台灣大哥大
Taiwan Mobile

企業資安檢測服務

社交工程演練介紹

Agenda

社交工程演練產品介紹

商業電郵詐騙持續攀升，防不勝防

新聞

美CISA公布網路釣魚演練結果，每10間就有8間企業有員工被網釣成功，教育員工回報網釣與實施抗網釣MFA成新重點

近期美國網路安全暨基礎設施安全局（CISA）公布一份網路釣魚資訊圖表（Phishing-infographic），當中揭露了CISA模擬網釣測試評估的結果，同時還彙整出防範網釣攻擊應關注的4大面向及具體行動

網釣攻擊突破防護與成功的機率，可能比你想要更高

根據這份報告的內容顯示，每10個接受CISA模擬網釣測試的人中，就有1人點擊連結，或是下載附件，而且，每10間企業組織就有8間至少1人淪為模擬網釣測試的受害者。此外，CISA也指出，有70%的惡意程式或惡意連結未被網路邊界防護服務阻擋，有15%的惡意程式未被端點防護產品阻擋，有84%的員工在收到惡意郵件的前10分鐘內，就逕自回覆敏感資訊或是點擊連結與附件，並且只有13%的目標鎖定員工回報自己遭遇網路釣魚事件。

有助於防止捲入網路釣魚攻擊的行動措施

4大面向	採取措施	對應CPG
阻擋誘餌	網路邊界安全防護強化	
	驗證電子郵件合法性採用SPF、DKIM與DMARC	8.3
	阻擋已知惡意網域、URL與IP位址	
不被誘騙	增進員工對於釣魚郵件的識別能力	4.3
	讓員工知道在所有通訊平臺都應保持警惕	4.3
回報網釣事件	將該郵件回報給公司的安全團隊，以及不要將惡意郵件轉寄給公司內其他人	4.3
	組織應變人員要能確認事件與防範入侵範圍擴大	7.1、7.2
保護整體範圍	導入可抗網路釣魚的多因素身分驗證	1.3
	審查並減少可存取關鍵資料與設備的帳號數量	1.7
	對密碼共享與重複使用做出限制，防止權限提升、取消用戶不必要的高權限	1.5、1.6
	做好安全更新、增加端點與EDR防護，以及實施軟體限制政策	5.1、2.1、2.2
	持續實施網路釣魚演練減少風險	5.6

資料來源：美國CISA，iThome整理，2023年2月

資料來源：iThome 2023/02

商業電郵詐騙持續攀升，防不勝防(續)

資料來源：iThome 2023/05

商業電郵詐騙持續攀升，防不勝防(續)

根據 2023年 iThome CIO 大調查中的數據指出，企業普遍認為「社交工程網路詐欺」是資安威脅中最難以防範的企業隱憂之一，

主要原因在於，其他的資安問題都有對應的防護系統或工具可以有效降低相關問題與損失，
但唯獨社交工程網路詐欺的問題都是來自於**員工對於資安風險的輕忽**所導致，因此建議企業需要長期與定期進行**「社交工程演練」**及**「資訊安全意識演練」**，培養員應有的資安認知，以達到隨時提高警覺的效果。

資料來源：iThome 2023

什麼是釣魚郵件

釣魚郵件是一種詐騙行為，通常通過電子郵件發送，以欺騙接收者提供個人信息。

駭客透過高度偽裝的**釣魚郵件**，搭配社交工程手法對目標企業發動攻擊。
這類釣魚郵件偽冒精良且手法高招讓人難以肉眼分辨，進而誘導受害者執行釣魚郵件中指示的動作。

電子郵件安全，可謂為企業與駭客安全攻防的前哨。
近幾年讓企業損失慘重的 **BEC金融詐騙**、勒索軟體、進階持續性滲透攻擊 (APT)，以及**銀行遭駭盜轉 18 億**的資安事件，都由一封釣魚郵件開始。

