

SHOPLINE

品牌電商

資安保護入門指南

資安趨勢解析 | 資安保護策略



INFORMATION SECURITY

# 目錄

## CHAPTER 1

---

### 資安 趨勢解析

全球資安發展趨勢觀察	04
品牌商家常見資安疑慮	05
常見資安攻擊種類介紹	06
社交工程攻擊手段介紹	08

## CHAPTER 2

---

### 資安 保護策略

個人資安保護建議做法	10
品牌官網資安保護方法	12
遇上資安危機處理流程	13
SHOPLINE 資安規格書	14
夥伴服務：Gogolook	15

# CHAPTER 1

## 資安趨勢解析

1-1. 全球資安發展趨勢觀察



1-2. 品牌商家常見資安疑慮



1-3. 常見資安攻擊種類介紹



1-4. 社交工程攻擊手段介紹



1-5. 企業面臨資安攻擊案例



# 全球資安發展趨勢觀察

在全球高度數位化的現在，「資訊安全」儼然成為企業營運的必修課，然而，資安議題深又廣，不僅需要在防禦範圍、駭客攻擊手法、資安弱點及員工資安意識等諸多面向扎根，更要與時俱進地升級資安保護技術，才能降低資安危機事件發生的可能。

放眼過往資安威脅的演進，早在 1980 年代就有電腦病毒的出現，而近代最廣為人知的，莫過於千禧年的 ILOVEYOU 蠕蟲 (Love Bug)，此蠕蟲會覆寫受感染電腦上的重要檔案，也會對受害者 Email 中收件人名單寄出病毒信，將感染規模持續擴大；爾後，隨著科技發展與行動裝置的普及，也開始出現針對手機的病毒，亦有針對 Mac OSX 作業系統等惡意程式 (Leap) 出現，基本上資安威脅都伴隨著大眾生活不斷演進，可以說是「哪裡有商機，哪裡就有攻擊」。

而綜觀近三年的資安威脅，變化多端的「勒索軟體」層出不窮，其攻擊精準又快速，另外有企業因「雲端服務攻擊」與「供應鏈攻擊」等損失慘重，也不乏看見時下火熱的 AI 人工智慧被有心人士惡意使用來竊取不法收益。面對這些潛在資安威脅，企業資安保護技術需持續迭代，像是防毒軟體、防火牆 (Firewall)、入侵偵測系統 (IDS) 與入侵防護系統 (IPS) 的出現，及 AI 人工智慧導入端點偵測及應變機制 (EDR) 的運用，都可以為企業挹注更多防護量能。



