Numbers you have to know …

In 2016

$1 Billion
Paid to Ransomware

$101 Billion
Spending in Cyber Security by 2020

4,281,795,808
Records Breached

1 Tbps
Largest DDoS attack

$6
To buy access to hacked server

123456 / qwerty / 1q2w3e4r
Password of 17% computer users

Source: Risk Based Security Report

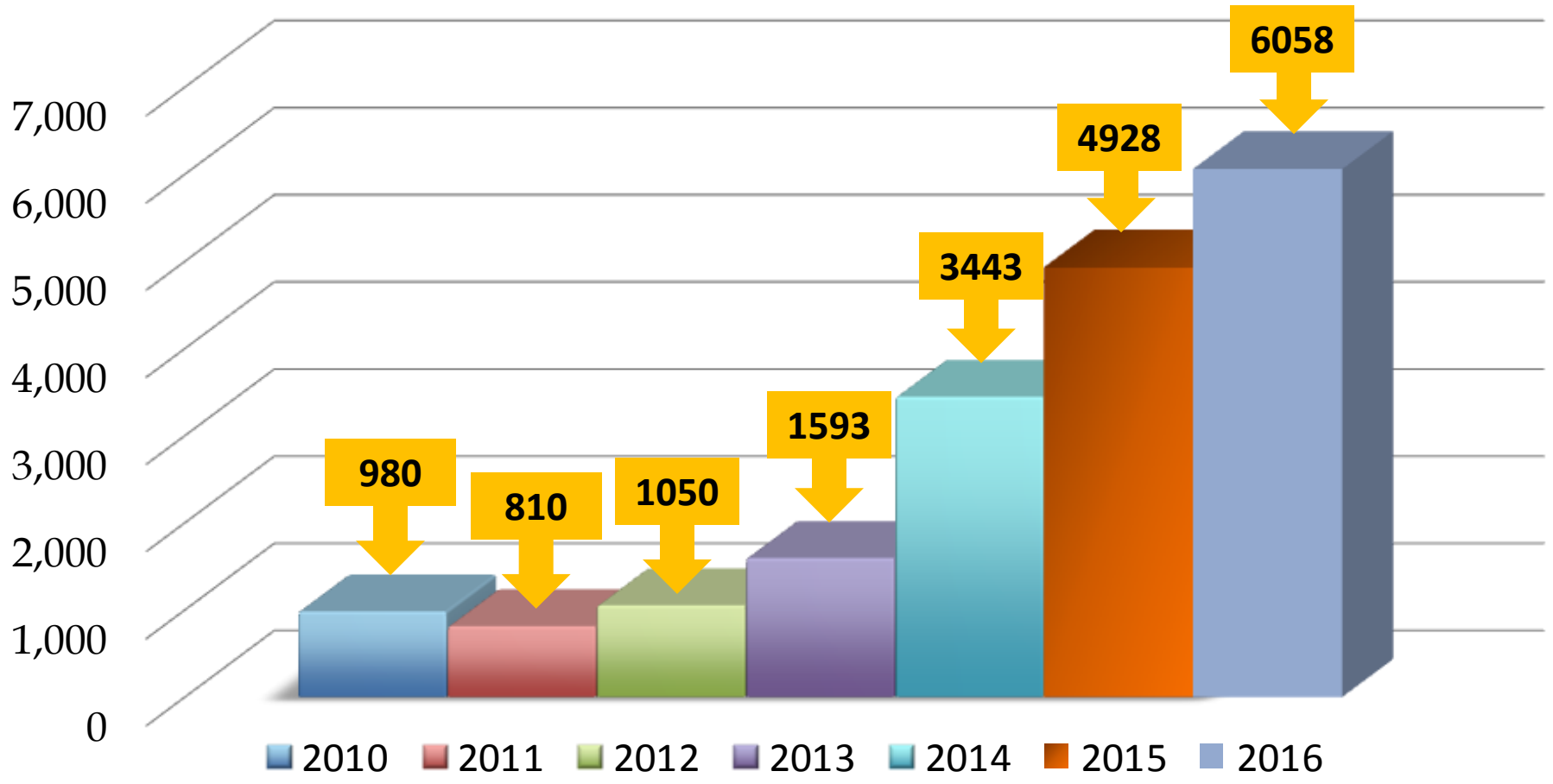
Cyber Security Situation in HK

	Ranking of HK (2013)	Ranking of HK (2014)	Ranking of HK (2015)
Global Threat Ranking	225	23	17
Asia, Pacific and Japan (APJ) Threat Ranking	58	8	7

Source: Symantec' Internet Security Threat Report

Cyber Security Situation in HK

Cyber Security Incident in HK



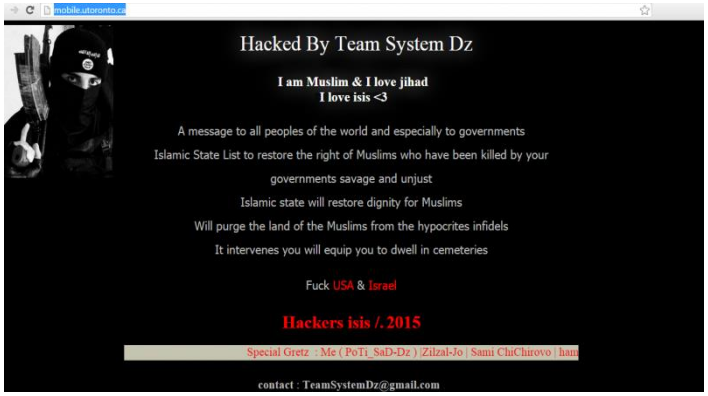
Source: HKCERT

Cyber Security Situation in HK

Common types of Cyber Attack

DDoS / Botnet

Malware (Ransomware)



