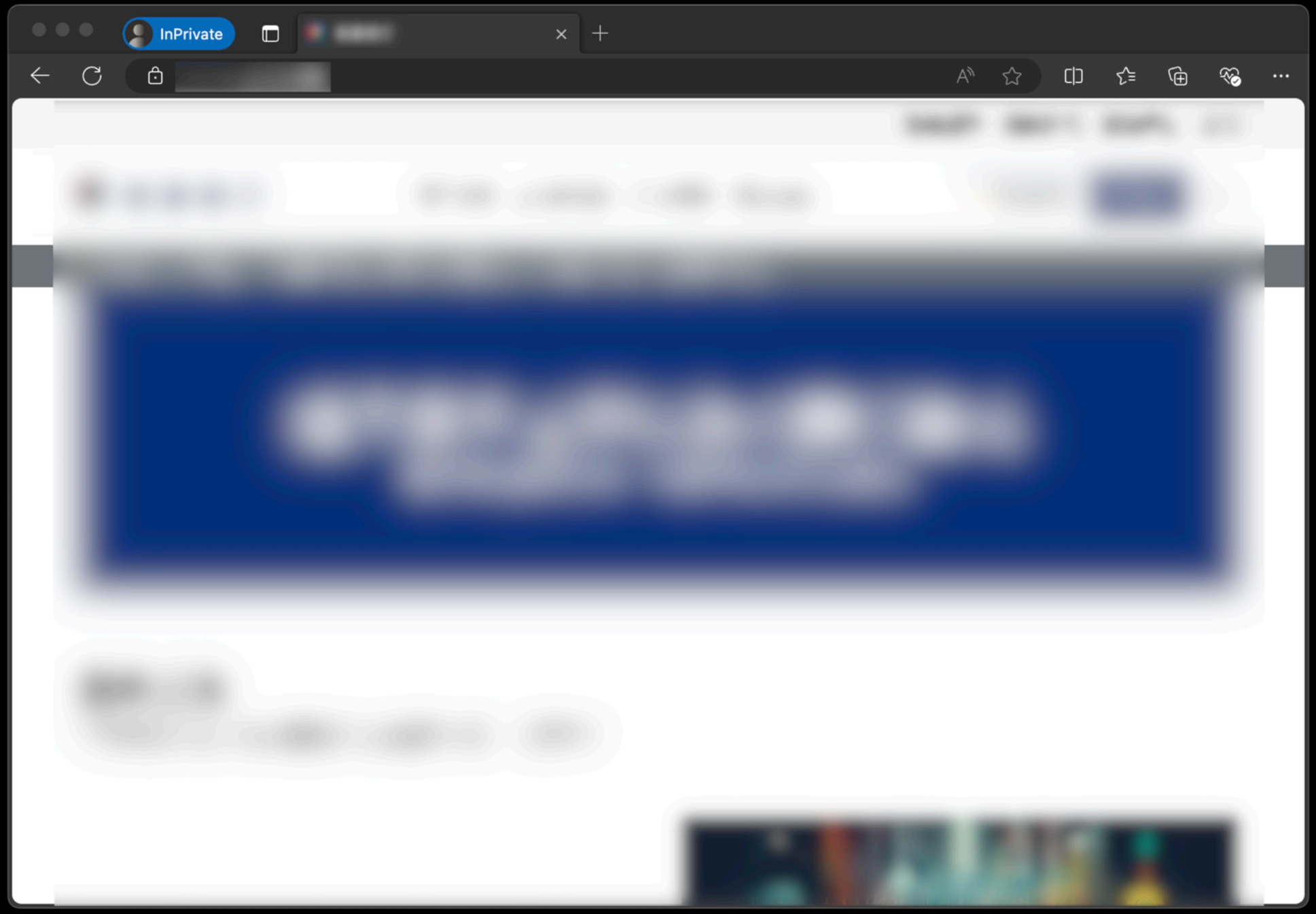