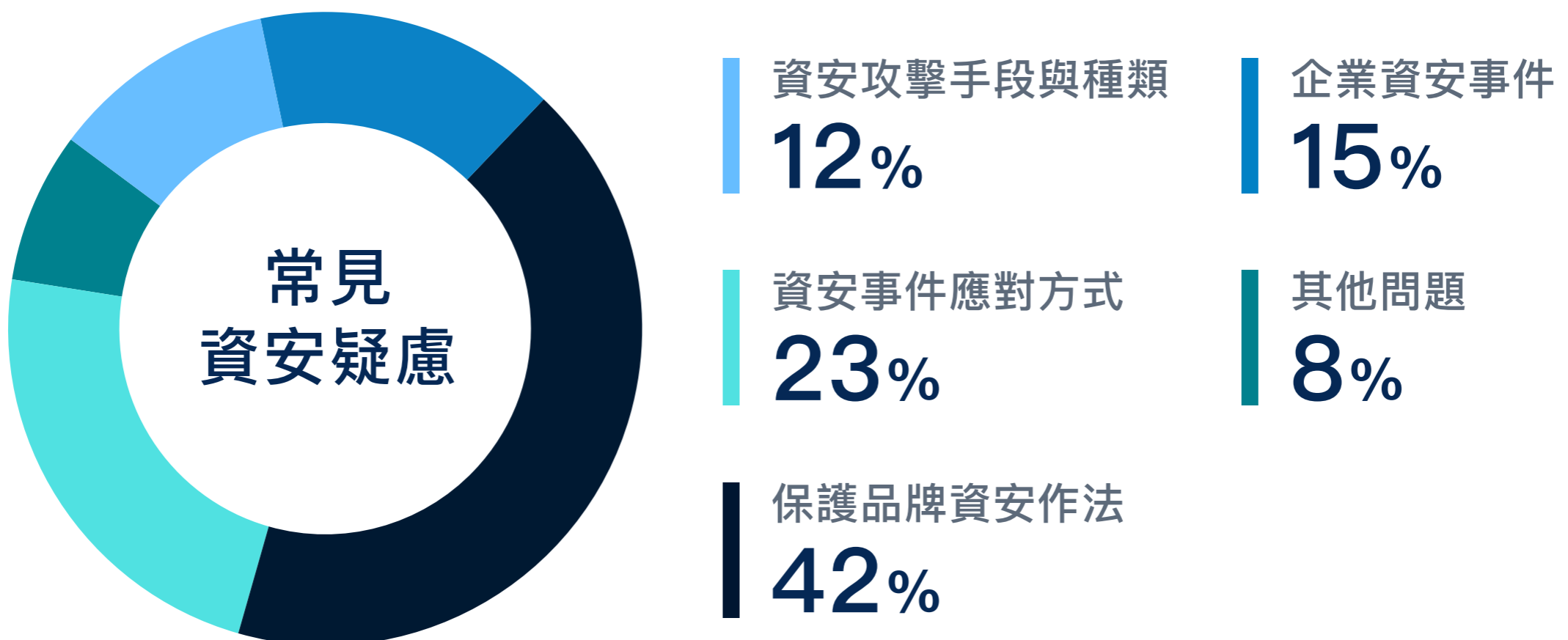
另一方面，根據 Fortinet 《[2024 全球資安威脅預測](#)》報告顯示，2024 年資安攻擊可能會鎖定醫療、金融等關鍵事業，並且攻擊更具有規模化；再來有觀察到「零時差攻擊」數量將持續攀升，且進階持續性威脅 (APT) 也因 AI 應用與 5G 普及的影響，使其變得更具多變性與破壞性，並且使得「社交工程」手段更具威脅性，以上都是須持續關注的議題。

# 品牌商家常見資安疑慮

在瞭解全球資安面臨到的挑戰後，根據遠見《[2023 資安長大調查](#)》中顯示，台灣上市櫃公司對於企業面臨的資安問題，有 65.1% 的企業表示最棘手的是「資安人才」的缺乏，其次則是資安政策法遵議題佔了 36%、認為企業文化已根深蒂固難以改變也有 28.8% 的比例。

然而，駭客攻擊導致資安外洩等事件頻傳，基本上不僅限於大企業與上市櫃公司，只要你擁有具有價值的資料（如消費者個資、產品研發資料等），都有可能成為攻擊目標，甚至駭客不僅會找尋企業資安防護漏洞，更有可能透過一些手段來欺騙與操弄公司內部人員心理，進而讓其上當受騙而洩漏機敏資料。

由此可見，資安保護不僅僅只是在軟硬體與工程技術等方面的提升，在「人」的面向更需要資安人才的加入，以及強化培養員工資安意識。此外，SHOPLINE 透過問卷調查現有商家對於資安議題的疑慮，結果如下：



依據結果顯示，SHOPLINE 商家對於「品牌如何保護資安」議題最感興趣，同時也想瞭解「資安事件的應對方法」與「資安攻擊手段」。因此本書後續內容將依照上述主題，提供商家們基礎的資安保護相關知識。



