redacted]

[redacted] have 7 new emails

To [redacted]

This message was sent with high importance.

Office 365

YOU HAVE 7 UNDELIVERED/PENDING MESSAGES

Dear [redacted]

Office 365 has prevented the delivery of 7 new emails

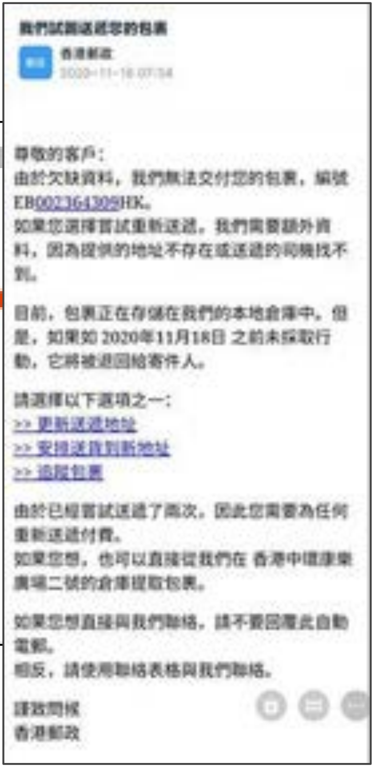
to your inbox as of Wednesday, July 17, 2019 6:36:34 PM because the

synchronization of messages failed due to error in the mail server.

You can review this here and choose what to do with them.

Read messages

2019 Microsoft Corporation. All rights reserved. |Acceptable Use Policy | Privacy Notice



我們試圖送遞您的包裹

香港郵政
2020-11-18 07:34

尊敬的客戶：
由於欠缺資料，我們無法交付您的包裹，編號EB002364309HK。
如果您選擇嘗試重新送遞，我們需要額外資料，因為提供的地址不存在或送遞的司機找不到。

目前，包裹正在存儲在我們的本地倉庫中。但是，如果如 2020年11月18日 之前未採取行動，它將被退回給寄件人。

請選擇以下選項之一：
>> 更新送遞地址
>> 安排送貨到新地址
>> 追蹤包裹

由於已經嘗試送遞了兩次，因此您需要為任何重新送遞付費。
如果您想，也可以直接從我們在 香港中環康樂廣場二號的倉庫提取包裹。

如果您想直接與我們聯絡，請不要回覆此自動電郵。
相反，請使用聯絡表格與我們聯絡。

謹致問候
香港郵政

Ref: https://www.hongkongpost.hk/tc/about_us/whats_new/notices/index_id_1005.html

Technologies you need to know

Can an email sender appear “fake”?

- YES. With specific configurations, the field of “email sender” can be set anything through commands or application.

```
telnet mail.server.com 25
HELO spoofdomain.com
MAIL FROM: <sender@spoofdomain.com>
RCPT TO: <recipient@yourcompany.com>
```

- To verify an email, “Email Header” should be reviewed to understand the source of real sender.

Ref: http://deadfake.com/Guide_To_Sending2.aspx
Ref: https://mxtoolbox.com/public/content/emailheaders/

Technologies you need to know

Targeted phishing attack

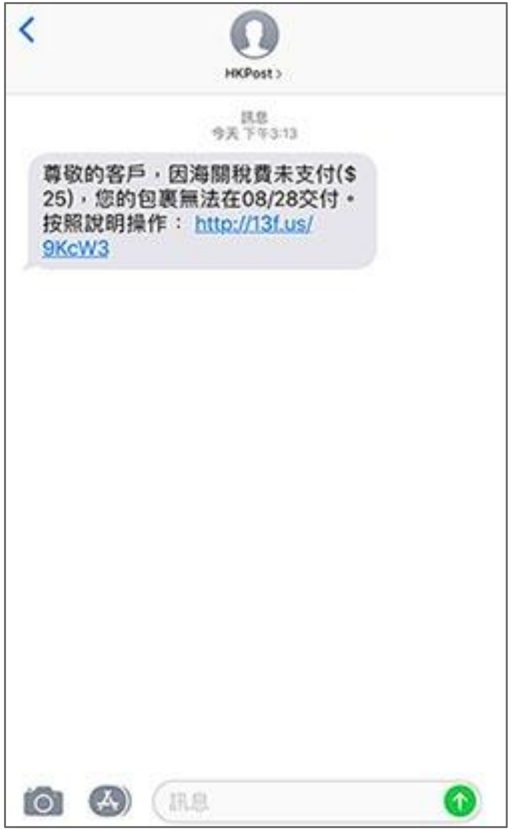
- Attacker may register a similar domain(s) of the target, and spoof as internal email.

```
From: attacker@yourcomqany.com
To: boss@yourcomqany.com
Cc: employee@yourcompany.com

Hi Boss,
Thank you for your approval.

Copied Employee,
Please follow up and make the transfer ASAP.
```