Defacement

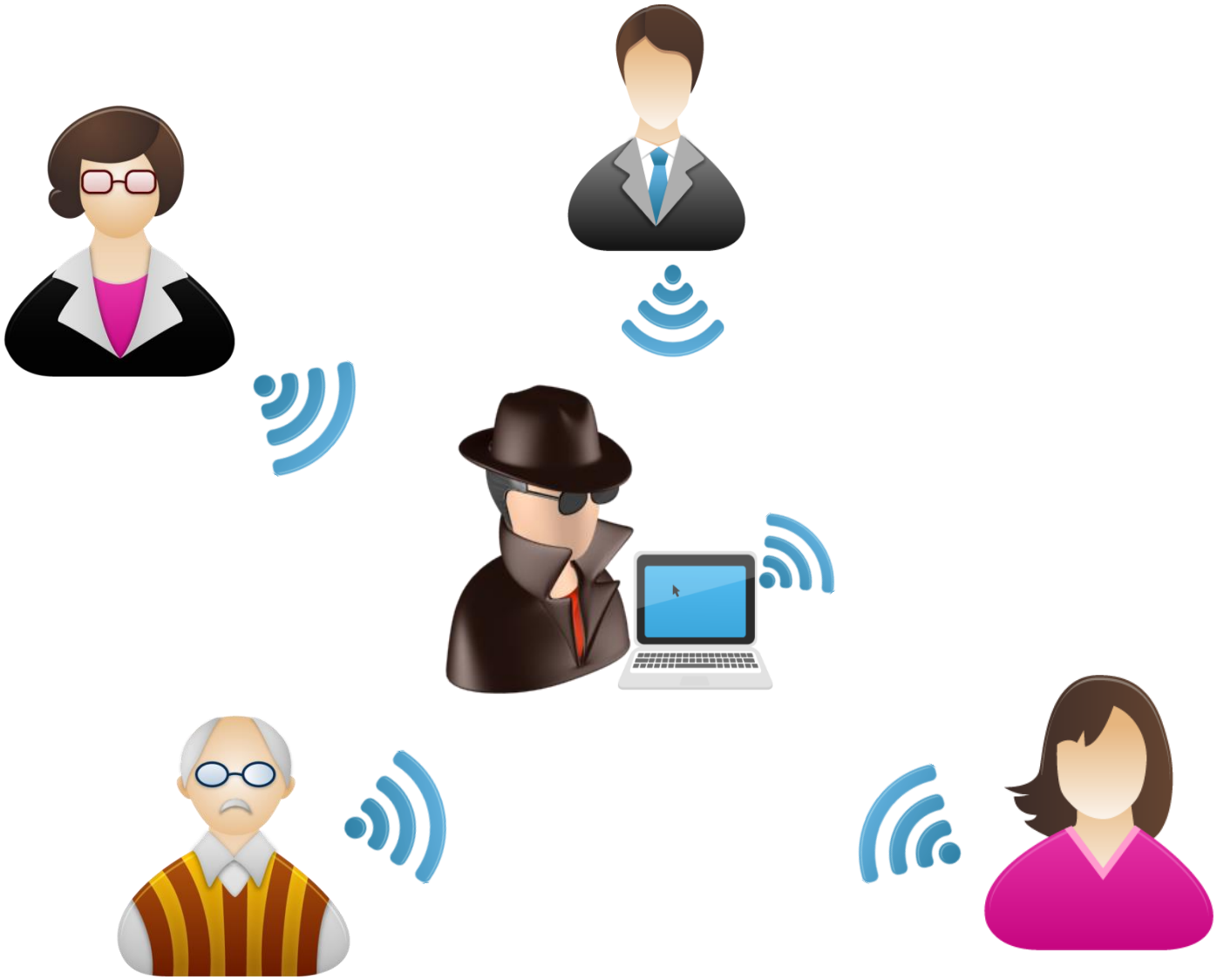
Phishing Email / Website

Sharing Outline

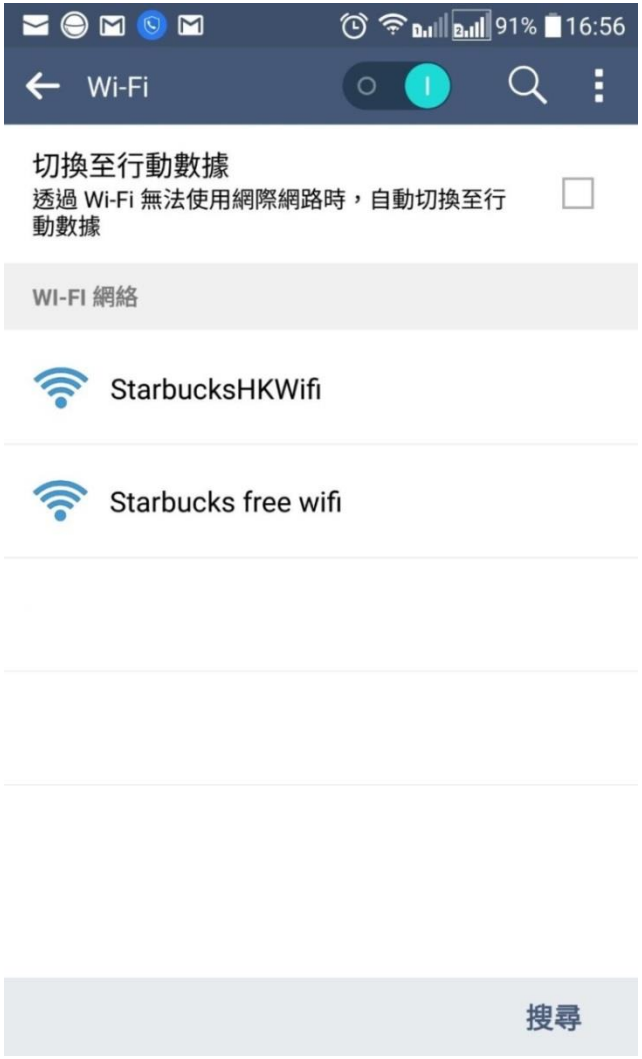
1. Public Free Wi-Fi
2. Ransomware
3. CEO Email Scam
4. Prevention Tips