Phishing
一般網路釣魚

無特定目標廣撒式發送
願者上鉤

Spear phishing
魚叉式網路釣魚

針對特定對象
進階持續性滲透攻擊

Whaling
鯨釣

針對高價值商業目標
商業電子郵件入侵(BEC)的前身

什麼是社交工程演練

- **社交工程**是一種利用人的社交技巧和心理學原理來進行詐騙或入侵的手法。

- **社交工程演練**是透過模擬現實世界中，駭客發送惡意郵件，試圖引誘收件人**「開啟信件」**、**「點擊連結」**或**「開啟附件」**的攻擊情境，透過**統計演練時的反應(**開啟率和點閱率)，來**進行安全漏洞分析**，深入了解攻擊的實際效果。

- **演練的目的**為通過討論和實際演練，為企業提供相應的訓練來**提升員工對電子郵件安全的警惕性**，加強大家對於這類資安意識的認識和應對能力，以**提高企業資安的防護能力**。

台灣大哥大
企業服務

社交工程演練服務

SOCIAL ENGINEERING PROCESS

演練設定

1. 匯入受測名單
2. 設定釣魚Email樣板

演練活動

1. 選擇受測者
2. 選釣魚Email

行為統計

1. 開啟郵件
2. 開啟附件
3. 點選URL
4. 登入釣魚網站
   並輸入資料

演練統計報表

1. 發送狀況統計
2. 行為統計
3. 被釣魚人員名單

教育訓練

1. 一小時線上教訓練

演練報告範本

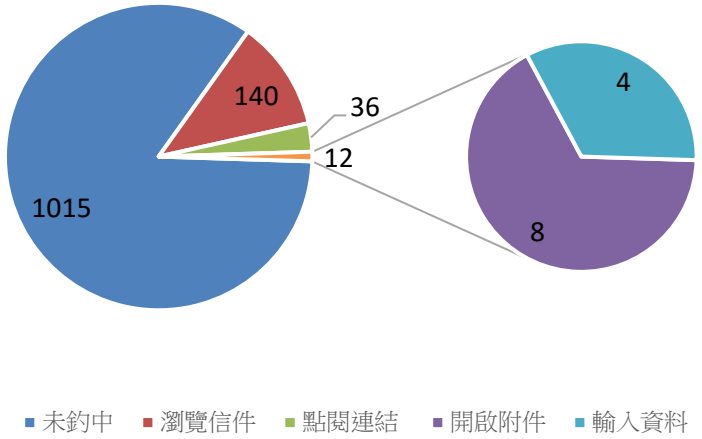
受測者總結果統計

依照測試結果分析，列出整體結果統計圖表，依據各類型範本郵件檢測結果，
蒐集所有檢測數據所統計出的整體人數結果統計圖表。

1. 依照受測人數統計之「**瀏覽郵件**」與「**點閱連結**」與「**開啟附件**」與「**輸入資料**」之人數統計報表：

受測人數	瀏覽信件		點閱連結		開啟附件		輸入資料	
	人數	比率	人數	比率	人數	比率	人數	比率
1200	140	11.66%	36	3%	10	0.83 %	4	0.33%

2. 依照人數統計之「**瀏覽郵件**」、「**點閱連結**」、「**開啟附件**」與「**輸入資料**」之人數統計圓餅圖：



演練報告範本

受測者行為依樣版統計

依照測試結果分析，列出整體結果統計圖表，依據各類型範本郵件檢測結果，
蒐集所有檢測數據所統計出的整體人數結果統計圖表。

1.依照不同類型之範本郵件，統計「瀏覽郵件」與「點閱連結」與「開啟附件」人數比率。

樣本編號	受測人數	瀏覽信件		點閱連結		開啟附件		輸入資料	
		人數	比率	人數	比率	人數	比率	人數	比率
1	1200	129	10.75%	33	2.75%	-	-	4	0.33%
2	600	63	10.5%	2	0.33%	8	1.33%	-	-
3	600	55	9.16%	1	0.17%	0	0%	-	-

