

CSCS 2024 工作報告

2024年, CSCS 提供了

- 為不同機構提供 7 次資訊安全培訓, 共約 40 小時
- 4 次資安事件處理
- 3 次資安健檢, 共約 20 小時

我們在服務中觀察到以下趨勢:

- 組織對於使用生成式 AI 感興趣, 同時對其有資料安全疑慮
- 針對性和客製化的網路釣魚電子郵件增加

針對這些趨勢, 我們建議非營利組織

- 在使用線上生成式 AI 工具之前, 詳讀這些工具的服務條款和隱私權政策, 並設定使用這些工具的內部準則
- 未經評估前, 避免將任何非公開資訊提交至線上生成式 AI 工具, 例如電子郵件草稿、會議記錄或錄音、資金提案等
- 提高對網路釣魚的警覺

我們建議組織推行下列簡單的措施:

- 使用分開的瀏覽器和帳號處理工作和私人事務, 例如在工作中使用 Firefox; 私人事務使用 Chrome, 並使用分開的 Google 帳號處理私人和工作。這將區隔不同性質的敏感資訊, 資安事件發生時可以將損害控制在一定範圍。
- 為 Google 和 Facebook 等重要的線上帳戶開啟兩步認證(多因素認證)。
- 改用 Signal messenger 進行敏感通訊。

CSCS 亦舉行了一些內部活動:

- 我們提供了一系列的種子講師培訓課程, 以吸引和招募新的資安講師。這一系列課程共有 12 位新進種子講師參加。
- 我們舉辦了一系列共 8 場的公開編輯松來更新我們的教材(投影片)。這有助於強化社群成員之間的關係, 並吸引外部的貢獻者。所製作的教材在此發佈:
<https://drive.google.com/drive/folders/1CXMIw9jHtBKbt8WfKWG2xZt01rmOgm3f>

展望未來:

- CSCS 將持續培訓我們的新進講師, 擴大我們的服務能力。
- CSCS 將持續舉辦每月一次的公開編輯松。我們歡迎對個人及非營利組織資訊安全有興趣的大眾參加。意者請聯絡 contact@cscs.asia 獲取活動資訊。

CSCS 2024 Activity Report

In 2024, CSCS have provided:

- 7 digital security training to different organizations, totaling about 40 hours
- 4 incident response cases
- 3 digital security health checks (audits), totaling about 20 hours

Through our service, we observe the following trends:

- Organizations are interested in the use of generative AI, while having data security concerns about them.
- Increase in targeted and customized phishing emails.

In response to these trends, we recommend non-profit organizations:

- Evaluate the terms of service and privacy policies of online generative AI tools before using them. Set organizational guidelines for using these tools.
- As a default rule, avoid submitting any non-public information to online generative AI tools, such as email drafts, meeting notes or recordings, funding proposals, and so on.
- Increase awareness of phishing.

Simple and high priority items that we suggest organizations to adopt:

- Use separate browsers and accounts for work and private matters, to better compartmentalize sensitive information, so that the impact of breaches is limited.
- Turn on multi-factor authentication for important online accounts such as Google and Facebook accounts.
- Switch to Signal messenger for sensitive communications.

In addition, we made efforts to strengthen our community's health and sustainability:

- We provided a series of Training of Trainer sessions to attract and recruit new volunteer trainers. This series of sessions were attended by 12 new trainers.
- We held a series of 8 public hackathons to update our teaching materials (slideshows). This helped strengthen the relationship of our community members, and attracted outside contributors. The resulting slideshows (in Traditional Chinese) are published here:

<https://drive.google.com/drive/folders/1CXMIw9jHtBKbt8WfKWG2xZt01rmOgm3f>

Looking forward to the future:

- CSCS aims to continue training our new trainers so we can grow our service capacity.
- CSCS aims to continue organizing public monthly hackathons to update our teaching materials. We welcome attendance from members of the public who are interested in personal and non-profit organizations digital security. For those interested, please contact contact@cscs.asia