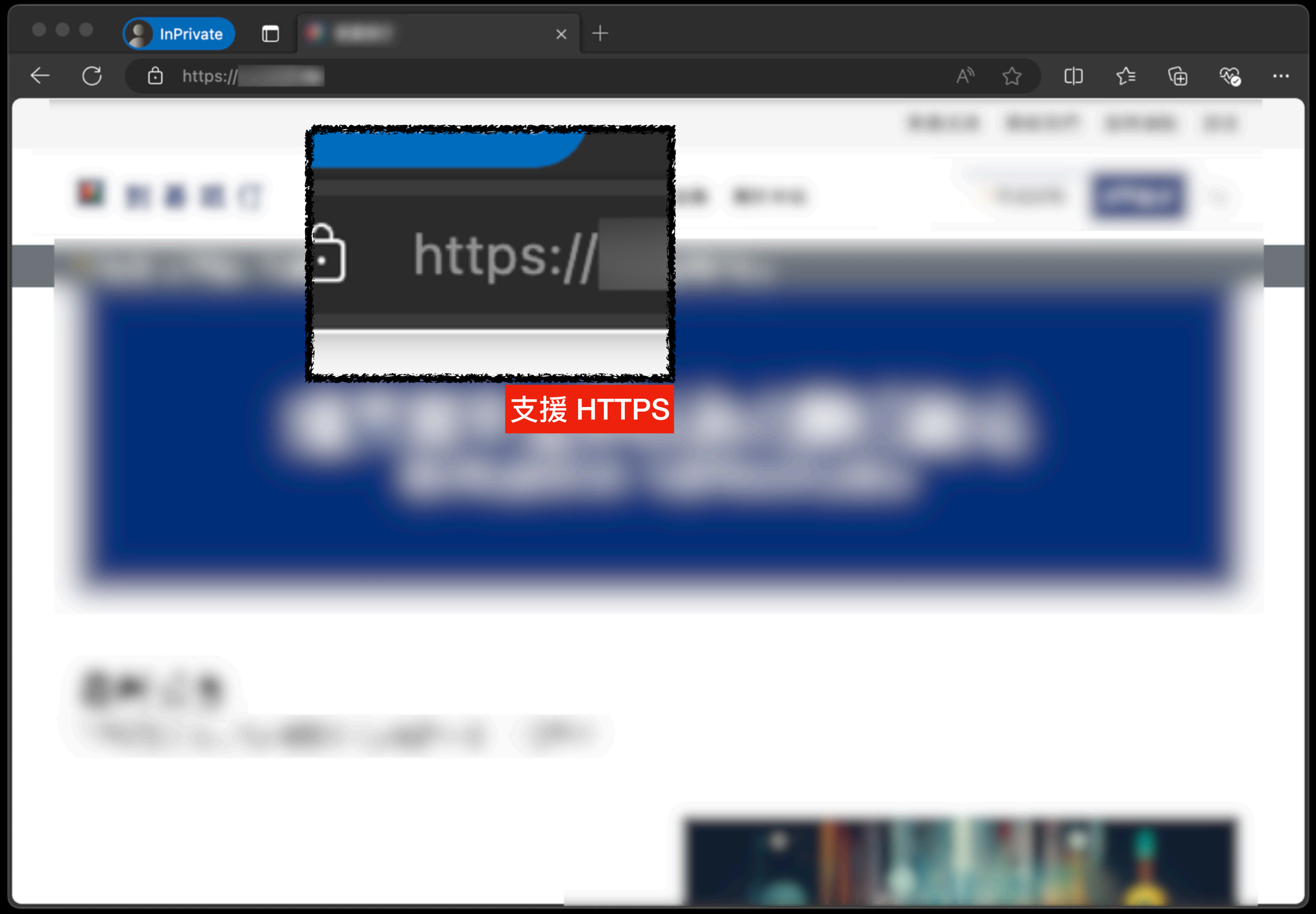
詐騙網站開發經驗分享

