數碼化 ✣ 茁壯成長

保護你的業務，免受欺詐威脅

在日新月異的網絡安全格局中，如何準備就緒，保持領先

PayPal

甚麼是欺詐經濟？

以往，我們認為只有獨立黑客和詐騙者會參與網上欺詐，而此類罪案僅屬個別事件。但近年來，集團式網絡罪犯大行其道，他們協調一致，部署精密，成為大部分網上欺詐的幕後黑手。企業必須採取同樣精密的保護措施，保障業務免受欺詐威脅。

疫情的影響無孔不入，一切由此改變，尤其在電子商務方面—新冠肺炎疫情爆發，令互聯網流量激增 60%，網購消費者的開支亦上升接近一倍[1]。時至 2021 年，欺詐威脅變得前所未見地嚴峻。正正由於網上欺詐活動猖獗，電子商務零售商面對損失超過 200 億美元的風險。相比之前一年，2021 年欺詐活動大幅增加 18%[1]。疫情期間，在壓力沉重的陰霾下，欺詐者乘機利用冒充慈善團體或世衛 (WHO) 與疾控中心 (CDC) 的電郵欺騙受害者；他們甚至會冒充政府組織、陷入困境的家人，或者銀行及信用卡公司，務求令受害者放下戒心，不幸上當[2]。

隨著欺詐經濟不斷發展，網絡罪犯日益明目張膽。他們越趨詭計多端、計算精密；此外，他們現在可利用更多不同的工具，在網上從商家身上騙取金錢。就如成為欺詐目標的商家般，網絡罪犯同樣熟知電子商務的機制，令他們能夠準確識別保安漏洞，以出其不意的方式攻破商家的弱點，敲詐獲利[3]。

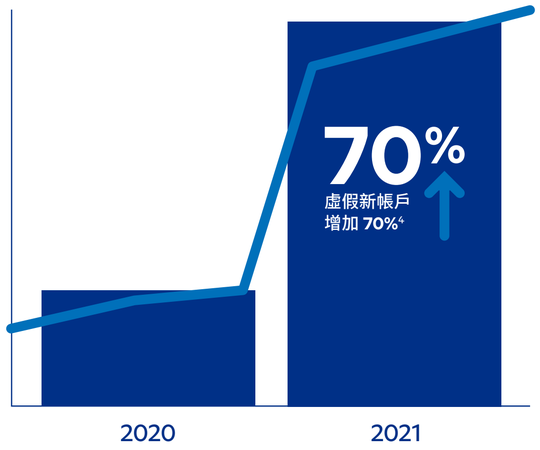
儘管欺詐情況猖獗，然而，各大小商家都較以往投入更多心力，以應對不法之徒的威脅。與此同時，客戶依然抱持極高期望—除了嚴密的保安措施以外，網購消費者仍希望享用快捷流暢的購物體驗。一旦購物耗時太久、需要填寫太多資料，又或流程過於複雜，他們便會放棄購物車，轉投下一間店舖選購。正因消費者的期望相當高，零售商在滿足其需求的同時，亦要保護業務免受各種網絡威脅侵害，令經營電子商務更具挑戰性。

1. Payments Dive，E-commerce fraud to surpass $20B in 2021, an 18% jump over last year, report finds，2021 年 4 月 30 日。 **2.** CyberCrime Support Network，COVID-19 Scam Alerts，2021 年 4 月 12 日。 **3.** Sift，Exposing the Multi-billion Dollar Fraud Economy，2021 年第 1 季。

欺詐肆虐全球，為商家帶來各種新挑戰

新帳戶欺詐個案激增

2021 年，註冊虛假新帳戶數字上升超過 **70%**[4]。



大膽瞄準更高價的目標

相比疫情前，現時每宗欺詐購物的價值平均高 **70%**[5]。

手機攻擊頻生

2021 年上半年，手機流量佔整體數碼流量 **50%**，而手機攻擊事件發生率則高達 **24%**[6]。

4. Business Wire，70% Increase in Fraudulent Account Registrations Puts Digital Accounts in the Crosshairs, Arkose Labs Reports，2021 年 8 月 5 日。 **5.** Retail Week，Every day is now Black Friday – and retailers need to prepare，2021 年 11 月 4 日。 **6.** Security Boulevard，Here's How to Fight Diverse Attacks Across Multiple Touchpoints，2021 年 10 月 8 日。

