

# OUCH!

## 本期話題

- 保護自己
- 保護電腦
- 給父母的建議

## 線上遊戲安全

### 議題緣由

玩線上遊戲是擁有快樂的好方法，但它也帶來了自己特有的風險。在本文中，我們將介紹如何在您和家人玩線上遊戲時保護自身。

### 保護自己

玩線上遊戲如此有趣的原因是您可以與來自世界上

任何地方的其他玩家進行交流。您通常不知道一同玩遊戲的對象是誰。雖然絕大多數線上的玩家跟您一樣只是想享受點樂趣，但還是有想造成傷害的人。您可以採取以下步驟來保護自身安全。

- 請注意任何要求您採取行動的訊息，例如點擊連結或下載檔案。就像是電子郵件釣魚攻擊一樣，在線上遊戲中，歹徒也會試圖愚弄或欺騙您，以感染電腦或竊取個資；因此，如果收到一個訊息，看起來奇怪、緊急、或像是天上掉下來的禮物一樣好的不可能為真，請合理懷疑這可能是一場攻擊。
- 許多線上遊戲擁有自己的金融市場，在這裡可以交易、交換甚至購買虛擬商品。就像真實世界一樣，在這些系統上有詐欺者會試圖欺騙您，竊取錢財或任何您累積的虛擬貨幣。因此，建議只與那些已經建立可靠信譽的人交易。
- 所有遊戲帳號請都使用高強度的密碼短語，這樣攻擊者就無法輕易地猜測出密碼並接管帳號。如果您的遊戲提供兩階段驗證，請使用它。此外，讓所有的線上帳號各自擁有不同的密碼，這樣一來，如果一個遊戲帳號資料被外洩了，其他帳號還是安全的。記不得所有的密碼嗎？請考慮使用密碼管理器。

### 保護您的系統

歹徒可能會嘗試入侵或控制用來玩線上遊戲的電腦；因此，需要採取一些措施加以保護。

### 客座編輯

Steve Armstrong是Logical Secure的創始人，也是SANS認證講師及CyberCPR事件管理平台的架構師。他以@Nebulator活躍於Twitter上，並與世界上許多大型遊戲公司合作，實現了自己的童年和職業夢想！

## 線上遊戲安全

- 請使用最新版本的作業系統和遊戲軟體來保護電腦。老舊和過時的軟體存在已知的漏洞，攻擊者可以用來入侵您的電腦。透過保持電腦和遊戲應用程式更新，可以消除大多數已知的漏洞。
- 請安裝防毒軟體，確保維持更新並即時檢查任何檔案。
- 只從信賴的網站下載遊戲軟體。網路攻擊者通常會建立一個假冒或已被感染的遊戲版本，然後透過自己的伺服器散佈出去。
- 玩家社群常開發遊戲插件 (add-on) 以添加新的遊戲內容。網路攻擊有時會用惡意軟體感染這些遊戲插件。跟下載遊戲時一樣，請確保從受信任的位置下載插件。此外，如果下載插件時被要求停用防毒軟體或更改安全設定，請勿使用它。
- 支援作弊行為的地下市場已如雨後春筍般湧現。除了不道德之外，許多作弊程式本身就是會感染電腦的惡意軟體。請不要安裝或使用任何類型的作弊軟體或網站。
- 請檢視目前遊玩的線上遊戲網站，許多遊戲網站都有關於如何保護您和系統的說明。
- 最後，請像使用電腦一樣謹慎地在您的行動裝置上玩遊戲。網路攻擊者現在也開始以行動裝置為目標了。



安全遊玩線上遊戲的關鍵是使用高強度密碼、確保電腦安全並請在收到奇怪訊息或請求時運用常識好好想想。

## 父母或監護人

兒童在玩線上遊戲時需要額外的保護和教育。教育孩子和開放的對話是保護他們最有效的步驟。要讓孩子們願意開口說話，我們最喜歡的技巧之一就是讓他們向您展示他們的遊戲如何運作，讓他們向您說明他們的線上世界，向您展示一個經典遊戲，甚至可以和他們一起玩遊戲。此外，讓他們描述在網路上遇到的人們。玩線上遊戲很多時候可能是孩子社交生活的重大部分。透過與他們交談（讓他們跟你說話），你可以發現問題，並且遠比使用任何科技手段更能夠有效地保護他們。另外，還有一些其他的方法：

## 線上遊戲安全

- 了解孩子正在玩什麼遊戲，並確保遊戲適合您孩子的年齡。
- 限制孩子在網路上分享的資訊。例如，他們絕對不能分享他們的密碼、年齡、電話號碼或家裡住址。
- 考慮將孩子的遊戲機放置於開放空間，以便隨時留意他們；此外，不應該讓年幼的孩子在房間裡或者熬夜玩遊戲。
- 可能會出現霸凌、粗話或其他反社會行為的問題。隨時注意您的孩子，如果他們玩遊戲後看起來很沮喪，則可能在網路上受到欺負。如果他們在網路上被欺負，讓他們停止玩遊戲，並且選擇其他更適合孩子的環境，或只讓孩子和信任的朋友們玩網路遊戲。
- 了解孩子的遊戲是否支援應用程式內購買功能以及它們提供何種程度的家長監護功能。

## 進一步了解

歡迎訂閱OUCH! 全民資訊安全意識月刊，以及瀏覽前期OUCH!檔案。想要進一步了解SANS資訊安全意識方案，請瀏覽我們的網站 [securingthehuman.sans.org/ouch/archives](http://securingthehuman.sans.org/ouch/archives)。

德欣寰宇為台灣專業資訊安全顧問公司。我們為客戶提供全方位安全整合解決方案。請至官方網站 <http://www.tsc-tech.com>或臉書@tsctech了解更多訊息。

## 參考資料

- 家庭網路安全: <https://securingthehuman.sans.org/ouch/2016#february2016>
- 社交工程: <https://securingthehuman.sans.org/ouch/2017#january2017>
- 密碼短語: <https://securingthehuman.sans.org/ouch/2017#april2017>
- 密碼管理員: <https://securingthehuman.sans.org/ouch/2015#october2015>
- 兩階段驗證: <https://securingthehuman.sans.org/ouch/2015#september2015>

OUCH!由SANS Securing The Human發行刊登，遵從[Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/)(創意公用授權條款4.0版)。在不更改本刊物內容的前提下，您能夠自由分享此月刊或使用於您的安全認知計劃。有關翻譯或其他資訊，請聯絡[ouch@securingthehuman.org](mailto:ouch@securingthehuman.org)。

編輯委員會: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley  
翻譯群: 邱俊傑、黃意雯、宋亞倫、孫權劭、王澤薇、葉力維、陳月娥



[securingthehuman.sans.org/blog](http://securingthehuman.sans.org/blog)



[/securethehuman](https://www.facebook.com/securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



[securingthehuman.sans.org/gplus](https://plus.google.com/securingthehuman.sans.org)