2.本行報表為依據指定受測者的行為，所統計之「瀏覽郵件」與「點閱連結」與「開啟附件」等受測者比率行為報表。

編號	受測電子郵件	部門	瀏覽郵件數	點閱連結數	開啟附件數	輸入資料數
1	abcdefg@mail.com.tw	企劃部	1	0	-	0
2	caewdwe@mail.com.tw	業務部	3	2	-	0
3	gweadew@mail.com.tw	會計部	1	0	3	5

演練報告範本

開啟郵件/點閱連結/開啟附件結果清單

依照不同編號之範本郵件，所統計個別受測者「瀏覽郵件」與「點閱連結」與「開啟附件」等之細部**時間紀錄表**。

編號	受測電子郵件	部門	瀏覽郵件時間	點閱連結時間	開啟附件時間	資料輸入時間
1	abcdefg@mail.com.tw	企劃部	2024-05-20 11:07	-	-	-
2	abcdefg@mail.com.tw	企劃部		2024-05-20 11:08		
3	abcdefg@mail.com.tw	企劃部			2024-05-20 11:08	
4	abcdefg@mail.com.tw	企劃部				2024-05-20 11:10
5	caewdwe@mail.com.tw	業務部		2024-05-20 11:08		
6	caewdwe@mail.com.tw	業務部			2024-05-20 11:08	
7	gweadew@mail.com.tw	會計部				2024-05-20 11:08
8	gweadew@mail.com.tw	會計部	2024-05-20 11:08			

社交工程演練時事類樣本

發信者：News < Ectoday@news.com>
主旨：比柬埔寨更恐怖「KK園區」！ 踏入就是「人生最後一站」
附件：人蛇集團詐騙招數.html

近來柬埔寨高薪詐騙案，引發國人討論，不過卻有名嘴透露，其實鄰近的緬甸也有一個「KK 園區」，才堪稱是最兇惡的「豬仔煉獄」，是所有詐騙園區人口販運的最終站，踏入那裏幾乎是有去無回，不是被凌虐至死，就是被載到公海摘除器官！一旦遇到不服從者，還會被送到「暗黑兵部」凌虐，慘無人道，堪稱人間「地獄18層！」
他表示，這kk園區據傳關了8000-9000名人稱「豬仔」的受害者，但一旦到了此處，就只剩絕望「因為你人到了那就是人生最後一站，你已經不是人了，你就是豬，你就是他的商品。」

而現在據傳有6個國家要成立小組，直搗KK園區救人，卻讓人更擔憂這些豬仔處境，因為若不是被立刻轉移到其他地方，就是有可能被「處理掉」。名嘴說「那些不中用的豬」最後的命運，就是被摘除器官，方法是將人先騙上船，一上船後就注射麻醉針，接著便開始活摘器官「因為活摘的器官才有用，放在零下四度的冰塊裡面直接賣到泰國以及賣到杜拜。」

名嘴賴憲政也說，在這園區裡，就算是詐騙集團表現良好的人，當到小幹部，也只能在園區自由活動。但只要一接近這園區4米高，有通電的圍牆，就會被那裏看守的人抓起來毒打後，送兵部，用關水牢、上銬毒打、不給食物、灌辣椒水的方式凌虐。而送兵部裡，據說一半的人進去都無法再出來，通常是過幾天就聽到消息，「已經處理掉了！」。