領先一步，戰勝網絡罪犯

隨著網絡威脅變得前所未見地複雜精密，且無孔不入，商家不應再單純將欺詐視為經營成本。去年，全渠道零售的欺詐個案發生率按年上升 50%，欺詐訂單數量則按年增加 9%[7]。商家應專注構建合適的基礎設施，保護業務免受欺詐威脅。

5 個保障業務的小貼士：

1. 監察網站，留意可疑活動
2. 從結帳流程入手，阻截網絡罪案
3. 加密資料，確保付款安全
4. 更新軟件以提升保安水平
5. 識別盲點，加強網絡優勢

7. Sift，Exposing the Multi-billion Dollar Fraud Economy，2021 年第 1 季。

1 監察網站，留意可疑活動

可疑活動可能對你的業務造成時間和金錢損失，不過，它們往往難以偵測，要保持警惕，必須付出心力。你可參考下列的方法，嚴密監察你的網站。

一旦撤銷付款頻生，你應謹慎留意。若客戶以不知情、已忘記曾經購買或誤解退貨政策為由，提交撤銷付款索償，實情可能是撤銷付款欺詐（也稱為友善欺詐或第一方欺詐）。94% 的商家將友善欺詐視為必須正視的問題[8]。

你可留意收貨地址是否位於不熟悉的市場，以及帳單地址和送貨地址是否不相符，以識別異常買家活動的訊號。此外，對於可疑的電郵地址、無法送遞的電郵、異常大額的訂單、或以多張信用卡繳付同一筆訂單的情況，你應格外警惕。

除了更密切留意網站活動外，你亦不妨向專家求助。在可行情況下，你可以將撤銷付款管理外判予第三方專家負責，以減輕你和員工監察網站的工作量。此外，你亦可利用各種工具，追蹤客戶的 IP 地址，一旦發現客戶來自高風險地點，便可收到警報。

PayPal Commerce Platform 提供一系列實用功能，包括防欺詐措施及賣家交易安全保障，利用機器學習技術適應你的業務，協助應對以上問題，大幅減低撤銷付款的風險，並於欺詐活動發生時為你提供保障。

8. Business Wire，8 Out of 10 Merchants Have Seen an Increase in Friendly Fraud, According to the 2021 Chargebacks911 Field Report，2021 年 6 月 2 日。