小畢 CrBoy

保護當事網站


InPrivate


InPrivate
https://
https://
支援 HTTPS

InPrivate

https://[redacted].tw

集團成員 聯絡我們 服務據點 語言

個人金融 Smart理財 法人金融 關於本站

當然要有些選單跟精美圖片

InPrivate

https://[redacted]k.tw

集團成員 聯絡我們 服務據點 語言

[redacted] 個人金融 Smart理財 法人金融 關於本站 登入網銀 我要申請

[redacted]

按鈕是一定要的

[redacted]

InPrivate

https://[redacted]nk.tw

集團成員 聯絡我們 服務據點 語言

[redacted] 個人金融 Smart理財 法人金融 關於本站 登入網銀 我要申請

[redacted]

哪個正經的網站不發些公告呢

最新消息

[redacted]

InPrivate

https://[redacted]ank.tw

集團成員 聯絡我們 服務據點 語言

[redacted] 個人金融 Smart理財 法人金融 關於本站 登入網銀 我要申請

⚠ 防詐提醒：網站外觀相似，不表示就是真實網站。使用時請注意網址是否正確，並應小心任何看似可疑的連結或網站。

⚠ 防詐提醒：網站外觀相似，不表示就是真實網站。使用時請注意網址是否正確，並應小心任何看似可疑的連結或網站。

提醒使用者避免詐騙！貼心！

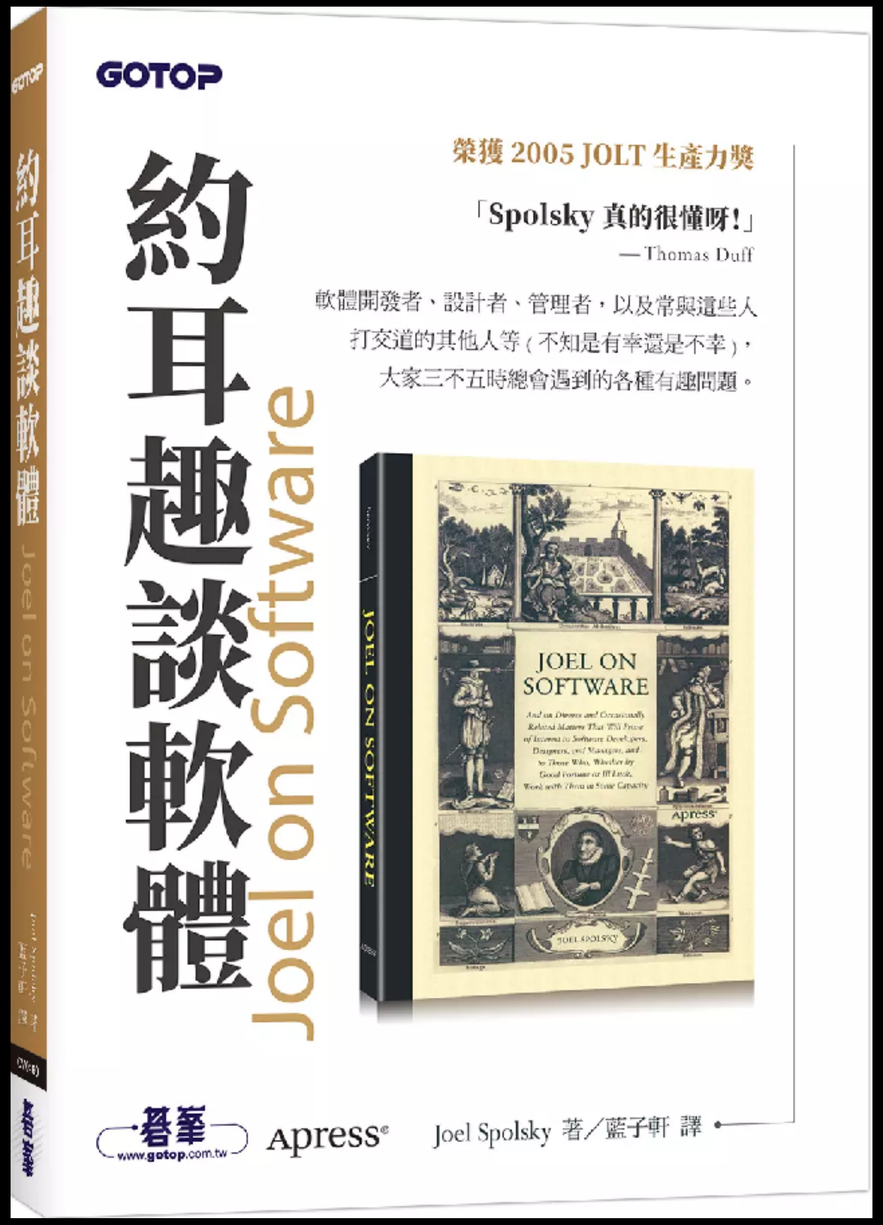
[redacted]