人蛇集團運送路線

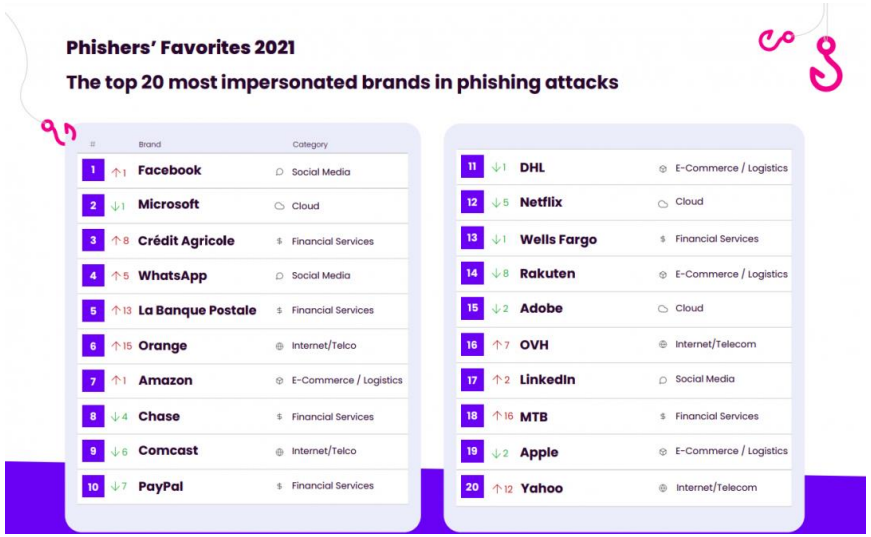
社交工程演練資訊類樣本

發信者：no.10barnd@ Internetfraub.com.tw
主旨：網路釣魚詐騙最愛冒用的十大品牌揭曉！駭客攻擊偏好挑在這個時間點
附件：出現木馬程式！10 萬名 Android 用戶密碼、卡號可能被偷.html

利用假冒各大品牌名義的網路釣魚詐騙攻擊活動，透過Email電子郵件、簡訊或一頁式網頁等各種途徑散播惡意網址，誘導至偽裝成合法登入的假網站，竊取個資盜刷信用卡等各式釣魚詐騙手法花招百出。

據國外網路安全公司 Vader Secure 發佈的最新報告指出，調查2021年1月至12月期間，監測高達184,977萬筆的網路釣魚詐騙頁面，統計數據顯示，駭客最愛冒用的前 20 大品牌之中，社群媒體平台的Facebook 為第一名，佔比達14%，微軟則是排名第二、佔比達13%。第三至五名依序為：Crédit Agricole 法國農業信貸銀行、WhatsApp與La Banque Postale 法國郵政銀行。

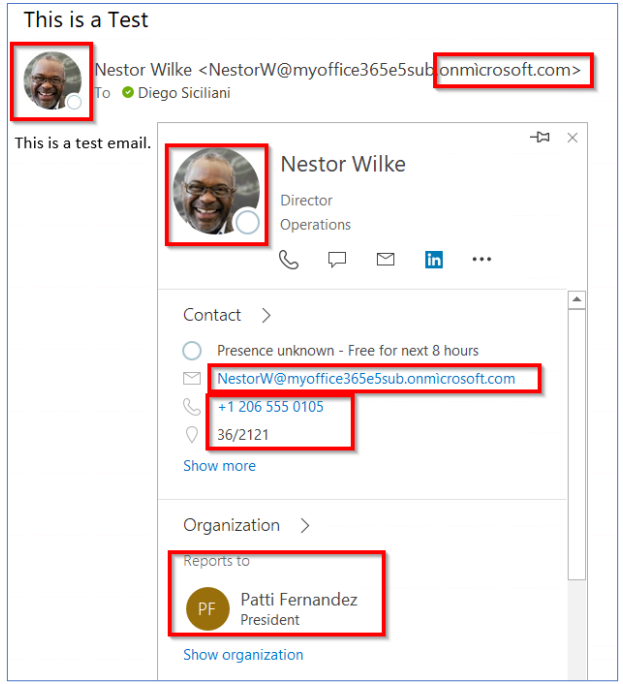
攻擊時間點分析



社交工程演練資訊類樣本(續)

發信者：wshdjgkx@outloak.com
主旨：Outlook曝安全漏洞恐遭駭利用！防堵網路釣魚詐騙官方釋修補快更新
附件：如何防範Outlook安全漏洞.html

習慣用Outlook收發電子郵件的用戶，可得多加留意了！據外媒Ars Technica 報導引述國外Dionah資安研究機構人員釋出的報告指出，日前發現存在於微軟 Office Outlook 365 的一項安全漏洞，導致用來可接受傳送郵件驗證郵件帳戶的SMTP伺服器，無法正確驗證國際化域名編碼，恐讓駭客藉機發起惡意攻擊活動時，利用該漏洞冒充為某個可信任的通訊錄聯絡人。