Public Free Wi-Fi

Public Wi-Fi Network



Public Wi-Fi Network



Advice :

- Turn off file sharing
- Use a VPN

Ransomware

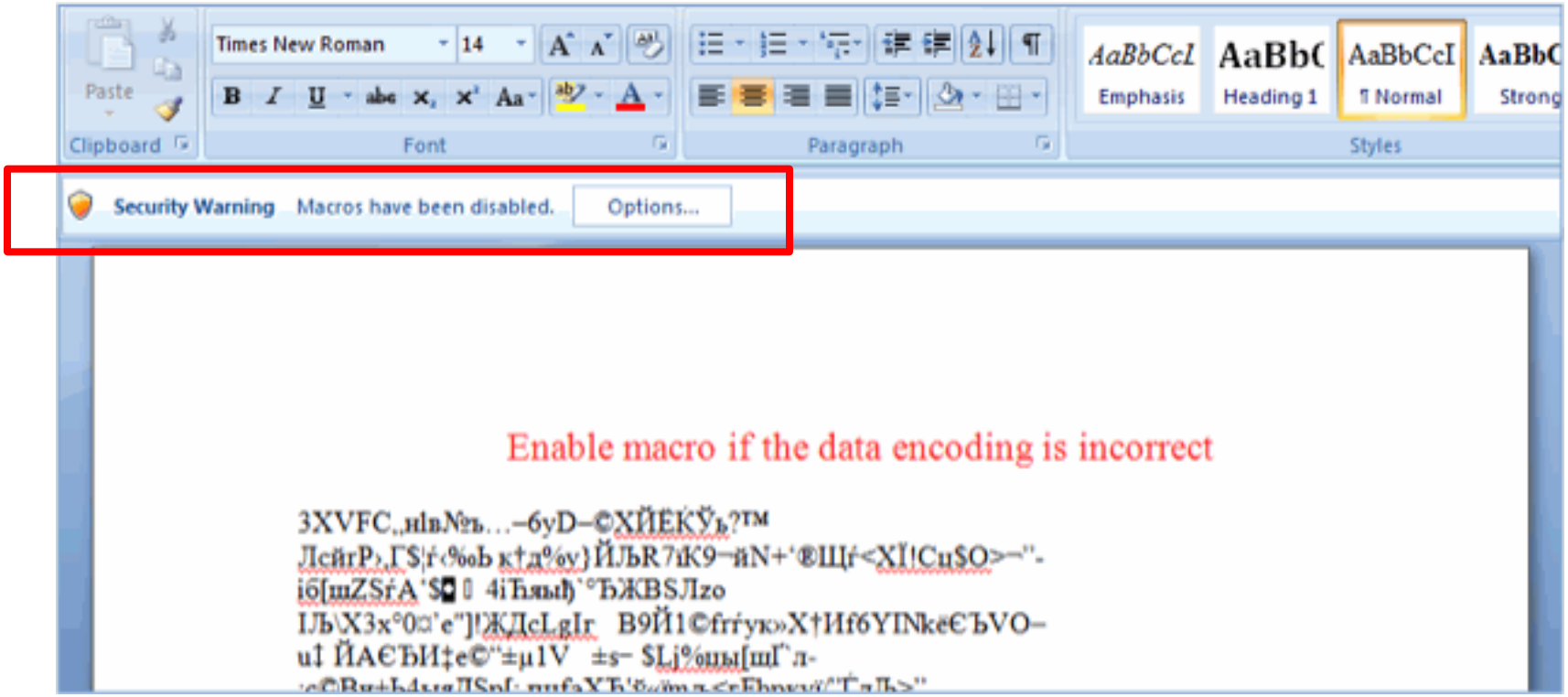
- CryptoLocker
- TorrentLocker
- TeslaCrypt
- Cryptowall
- CTB-Locker
- KeRanger
- Locky
- SamSam
- CryptXXX
- Cerber

Email Attachment

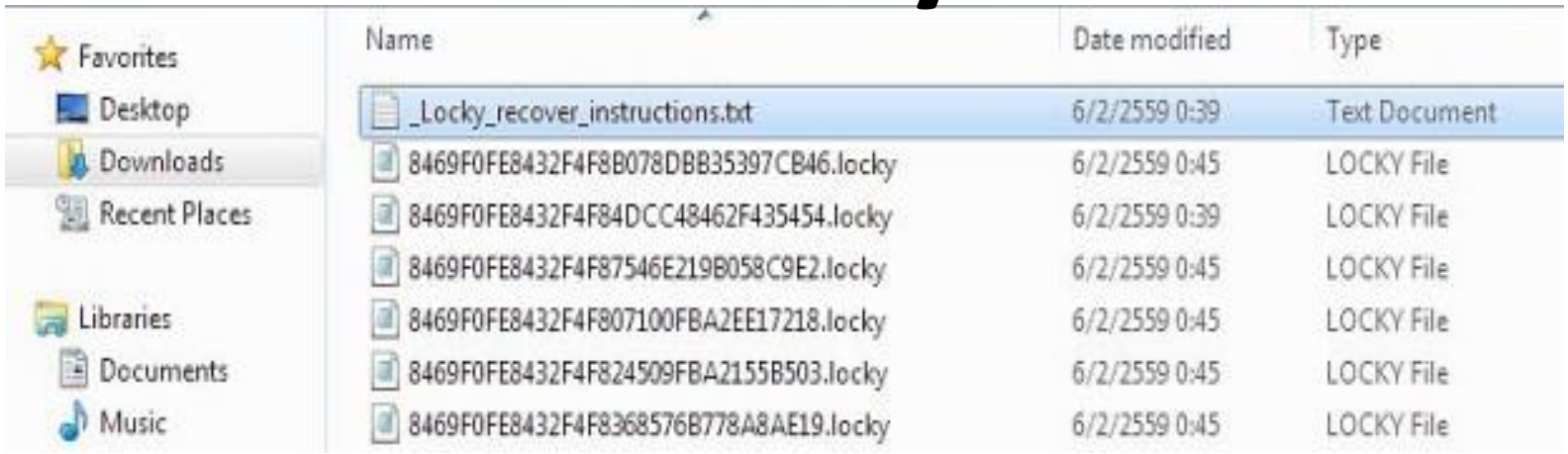
1. summary.exe, quotation.rar, invoice.zip, payment.js

