UDomain

在電子支付熱潮下，怎樣保護個人及公司財產

陳靖龍
UDomain 網絡保安研究主管

簡歷 - 陳靖龍

- UDomain (2018至今)
- 執行滲透測試和安全監控
- VXRL 會員
- 網絡安全研究（例如：JTAG Debugger、Facebook Botnet）
- eBay , Apple , ASUS 認可
- Defcon 26/27 硬件村成員
- HITCONCMT 2019 零日 攻擊會議講者
- eClass Platform Authentication Bypass (CVE-2019-9884)
- eClass Platform Unauthenticated SQL Injection(CVE-2019-9885

C|EH Certified Ethical Hacker

BTA CERTIFIED BLOCKCHAIN SECURITY PROFESSIONAL

OFFENSIVE security OSWP

OFFENSIVE security OSCP

OFFENSIVE security OSWE

OFFENSIVE security OSCE

OFFENSIVE security OSEE

OFFENSIVE security OSEP

大綱

1	電子支付熱潮
2	相關新聞
3	模擬網絡釣魚
4	如何保護個人財產
5	企業需要注意事項


支付宝
ALIPAY
Pay
EPS
易辦事
G Pay
mastercard.
MasterCard
paypass
八達通
Octopus
SAMSUNG
pay
Tap&Go
TNG
香港人的電子錢包
UnionPay
銀联
Quick
闪付Pass
VISA
Visa
payWave
WeChat Pay
7-ELEVEN
7-FANS


消費券計劃
Consumption Voucher Scheme
$5,000
立即登記
上載身分證複本
(只限在登記時被要求的登記人)
齊齊消費
帶旺經濟

跨境支付佔總交易量約16%

香港成PayPal重點跨境市場

電子消費帶旺經濟

轉數快月增23萬個新登記

警方近日接報，指有騙徒假冒成銀行職員，再透過即時通訊軟件 WhatsApp 向受害人發訊息，表示可預先為其登記領取 $5000 電子消費券。事主表示當自己提交所有資料後，其電話號碼隨即失效，於是便向相關銀行查詢，發現有人利用其身份開通電子支付平台帳戶，並以其名義在銀行帳戶提取 2 萬元到電子支付平台，事主懷疑受騙後報案。

https://ezone.ulifestyle.com.hk

【電子消費券騙案】代申請消費券騙個人資料 開通支付平台盜取 2 萬元

| 徐慧兒 | 03-06-2021 13:02 | Like 36

近期發生的電騙案件中，很多受害人為長者，他們被騙開網上銀行戶口後，會被要求交出密碼，其後存款會於短時間內被轉走。

https://www.hk01.com

網絡安全相關新聞及損失

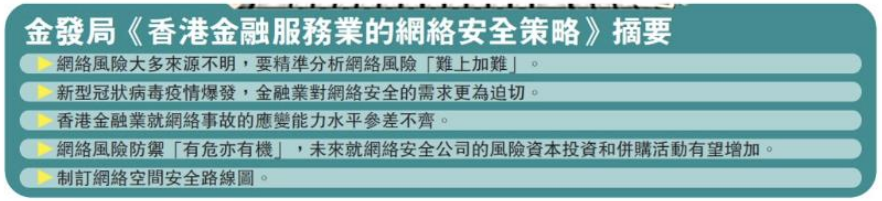
- 疫情開展遙距工作模式及網上消費
- 智慧城市和金融科技發展
- 製造有利黑客攻擊條件

網絡攻擊令港潛在經濟損失2500億 金發局倡訂網安路線圖

2021-06-10 16:40

來源：香港商報

金發局最新在《香港金融服務業的網絡安全策略》報告中指出，金融服務業是網絡攻擊的主要目標，海外研究估計網絡安全事件對香港造成的潛在經濟損失，將高達320億美元(約2496億港元)。報告建議當局立法保護網絡空間，同時鼓勵公私營界別合作，使香港有能力應對網絡風險。



報告指，網絡風險大多來源不明，要精準分析網絡風險可謂「難上加難」，香港就網絡事故的應變能力水平參差不齊，加上個人的網絡風險意識普遍較弱，在第五代(5G)流動網絡覆蓋及其他智慧城市基建之下，科技發展將使到黑客及網絡犯罪分子更為有機可乘。