SMS Phishing (SMishing)

With malicious link

- The message sender displayed a number with prefix +852 or a spoofing name.
- Common theme of SMS, e.g. bank account login, package delivery
- The link may redirect to a landing page/ file download
- Aim:
  - Redirect user to a phishing page, and lure user to input credential
  - Lure user to install malicious mobile app
  - System intrusion, Steal information



HKPost >

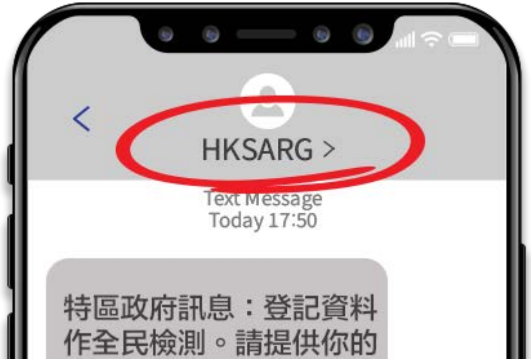
訊息
今天 下午3:13

尊敬的客戶，因海關稅費未支付($25)，您的包裹無法在08/28交付。按照說明操作： http://13f.us/9KcW3

Ref: https://www.hongkongpost.hk/tc/about_us/whats_new/notices/index_id_1005.html

Technologies you need to know

- Believe attacker use oversea SMS API service
- SMS sender is not required a phone number
- Then, send a bulk of spam SMS to local users



HKSARG >

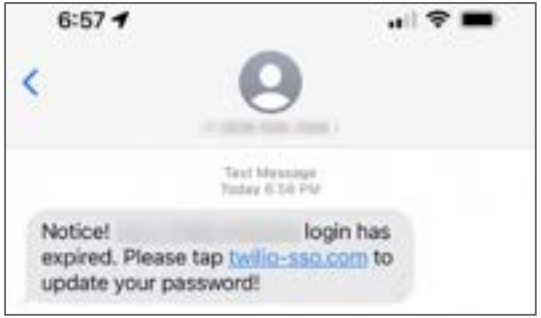
Text Message
Today 17:50

特區政府訊息：登記資料
作全民檢測。請提供你的

Ref: https://cyberdefender.hk/852_sms/

SMS Phishing (SMishing) - Case of Cyber Incident

- 2022-Aug - Cloud communication company Twilio, two employee were phished by spoofed SMS.
- It impersonated IT department, and asking to change password. Then, gained the login credential.
- After the investigation, Twilio identified approximately 125 customers whose data was accessed by attacker.
- One of the customers is Signal (instant messaging service). It has about 1,900 affected users.
    - For approximately 1,900 users, either 1) their phone numbers were potentially revealed as being registered to a Signal account, or 2) the SMS verification code used to register with Signal was revealed.



[redacted]

Text Message
Today 6:56 PM

Notice! [redacted] login has expired. Please tap twilio-sso.com to update your password!