最新消息

[redacted]

身為一個軟體開發者

約耳趣談軟體


GOTOP
約耳趣談軟體
Joel on Software
榮獲 2005 JOLT 生產力獎
「Spolsky 真的很懂呀!」
—Thomas Duff
軟體開發者、設計者、管理者，以及常與這些人
打交道的其他人等（不知是有幸還是不幸），
大家三不五時總會遇到的各種有趣問題。
JOEL ON SOFTWARE
apress
碁峰
www.gotop.com.tw
Apress
Joel Spolsky 著／藍子軒 譯

Joel on Software 繁中備份 / 讓錯的程式看得出錯

此篇文章是從 Joel on Software 繁中翻譯備份而來

讓錯的程式看得出錯 Making Wrong Code Look Wrong

作者：周思博 (Joel Spolsky)
譯：Paul May 梅普華
Wednesday，May 11，2005
屬於 Joel on Software, https://www.joelonsoftware.com/2005/05/11/making-wrong-code-look-wrong/

時間回到 1983 年九月，我第一個真正的工作是在以色列的 Oranim。這家大型麵包工廠每晚都用六個貨機般大的巨型爐子烤出為數十萬的麵包。

我第一次走進那家麵包廠時覺得裡頭實在髒得離譜。爐壁發黃機器生鏽而且到處都是油。

「這裡一直都這麼髒嗎？」我問道。

「什麼？你講這什麼話？」經理回答說。「我們才剛打掃過。這已經是幾週以來最乾淨的時候了。」

說得真好！

我花了好幾個月每天早上打掃才真正瞭解他們的意思。對麵包工廠來說，乾淨是指機器裡沒有生麵糰在烤，垃圾堆裡沒有發酵的麵糰，而且地板上也沒有堆生麵糰。

乾淨並不是指爐子漆得雪白亮麗。爐子大概十年才會漆一次，並不會每天都來一回。乾淨也不是說把油擦得乾乾淨淨。事實上很多機器都得定期上油，一層薄

「讓錯的程式看得出錯」

"Making Wrong Code Look Wrong"

讓詐騙網站看得出詐騙

Make Fraud Site Look fraud

InPrivate

https://[redacted]ank.tw

集團成員 聯絡我們 服務據點 語言

[redacted]

個人金融 Smart理財 法人金融 關於本站

登入網銀 我要申請

防詐提醒：網站外觀相似，不表示就是真實網站。使用時請注意網址是否正確，並應小心任何看似可疑的連結或網站。

🔔 防詐提醒：網站外觀相似，不表示就是真實網站。使用時請注意網址是否正確，並應小心任何看似可疑的連結或網站。

[redacted]

最新消息

[redacted]

InPrivate

https://[redacted]bank.tw

集團成員 聯絡我們 服務據點 語言

[redacted]

個人金融 Smart理財 法人金融 關於本站

登入網銀 我要申請

防詐提醒：網站外觀相似，不表示就是真實網站。使用時請注意網址是否正確，並應小心任何看似可疑的連結或網站。

這其實不是你以為的銀行網站

惡意的詐騙會把網站做得更像讓你難以區分

最新消息

恭喜網站上線！各方祝賀本行越來越有哏，生意興隆！

故事的起源

作者 Dal (Dal)
標題 某銀行PDF帳單 不是用銀行的email 寄來的
時間 Mon Aug 12 20:11:02 2024
看板 creditcard