收到Email來信顯示的寄件人名稱與信箱網址時，駭客會以魚目混珠的方式，於網域名稱系統中巧妙地以拉丁語系的文字混雜其中，成功偽裝為可信任的來源的形式，讓收件人在看到該假冒的寄件人郵件地址時若沒有多加辨識，很容易就會失去防範警覺戒心，掉入惡意釣魚詐騙郵件的陷阱。仔細看寄件人網址名稱，於英文字母顯示的字串中，「i」被巧妙地替換為拉丁語系的「ì」。（圖翻攝Ars Technica）

據悉，受該漏洞影響的版本為Windows 365 32位元與64位元。微軟在收到上述與Outlook安全漏洞的相關通報後，已於目前最新版本獲得修補。建議使用Outlook用戶，務必盡快把版本更新到「Outlook 16.0.14228.20216 」最新版本，以避免駭客趁機透過高度偽裝的釣魚郵件詐騙，導致個人裝置資安恐遭外洩風險。

資安事件：假冒「衛福部」釣魚郵件夾帶惡意網址竊個資、電腦恐中毒

社交工程演練健康類樣本

發信者：News < News@ectoday.com >
主旨：2023流感疫苗對象、時程、公費自費廠牌、副作用一次看
附件：流感疫苗施打對象與時程.html

台灣流感病毒一年四季都存在，2023年9月第3周門急診類流感就診人次達109,054人次、新增39例流感併發重症，其中33位患者有慢性病史，35位沒有接種本季流感疫苗，施打流感疫苗能有效降低感染與重症。

究竟2023年那些族群為公費流感疫苗優先施打的對象、流感疫苗可能產生哪些副作用？哪些人不適合接種流感疫苗？《Hello醫師》為你一次解答流感疫苗的所有注意事項，並提醒大家在享有疫苗保護力的同時，也需準備於不良反應發生時盡早就醫。

2023流感疫苗副作用和接踵疫苗注意事項

社交工程演練旅遊類樣本

發信者：service@creetivqpxp0.com
主旨：「2023 文博會」即將於台北重要的五大文創園區盛大開幕
附件：

在仔細探索 2023 文博會的活動內容之前，先來和大家介紹一下所謂的「 文博會 」究竟是什麼！

「 文博會 」，全稱為「 台灣文化創意博覽會 」，從 2010 年就開始策辦，中間經歷了多次的轉型，展場規模更是逐年擴大，目前可以說是我國國內最重要的文創分享&交易活動！除了讓各類文創作家參與其中展示、販售自己的心血，文博會更希望可以透過不同策展方式，讓民眾可以深入理解當地文化、帶動國民對文化議題的思考，盼可達到以文化策展與商業發展動能並行的願景！

文博會歷經 13 年發展，如今在 2023 年終於再次回到「台北」舉辦，究竟北市會如何規劃此次的大規模文博會呢？點擊下面連結來了解吧！

2023文博會展區介紹





社交工程演練生活類樣本

發信者：foadpanda news@foadpanda.com
主旨：foadpanda 首度公開疫後關鍵報告
附件：foadpanda使用習慣調查結果.html

外送成日常、消費預算轉線上、餐廳營運模式大翻轉
日用品外送疫軍突起成長逾六成 雲端餐廳成長近八成

疫情大幅改變生活型態，外送平台成消費者日常與產業轉型的重要關鍵，更基於此發展出「疫」外新經濟模式全台最大即時外送平台 foadpanda 於日前公佈「疫後關鍵報告」，針對消費習慣轉變、店家營運模式、外送產業發展等三大面向進行剖析。值得關注的是，疫後外送需求並未隨著店家開放內用、疫情趨緩而減低，消費者健康意識更高，更建構起「安全庫存」消費習慣，習慣平日就事先採購常用食材及生活用品以備不時之需，且從美食到日用品均高度依賴外送平台。同時餐飲業經營策略亦因疫情大幅調整，加入外送服務後，銷售型態更有彈性且能因應疫情變化作最佳調整。外送平台則在數位轉型、疫情催化的情況下，更朝向優化訂餐體驗、強化訂閱用戶服務內容等多面向積極發展。