2. summary.doc, quotation.xlsx, statement.ppt

Macros


Times New Roman
14
Paste
Clipboard
Font
Paragraph
Styles
Emphasis
Heading 1
Normal
Strong
Security Warning
Macros have been disabled.
Options...
Enable macro if the data encoding is incorrect

Locky

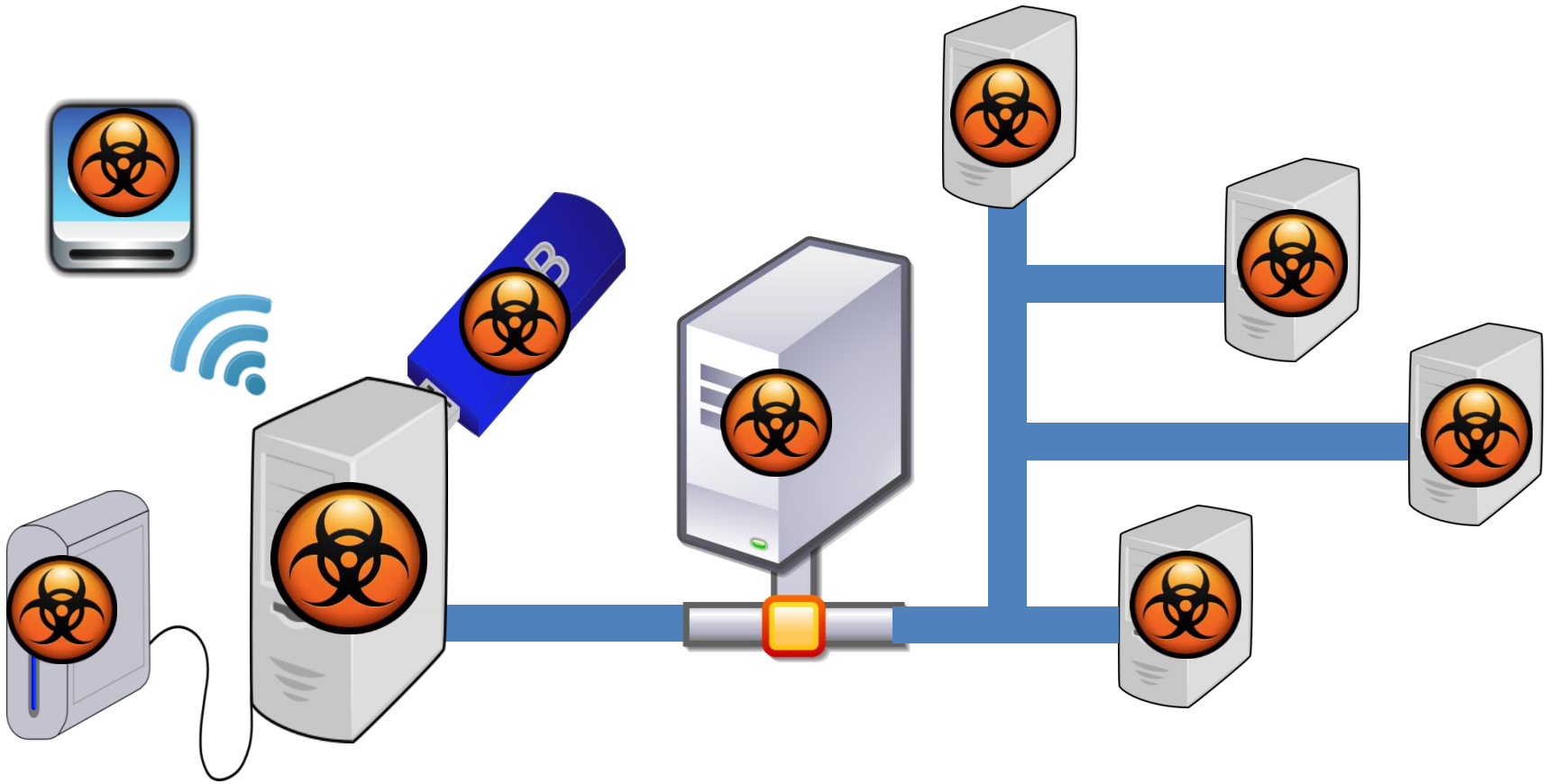


.7z; .rar; .m4a; .wma; .avi; .wmv; .csv; .d3dbsp; .sc2save; .sie; .sum; .ibank; .t13; .t12; .qdf; .gdb; .tax; .pkpass; .bc6; .bc7; .bkp; .qic; .bkf; .sidn; .sidd; .mddata; .itl; .itdb; .icxs; .hvpl; .hplg; .hkdb; .mdbackup; .syncdb; .gho; .cas; .svg; .map; .wmo; .itm; .sb; .fos; .mcgame; .vdf; .ztmp; .sis; .sid; .ncf; .menu; .layout; .dmp; .blob; .esm; .001; .vtf; .dazip; .fpk; .mlx; .kf; .iwd; .vpk; .tor; .psk; .rim; .w3x; .fsh; .ntl; .arch00; .lvl; .snx; .cfr; .ff; .vpp_pc; .lrf; .m2; .mcmeta; .vfs0; .mpqge; .kdb; .db0; .DayZProfile; .rofl; .hkx; .bar; .upk; .das; .iwi; .litemod; .asset; .forge; .ltx; .bsa; .apk; .re4; .sav; .lbf; .slm; .bik; .epk; .rgss3a; .pak; .big; .unity3d; .wotreplay; .xxx; .desc; .py; .m3u; .flv; .js; .css; .rb; .png; .jpeg; .txt; .p7c; .p7b; .p12; .pfx; .pem; .crt; .cer; .der; .x3f; .srw; .pef; .ptx; .r3d; .rw2; .rwl; .raw; .raf; .orf; .nrw; .mrwref; .mef; .erf; .kdc; .dcr; .cr2; .crw; .bay; .sr2; .srf; .arw; .3fr; .dng; .jpeg; .jpg; .cdr; .indd; .ai; .eps; .pdf; .pdd; .psd; .dbfv; .mdf; .wb2; .rtf; .wpd; .dxg; .xf; .dwg; .pst; .accdb; .mdb; .pptm; .pptx; .ppt; .xlk; .xlsb; .xlsm; .xlsx; .xls; .wps; .docm; .docx; .doc; .odb; .odc; .odm; .odp; .ods; .odt

Source : www.virusresearch.org

Locky

- Delete the Shadow Copy and Restore Point
- Infect other device within the network



Mitigation

- Unplug the power
- Detach the infected terminal from the network
- Detach all external storage device from the infected terminal

NO MORE RANSOM!

EUROPOL EC3 | European Cybercrime Centre

POLITIE

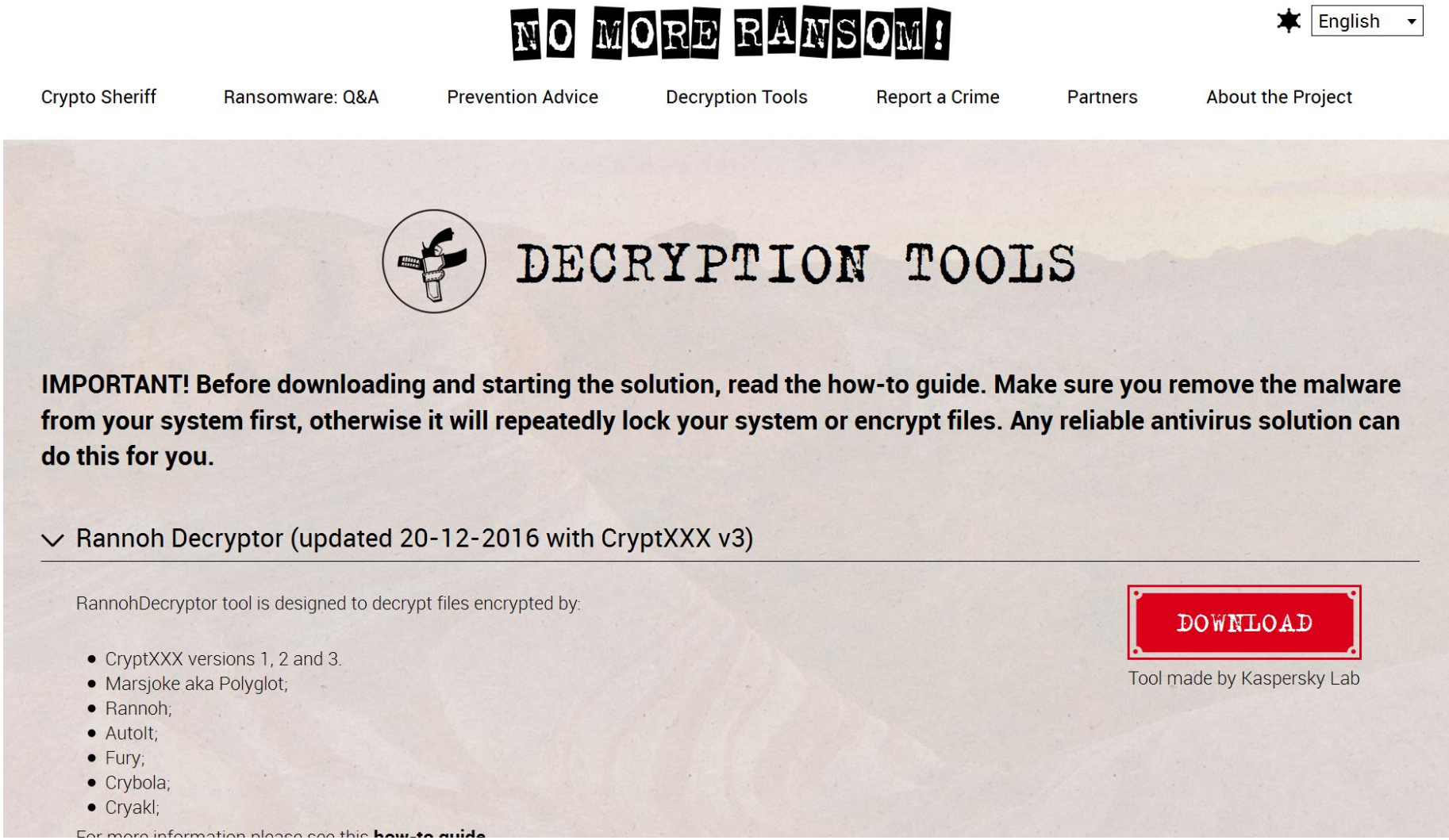
KASPERSKY lab

intel Security

Powered by:

powered by amazon web services

Barracuda



Source : http://ransomwaretracker.abuse.ch/

CEO Email Scam

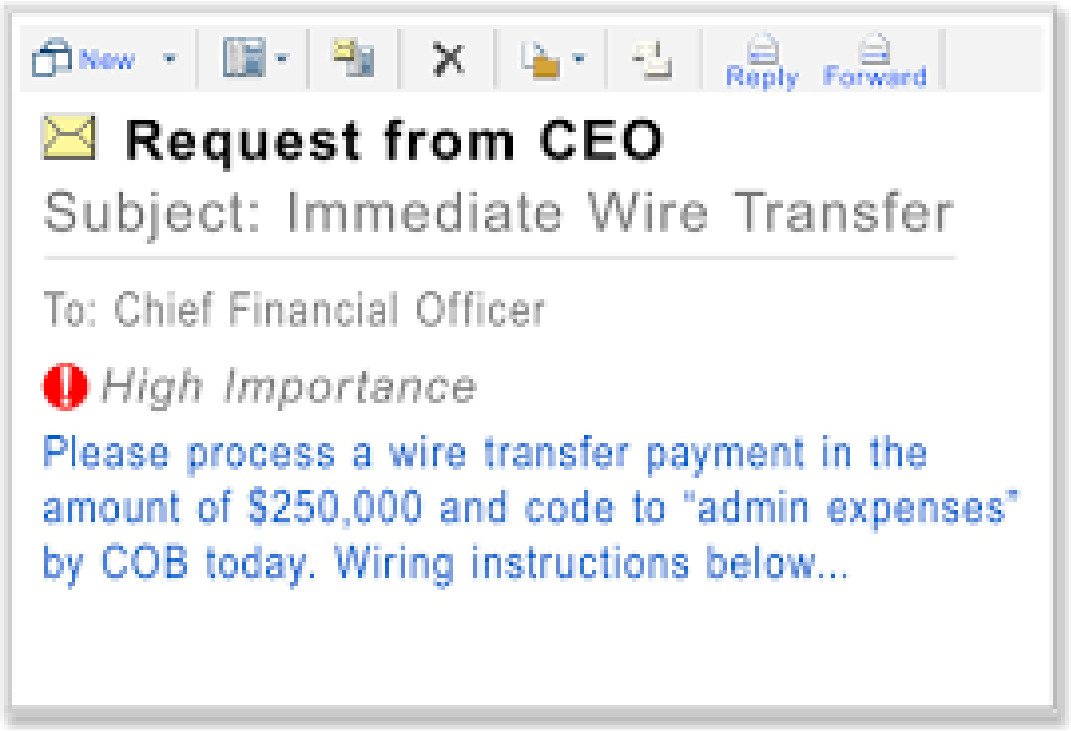
Email Scam

	2014	2015	2016
No. of Case	1236	994	883
Amount of Loss	991M	1376M	1783M

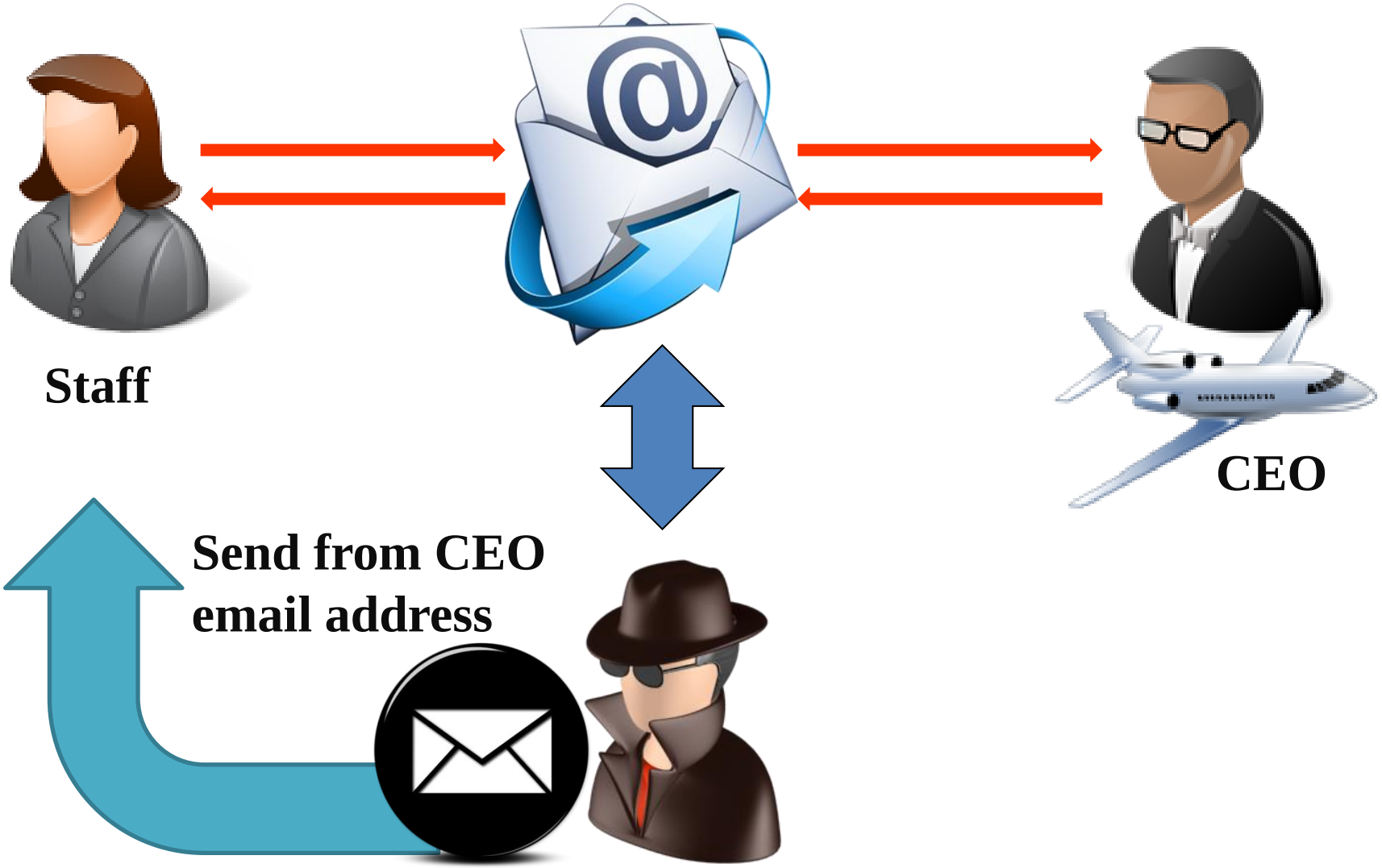
Corporate	Personal
867	16
1782M	1M

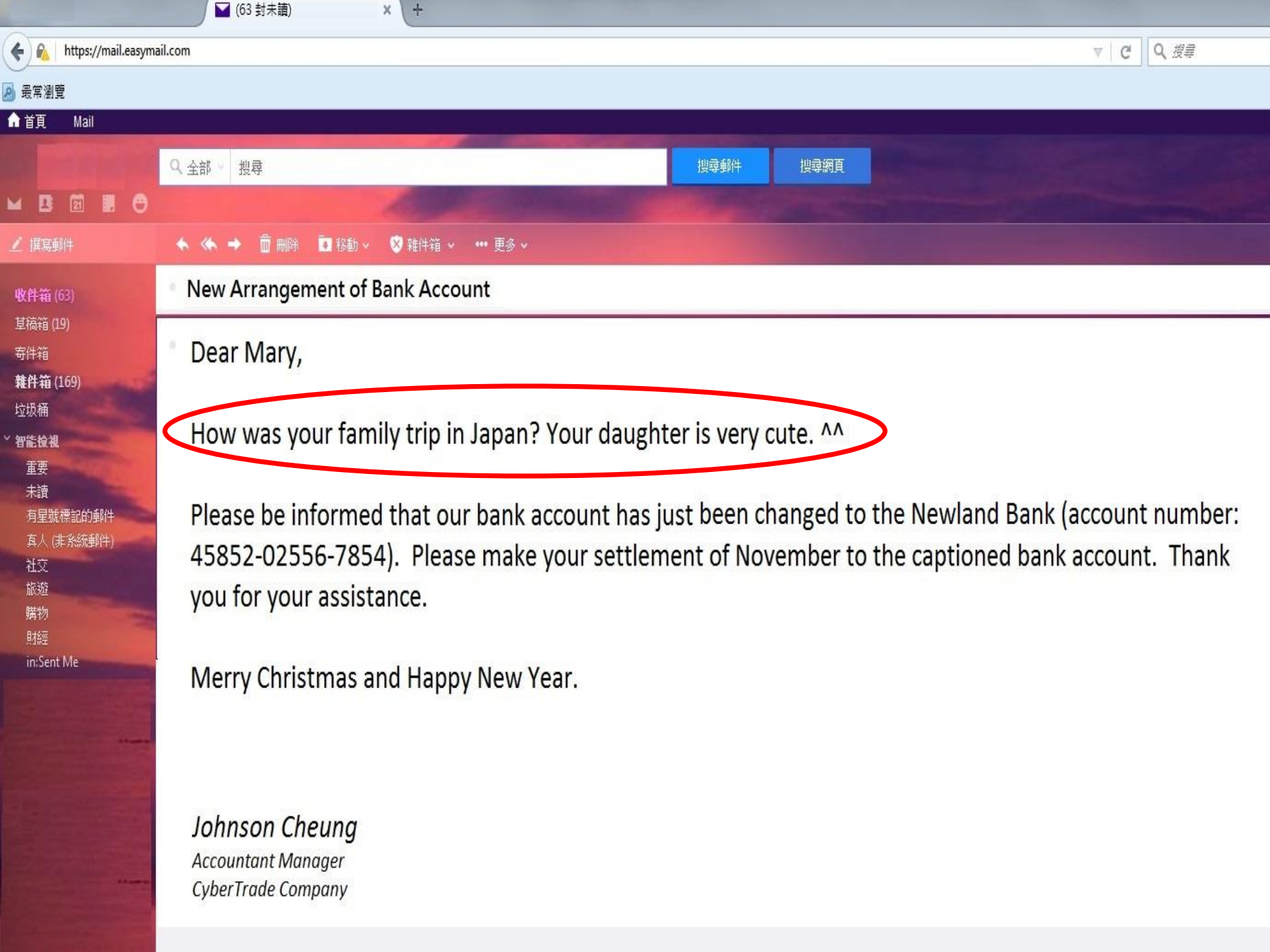
Email Scam (Corporate)

That email from your CEO could be a scam…..



Email Scam (Corporate)




(63 封未讀)
https://mail.easymail.com
搜尋
最常瀏覽
首頁
Mail
全部
搜尋
搜尋郵件
搜尋網頁
撰寫郵件
刪除
移動
雜件箱
更多
收件箱 (63)
草稿箱 (19)
寄件箱
雜件箱 (169)
垃圾桶
智能檢視
重要
未讀
有星號標記的郵件
真人 (非系統郵件)
社交
旅遊
購物
財經
in:Sent Me
New Arrangement of Bank Account
Dear Mary,
How was your family trip in Japan? Your daughter is very cute. ^^
Please be informed that our bank account has just been changed to the Newland Bank (account number: 45852-02556-7854). Please make your settlement of November to the captioned bank account. Thank you for your assistance.
Merry Christmas and Happy New Year.
Johnson Cheung
Accountant Manager
CyberTrade Company