Ref: https://www.twilio.com/blog/august-2022-social-engineering-attack
Ref: https://support.signal.org/hc/zh-tw/articles/4850133017242-Twilio-Twilio-事件-Signal-使用者須知

Technologies - Other phishing channels

Phishing phone call

- Believe it makes use of VoIP (Internet Call Service)
- The caller is not required to register a permanent call number
- The caller can choose any region call number during the registration. E.g. the call number with +852 prefix
- Then, he can impersonate a Hong Kong local caller

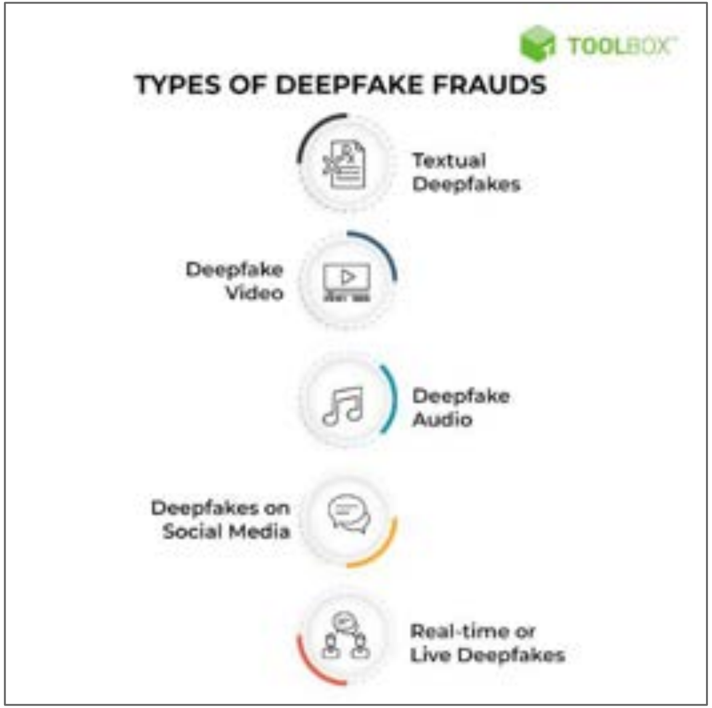
IM (Instant messaging) service

- E.g. WhatsApp, Telegram, Signal
- With a registered phone number or API call service, spammer can send a bulk of messages in the channel.

Deepfake Tech (深偽技術)

Deepfake Tech

- Deepfake is a combination of “deep learning” and “fake”
- leverage powerful techniques from machine learning (ML) and artificial intelligence (AI) to manipulate or generate visual and audio content synthetic media
- in which a person in an existing image or video is replaced with someone else's likeness, to fool the media viewer or a technology system

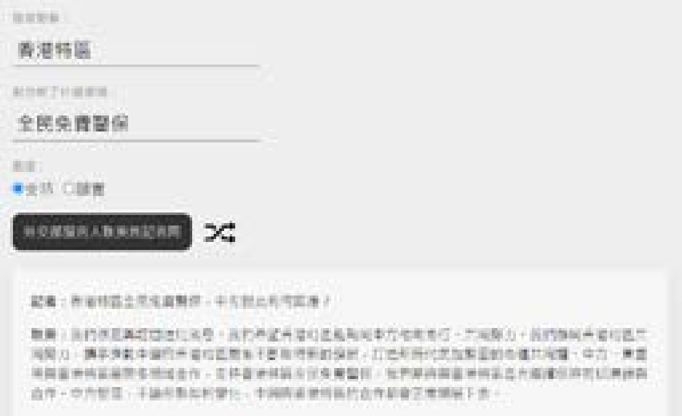


Ref: https://www.spiceworks.com/it-security/cyber-risk-management/articles/what-is-deepfake/

Deepfake Tech

Textual deepfake

- With matured natural language processing (NLP), AI-generated writing can now compose human-looking pith and clarity
- E.g. Article generator, Chat bot



[illegible]

香港特區

[illegible]

全民免費醫保

● [illegible] ○ [illegible]

記者：[illegible]

耿爽：[illegible]