# 常見資安攻擊種類介紹

在規劃資安保護策略之前，必須先來瞭解近年常見的資安攻擊究竟有哪些，而台灣是全球供應鏈關鍵據點，亦是駭客常來造訪的地區，根據 Fortinet 《[2023 上半年全球資安威脅報告](#)》指出，亞太地區偵測到超過 4,120 億次惡意威脅，其中台灣佔比逾五成（55%），相當每秒就有近 1.5 萬次攻擊發生。此外根據《[iThome 2023 資安大調查](#)》顯示，台灣「社交工程」與「勒索軟體資安事件」是企業最擔憂的資安威脅，且社交工程更是各種攻擊的源頭，因此本書將盤點常見的攻擊手段盤點如下：

1

## 社交工程

Social Engineering

通過誘騙詐欺等手段（如釣魚信件等），誘導受害者進行某些操作以達成攻擊目的之手段，近年更衍伸出各種誘騙手段結合且具有針對性的「混合型社交工程」，讓受害者上當後造成嚴重損失。

2

## 勒索軟體即服務

Ransomware-as-a-Service, RaaS

以惡意程式碼加密鎖住受害者系統或檔案，並向其勒索金錢後，才重啟使用與存取權限。

3

## 分散式阻斷服務攻擊

Distributed Denial of Service, DDOS

透過向目標發送大量請求使其超出處理能力，導致網站或伺服器無法正常運作。

4

## 蠕蟲病毒

Worm

一種會自己複製並且能夠自動散播到其他電腦的電腦病毒，不需要使用者幫忙也不用附著在其他檔案上。它們經常透過利用網路上的漏洞迅速傳播，造成許多電腦感染並帶來嚴重的損失。常見的像是 Wannacry、DoublePulsar 等。

# 常見資安攻擊種類介紹

5

## 進階持續性威脅

Advanced Persistent Threat, APT

是精心策劃的針對性攻擊，以長期網路攻擊配合病毒等多方位持續攻擊來達成目標，近年 AI 人工智慧技術也常會被有心人士拿來強化 APT 的攻擊破壞性。

6

## 惡意軟體

Malware

藉由病毒、木馬程式、間諜軟體等在受害者的設備上執行惡意操作來達成攻擊目的。

7

## SQL 注入

SQL Injection

利用應用程式未適當驗證數據的攻擊方式，在輸入字段中插入惡意 SQL 代碼以竊取數據庫中的資訊等操作。

8

## 跨網站指令碼攻擊

Cross-site Scripting, XSS

將惡意的 JavaScript 代碼嵌入到目標網頁上，當使用者瀏覽目標網頁時執行代碼來竊取資料。

9

## 零時差攻擊

Zero-Day Vulnerability

利用尚未被企業或軟體開發商發現或修補的漏洞進行攻擊。

而對於公司內部有資安相關人員的企業來說，能夠針對各種攻擊進行即時的排查與處理，但對尚未有充足資源的商家來說，多加瞭解資安威脅與過往案例，勢必能夠協助商家提高警覺，減少風險。

# 社交工程攻擊手段介紹

根據台灣資安署指出，多數資安威脅是因內部人員點擊「釣魚連結」所致，顯示企業內部對於社交工程的防備意識尚有進步空間。本書也進一步分享常見社交工程類型：





# CHAPTER 2

## 資安保護策略

2-1. 個人資安保護建議做法

2-2. 品牌官網資安保護方法

2-3. 遇上資安危機處理流程

2-4. SHOPLINE 資安規格書

2-5. 夥伴服務：Gogolook

# 個人資安保護建議做法

針對個人資安保護基本原則就是要「提高警覺」，以下提供七種建議作法：

## 一、基本使用裝置防毒

在電腦與手機安裝掃毒與防毒軟體 / APP，做到最基礎的保護。

## 二、強密碼設定與管理工具

密碼建議「設定 8–12 碼，包含英文大小寫及特殊符號」，且推薦個人在各平台密碼可設定 3 組不重複密碼進行替換，也可以用 1Password、Proton Pass 等密碼管理工具來管理登入密碼。此外，可避免弱密碼的使用，以下為常見弱密碼列表（參考 NordPass 台灣地區弱密碼排行）：

