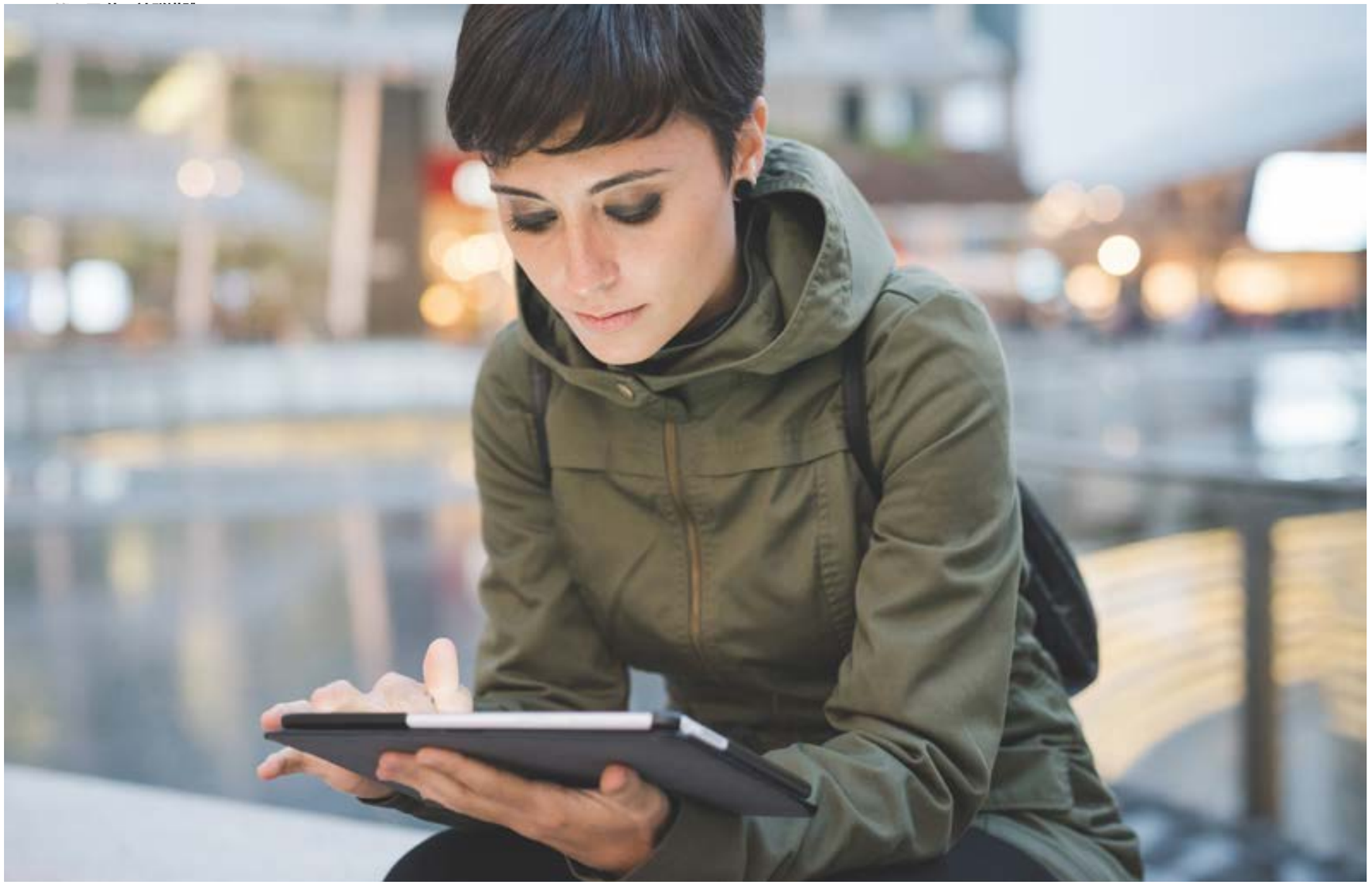
適用於所有人的網路安全。

保持安全的說明與建議
在家、工作時、在網路上和
出門在外時。



www.fidelity.co.uk

Fidelity™ INTERNATIONAL

適用於所有人的網路安全

富達國際認為網路安全是經營業務的重要一環。我們的所有工作皆以客戶為尊，因此最重要的是，我們必須盡力確保網路防禦措的完善，以保護客戶交託給我們的資訊。这對我們的個人生活中和工作同等重要。

本指南包含有關網路安全意識重要性的關鍵資訊，以及簡單又有效的訣竅，以幫助您在日益數位化的網路世界中保持安全。由於許多人逐漸適應在家與辦公室工作的型態，我們需要保持警覺，並了解自己也包括同事、朋友和家人所面臨的現有與新的威脅。

為此，我們為您製作本指南，讓您與家人和朋友分享，提供在家、線上和出門在外時，確保網路使用安全的協助與建議。

感謝您的閱讀 - 祝您平安順心。

Stuart Warner
科技部主管
富達國際

[1]www.fidelity.co.uk: 富達如何保護您以及您如何保護自己。

保護您分享的內容

在**31.7億**網際網路使用者中，約有**23億**的使用者活躍於社群媒體中。這些使用者每個人平均擁有**5.54個社群媒體帳戶**。單去年一年，社群媒體的使用量就增加**1.76億**。

來源：brandwatch.com

社群媒體可讓您用充滿趣味且高效率的方式與舊友保持聯繫（並結交新朋友）、分享興趣並掌握最新趨勢。不幸的是，Facebook, Twitter, YouTube, Pinterest 和 LinkedIn 等網站也同樣受到罪犯歡迎，箇中原因可能讓您感到十分驚訝。

花時間使用社群媒體的任何人都知道它為何如此令人沉溺，且充滿娛樂性。您可以獲得即時的回應和意見反應，有時討論的內容甚至可真切改變人們的生活；小至穿著或飲食，大至國家的政府和政治都能產生影響。

但大家都知道社群媒體也有陰暗的一面。我們都讀過「過度分享」的故事[2]，例如，您可能聽過某人因為在 Facebook 分享不雅的度假照片，導致搜尋他們的名字後出現的不雅內容讓他們找不到工作。

但使用社群媒體真正的危險之處在於活躍的犯罪分子，他們會利用找到的東西牟利。接著讓我們了解駭客想取得的資訊，以及他們獲得這些資訊後可以如何使用，並提供有關保持安全和避免不小心過度分享自身資訊的通用建議。

駭客剖析

假設我是想使用您網路身分的駭客。您在網際網路上登入任何網站時（從網路銀行到電子郵件），網站都會要求您回答一些安全問題。這些問題通常是您母親的娘家姓氏、寵物的名字、出生日期、童年綽號等。

