OUCH!2021年9月

保護帳號的簡單步驟

網路犯罪分子是否擁有存取您的電子郵件或銀行帳號的魔杖，而您卻無能為力？如果您可以採取一個簡單的步驟來幫助保護您免受網路犯罪分子的侵害並讓您能夠安全地充分使用科技，那不是很好嗎？雖然無法僅靠一個方法就阻止所有網路罪犯，但您可以採取的最重要步驟之一，是為您最重要的帳戶啟用稱為雙因子身份驗證（有時稱為 2FA、兩步驟驗證或多因素身份驗證）的機制。

密碼的問題

您很可能已經在使用某種類型的密碼在保護您的帳號。有幾種方法可以驗證您的身分以登入帳號：您擁有的東西、您知道的東西、您是什麼或您所在的地方。當您採用多種身份驗證方法時，您和網路犯罪分子之間就增加了一層額外的保護——即使他們破解了一種方法，他們仍然需要繞過其他因子才能存取您的帳號。密碼根據您知道的資訊來驗證您是誰。密碼的危險在於它們會單點失效。如果網路罪犯可以猜出或揭露您的密碼，他們就能夠存取您的重要帳號。此外，網路罪犯正在開發更快更好的技術來猜測、破壞或繞過密碼。幸好，您可以使用雙因子身份驗證反擊。

雙因子驗證

增加雙因子驗證是比僅依賴密碼更安全的解決方案。它的工作原理是需要不只一種，而是兩種不同的方法來驗證身分。如此一來，即使您的密碼被洩露，您的帳號仍然受到保護。您的 ATM 卡片是一個例子：當您從 ATM 提款時，您實際上在使用一種雙因子身份驗證。要取得您的錢財，您需要兩樣東西：您的 ATM 卡片（您擁有的東西）和您的 PIN 碼（您知道的東西）。如果您弄丟了 ATM 卡，任何找到您的卡片的人都無法提領您的錢，因為他們不知道您的 PIN碼。如果他們只有您的 PIN碼 而沒有卡片，也是相同情況。攻擊者必須同時擁有兩者才能突破您的 ATM 帳號。您有兩道安全防護，雙因子身份驗證的概念類似於此。

線上使用雙因子身份驗證

您要為每個帳號單獨設定雙因子身份驗證。

其實很簡單：您通常只需要將您的手機與您的帳號同步即可。這樣，當您需要登入時，您不僅要使用帳號名稱和密碼，還要使用從手機中取得的特殊一次性代碼。概念是需要組合您的密碼和一次性代碼才能登入。通常，此特殊代碼將以簡訊發送到您的行動裝置或電子郵件。您的手機也可能有行動應用程式（例如 Google 或 Microsoft Authenticator 應用程式），可以為您產生特殊代碼。在可行的情況下，行動應用程式被認為是獲取特殊代碼的最安全選擇。

之所以如此簡單，是因為您通常只需要從用於登入的任何電腦或裝置上執行一次此操作。一旦網站或您的帳號識別出您的裝置，接下來您通常只需要密碼即可登入。每當您或其他人嘗試使用您的帳號，但從不同的電腦或裝置登入時，將不得不再次使用雙因子身份驗證。這代表若是網路罪犯獲得了您的密碼，他們仍然無法存取您的帳號，因為他們無法取得特殊代碼。

請記住，雙因子身份驗證通常不會預設啟用，因此您必須為每個重要的帳戶（例如銀行、投資、退休或個人電子郵件）自行啟用。雖然一開始似乎需要更多的手續，但一旦設定好就非常容易使用。

客座編輯

Lysandra Capella 在資訊安全和技術領域擁有超過 15 年的工作經驗。她是 系統與網路安全研究協會 SANS AUD507 的學院培訓講師，專注於評估和管理風險。在教學以外的時間，Lysandra 支援執行管理團隊制定策略、安全保障和 IT 治理。 https://www.linkedin.com/in/lysandracapella/。

參考資源

輕鬆設密碼： https://www.sans.org/sites/default/files/2019-04/201904-OUCH-April-Chinese%2CTraditional%28Taiwanese%29.pdf

密碼管理器：

https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt27ecddc00595b1e8/604a690fe122b53af5512eb1/202004-OUCH-Taiwanese.pdf

翻譯：宋亞倫 德欣寰宇科技股份有限公司