Threat Hunting

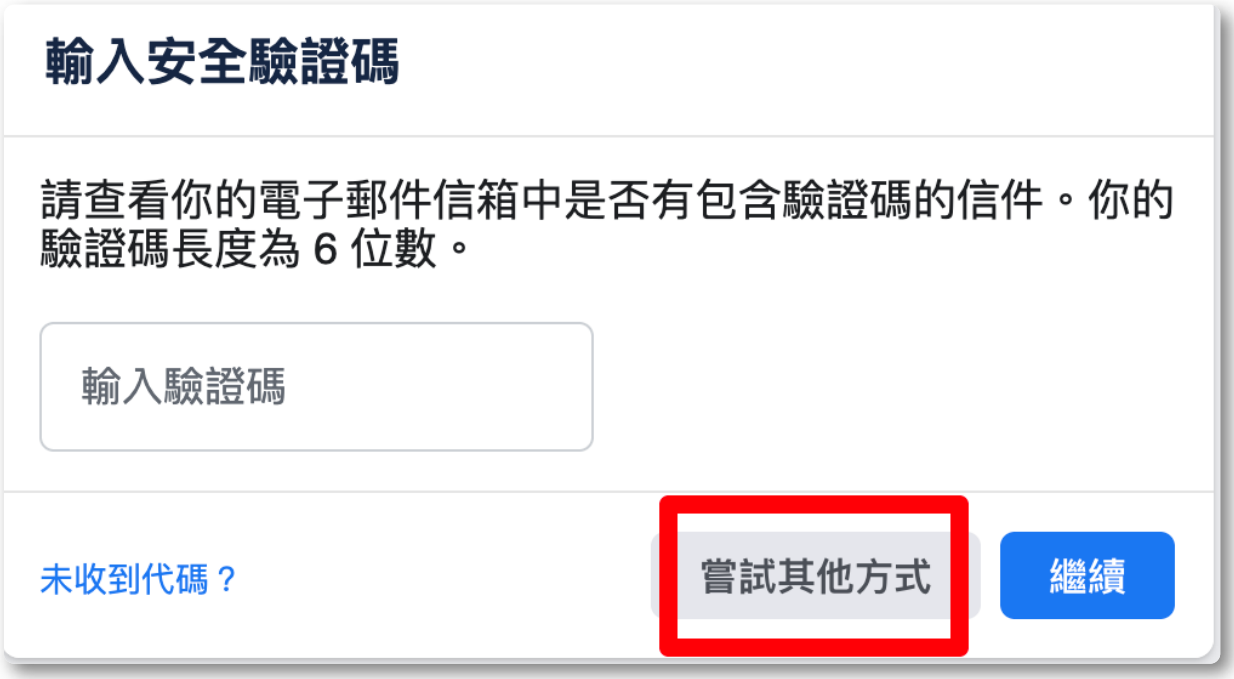
HW11

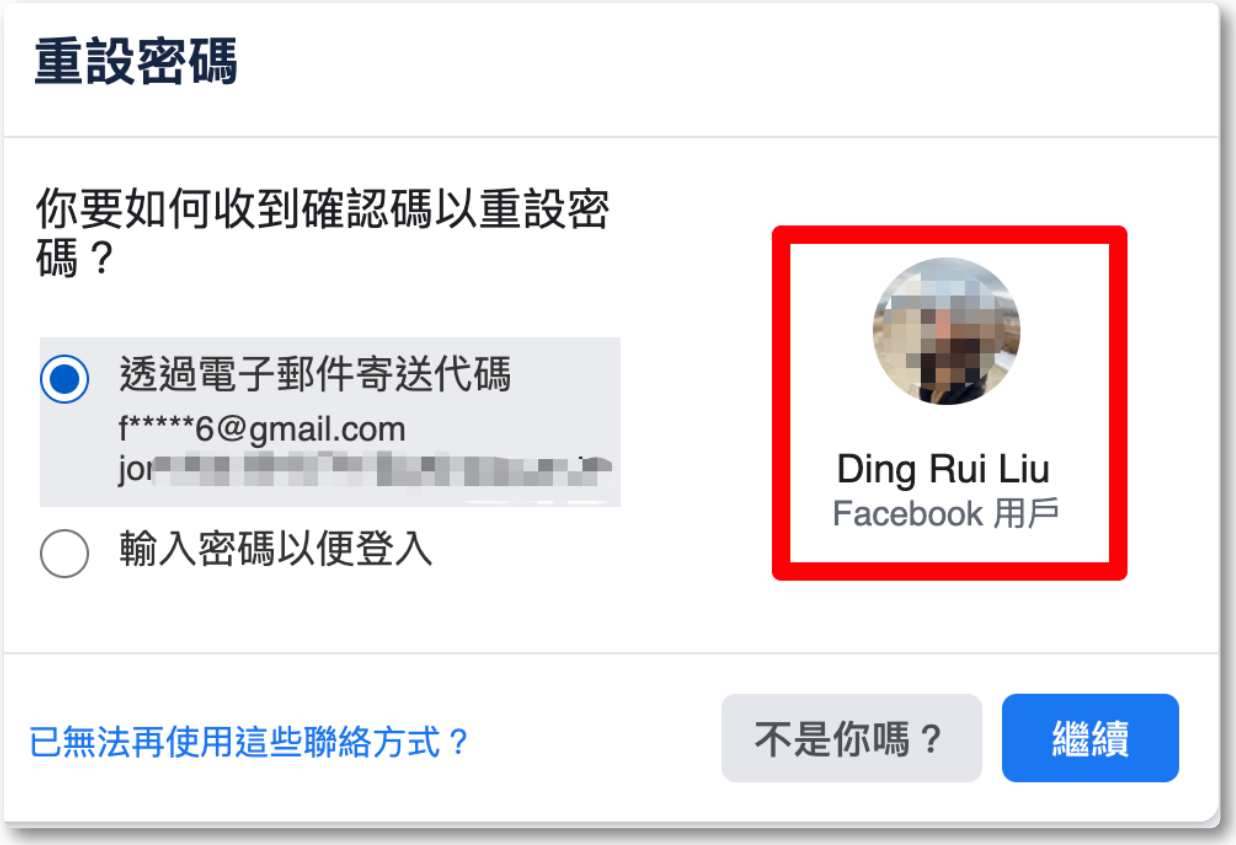
Name: 劉定睿 ID: M11409313

Date: 2025-12-01

目錄

Password Reset Leakage Analysis





- Observed leakage
  - backup account in masked
  - Username
  - Protrait
- Security impact
  - attack can link another email togather.
  - attacker can link the username and email.
  - attacker can confirm the user by protrait. if the different account use the same username.
- Attacker exploitation scenarios
  - send the phishing mail.
  - brute force the password.
  - try to searching the leak database if the email has been suffered leakage incident, attacker can exploit “Credential Stuffing”.
- Recommendations to improve design
  - do not show the personal information in the front-end, api ...

Profile Tracking with Nexfil

- NExfil results :

```
└─$ docker run -it --rm sherlock/sherlock jonafk555
[*] Checking username jonafk555 on:

[+] BugCrowd: https://bugcrowd.com/jonafk555
[+] CryptoHack: https://cryptohack.org/user/jonafk555/
[+] Discord: https://discord.com
[+] Docker Hub: https://hub.docker.com/u/jonafk555/
[+] GitHub: https://www.github.com/jonafk555
[+] GitLab: https://gitlab.com/jonafk555
[+] Gravatar: http://en.gravatar.com/jonafk555
[+] HackMD: https://hackmd.io/@jonafk555
[+] SpeakerDeck: https://speakerdeck.com/jonafk555
[+] TryHackMe: https://tryhackme.com/p/jonafk555
[+] VirusTotal: https://www.virustotal.com/gui/user/jonafk555
[+] WordPress: https://jonafk555.wordpress.com/
[+] YouTube: https://www.youtube.com/@jonafk555
[+] livelib: https://www.livelib.ru/reader/jonafk555

[*] Search completed with 14 results
```

sherlock is the similar tool but better than Nexfil. It can provide the more precision result.

- visualization the intelligence by notebooklm mind map.