2 從結帳流程入手，阻截網絡罪案

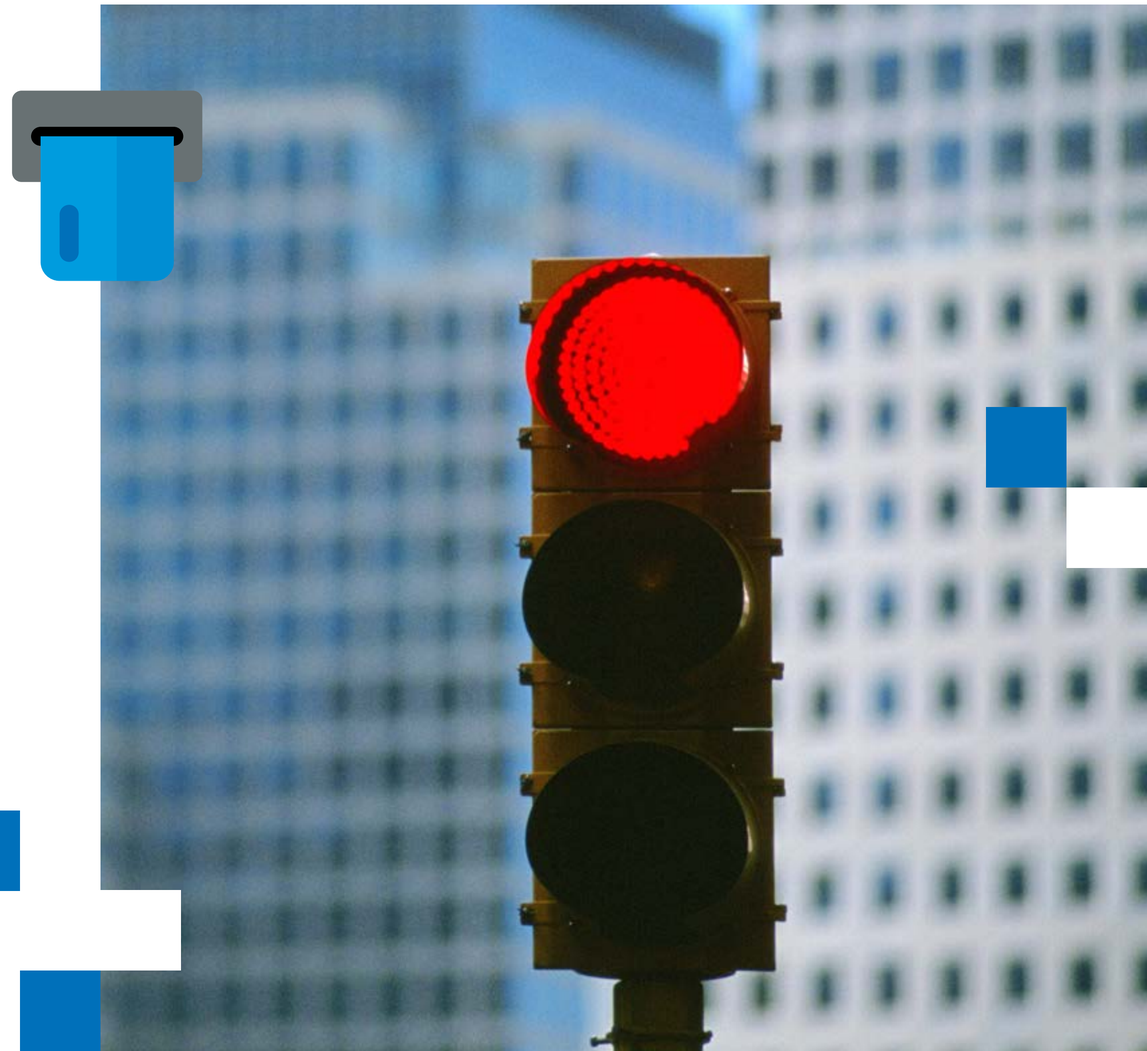
59% 的商家發現涉及無卡交易的欺詐個案有所增加。你可在結帳流程中採取防欺詐解決方案，以助提前阻截此類攻擊[9]。

4 分之 1 的商家在推行付款保安解決方案時遇上困難。當你嘗試各種電子商務付款選項時，必須採取以下步驟[9]。

你可要求客戶輸入信用卡安全驗證碼 (CVV)，堵截網絡罪犯以虛擬方式進行無卡交易欺詐—原因是根據 PCI 合規要求，商家不得將 CVV 與信用卡號碼一同儲存，因此，此做法能確保客戶必須持有實體卡，方能購物[10]。

地址驗證系統 (AVS) 會將信用卡關聯之帳單地址的數字部分與信用卡公司的存檔地址比較，助你識別可疑活動。而大部分付款處理系統亦已內建 AVS，但為保險起見，你最好向付款處理服務商再三確認。

最後，你可在防欺詐措施中加入速度檢查，以限制每日單一客戶的交易金額或次數。你可針對業務需求，設定合理的上限值，並於有人試圖超越上限時接收通知，甚至自動取消交易。一般而言，此方式可有效防止欺詐者利用盜取得來的信用卡兌現最高簽帳額。



9. Payments Dive，Merchants say they're losing revenue to online fraud, FIS report finds，2021 年 7 月 12 日。 **10.** Big Commerce，Ecommerce Fraud Protection for Online Merchants: The Ultimate Guide。