弱密碼排名	密碼	駭客破解所需時間	密碼被使用次數
1	admin	< 1 秒	8,430
2	123456	< 1 秒	8,035
3	a123456	< 1 秒	6,843
4	12345678	< 1 秒	3,730
5	1qaz2wsx	< 1 秒	3,542

## 三、對釣魚訊息提高警覺

對於收到的 Email 或簡訊都先用「看」的，並留意信件寄件者資訊是否正確（其信箱名稱 / 地址 / 簽名檔等拼字是否正確），而帶有不明連結或按鈕、附件檔案、QR code 等千萬不要點擊與掃碼，更不要在信件或簡訊中進行「帳號登入」、「信用卡資訊輸入」、「提供重要證件」等，可先查證再說，倘若想要查證信件中的連結是否安全，可以透過一些知名的資安檢測網站（如：[Safeweb](#) / [VirusTotal](#) / [TRENDMICRO](#)）確認其安全性，而釣魚信件的寄件人信箱常會假冒你熟悉的公司、品牌，並用相似名稱混淆你，在內文與信內網址等都會包含許多「拼寫錯誤」或「文法錯誤」，甚至以台灣公司來說，基本上也不會出現簡體字等內容，因此覺得可疑時請向寄件者確認，若無法聯絡寄件者，再次強烈建議勿點連結或附件檔案，而對於釣魚網站連結，也可以加入「[資策會安心點瀏覽器插件](#)」來提醒自己。