現在思考一下您的社群媒體帳戶。如果我知道您的電子郵件位址，我需要花多少時間才能找到這些問題的答案？您的 Facebook 是否放了寵物的照片？您曾提過寵物的名字嗎？有人曾在留言區稱呼您的綽號嗎？是否有人提及您的生日？

您了解了吧。

研究社群媒體後，我只需要在您的電子郵件帳戶中按一下「忘記密碼」的連結。然後我就可以輕鬆使用這些找到的詳細個人資料，回答您的安全性問題。

現在，我已經掌握您的主要電子郵件帳戶，我可以利用它找出您所有的網路帳戶（別忘了，我可以看到您所有的郵件，因此我知道您登入的網站），然後按一下「重設密碼」。然後將重設要求傳送到我控制的電子郵件帳戶，讓我可變更您所有的密碼，讓您無法登入自己的帳戶。

思考一下，如果駭客擁有這種存取權限，他們將對您的生活造成多大的損失。他們是否可填寫貸款申請？是否可申請信用卡？在亞馬遜購買他們想要的東西？或單純探知您最私人的秘密…

[2]Mashable.com: 因不當使用社群媒體而失業的 10 個人

Fidelity INTERNATIONAL

整體而言，**60%**的青少年網際網路使用者會在社群媒體上分享自己的照片，其次是朋友和家人的照片。**一半的青少年**也經常分享和更新他們當下正在做的事。

來源：statista.com

小心謹慎您要分享的內容
若想在使用社群媒體的同時保持安全，第一步是：貼文前先審慎思考。上傳任何可用於入侵您網路帳戶的資訊時都須小心謹慎。這代表您必須保護您的住家住址、電子郵件位址、電話號碼和生日。將安全性問題視為另一層安全防護，視為密碼使用；使用虛構的複雜代碼或詞彙填寫答案。

區分公用和私人用途
每個人都有想分享個人事物的時刻。如果需要分享，最好的方法就是**私密**貼文。

檢查社群媒體網站的隱私權和安全設定，只讓家人和朋友看到您的頁面。這些設定都有其存在的理由。[3]

盡量不要讓他人掌握您時時刻刻的動向
讓大家隨時知道您的所在位置，就代表他們也知道您不在家的時間。

任何檢視您 Twitter 摘要（或 Foursquare, Google Buzz　時間表等）的人，都知道闖空門行竊的最佳時機。[4]

整理擁有資訊
如果您已不再使用某個網站，請刪除該帳戶。不要隨意放置無人看管的帳戶，讓任何人有可乘之機…

三思後再貼文
在網路發佈的內容將永遠留在網路上。始終花時間思考：一年內（甚至是隔天早上…）被別人看到您打算分享的內容後，您是否感到高興。

如果您敬仰的人看到您的貼文，您是否會感到不舒服？ 或者換個想法；您是否願意希望這則貼文成為終身摘不掉的標籤？如果答案是否定的，那麼最好不要點選「傳送」。

了解朋友的身分
擁有超長的「好友」清單可能是件令人興奮的事，但您有對他們的了解是？

如果您像信任家人般信任他們，那您當然可以分享一切。例如，您願意讓他們進入家中嗎？如果不願意，那麼請在分享祕密前謹慎思考。

如果對方看起來或感覺很可疑，請刪除
要求您登入從沒聽過的網站、陌生人的交友請求、線上廣告以及電子郵件和推文中的不明連結，都是網路罪犯試圖竊取個人資料的方式。點選前先深入研究。或直接刪除。

[3]identity.utexas.edu: 如何管理您的社群媒體隱私權設定。

[4]Pleaserobme.com: 提高過度分享的意識。

“社群媒體上發佈的內容將永遠保留在 Google 上。”

YourSocial.com

隨時保持數位安全

全球有超過**26億**的智慧型手機使用者。**87%**的人總是隨身機攜帶智慧型手機。2016年在行動裝置進行的搜尋次數比在電腦上的**多**。

來源：deviceatlas.com

如果您經常攜帶行動裝置，如平板電腦、智慧型手機或筆記型電腦，您外出時也需要與在家時同樣重視數位安全。除了裝置更容易遺失（或遺忘）外，您還將裝置帶離受保護的私人 WiFi 環境，進入廣大且充滿惡意的世界。

如今，越來越多的敏感性資料被儲存在行動裝置上，例如電子郵件、財務和工作的詳細資料、公司狀況和旅行路線等。我們希望隨時隨地都能立即存取和編輯這些資料。

使用可攜式硬體，存取儲存在雲端的資訊也越來越普遍。Dropbox, Evernote, Microsoft OneDrive 和 Apple iCloud 這類數位儲存服務代表我們可以將所有資料組合放在口袋或包包中，隨身攜帶。

除此之外，越來越多人將智慧型手機作為信用卡、智慧鑰匙和健康監視器（以及其他應用程式）使用，因此您一定可以理解預防未授權使用者將您的個人資料視為寶庫有多重要。

而且，由於您隨身攜帶行動裝置，因此裝置被遺忘、遺失、被駭客入侵或被竊的可能性非常高。而這就是即時存取的代價，但您可以採取一些行動，將風險降至最低。

使用內建功能

保護資料最簡單有效的措施之一，就是撥出時間瀏覽裝置上的安全設定。使用需要密碼才可解鎖的螢幕鎖定功能，預防隨機且未授權的使用者。[5]

尋找和清除

Android, iOS 和 Windows 作業系統的標準設定均破播遠端尋找/鎖定/抹除功能。確定您已啟用並熟悉這些功能，以在裝置遺失時快速使用這些功能。

行動 Wi-Fi 安全威脅

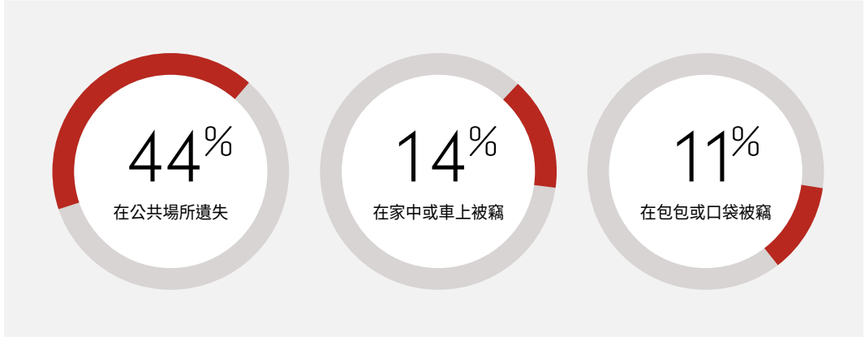
如果在咖啡廳、圖書館或其他公共場所使用免費的 WiFi，請先找到標誌或與工作人員確認網路名稱，然後再連線。在 Windows 裝置上，確認*安全類型*顯示為 WEPor WPA2，在 Mac iOS 上，確定 WiFi 設定顯示出掛鎖符號。[6]瀏覽後，請務必登出所有已登入的服務。然後設定您的裝置忘記網路。