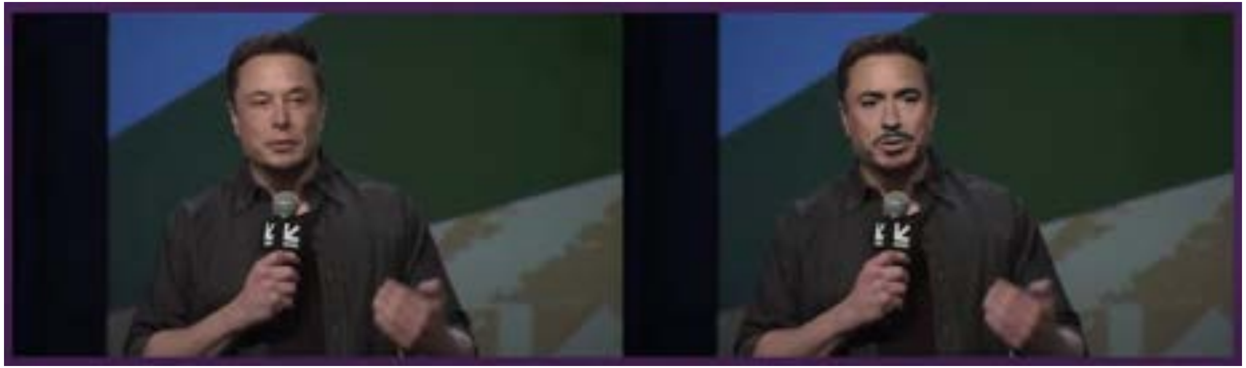
- Demo: Geng Shuang Emulator
- https://gengshuang1.github.io/

Deepfake Tech

Deepfake video/audio

- Use AI generate visual and audio content synthetic media
- No more “Photo tells the truth”, “Video tells the truth”

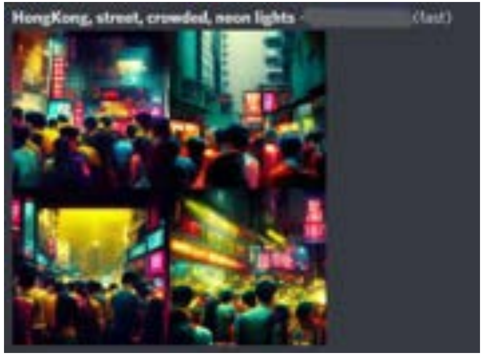
Elon Musk as Tony Stark



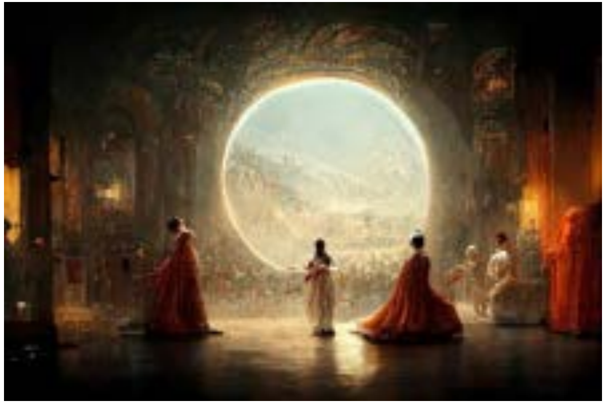
Ref: https://www.youtube.com/watch?v=lSM-9RBk3HQ

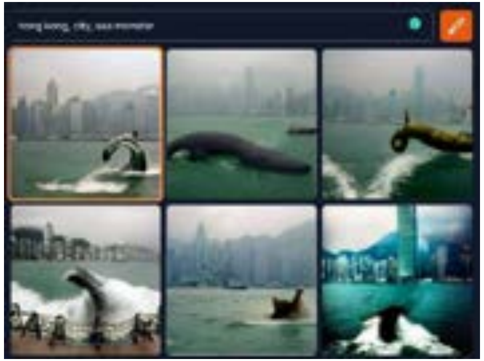
Deepfake Tech

- E.g. Image generator
- AI-generated artworks “Théâtre D’opéra Spatial” joined in an art competition and won the first prize



HongKong, street, crowded, neon lights - [redacted] (fast)





hong kong, city, sea monster

Ref: https://www.chinatimes.com/realtimenews/20220904001063-260408
Ref: https://www.midjourney.com/ Ref: https://www.craiyon.com/