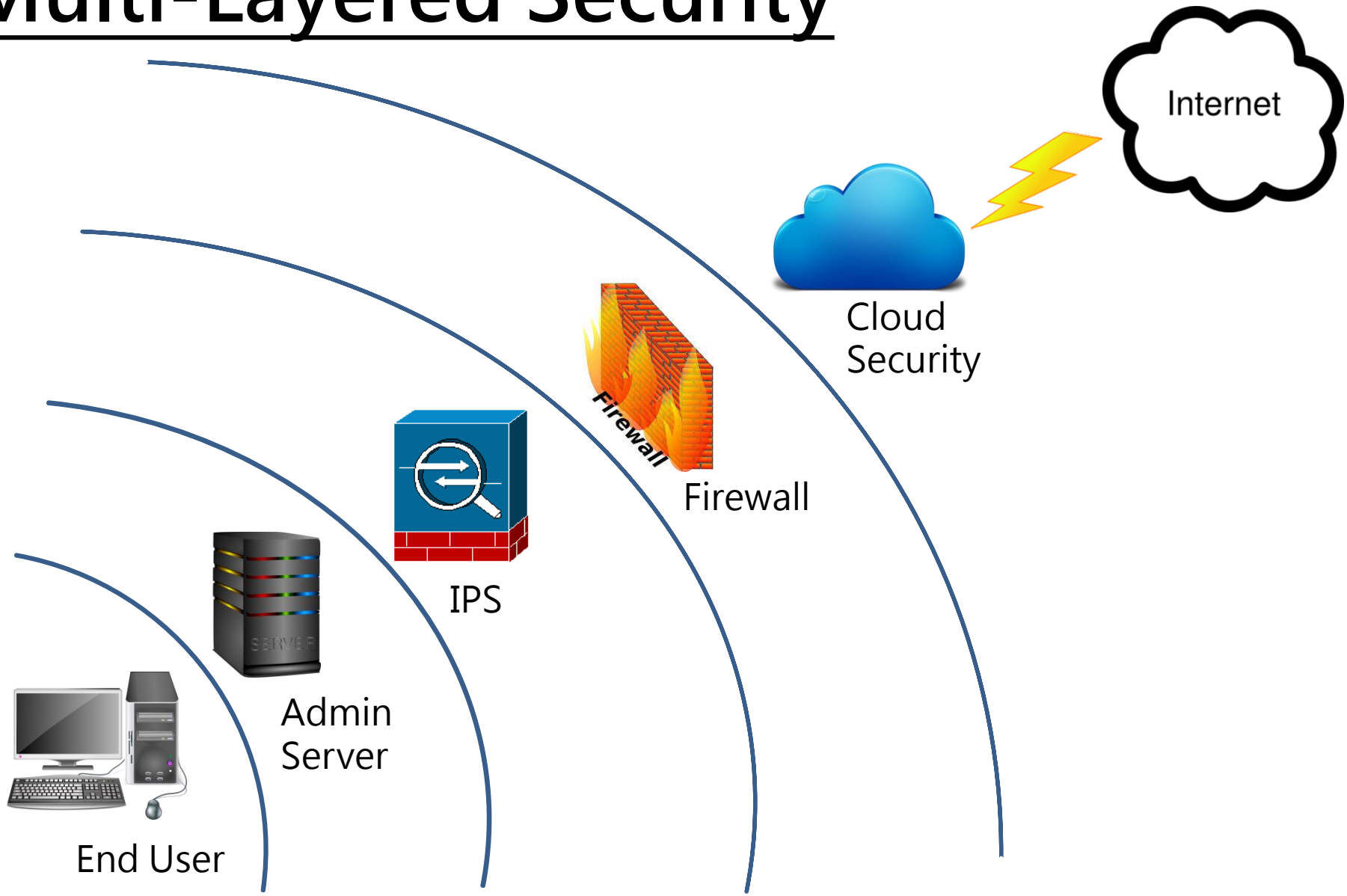
How Begins

- Phishing Executive
- Email to employee with look-alike domain

  e.g. leader.com / leader.com

Prevention Tips

Multi-Layered Security



Parisa Tabriz

Security Princess of Google

教育公眾始終是重要一環

雖然 Google 在背後已擋掉很多危險，但如果網民仍執意在提醒後仍瀏覽有危險的網站，那問題仍然沒解決。就像每一個保安專家所說，任何防火牆也不及使用者自己的安全意識重要，因此要真正做到安全的互聯網使用環境，除了有一個安全的瀏覽器，教育公眾始終是重要一環。

不管是作為一個資訊保安專家要教育公眾，還是作為女性工程師希望有更多女性參與這行業，Parisa 一直有參與不同的團體的網絡安全教育，例如親身參與女童軍或兒童的黑客松活動，讓她們親身感受網絡安全的重要性，培育未來的網絡安全工程師。

最後 Parisa Tabriz 給了幾個建議網民，雖然是老生常談，但仍然值得一再提醒：

- **便宜莫貪：**各種用優惠或免費招徠的網站或下載，都要留意是否釣魚或惡意軟件。
- **不要重覆使用密碼：**曾使用的密碼有可能因網站資料外洩而被黑客知悉，黑客會試圖使用舊密碼登入你的其他網上服務。事實上，Mark Zuckerberg 的 Twitter 帳號就是因為這而被入侵過。如怕忘記密碼，Parisa 就建議使用 Chrome 的密碼管理員功能。
- **避免使用公共電腦和定期檢查帳戶安全：**如果必須使用公共電腦登入，Parisa 就建議使用多重登入認證，這樣即使黑客偷取到密碼也難以登入帳號。
- **小心下載的軟件和應用程式：**近年常見的勒索軟件和木馬都利用網民疏忽而入侵，Parisa 就建議網民檢查 Google 帳戶有沒有可疑的登入。
- **保持軟件在最新版本：**就算漏洞發現了並修復了，但使用者沒安裝更新也沒用。雖然 Chrome 會自動更新，但其他瀏覽器插件或軟件並非如此，因此仍得留心。

Source: Unwire.pro

Backup Policy

- Best Practice 3-2-1

Management Solution

- Data Access Control
- Device Management
- Application Management
- Incident Response Mechanism

Ultimate Tips

- Keep Applications and OS update
- Keep Applications and OS update
- **Keep Applications and OS update**