[5]Lifehacker.com: 如何加密和隱藏整個作業系統，以防他人窺探。

[6]Lifehacker.com: 保護您的隱私的最佳瀏覽器附加工具。

最常見的手機失竊方式

IDG Research 和 Lookout Mobile Security 對 2,403 名聲稱自己的智慧型手機曾在 2014 年失竊的受訪者進行問卷調查。



每53秒
就有一台筆記型電腦失竊。
每年有7千萬支
智慧型手機遺失，
其中僅**7%**成功物歸原主。
筆記型電腦遺失
造成的損害中，
80%來自資料洩漏。

來源：
channelpronetwork.com

備份

離家前，請先確定已備份所有資料和設定，最壞情況下您最多只會損失硬體裝置...[7]

取得行動裝置防火牆

使用插入飯店乙太網路插孔的「旅行路由器」或商務中心的 WiFi，建立即時又安全的熱點，以提供額外的保護，防止惡意使用者連線到相同的 WiFi 網路。許多型號皆可指定唯一密碼作為附加保護措施。

多數筆記型電腦都將安裝軟體防火牆納入標準配備，但這些防火牆有可能被病毒或其他惡意軟體停用。使用自己的無線路由器可有效提升額外的安全層級。

保持最新狀態

確保所有裝置都已使用安全與系統軟體，完整安裝修補程式並更新至最新版本，並為已安裝的應用程式開啟自動更新功能。

上鎖或遺失

如果您有可攜式電腦，請考慮購買高品質的纜線鎖。纜線鎖是可插入電腦插槽的細鋼絲繩，可牢固鎖在任何堅固的物體上（例如壁掛支架或金屬桿）。雖然花時間就可剪斷纜線鎖，但與未上鎖的電腦相比，可大幅降低您的電腦對投機小偷的吸引力。[8]

最重要的關鍵

隨身攜帶裝置，或不讓裝置離開您的視線！

[7]tabtimes.com:
保全公司揭露行動裝置遺失和被竊所造成的損失。

[8]consumerreports.org:
2013年，智慧型手機竊盜案增加至310萬件。

Fidelity INTERNATIONAL

為子女打造更安全的網路環境

孩子喜歡電腦和網際網路，就這麼簡單。[9] 許多父母深知他們可以整天泡在網路上，這是因為他們看到的都是美好的一面。遊戲、影片、貓咪、貓咪影片、與朋友聊天、貓咪、任何天馬行空問題的答案、虛構的名人八卦、流行音樂、Google 地球和…貓。

8至11歲的孩子中**有五分之一，而**12至15歲的孩子中**有十分之七**擁有社群媒體個人檔案。ChildLine 網站的瀏覽量**超過320萬次，**較2013和2014年**增加5%**

來源：nspcc.org.uk

但是就像生活中的許多事情一樣，他們不了解其中的危險性。他們不了解密碼安全、網路小白與「網路規範」、網路釣魚、網路犯罪、駭客攻擊以及多數成年人都知道的各種其他安全問題。

網際網路是瘋狂且不受監管的地方，這個環境與我們希望保護孩子的願望完全背道而馳，但他們迫不及待地想要進入網路世界，那麼您該從何處著手呢？

控制環境

所有網路瀏覽應用程式皆有安全設定，深入了解這些設定。部分功能強大的專屬軟體程式，還可讓您篩選特定網站和程式的存取，並在孩子瀏覽受限網站時收到電子郵件警示，甚至還能進行鍵盤側錄。

許多孩子可能不需要這種等級的監視，不過您可以親自研究，尋找適合自己使用的方式。但請記住，沒有系統可提供 100% 萬無一失的安全。

陪伴孩子

如果您的孩子年齡尚小，千萬別讓他們獨自上網。您不會讓孩子在陌生的城市裡自由奔跑，老是進出陌生人的房子，對吧？因此無論您的安全設定的嚴密程度，都別讓孩子獨自上網。

進行開誠布公的溝通

多數父母都希望給予孩子自由的同時，也能讓他們保有純真。這中間的平衡很難拿捏，但您可以與孩子開誠布公討論他們可能遇到的危險，進而達到這個目標。討論的直白程度取決於您和孩子，但最重要的是，至少要開始談論不當內容和壞人的存在。[10]

訓練小小「安全助手」

下次必須更新系統軟體或安裝安全修補程式時，讓孩子親自實作，並告訴他們此舉的*理由*及必要性。

教導他們如何建立高強度密碼，並一起上網進行安全性研究調查。您或許也可能因此學到一些東西。

[9]Internetmatters.org: 幫助父母保護孩子安全使用網路。

[10]Thinkuknow.co.uk: 測試自己和孩子對網際網路安全的了解程度。

更安全的鎖與更具智慧的鑰匙

70%的人
沒有為每個網站設定
唯一的密碼。
10,000個最常用的密碼
可存取
98%的帳戶。

來源：
passwordresearch.com

密碼是進入數位世界的鑰匙，我們需要使用密碼存取各種網站，從銀行帳戶到電子郵件，無一不包。這可能會帶來不便，但如果我們想確保資訊安全，那密碼的存在就至關重要。接下來我們將討論如何透過選擇更優質且強度更高的密碼，保護帳戶安全。

密碼是容易理解和使用，且成本低廉的安全措施。它們已成為我們管理網路安全和證明身分的標準方法，不僅每天處理業務的公司需要密碼，透過電子郵件和社群媒體與親朋好友進行交流時也需要密碼。

例如，面對面進行銀行業務往來的時代，我們需仰賴簽名、附照片的身分證件、帳號的組合，通常還包含與櫃員的熟識程度，確認我們的身分。但在網際網路時代，只要兩樣東西就可代表我們的身分，那就是使用者名稱和密碼。

而這兩個要素（使用者名稱和密碼）的成功運用，導致整個體系變得非常脆弱。每組帳戶、個人檔案和應用程式都需使用密碼才可登入，日益複雜的密碼要求導致俗稱的「密碼超載」現象。

[11]teamsid.com:
公布 2015 年最差密碼。

[12]passwordmeter.com
password.kaspersky.com:
安全密碼檢查網站。

老實說，這種要求對多數使用者而言實屬不切實際[11]，且許多使用者會利用破壞密碼管理的基本規則，因應這種情況。在多個網站使用重複的密碼、盡量使用最簡單最簡短且方便猜測的密碼[12]（請見下表）。

密碼如何被竊取？
駭客可使用許多常用的技術，破解您的密碼，[13]其中許多技術只需運用簡單且方便使用的預先編寫軟體，而這些軟體不需要任何特殊的技巧就可使用。話雖如此，「不安全」的密碼設定也是導致我們如此脆弱的原因。