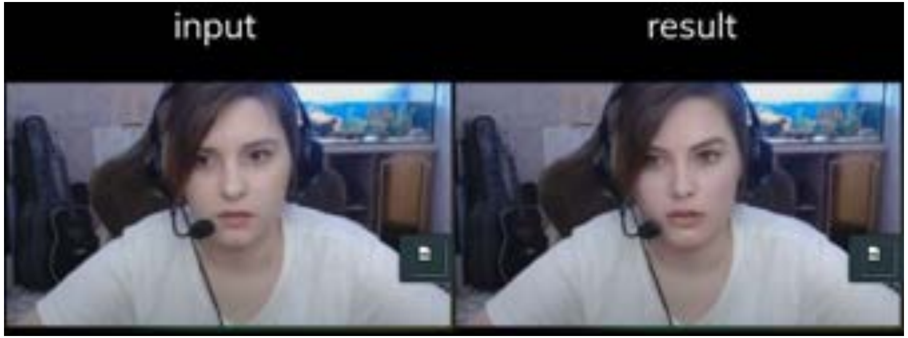
Deepfake Tech

- E.g. AI face swapper
- It can be done in PC or mobile phone app
- Steps:
  - 1. Extract faceset from source and destination videos
  - 2. AI training the model
  - 3. Composite and render the video
- Also, generate deepfake voice

Ref: https://www.youtube.com/watch?v=LNVY51r63Ac
Ref: https://www.youtube.com/watch?v=cQ54GDm1eL0

Deepfake Tech

- E.g. Real-time face swapper
  - Using well-trained faceset
  - Swapping face in a real-time source video

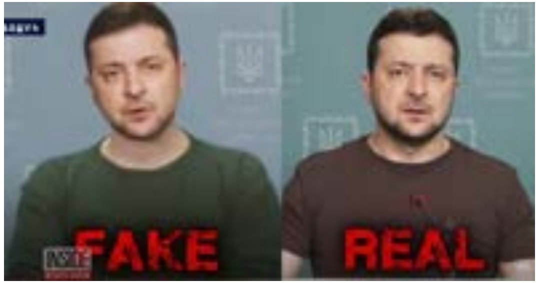


- E.g. Face Animator module
  - It only requires a static target photo

Ref: https://www.youtube.com/watch?v=0p-nNSvB7KA
Ref: https://github.com/iperov/DeepFaceLive

Deepfake we worry #1

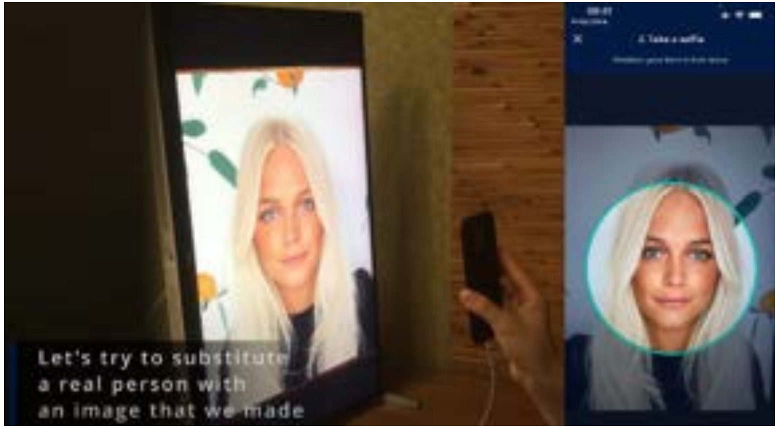
- Misleading video, blurring the truth
  - The product is like a stunt movie, it can be fake
  - Impersonating a public figure, posting improper video or false statements