3 加密資料，確保付款安全

一旦資料未有加密，網絡罪犯便有機可乘。他們可利用這個漏洞，輕易取得信用卡號碼、密碼等機密資料。儘管網絡罪犯趨向轉投更高價值的目標，然而，許多不法之徒仍不會放過這些機會，輕鬆敲詐一番。

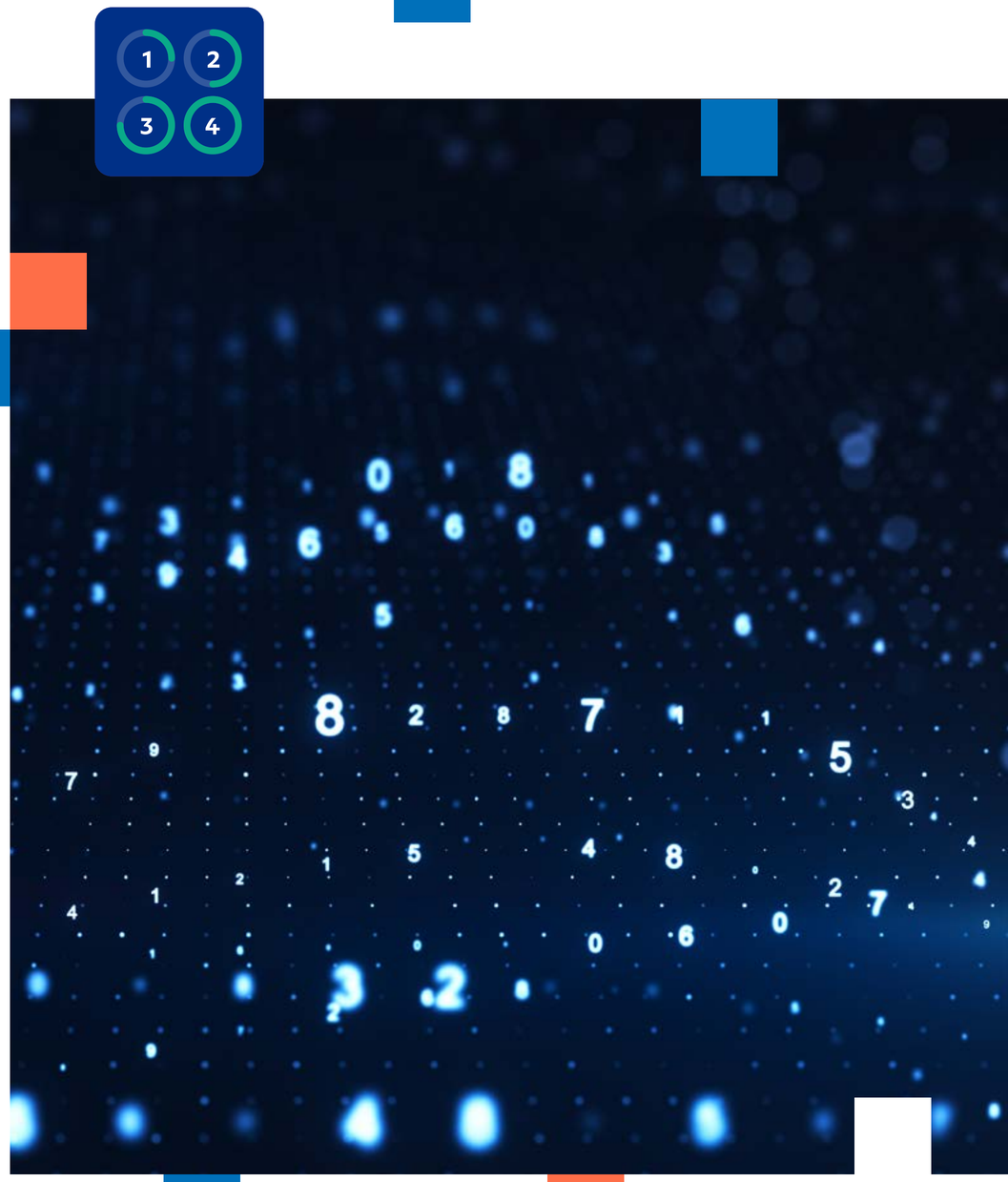
每天都有大量敏感資料在互聯網上傳輸，這些資料落入罪犯手中亦不足為奇。不過，你可以採取若干措施，避免你的業務和客戶身受其害。