破解密碼：
假設您將自己喜歡的網路購物網站的密碼設為「MySecurePassword」。您進入帳戶登入頁面輸

2015 年 10 大最常用密碼
SplashData 的第五屆年度「最差密碼清單」顯示人們仍持續將自己置於風險中。

排名	密碼	排名變化
1	123456	不變
2	密碼	不變
3	12345678	上升 1 名
4	qwerty	上升 1 名
5	12345	下降 2 名
6	123456789	不變
7	football	上升 3 名
8	1234	下降 1 名
9	1234567	上升 2 名
10	baseball	下降 2 名

入這組密碼時，不會以「MySecurePassword」的形式儲存在商店資料庫中，而是會進行「*雜湊*」處理。

雜湊會將由標準單字和數字組成的密碼（名為純文字）轉換為看似毫無意義且名為*雜湊*的隨機混雜文字字串。（假設）「MySecurePassword」的雜湊為Vxc5$MnfsQ4iN$ZMTppKN16y/tlsUYs/obHlhdP.Os80yXhTurpBMUbA。

如您所見，雜湊看起來一點也不像密碼。因此即使有人可以掌握您帳戶的雜湊（令人意外地簡單），您的資料仍然很安全，對吧？

錯！駭客只需要這組雜湊代碼字串和一些免費的軟體，他們就可對您的密碼雜湊進行逆向工程，直到他們找出「MySecurePassword」為止。您不必是國際犯罪幫派份子或秘密特工就能辦到…甚至連 12 歲小孩都能輕而易舉辦到。以下是破解密碼的方法：[14]

字典式攻擊：字典攻擊會使用一種程式，該程式透過雜湊軟體，執行包含數百萬個標準單字、詞語、數字字串、名言和組合詞的資料庫，直到程式找到與您的密碼雜湊相符的內容，然後在一分鐘內反覆執行數千次的流程，直到詞彙「MySecurePassword」產生出字串「Vxc5$MnfsQ4iN$ZMTppKN16y/tlsUYs/obHlhdP.Os80yXhTurpBMUbA」為止。字典資料庫的運用更是大幅加速此一流程，因為多數人都使用名稱、地點、動詞、形容詞和名詞，建立密碼。

暴力攻擊：暴力攻擊與字典攻擊類似，但不會使用已知的單字和詞語，比對密碼雜湊，而是使用*所有*字母、數字和特殊字元，嘗試破解代碼。想像一組由三個數字代碼構成的密碼，暴力攻擊會依次嘗試每種可能的組合，例如首先是 1-2-3，然後是 1-2-4，依此類推。所需的時間比字典攻擊更長，但卻非常有效。

破解您的安全性問題：許多人會使用姓氏、寵物名、年齡、出生日期、喜愛的顏色/歌曲/運動明星和名人作為密碼的基礎。如果您曾在社群媒體發佈相關資訊，您的帳戶就有被駭客入侵的風險。[15]請參閱章節：本手冊中的「使用社群媒體」章節詳細介紹破解方法，以及您可以採取以防止密碼被破解的措施。[16]

使用簡易密碼：最糟糕的莫過於是 10 大最常用密碼的使用者之一（請參閱本文的第 1 頁）。如果密碼少於 10 個字元，且不包含任何大寫字母、特殊符號（如 *&^%$£@）或數字的組合，就是將您的安全性置於風險中。

重複使用密碼：電子郵件、銀行、社群媒體和購物網站都使用不同的密碼會造成記憶困難，但請記住，如果所有網站都使用相同的密碼，則只要其中一組密碼被破解，相當於所有密碼也都被破解。所有網站都使用同一組密碼代表您可能會遺失所有密碼。

2015年，美國國稅局因仍在許多安全系統上使用密碼：**「password」**而遇到大麻煩。

來源：
theguardian.com

[13]security.blogoverflow.com: 為何密碼應進行雜湊。

[14]security.stackexchange.com: 字典攻擊和暴力攻擊的不同之處？

Fidelity INTERNATIONAL

2010年1月，
Twitter禁用
370組使用者的密碼，
原因是太容易被破解。
這些密碼包含下列詞組：
「000000」
「letmein」
「aaaaaaaa」
「whatever」
和**「stupid」**

來源：
trendhunter.com

了解駭客

您可能聽說黑帽駭客和白帽駭客這兩個詞，但您知道其中的區別嗎？區別就在於道德感…

白帽駭客

具道德感的電腦駭客，專精於測試組織的安全系統。

黑帽駭客

擁有廣泛知識，並以破壞網際網路安全為目標的駭客。

灰帽駭客

雖然道德界線模糊，但沒有惡意並具備優秀駭客技術的駭客。

激進駭客

因政治或道德原因而進行駭客入侵，通常與言論自由和人權相關。

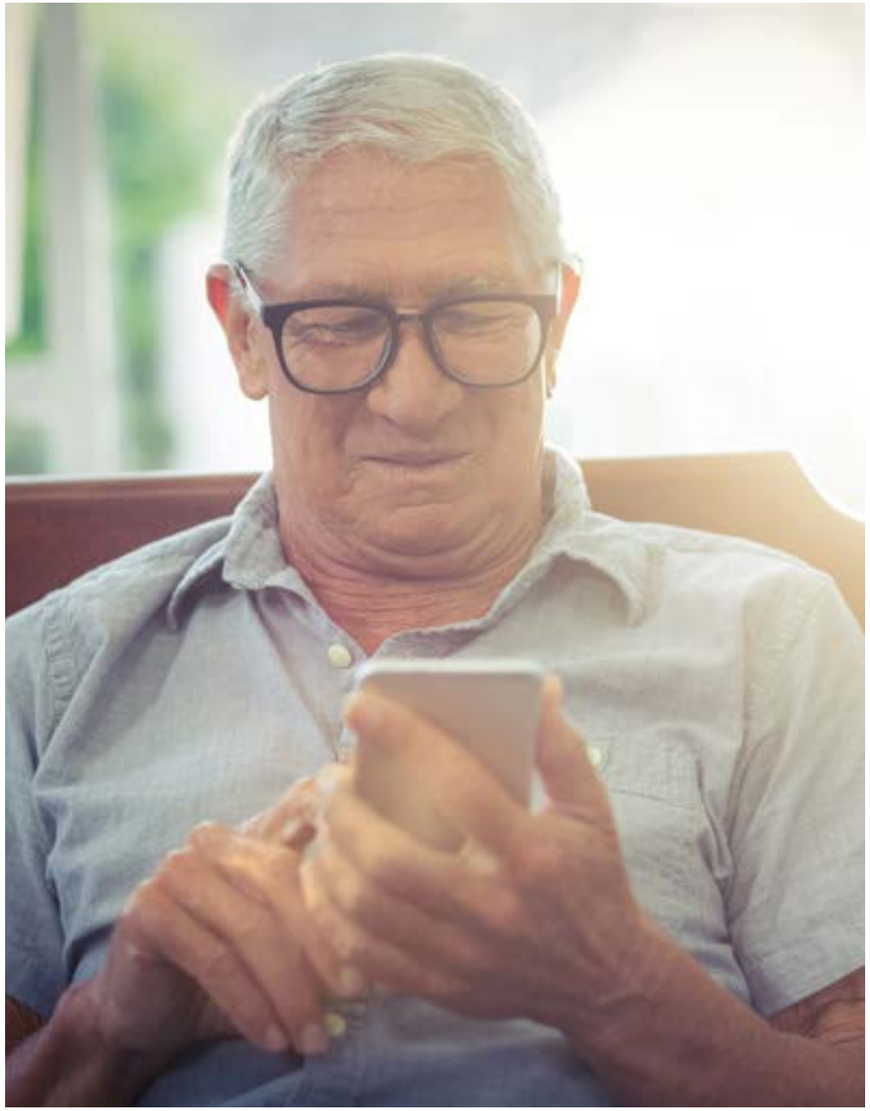
您可以如何應對？

沒有什麼是無法破解，但您可以透過遵循下列10點，盡可能提高破解密碼的難度：[17]

1. 確保每個網路帳戶都使用不同的密碼。
2. 考慮使用密碼管理工具。密碼管理工具可針對您使用的所有網站產生、記錄、加密和儲存密碼資訊，並協助您自動登入。使用主密碼進行存取代表您只需記住一個安全密碼。
3. 使用值得信賴的密碼強度分析網站，檢查選擇代碼的強度。
4. 切勿在網咖或圖書館等公用或共用電腦上輸入密碼。
5. 同樣地，如果您使用不安全的公用Wi-Fi進行連線，切勿輸入密碼。[18]
6. 定期變更密碼，請勿重複使用密碼。
7. 請勿將您的密碼告訴任何人。永遠別這麼做。
8. 使用至少十個混合小寫字母、大寫字母、數字和特殊字元的字元組合。使用達到允許字元數的密碼。
9. 切勿在登入的情況下，讓裝置無人看管。
10. 確定沒人看到您輸入密碼。

[15]slate.com:
您在哪個城市度蜜月？以及其他古怪愚蠢的銀行安全性問題。

[16]goodsecurityquestions.com:
優質的安全性問題符合五個標準。



只要**10**分鐘
就可以破解
6個字元長的
小寫密碼。
額外增加兩個字母
和一些大寫字母，
破解時間就會
大幅延長至**3年**。
只需新增一個字元、
一些數字和符號，
就需要**44,530年**的時間
才能破解。

來源：
Stopthehacker.com

[17]passwordday.org
建立密碼的建議和資訊。

[18]usa.kaspersky.com:
公共 WiFi 網路貸給使用者許多安全風險，但幸運的是，有許多訣竅可保持網路安全。

提高警覺，保持安全

2014年，
約有**3180萬**
美國消費者的信用卡被盜刷，
受影響人數是
2013年的三倍。
與去年同期相比，
2015年第一季英國的
身分詐騙比例
上升至**27%**，
佔所有舉報的詐騙犯罪中
將近一半。

來源：
nasdaq.com

從組織性的犯罪幫派到秘密監視，甚至外國犯罪分子的駭客入侵似乎都無所不在，隨時準備利用通訊和資料儲存新興領域中的所有弱點。多數人都可以毫無問題使用網際網路，但是如果他們不採取基本的安全預防措施，任何人都可能成為網路犯罪的犧牲品。

一些行為乍看之下似乎完全無害，例如使用電子郵件應用程式、搜尋網際網路、下載檔案、玩遊戲及註冊新網站和服務，這些都可能讓您的電腦或行動裝置被病毒或間諜軟體感染，導致您的資料遺失、身分被冒用，甚至面臨嚴重的詐騙行為。

要避免成為此類攻擊的受害者，最佳的防禦方法就是盡力了解網路罪犯用來嘗試破解並存取電腦的手段和技術。[19]因為他們可以成功入侵的原因就是您給了他們機會。

檢視對面的方塊，閱讀描述網路犯罪常見類型的術語，您可能已經知道其中一些。

在後續頁面中，我們將詳細探討，讓您了解它們的運作原理以及該如何避免成為受害者。

網路犯罪術語說明

殭屍網路
感染您的電腦並將其變成為可遠端控制的「奴隸」（俗稱「殭屍」），犯罪幫派可利用這些奴隸代替他們犯罪。

網址嫁接
將您從合法的網址重新導向至偽造的網站。

網路釣魚
偽造看似來自真實公司的虛假電子郵件、文字訊息和網站，以此收集您的個人資訊（例如密碼），或引導您開啟將感染電腦系統的連結。

勒索軟體
勒索軟體是惡意軟體，可以對電腦上所有的資料進行加密並顯示訊息，要求您付款，才可讓檔案恢復正常。

間諜軟體
在您不知情的情況下，收集您的個人資訊（密碼、瀏覽歷程記錄等）。
通常在您從網際網路下載檔案時，在未經您同意或不知情的情況下安裝。

特洛伊木馬
偽裝成或隱藏於合法（或看似合法）程式的惡意軟體。

[19]getsafeonline.org:
保護您和您的電腦。

在社群媒體進行網路釣魚

Barracuda Networks 對 20 個國家中，表明使用社群媒體時遇到安全漏洞和隱私權問題的使用者進行調查。

54% 受到網路釣魚攻擊	23% 收到惡意軟體
13% 密碼被竊	17% 帳戶被劫持

網路釣魚

*網路釣魚*通常會透過電子郵件進行，藉此收集個人資訊或破壞技術，以達到獲得經濟利益或進行惡意活動的目的。網路釣魚電子郵件中通常包含詐騙網站的連結，或包含惡意軟體的附件，按下連結或下載檔案就會啟動該程式。

全球每天都有數百萬封網路釣魚電子郵件被傳送給毫無戒心的受害者。部分網路釣魚很容易被識破為詐騙郵件，但有一些卻很具說服力。該如何區分詐騙和真實的電子郵件？以下我們收集六種辨別潛在網路釣魚電子郵件的方法：

1 郵件包含可疑或無關的網址

如果您認為內容十分可疑，請檢查所有內嵌網址的完整性。網路釣魚電子郵件中的網址可能看似非常正確，但如果將滑鼠游標懸停在連結上，您就可看到實際的超連結網址。如果超連結的網址與顯示的網址不同，則這可能是一封詐騙郵件。