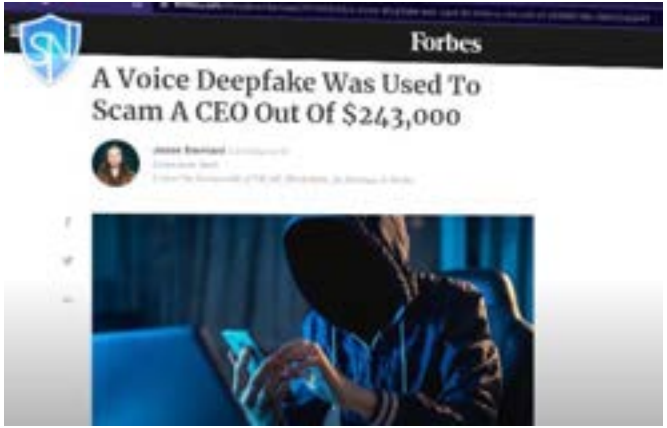


Ref: https://www.weekendhk.com/weekspecial/日本美女電單車手-gotrip-1120761/
Ref: https://inews.hket.com/article/2283269/朱茵變楊冪%E3%80%80Deepfake%20AI換臉或成勒索工具
Ref: https://www.youtube.com/watch?v=enr78tJkTLE

Deepfake we worry #2

- It may bypass face or voice recognition, leading to false authentication
  - E.g. Customer’s identification in mobile app, Voice recognition feature.





A Voice Deepfake Was Used To Scam A CEO Out Of $243,000

Ref: https://www.youtube.com/watch?v=98Ixy-HoMn0&t=64s
Ref: https://www.youtube.com/watch?v=CeYLyeWhi4E&t=391s

Security Tips

Security Tips

- Need to be calm and rational, when receiving any information
- “Fact Check”
- Think twice, especially handling “Personal Credential” and "Money Related Activities"
- E-account/Credential
    - Enable 2FA/MFA feature
    - Never provide any passwords or authentication codes to third parties

Ref: https://www.adcc.gov.hk/zh-hk/alerts.html

Security Tips

- “Fact Check”

香港浸會大學 HONG KONG BAPTIST UNIVERSITY

傳理學院 School of Communication

事實查核

Factcheck Lab 事實查核實驗室

判詞顯示主要考慮是否夥同他人

網傳法官稱「不排除貪玩」撤少年非法集結定罪，判詞顯示主要考慮被告是否夥同他人

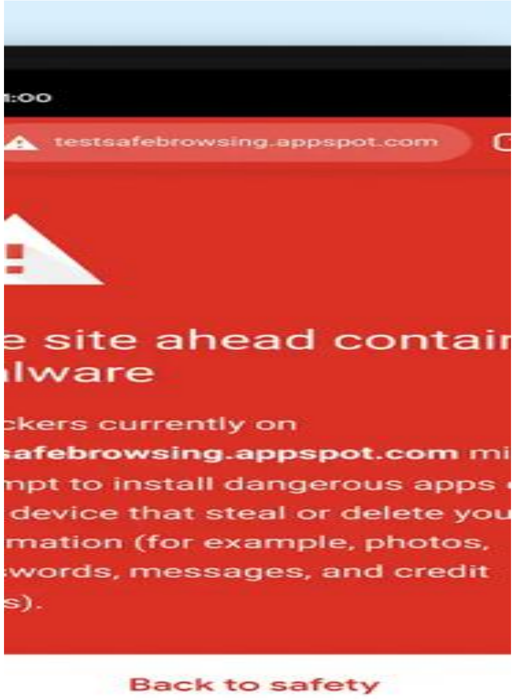
Ref: https://factcheck.hkbu.edu.hk/home/fact-check/
Ref: https://www.factchecklab.org/

Report & Feedback

Report & Feedback

Phishing Link - Report

- Report to Google Safe Browsing
  - https://safebrowsing.google.com/safebrowsing/report_phish/
- Report to HKCERT
  - https://www.hkcert.org/form/incident-report-end-user-sme/
  - hkcert@hkcert.org