趨勢一：不「疫」外！消費者健康意識抬頭、多元化購餐型態受歡迎
趨勢二：疫後店家營運模式大翻轉 雲端餐廳蓬勃發展
趨勢三：產品與服務All IN 1 foadpanda 邁向整合式外送平台

社交工程演練生活類樣本(續)

發信者：einotice@fiia.gow.tw
主旨：雲端發票中獎通知
附件：如何領獎.html

親愛的消費者您好：
恭喜您民國112年3-4月雲端發票有1筆中獎發票！請參考明細。
提醒您，電子發票服務不會指示您操作ATM，如接獲不明及可疑電話或簡訊，
應立即撥打客服專線或反詐騙電話，
保持鎮定並再三查證，以免落入詐騙陷阱。

發票號碼	中獎獎別	中獎金額
GH8****662	六獎	200

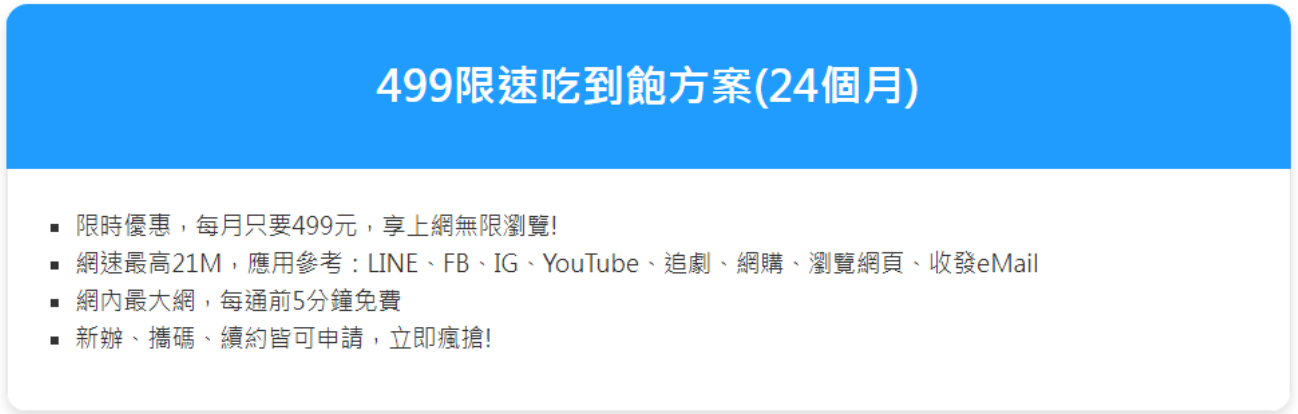
1.請依據載具類別至超商事務機列印中獎電子發票證明聯(會員卡載具由營業人提供電子發票證明聯)，至兌獎單位領獎。
2.請立即將卡片歸戶至手機條碼，即享有自動對獎、中獎主動通知及獎金自動匯入等服務。
3.建議您至電子發票整合服務平台設定銀行帳戶並啟用匯款，次期中獎獎金會自動匯入您設定之銀行帳戶中。
感謝您使用雲端發票，敬祝愉快。

如您有其他問題，請與我們聯繫：
客服專線 / 客服信箱
此封信件僅供中獎通知，非領獎證明，中獎發票兌領方式依據消費者開獎前實際設定為準。

社交工程演練生活類樣本(續)