2 郵件的拼寫或文法不佳

大型組織傳送郵件時，通常會檢查拼字、文法和合法性，如果內容充滿拼字錯誤，則該封郵件可能不是來自大型公司的法律部門。

3 郵件要求提供個人資訊，尤其是密碼

信譽良好的公司絕對不會要求您透過電子郵件，傳送或確認密碼，或登入詳細資料。公司或者已掌握這些資訊，且他們有許多其他的方法可以確認您的身分，因此這是一封詐騙郵件。

4 缺少個人問候語或任何自訂資訊

來自銀行、信用卡公司和其他具安全意識組織的合法電子郵件的網址，通常包含部分帳號或使用者名稱。看到如「尊敬的使用者」這類問候與時應提高警覺。

5 緊急情況

郵件中提到您必須立即採取行動，以免造成財務損失或存取中斷事件，這類郵件通常希望讓您未經思考就採取行動。花時間調查，仔細檢查超連結，然後使用其他方式（如撥打已知的電話、親自拜訪、透過手動輸入網址進入網頁等）與寄件者聯絡。

6 有些東西看起來「不大對勁」

可能是標誌不大一樣，或者是郵件的措辭有些奇

> “駭客已入侵連接網際網路的鏡頭系統、智慧型電視，甚至是嬰兒監視器。”
>
> Molly Wood,
> 紐約時報

2015年，
一共有**1,966,324**則
嘗試進行惡意軟體感染的
註冊通知，
這些通知的目的是
透過網路存取銀行帳戶，
竊取金錢。

來源：
securelist.com

怪，有時一些東西看起來就是不太對，請試著相信這種感覺。事實上，預防詐騙最好的方法就是我們的警覺心。

心存懷疑就放棄
如果您對電子郵件、連結或附件的合法性存疑，最好的應對方法就是刪除。不要開啟、轉寄或儲存郵件以待日後給其他人看，保持安全比日後後悔要好得多。

網路釣魚是犯罪分子最常用的手法，以此誘使您感染自己的電腦或竊取您的個人資料。一旦犯罪分子成功，他們還會做什麼？他們可能會啟動勒索軟體攻擊：

數位劫持
勒索軟體[20]是駭客越來越常使用的撈錢手段。這種數位勒索分為兩種類型：

鎖定螢幕型勒索軟體
使用影像鎖定您的螢幕，影像會要求您付款並顯示付款明細。

加密型勒索軟體
加密系統硬碟（包括網路磁碟機、外接硬碟、USB，甚至雲端儲存裝置）上的*所有*檔案，讓您無法開啟檔案，並要求付款以重新取得存取權限。

有時，勒索軟體病毒還會向使用者傳送自稱來自執法機構的訊息，表示偵測到非法線上活動，進而要求支付罰款以避免被捕。

您可以採取的行動
即使支付贖金，也無法保證您可以取回檔案。如果犯罪分子不肯兌現承諾，您也無法向任何人投訴。如今，與您接觸的人愈發可能只是向專業的犯罪程式設計師購買勒索軟體病毒，他們甚至不知道該如何將您的資料還原，即使您付出贖金。

法律威脅的目的是為了嚇唬和恐嚇您，這些訊息並非來自執法機構，也沒有獲得法律授權。警察部門不會利用這種方式聯絡您。

您必須認知到資料可能無法還原的事實，但您也可以嘗試向值得信賴的專家尋求專業建議，了解否有機會修復電腦並取回資料。

確保資料安全的唯一方法，就是將最重要的個人檔案備份在卸除式外接儲存磁碟上。

您是殭屍大軍的一員嗎？
具備網際網路功能且被名為「Bots」的遠端控制機器人程式感染，以建立*殭屍網路*的電腦大軍。[21]

殭屍網路是駭客世界中沉默的獵手，所有被感染的電腦都被稱為「殭屍」，會與類似的感染電腦合作，在單一主機的控制下組建成殭屍大軍。您可能在不知情的情況下成為殭屍大軍的一員。

駭客成功組建殭屍網路後，他們就可以利用電腦大軍，對網站傳送大量的資訊要求，或反覆傳送相同的要求，導致該網站超載並進而關閉（被稱為分散式阻斷服務（DDoS）攻擊）。這類攻擊可用來勒索公司，索取金錢以停止攻擊。

殭屍大軍的指揮官還有另一種選擇，那就是利用感染的網路，傳送數百萬封垃圾郵件並傳播病毒和惡意軟體。而且都是透過您的電腦執行。[22]

您可以採取的行動
您可以採取一些措施，降低攻擊者劫持電腦系統的可能性：

防火牆
安裝防火牆並設定監視和控制進出電腦的流量。

使用電子郵件篩選器
套用智慧型篩選條件可限制垃圾電子郵件進入郵件應用程式的數量和類型。

提高警覺
如果您發現網際網路連線速度很慢，請使用系統工具，檢查數據機正在處理的流量。如果流量很高，但您沒有下載或上傳任何內容，這很有可能代表您已成為殭屍網路的一分子。[23]

信任的技術支援
部分詐騙者甚至冒用網際網路服務供應商技術支援部門的身分。他們會告訴您，他們需要您授予遠端存取您電腦的權限，讓他們移除可識別的惡意檔案或軟體。如果您尚未聯絡網際網路服務供應商或電腦服務台，那您可以確定這些要求屬於詐騙行為。

如何判斷您的電腦是否已感染

下列清單可以協助您確定電腦是否有問題。您可能會遇到以下其中一項、多項或全部的情況：

- ✔ 隨機出現非預期的快顯視窗，這可能是被間諜軟體感染的跡象
- ✔ 程式似乎開始自動執行
- ✔ 您的安全軟體已停止執行
- ✔ 啟動電腦所需的時間比平時更長，有時電腦會自行重新啟動或根本無法啟動
- ✔ 您的電腦顯示器看似失真
- ✔ 需要花很長的時間才能啟動程式
- ✔ 檔案和資料消失或被移動
- ✔ 系統軟體經常損毀
- ✔ 您的首頁神奇的被變動
- ✔ 您的記憶體預料外出現不足情況
- ✔ 檔案和資料被重新命名
- ✔ 網際網路瀏覽和載入網頁的速度很慢

如果您認為您的電腦已感染，請更新安全軟體並執行完整的檢查。如果您沒有發現任何可疑事物或不確定該採取的行動，請尋求值得信賴的專業人員協助。

在有唯一使用者的
753,684台電腦上
被偵測到勒索軟體程式；
179,209台電腦
成為加密型勒索軟體的目標。

來源：
securelist.com

[20]blog.trendmicro.com:
勒索軟體是2016年最大的威脅之一。

[21]welivesecurity.com:
前5大最可怕的殭屍網路。

殭屍網路最嚴重的5個國家
截至2016年9月
1 印度：2326660
2 越南：1009151
3 中國：796087
4 伊朗：651753
5 巴基斯坦：458816

來源：
spamhaus.org

電腦病毒
惡意電腦程式通常會以電子郵件附件或下載的形式傳送，進而感染電腦病毒。通常得以讓犯罪分子存取您的電腦、掃描密碼等個人資訊、劫持您的網頁瀏覽器和停用安全功能。