【持續更新】26組即將來台韓星整理：IU票價公開、MAMAMOO玟星、輝人、ITZY、SJ接棒來台

TVBSS TVBSS@mail.hotmailcloud.com 透過 mailrelaysrv.com  
寄給我 ▾

\* 釣魚信件示意圖

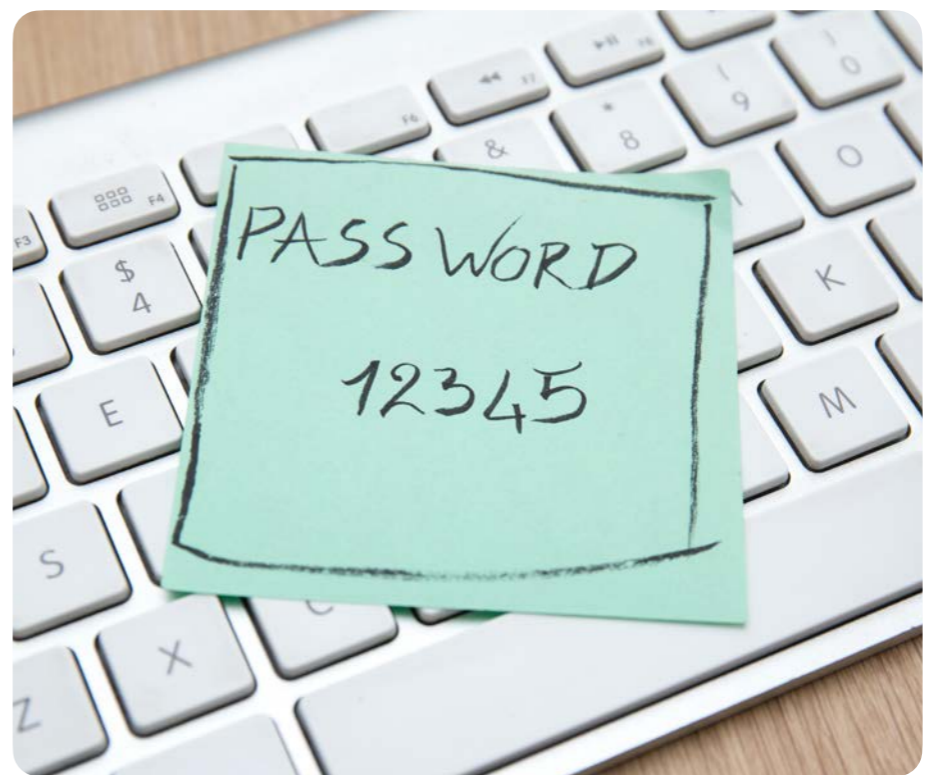
# 個人資安保護建議做法

## 四、公私訊息管道需分開

請勿使用公務信箱接收私人信件，或訂閱非公務用途之網站訊息，切勿轉寄公司內部資訊至私人信箱與儲存空間中；涉及機敏資料，勿將人情凌駕於資安保護原則上，遇到同業親友詢問公司機密資訊等情況，皆須保持警覺並瞭解動機，勿輕易談論與提供憑證授權等。

## 五、避免公開資訊洩漏線索

現在只需要透過照片與影像中「一丁點」線索，駭客就能找到你的位置與資訊，甚至他們會用意想不到的手法來得知個人或是企業的重要情報。如個人或是公司公開的照片、影片等資訊中，就可能有機會造成你的權益受損，像是照片「檔案資訊」有時會包含 GPS 定位資料等，這都是你可能在表面上「看不見」的線索。



另外像是有些人會習慣把各種平台密碼記錄在便條紙上，並張貼於電腦螢幕、辦公座位區等，亦或是記錄在電腦的記事本中，這些資訊都有機會發生洩漏的可能，因此個人相關的重要資訊切勿讓他人輕易取得。

## 六、避免將重要資訊餵給 AI 工具

由於坊間有眾多 AI 工具屬於開源的系統，因此在使用這些工具時，應該避免將個人的機敏資訊提供給 AI，以減少重要資訊散佈出去的可能，像是聯發科就有開發內部使用的生成式 AI 平台 DaVinci（達哥），讓員工可以安心使用 AI 工具所帶來的便利性。

## 七、培養資訊安全知識

時刻保持資訊安全知識的累積，並且瞭解各種資安攻擊手段，勢必能在碰上危機時能更加冷靜，同時也能針對可能的漏洞與弱點進行補強，防止品牌在被攻擊後持續擴大損失範圍。

# 品牌官網資安保護方法

品牌商家在保護官網資安方面，除了每位員工做好個人資安保護外，針對「品牌官網」的基礎保護方面，亦可以參考以下方法：

## 1 商店後台權限管理與密碼定期更換

依據「職務內容」設定後台管理員帳號的權限，避免所有使用者皆有全權，且人員能定期更換商店後台登入密碼，與登入後台使用的 Email 帳號也建議定期變更密碼；另外日常公司用電腦、公務機等裝置務必定期掃毒，同時勿使用公共電腦或公共網路來操作後台管理。

## 2 商店後台登入「雙重驗證」與「限制登入 IP」

商店後台開啟登入「雙重驗證 OTP」，降低駭客入侵機率，同時可以設定限制網站後台登入的 IP 位址，多重關卡增加駭客入侵難度。

## 3 阻擋機器人：Google reCAPTCHA 驗證

在註冊帳號、登入帳號或是下單結帳時，可加入 reCAPTCHA 防止機器人不斷用不同帳號密碼嘗試登入，以確保資料傳輸的安全性。

## 4 開啟金流端 3D 認證

為避免顧客信用卡遭盜刷而產生「扣回爭議帳款」，建議商家應開啟金流端 3D 驗證。

## 5 隱藏顧客重要資訊並限制資料匯出權限

按權限設定隱藏重要資訊，僅讓負責相對應工作的人員能看到該看的資訊；在隨貨附上的單據不含完整顧客資料，以避免顧客未妥善銷毀而導致個資外洩。在匯出網站資料時可能因多次匯出到不同電腦中，導致中毒電腦外洩資料，因此在資料匯出時需要限制匯出權限外，也要隱藏重要顧客資訊，如電話隱藏後 3 碼等。