發信者：5G499@chphone.com.tw
主旨：員工優惠方案：5G上網吃到飽只要$499，加抽iPhone 14
附件：員工活動專屬優惠碼.html

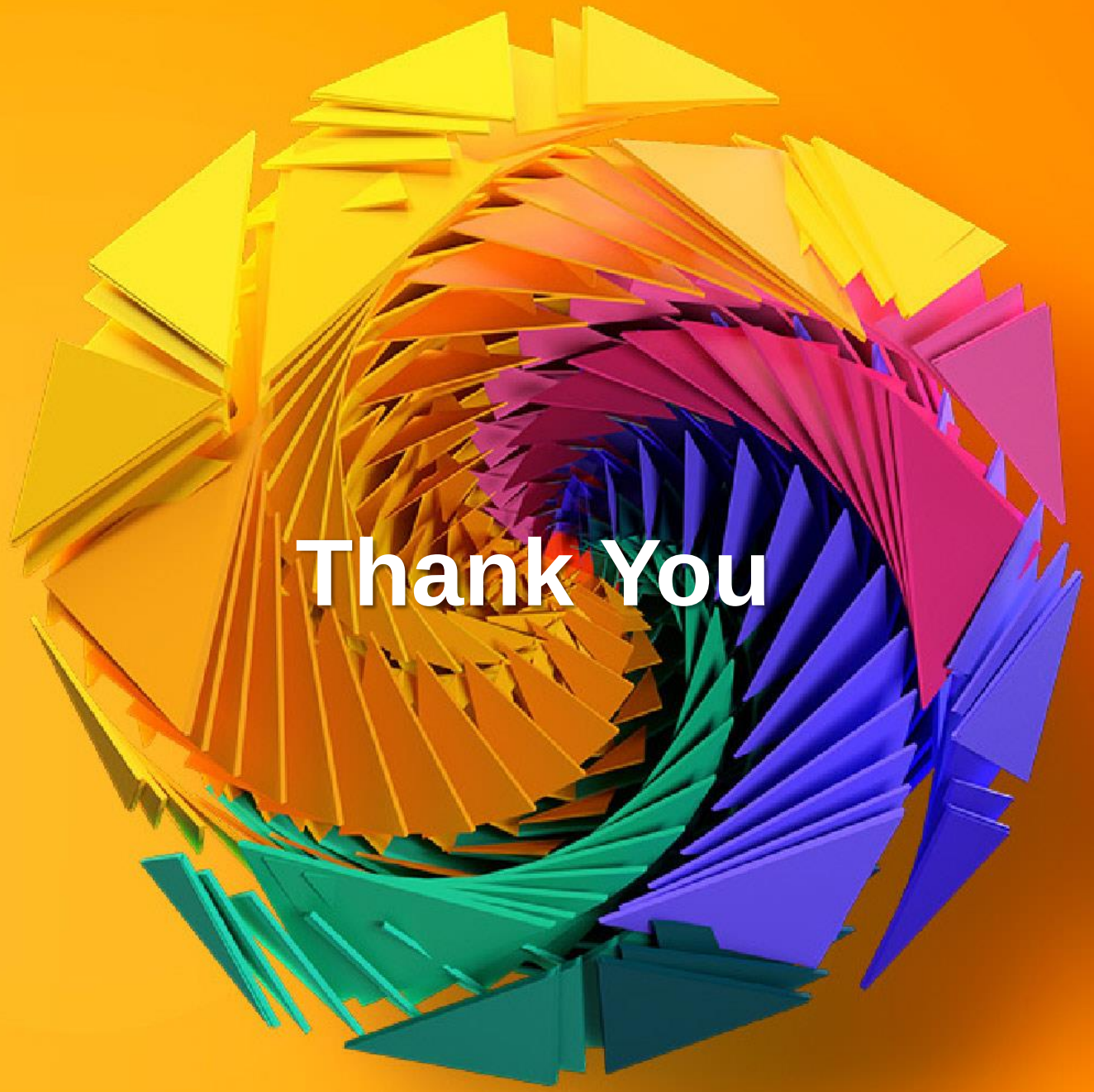
好禮享不完，5G上網吃到飽



活動期間：即日起~112/12/25止。
適用對象：全體員工。
集團加碼：所有申辦人員中抽選iPhone 14 共5名。

立即申辦
活動注意事項

台灣大哥大
企業服務



Thank You