採用端對端加密技術，可確保資料經加密後才透過互聯網傳輸，以應對以上風險。此外，由於各式私隱及當地資料保護法律的限制，任何需儲存或分享資料的企業都必須採取此措施[11]。

你可更進一步，利用強大的傳輸層安全性協定(TLS)配置，以實踐安全可靠的HTTPS連接規格。作為目前的業界標準，TLS 配置確保你的資料以安全的方式在互聯網上傳輸。

你應遵循嚴格的資料保護要求，以確保付款合作夥伴與你同行，攜手保護你的資料安全。

PayPal 的付款平台由最頂尖的端對端加密技術提供支援，從 TLS 與 HTTPS 連接、以至公鑰固定，均實踐全方位保安策略，符合一系列嚴謹要求，完美保護傳輸中及靜態的資料。



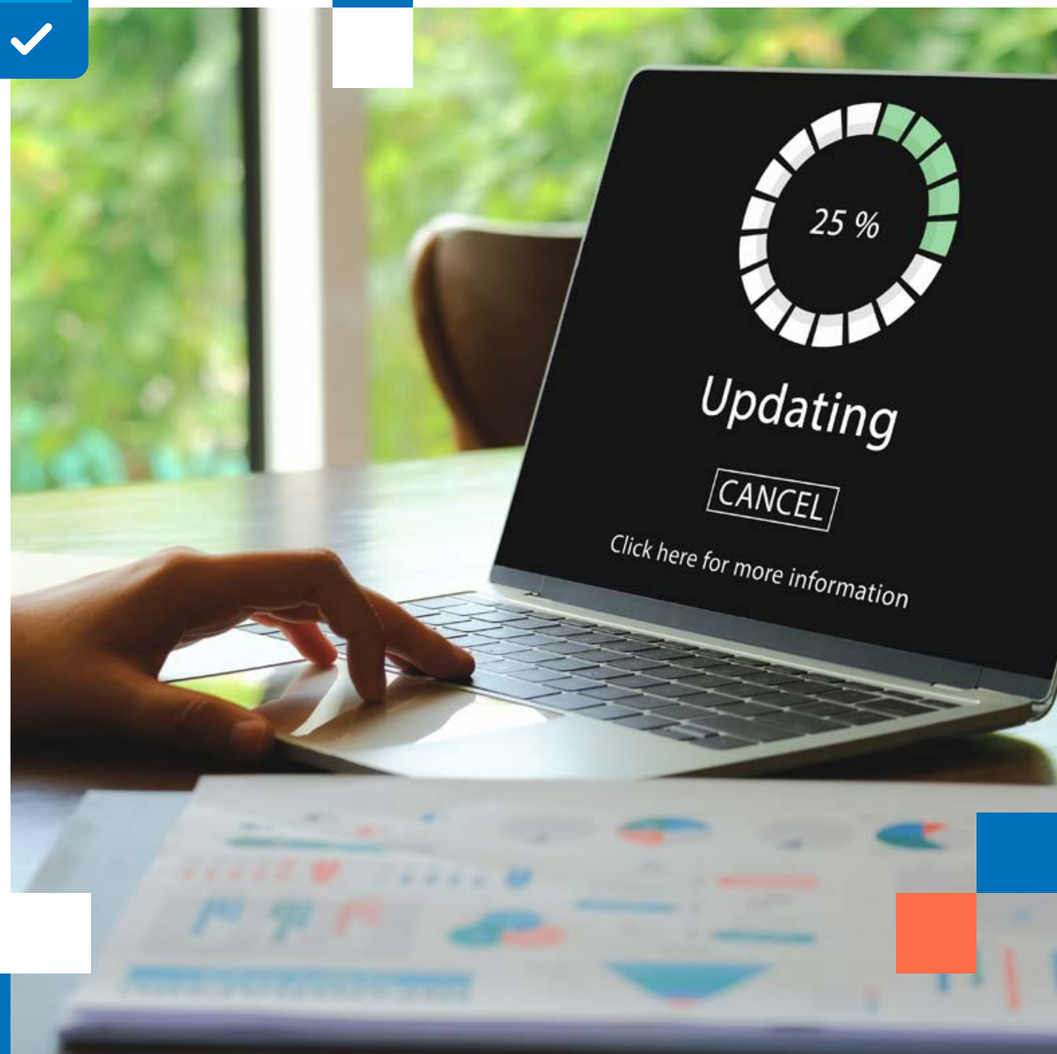
11. Insurance Business Magazine, Ten ways to protect your business from cyber attacks, 2021 年 3 月 20 日。