# 遇上資安危機處理流程

當商家遇上任何資安危機時，亦可以參考以下方法：

## ● STEP 1：成立事件應變小組

建議在第一時間籌組事件應變小組，成員可以有公關（發言人）、法務、IT等成員。另外需要指定此小組的組長，負責整體指揮和協調應變行動。

## ● STEP 2：評估現況並阻止擴散

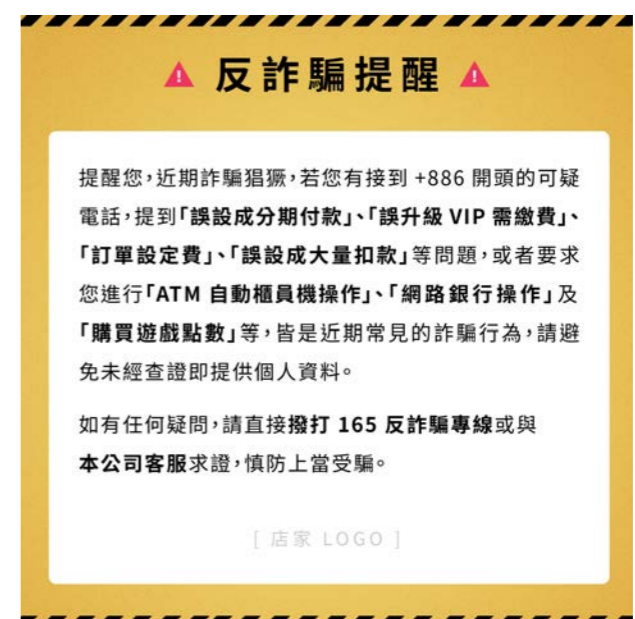
釐清「攻擊手法與規模」、「感染源」與「影響範圍」，並由應變小組成員布達給內部相關團隊、回報給後端人員知曉以深入調查，必要時，亦需調度好應對問題的客服人員等，盡可能快速確認事件的細節狀況並做初步回應策略，以爭取後續復原時間。

## ● STEP 3：調查並蒐集相關證據

遇到任何資安威脅時，在釐清攻擊狀況後勢必需要找到攻擊源頭，並盡快排除問題，才能妥善封鎖問題根源並進行後續回復，這部分必須仰賴工程師與技術人員，或協同資安專家進駐處理；倘若判斷可能是「合作廠商」造成資安事件發生，亦可請該廠商進行相關調查，以釐清權責。另外一定要「蒐集攻擊相關證據」，妥善紀錄包含人、事、時、地、物等資訊，以保障商家自身及顧客權益，同時像個資外洩等事件可能會牽扯到法律訴訟，為確保後續處理能有所依據，建議要詳實紀錄、保存受攻擊之證據。

## ● STEP 4：通報 165 並發表聲明

一定要通報 [165 反詐騙專線](#)，假如是被偽冒網站的話也可以進行[釣魚網站通報](#)，同時於公開管道(社群平台、企業官網、通訊軟體等)告知顧客與合作夥伴情況，及保持品牌客服管道暢通，隨時分享處理進度。



## ● STEP 5：強化資訊安全保護網

在威脅排除後，最重要的是「預防下次情況的發生」。建議商家在事後覆盤時針對資安漏斗進行強化，制定改善計畫，若商家缺少資安人才的配置，也推薦尋找坊間專業資安保護公司（數聯資安、如梭科技等），進行資安滲透測試等，同時也推薦商家定期安排公司內部同仁進行資安主題教育訓練，培養資安意識來強化整體公司防詐免疫力（素材參考：[165 防詐宣導影片](#)）。