總算改回PDF帳單
BUT

寄件者 email 不是銀行的
找某寄信公司.com.tw 代發

被Gmail 分到垃圾郵件之外
還有個資疑慮！

(你說PDF有密碼保護呀！部分身分證號的密碼應該沒啥保護作用吧)

--
※ 發信站: 批踢踢實業坊(ptt.cc), 來自: 36.228.208.25 (臺灣)
※ 文章網址: https://www.ptt.cc/bbs/creditcard/M.1723464664.A.F18.html
噓 operatorm : 分類已死 08/12 20:39
噓 catuncle1 : 這位是不是腦筋有問題啊，明明是某銀行.某寄信公司 08/12 21:24
推 lianpig5566 : 就算是[redacted]一樣不是[redacted]網域阿 08/12 21:29
→ Sheng98 : 那要[redacted]銀行背書[redacted].com.tw 是自己 08/12 21:30
→ Sheng98 : 其它網域 08/12 21:30
噓 orange21 : 貓叔可以先搞清楚再嗆嗎xdddddd 08/12 21:48
→ catuncle1 : 是你們搞清楚再嗆，人家銀行找外包，何必非要自己的 08/12 21:50
→ Dal : [redacted].com.tw 是由[redacted] 08/12 21:50
→ Dal : 有限公司)，股東成份裡面應該沒有[redacted] 08/12 21:50
→ Dal : 的人。應該就只是個 資訊服務公司。 08/12 21:50

這位是不是腦筋有問題啊，
明明是 某銀行.某寄信公司

人家銀行找外包，何必非要自己的 mail server 才行

我：？？？？

原PO說不是銀行的，明明
就有 某銀行 ，有問題嗎

其實很多銀行的紙本帳單
都是傳檔案給專門印帳單
的公司印刷、封裝、郵寄
的。申請的時候都放棄這
些權利了

那要 某銀行 背書 某銀行.某寄信公司 .com.tw 是自己其它網域

紙本帳單是銀行自己送嗎?
找郵局會不會有個資疑慮?

最搞笑的是， 某銀行 的官網說：詐騙集團會使用與本行相似的網址發送電子郵件或簡訊，極有可能是要進行詐騙的前置行為

我：👍👍👍👍

用非自身的網域 以後被詐騙集團利用的機會很高

防釣魚教戰一點就是確認網址 寄件人
結果銀行自己沒遵守 造成使用者混淆

「怎麼沒人搞清楚其實你找 Google 或微軟發信也是一種外包」

「蛤叫人家發信不會設 SPF 喔？」

「啊你各位看到網域都不看後面的嗎」

「找外包發信沒問題啊，可是這個外包用自己名義發信捏😆」

「沒有啦網域名稱不能有底線」

「咦進線要求客服重送就會是銀行自己的 domain 喔？」

–當時的我腦袋亂七八糟

「欸我也來看一下我的帳單🧐」

不看不知道，一看嚇一跳😮

- 綜合電子對帳單是用 server@###bank.[發信服務商].com.tw
- 廣告信跟登入成功通知是用 ebanking@###bank.com
- 轉帳交易通知是用 ebanking@mht.###bank.com
- 官網的網址是 https://www.###bank.com.tw/
  - https://www.###bank.com/ 會轉到官網
  - 但是 http://###bank.com/ 會噴 IIS 的 403
- 有人提到的 ###.com 是不通的