特洛伊木馬
特洛伊木馬會偽裝或隱藏在合法軟體中，是一種會自行安裝並自動執行的執行檔。成功安裝後，可以刪除或複製您的檔案、透過網路攝影機觀察您或記錄您的按鍵輸入（例如您在線上輸入的信用卡詳細資料）。

蠕蟲
與病毒不同，蠕蟲可以自行執行，而不需附加在您的檔案或程式中。會隱藏在您的電腦記憶體中，並將自己傳送到使用相同網路或網際網路的其他電腦上。指數複製率不僅會威脅個人，還會威脅到網際網路。

網路詐騙的運作原理

您上網時，駭客會利用您的網際網路通訊協定 (IP) 位址，識別您的網際網路服務供應商。他們知道您的寬頻連線的供應商時，他們就可以輕鬆假裝自己是該公司的合法技術支援人員。

詐騙技術人員會透過電腦螢幕上的通訊視窗或電話說服您，表明他們需要控制您的電腦，才可從系統中刪除感染的檔案。如果您給予他們存取權限，他們將指示您付款以移除所謂的惡意檔案。

您可以採取的行動

切勿將遠端存取權限，給予任何您未明確要求在電腦上作業的工作人員。[24]

無視技術支援視窗、關閉視窗和/或掛掉電話。直接使用您熟悉的號碼或曾撥打的號碼，聯絡您的網際網路服務供應商，並說明情況。

如果您授權遠端存取，則您的系統可能被威脅。如果遇到這種情況，您應該中斷裝置連線、重新安裝作業系統，或將電腦攜至信譽良好電腦支援服務中心，重新安裝電腦系統。保存完整的資料備份此時將大有幫助。

詐騙電話

不僅是在 21 世紀，無論身處的時代，網路罪犯都會使用最先進的科技，竊取您的安全資訊，因此電話詐騙目前仍是罪犯的熱門手法。[25]

所謂的*語音釣魚*（語音釣魚）詐騙者會致電給您，假裝是您往來銀行的工作人員，警告您帳戶出現可疑活動，或是加裝是您的第四台公司甚至是警方，聲稱您是信用卡詐騙的受害者。這一切的目的，都是為了讓您透露帳戶詳細資料與密碼。

[22]uk.norton.com/botnet: 機器人和殭屍網路 - 日益嚴重的威脅。

過去五年間，
超過**2700萬**名美國人
成為身分盜竊的受害者。
僅去年一年，
就有**900萬**人
發現自己的身分被竊。

來源：
stopthehacker.com

遇到下列情況時，必須提高警覺：
有人致電告知，您的信用卡被盜用。來電者建議您掛斷電話並回電，確認他們的身分；罪犯會選擇不放下聽筒，讓您的電話線路保持開放狀態，看似您連接到撥打的安全號碼。有人要求您將現金轉入新帳戶，即使他們說這是您名下的帳戶。

您可以採取的行動

切勿因對採取的行動感到不安而備感壓力。如果事情看起來不大對勁，那就暫停並花時間思考…
切勿害怕掛斷電話，只要保持有禮而堅定的態度就沒問題了。

[23]f-secure.com: 殭屍網路快速指南 - 定義、運作方式以及可能造成的危害。

職場共事

根據
Shred-it / Ipsos Reid Information
Security Tracker
的調查，
47%的受訪者表示
他們已固定控制台
並使用專業的碎紙服務
銷毀敏感文件，
但**46%**的受訪者
沒有銷毀安全資訊的
直接負責人

來源：
shredit.com

隨著金融犯罪的增加，在工作場所隨時保持警覺也十分重要。雇主愈發依賴資訊系統，他們收集，儲存和使用的資料量不斷增長。他們有責任對收集的資料類型及其儲存方式保持開誠布公與誠實的態度，但每個人都必須自問*我該如何才能協助確保資料安全？*

我們都有權利在安全的環境中工作，這包括實體環境和數位環境。培養這種文化不僅需要遵守當地政府的準則或部門政策，同時也是一種心態。

平衡風險
只要有人的存在就有風險，事實就是如此，但風險與自由間必須始終保持平衡。

如果您無法確保資料安全，則您任職的公司就不適合與進行業務往來，同時您還需確保公司落實的安全流程確實有助益，而不是阻礙。[26]知識必須可以自由流動，且您需要以靈活的方式應對各種情況...這就是所謂的平衡。以下是可以協助保護您的資料，以及您的公司、客戶和同事的一些方法。

密碼
無論在任何情況下，請勿告知他人您的工作密碼。換言之，不要將密碼記錄在便條紙上，並貼在電腦正面，好嗎？如需詳細資訊，請參閱「密碼」章節（第 14 頁）。

電子郵件
這是我們都會做的行為，聽起來理所當然（也*確實*理所應當），但並不妨礙大家每天繼續這麼做——那就是*盡力*確保將電子郵件傳送給正確的收件者。

將機密或敏感資訊傳送給不應傳送的對象是最常見錯誤之一，不僅會讓我們感覺尷尬，還會導致公司面臨風險。請花時間思考是否應加密電子郵件，並在按下「傳送」前再三仔細檢查收件者。

另外，請勿將公司電子郵件作為除工作以外的其他用途使用；這錦慧讓您的收件匣塞滿垃圾郵件，並提高被網路釣魚攻擊的可能性（請參閱「網路犯罪」第 20 頁）。

鎖定您的螢幕
您離開辦公桌時，請記得將電腦設定進入睡眠模式或啟動螢幕鎖定功能。如此一來，如果有人想查看您的工作內容，他們就必須取得您的密碼（只要密碼沒有寫在紙條上，並貼在鍵盤背面）。

將工作帶回家
確認將工作檔案帶回家的相關公司政策。如果公司允許將檔案帶回家，請確保移除資料前加密檔案，或將檔案放置在被密碼保護的磁碟上，即使磁碟遺失，仍可繼續保護資料。

[26]inspire-success.com:
工作場所的12大IT安全訣竅

Fidelity INTERNATIONAL

2015年，金融服務組織中所偵測的安全事件中有41%是因受信賴存取權限的第三方對象而起。在工業產品組織中有**62%**的安全事件涉及現任或前任員工。

來源：pwc.com

回報裝置遺失或被竊

如果您遺失與工作相關的資料，請務必盡快告知相關部門。坦白說，如果敏感資訊落入危險分子手中，且您的公司卻沒有做好準備，那情況將會非常糟糕。

三思後再點選

從網際網路下載任何內容到您的工作電腦上時，必須非常小心謹慎，尤其是「執行檔」(.exe)。您幾乎無法判斷檔案內容是否如自稱所述，還是其中確實藏有惡劣病毒，伺機感染公司的整個系統。