# SHOPLINE 資安規格書

## 一、商店前後台與第三方金流串接

符合台灣個人資料保護法與主管機關數發部規範/遵守 APEC 認證資訊安全保護 (CBPR)

- **【使用 SSL / TLS1.2 ( 含 ) 以上等級的安全憑證來進行傳輸加密協定】**：防止數據傳輸過程中遭他人竊取、更改
- **【可疑 IP 判斷阻擋機制】**：即時擋下 DDoS 攻擊，並同時確保系統的高效運作
- **【每季進行資安弱點掃描】**：確保系統沒有中高風險安全漏洞，避免駭客入侵
- **【每年委由第三方進行滲透測試】**：由公正第三方進行模擬駭客攻擊測試，提升系統資訊安全
- **【配置兩位全職人員專職處理資訊安全】**
- **【資料儲存於 AWS 新加坡伺服器】**：資料儲存在新加坡，所有用戶的資料皆遵循最小權限原則進行存取，且資料庫最高權限管理團隊為台灣團隊
- **【使用硬碟加密技術進行資料保存】**：以高規格保護商店資料
- **【Watchmen 商譽保護服務 (夥伴服務)】**：提供全台 SHOPLINE 商家註冊 Whoscall 認證號碼，讓商家來電或簡訊號碼顯示為經過認證的安全名單，提升顧客接聽率與回撥率，更降低受騙風險

## 二、金流服務 SHOPLINE Payments

符合台灣金融法規與安全規範 / 支付卡產業資料安全標準 (PCI DSS) 最高安全準則

- **【服務串接符合 PCI DSS Level 1】**：有效控制持卡人資料，包括預防、檢測和對安全事件之適當反應，從而減少信用卡詐騙

## 三、網路商店功能

- **【商店登入雙重驗證】**：有效大幅降低駭客入侵機率
- **【指定登入 IP】**：限制商店後台登入 IP 防止駭客入侵
- **【Google reCAPTCHA 註冊驗證】**：防止駭客使用機器人不斷用不同帳號密碼嘗試登入，同時確保資料傳輸的安全性
- **【隱藏訂單明細】**：遵循最小權限原則，避免資料給不需要看到的人看到
- **【匯出報表雙重驗證】**：確保商店資料下載安全
- **【隱藏報表內顧客的部分個資】**：遵循最小權限原則，避免資料給不需看到的人看
- **【新增「反詐騙宣導」預設分頁、頁尾新增反詐騙警語】**：幫助商家強化顧客反詐騙意識

# 夥伴服務：Gogolook

**Gogolook** 是一間致力於建構全球信任網絡，以電話號碼資料庫和 AI 技術為核心打造不同應用場景的信任科技 (TrustTech)，提供企業和個人風險管理解決方案。而 Gogolook 合作身為 SHOPLINE 強力的合作夥伴，其也提供了「Watchmen 商譽保護服務」方案給予 SHOPLINE 商家，讓商家可以註冊「Whoscall 認證號碼」，將品牌的來電或是簡訊 (限 Android 系統) 號碼顯示為「經認證的安全名單」，使品牌在 700 多萬個 Whoscall 用戶端，能夠明確顯示出企業名稱、電話目的等，以減低品牌顧客受到詐騙的風險，同時也能提高顧客接聽品牌來電的機率。



此外，商家也能使用「偽冒偵測系統」服務，其可以替品牌 24 小時全面性地監控品牌是否「有遭偽冒的狀況」發生，透過 AI 技術即時偵測品牌電話號碼與簡訊的偽冒狀況，立即阻絕可能發生的詐騙行為，打造完整的監測、預警、防護的一站式服務，與 Whoscall 結合運用，即時保護你的品牌商譽與顧客權益。

# SHOPLINE

## 全球智慧開店平台



立即搜尋 SHOPLINE

免費試用  
網路開店



免費獲取  
開店資源



點擊圖案追蹤  
SHOPLINE 社群