4 更新軟件以提升保安水平

一旦軟件過時，你便會為網絡罪犯打開大門，恭迎他們入侵系統[12]。你應採取以下幾項措施，避免網絡罪犯在你不知情的情況下自出自入。

儘管你只需保持操作系統 (OS) 為最新版本，便可簡易有效地為業務加強保護，然而，95% 的網站仍在運行具有已知漏洞的過時軟件[13]。 操作系統供應商不斷推出保安修補程式，以更新其系統，確保領先一步，應對日新月異的威脅、病毒和惡意軟件。即使是最小規模的操作系統更新，也能為你的業務保安帶來重大影響[12]。

此外，你亦可採用企業級反惡意軟件及反間諜軟件，以阻截針對過時軟件漏洞的攻擊，同時，你亦應定期更新這些軟件[14]。值得留意的是，你不應採用免費限制版軟件和客戶版軟件，因為它們的功能和對業務需求的覆蓋有限，長遠而言可能令你得不償失。



12. Business 2 Community, Top 5 Risks of Using Outdated Software in Your Company, 2021 年 6 月 14 日。 **13.** Cybernews, 95% of websites run on outdated software with known vulnerabilities, 2021 年 3 月 18 日。
14. Business 2 Community, 6 Ways to Keep Your Business Data Safe, 2021 年 10 月 26 日。

5 識別盲點，加強網絡優勢

網絡罪犯是高科技的竊賊，他們熟知如何利用技術與創新，同時如老派的扒手般，瞄準受害者的盲點。例如，當遊戲和加密貨幣領域的互聯網流量激增時，網絡罪犯洞悉到由於流量激增，風險團隊會不勝負荷，因而無法將他們一網成擒[15]。

網絡罪犯利用精密的策略，發動攻擊以獲取豐厚利潤，因此，你必須緊貼最新情況，並做好準備。你應清晰了解你的漏洞，更重要的是，別低估網絡罪犯。

大部分商家可能都會遇到一個弱點—高流量的季節性購物活動，例如黑色購物節 (Black Friday)、Cyber Monday 和雙 11。在銷售額飆升的同時，一系列干擾亦隨之出現，令網絡罪犯有機可乘。

另一方面，異常低流量的情況可能會造成另一個盲點。當運輸交通業因新冠肺炎疫情經歷流量急跌時，網絡罪犯便乘機入侵客戶久未使用的帳戶，以盜取獎賞積分和付款資料[15]。

在旺季期間，你應採用合適的保護措施，以安心享獲利潤；當淡季來到時，你亦應保持警惕，令欺詐者無從入手。

15. Sift，Exposing the Multi-billion Dollar Fraud Economy，2021 年第 1 季。

以 PAYPAL 加強網絡安全

電子商務不斷發展，加上網絡罪案持續增加，網絡安全頓成全球焦點。隨著欺詐行為越趨精密複雜，無孔不入，值得信賴的付款合作夥伴變得必不可少。與 PayPal 攜手合作，你便可安心處理每筆交易。我們擁有強大的網絡，每日以安全的方式處理超過 1,000 萬筆付款，同時，每處理一筆交易，我們的技術都變得更智能。來利用一系列實用工具，安全無憂地經營全球銷售業務。

開始使用 →