與資訊安全部門合作

如果您的公司有 IT 或資訊安全部門，請聯絡他們。詢問他們採取的措施，以保護您的資料安全，以及您可以採取的方法，以保護公司。了解發生問題時需要聯絡的人員，以隨時做好準備。

這是數位時代，[27]以前只需確定鎖緊窗戶，並在下班後啟動夜間警報裝置就可以。但如今，不僅是財務和設備會被竊，遺失資料的企業還可能失去客戶、聲譽和所有的一切。這就是 21 世紀的工作場所，試著融入這樣環境吧。

現實世界的安全性

避免犯罪分子染指公司資料的實務不僅適用於虛擬世界中的聰明思維，在現實世界中您同樣可以採取行動。[26]

勇敢發聲

如果您的公司配備門禁系統或簽發ID證件，則您的公司可能也已設立安全部門。如果看到無證件者，或者發現任何不尋常的事，請養成舉報的習慣。您不需要直接與他人對質，只需讓他們知道您的擔憂即可。罪犯希望我們畏縮，用沉默面對一切，請以行動證明他們的想法錯誤。

乾淨整潔

以處理數位素材相同的安全等級，處理所有印刷素材：您離開辦公桌時，請將桌面上的敏感文件清空，並在下班時將文件上鎖，並確認您未在影印機或印表機上放置任何機密資訊。列印文件使用完畢後，請不要隨意丟棄，應放入碎紙機中銷毀。

保持機密

請勿透過電話或電子郵件，將您的個人或機密詳細資料透露給您不認識的人，除非您確定索取資料人員或公司的身分，以及他們希望取得的原因。且不要在公共場合或網路上提及任何機密工作細節，因為您永遠不知道有誰會聽到這些內容...

[26]getsafeonline.org:
實體安全與網路安全同等重要

病患資訊如同放射性物質，必須妥善保護。必須安全控制。嚴正以待。

Arthur R. Derse 博士
美國生命倫理中心

[27]cio.com:
我們都為資訊安全的世界而努力

Fidelity INTERNATIONAL

棉薄之力帶來長遠的影響

2015年第1季（1月至3月），英國**86%的成年人（4470萬）**在過去3個月內曾使用網際網路（近期使用者），預估比2014年第1季（1月至3月）的85%增加1%。

11%的成年人（590萬）從未曾使用網際網路，比2014年第1季（1月至3月）下降1%。

來源：ons.gov.uk

網際網路…不是狂野的西部、也不是鬧鬼的森林。橋下沒有巨魔，峽谷中也沒有土匪。我們剛才討論的是一些最糟糕的情境，請不要灰心喪志，闔上本書，並發誓永遠都不上網。我們只是希望您花點時間思考並更新您的安全知識。我們保證花的時間肯定物超所值。

遵循一些明智的程序將大幅減少您淪為網路犯罪或身分盜竊受害者的機會。[26]許多罪犯正在想方設法，以最輕鬆的方式，獲取最大的利益。與採取明智措施鎖上家中門窗的家庭相較，門戶大開的家庭被搶的可能性高。同樣的，受到智慧安全程序保護的電腦或帳戶，對駭客的吸引力遠遠不及缺乏保護的電腦或帳戶。重點是：別讓他們輕鬆得逞…

保護您的裝置
持續更新作業系統、應用程式和網頁瀏覽器至最新狀態，是您確保安全最簡單且最有效的措施之一。

確定已開啟*自動更新功能*，取得最新版本的作業系統與安全修補程式。

保護您的資料
使用智慧密碼，且不同帳戶使用不同的密碼：請參考本書的*「密碼安全性」*一節，了解更多資訊。

僅透過安全連線傳算資訊，傳送任何敏感資訊，例如信用卡詳細資料時，請先在位址欄中找到**https://** 或**掛鎖圖示**。如果您要在公共或共用電腦上存取受密碼保護的帳戶或網站，請記得完成後登出並關閉瀏覽器視窗。

安裝一些防護性軟體，最好是包含防毒/惡意軟體和防火牆元件的安全套裝軟體。

不要過度分享
思考如何使用社群媒體；設定隱私和安全設定，並思考罪犯可能會如何利用您發布的資訊。請檢視*「使用社群媒體」*頁。

不要上鉤
特別緊善小心網路釣魚；電子郵件、推文、偽造網站中的連結，以及不切實際的網路優惠，都是駭客試圖竊取個人資料的方法。學會抱持懷疑的態度，且您察覺「不對勁」時，不要害怕將其刪除。您可以在*「網路犯罪」*章節，了解更多資訊。

備份
聽起來可能很煩人，但是請定期將所有不可取代的照片、工作檔案和其他數位資訊備份到卸除式硬碟上。此舉可在您的硬碟或雲端帳戶出現狀況時，確保獲得妥善保護。

做好準備
做好最壞的打算。保留紙筆抄寫的電子郵件、電話號碼和朋友與聯絡人地址，以防您的身分和帳戶被竊。確定您知道正確的號碼，以取消信用卡和凍結銀行帳戶，並找出相關詐騙或執法部門的名稱和號碼，以限制罪犯毫無限制使用您的財產的時間。

[26]staysafeonline.org: 國家網路安全聯盟分享他們保持安全的訣竅與技巧。

2015 年的數位、社群和行動
2020 年 1 月，全球將近 42% 的人口可以存取網際網路，wearesocial.com彙整出這些數字，繪製出 2020 年初全球人口數位使用的概觀。

三思而後行
許多詐騙案都是利用我們對獨一無二、一次性、限量和低價優惠的渴望乘虛而入。這些不切實際的優惠騙局，經常掩蓋背後的惡意。學習如何看穿騙局。了解他人受騙的方式與原因。請記住，我們都渴望獲得免費的假期和iPad，但是您根本不可能透過填寫線上表格獲得。這只是一場騙局。

最後…
雖然網路世界只是數位世界，但不代表不是現實世界。[27]

在網路上與人相處變得如此容易，但網路上發生的事情至關重要，而且影響深遠。與他人相處時，記得將心比心。表現出友善態度，提高警覺，保持安全。

“親愛的網際網路使用者，您有天會因為沒閱讀此內容而後悔。謹此，條款與條件。”

不明人士，Facebook.com

[27]youtube.com: 網際網路如何運作？

本手冊的資訊由富達國際從公共來源取得。富達國際的員工以謹慎的態度彙整本文資料，並在發佈時驗證其準確性，但是因一些富達國際無法控制的因素，本手冊的內容可能會有失準的狀況，因此僅供參考。

富達國際僅負責本手冊的出版與發行，根據本手冊之資訊所採取的任何行動結果，或是本手冊中的任何錯誤或遺漏，富達國際概不負責。因或與使用和依賴本手冊的任何資訊相關而直接或間接導致的索償、損失或損害，富達國際明示放棄向任何人承擔任何義務與責任。富達國際係指 FIL Limited 和/或其子公司。