根據報告引述的數據，2018年因網絡攻擊對銀行及保險業所造成的平均損失，分別約為1800萬美元及1500萬美元；隨著新冠肺炎疫情爆發，各國政府、機構及個人因應時勢開展實行遙距工作及採用虛擬會議等新的網上活動，全球的網絡罪犯亦在這場危機中蠢蠢欲動。

模擬網絡釣魚

如何保護個人財產

智能電話、智慧型手錶已成為你的銀包

切記

Dos

- 留心來電號碼
- 主動向機構、銀行或公司核實來電者身份
- 採用雙重認證或生物認證
- 設增值金額的上限

切勿

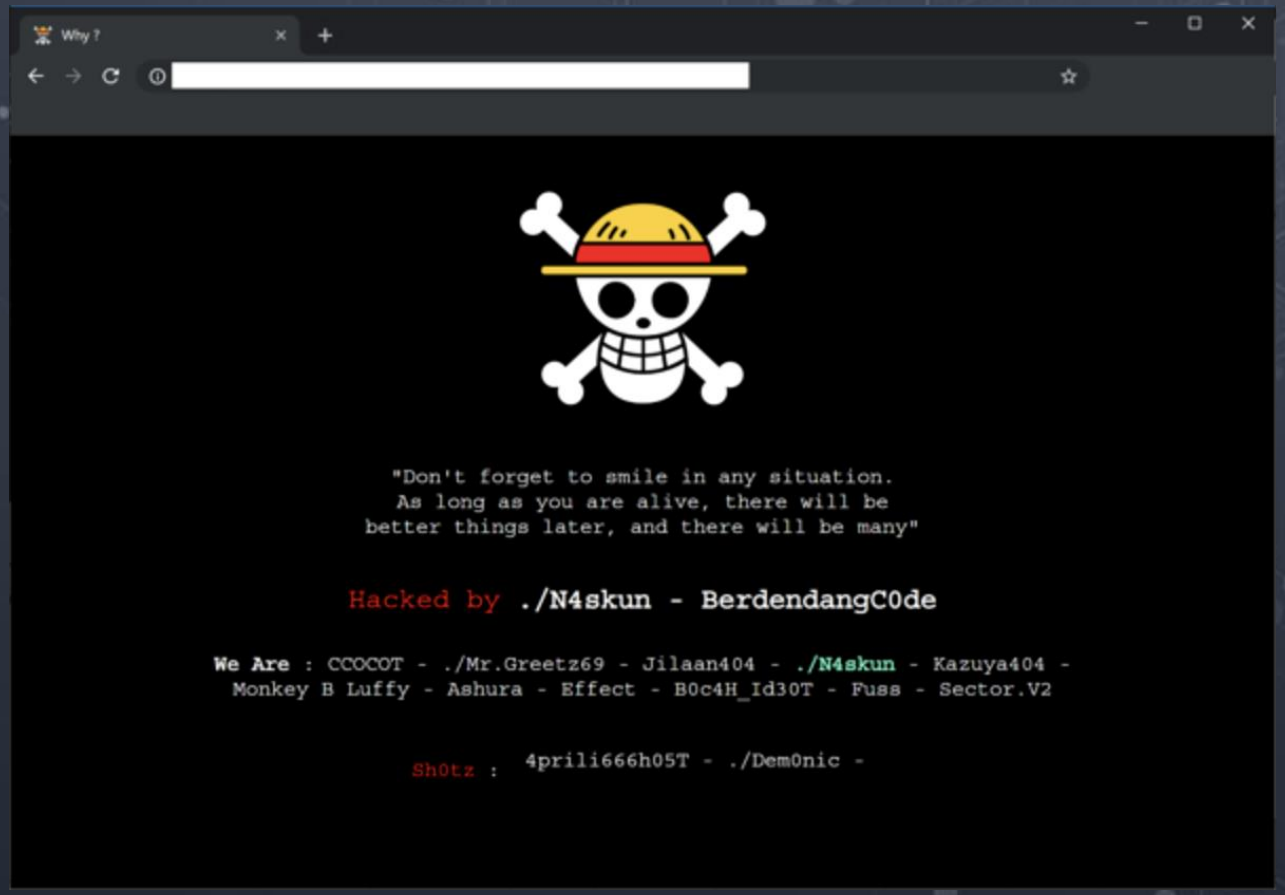
Don'ts

- 使用非官方軟件或平台
- 向陌生人提供敏感資料
- 在社交媒體分享太多個人資料

企業需要注意事項？

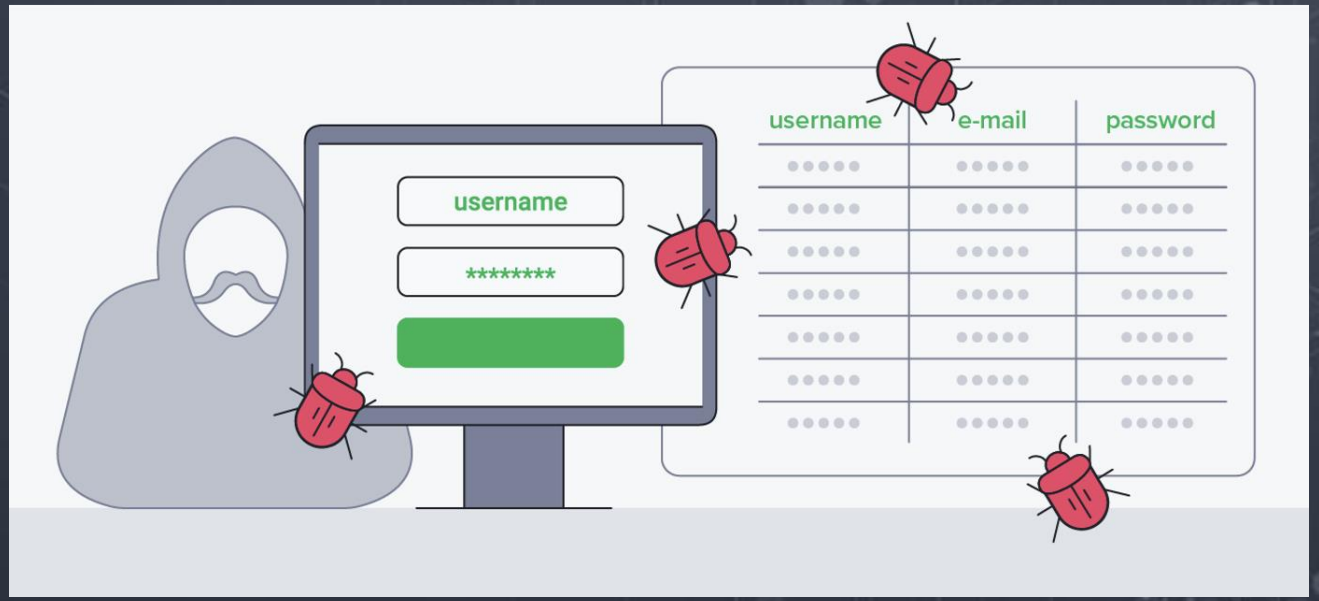
網頁竄改 (Web Defacement)

- 改變網頁外觀的攻擊
- 表達政見
- 展示能力
- 隨機攻擊



代碼注入 (Code Injection)

- 在網頁中插入代碼
  - Command injection
  - Sql injection
- 讀取數據庫資料
- 全權控制服務器



金融行業網絡安全指引

- 金管局
  - 網絡防衛評估框架
  - 監管政策手冊 TM-E-1
- 證監會
  - 降低及紓減與互聯網交易相關的黑客入侵風險指引

企業資安待辦清單 (To Do List)

- ✓ 確保電腦及伺服器採用最新的保安修補程式及安裝最新定義檔的抗惡意軟件
- ✓ 安裝桌面電郵過濾(Anti-Spam)產品，以偵察和阻截欺詐電郵。
- ✓ 定期進行滲透性測試(Penetration Test)及僱員安全意識訓練(Security Awareness Training)
- ✓ 定期備份 (3份備份 - 2種格式 -1份存放異地，如雲端）

多謝!