:00

testsafebrowsing.appspot.com

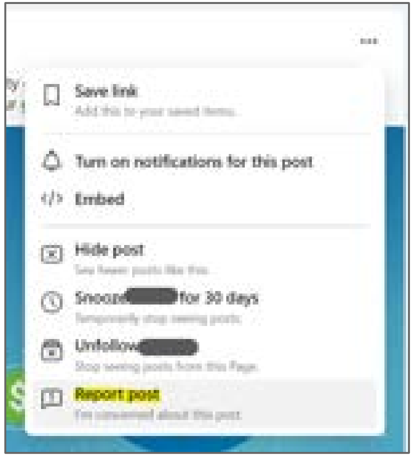
e site ahead contai
lware

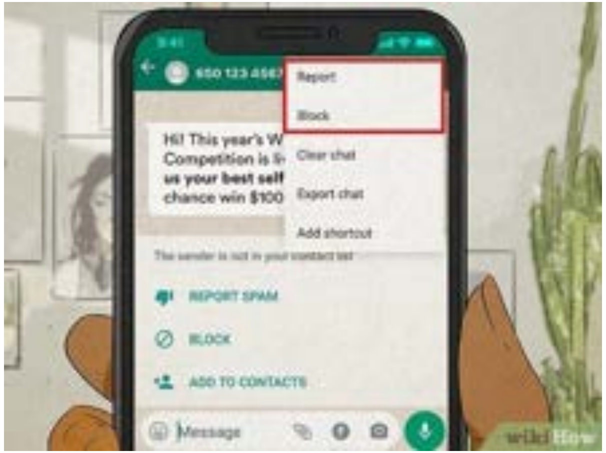
ckers currently on
safebrowsing.appspot.com mi
npt to install dangerous apps
device that steal or delete you
mation (for example, photos,
words, messages, and credit
s).

Report & Feedback

Social media/ IM service - Report

- Search “Report Abuse” to find out how to report the scam


Save link
Add this to your saved items.
Turn on notifications for this post
Embed
Hide post
See fewer posts like this.
Snooze [redacted] for 30 days
Temporarily stop seeing posts.
Unfollow [redacted]
Stop seeing posts from this Page.
Report post
I'm concerned about this post.



Hi! This year's W
Competition is li
us your best self
chance win $100

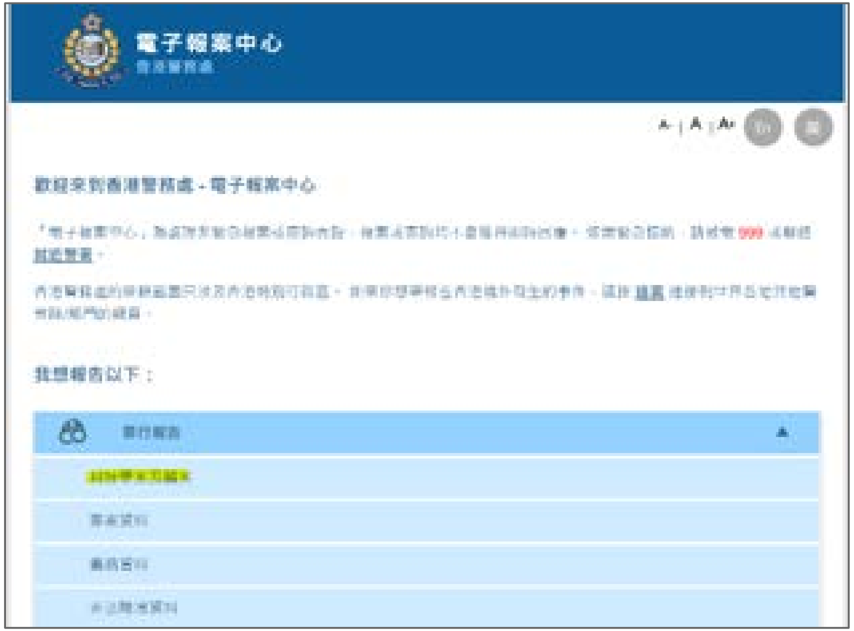
The sender is not in your contact list

Ref: https://zh-hk.facebook.com/help/263149623790594
Ref: https://www.wikihow.com/Identify-a-Fake-WhatsApp-Number

Report & Feedback

Fraud case

- Suspect being scammed
- Report
  - Technology Crime and Deception



電子報案中心
香港警務處

歡迎來到香港警務處 - 電子報案中心

「電子報案中心」[illegible] 999 [illegible]

[illegible]

我想報告以下：

罪行報告

[illegible]

Ref: https://www.adcc.gov.hk/zh-hk/report.html

Q&A

Thank you

Mr. Frankie Wong
frankie.wong@pisa.org.hk