寄件者好幾個

網站跟 email 的 domain 不一致

網域名稱沒辦法給人信心

不是漏洞，而是 UX 問題

長得更像是真的網域？

好像大家都會漏掉 .tw

真的漏了😆

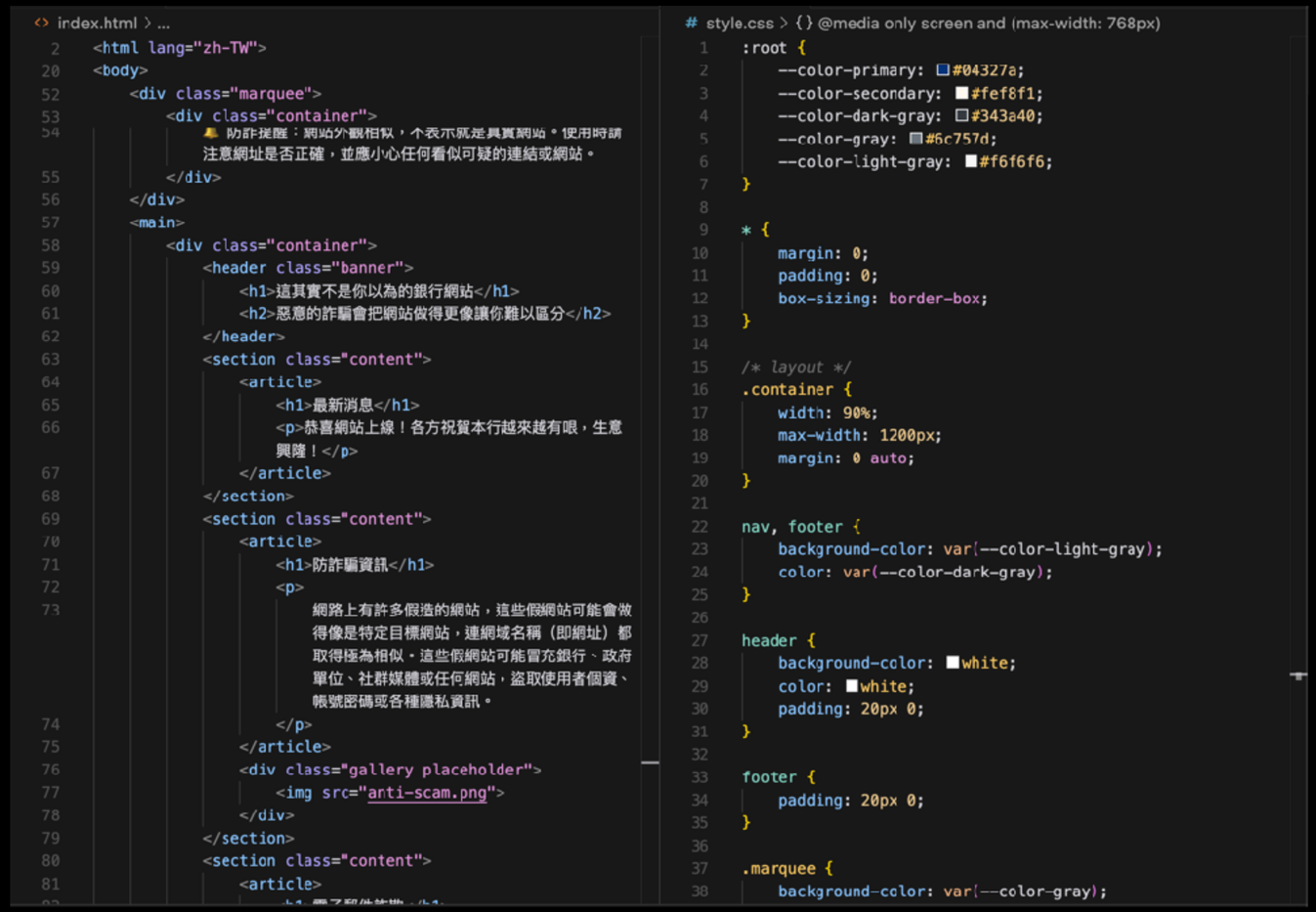
相信最近都有受到感召


拜託ATM
BATTLE
頂尖大學金頭腦爭霸戰
成功大學
TVBS歡樂台 HD
我們是做好駭客

為了避免這個網域被惡意利用

衝動購物

應該要做點什麼



做點即將失傳的傳統手工藝好了

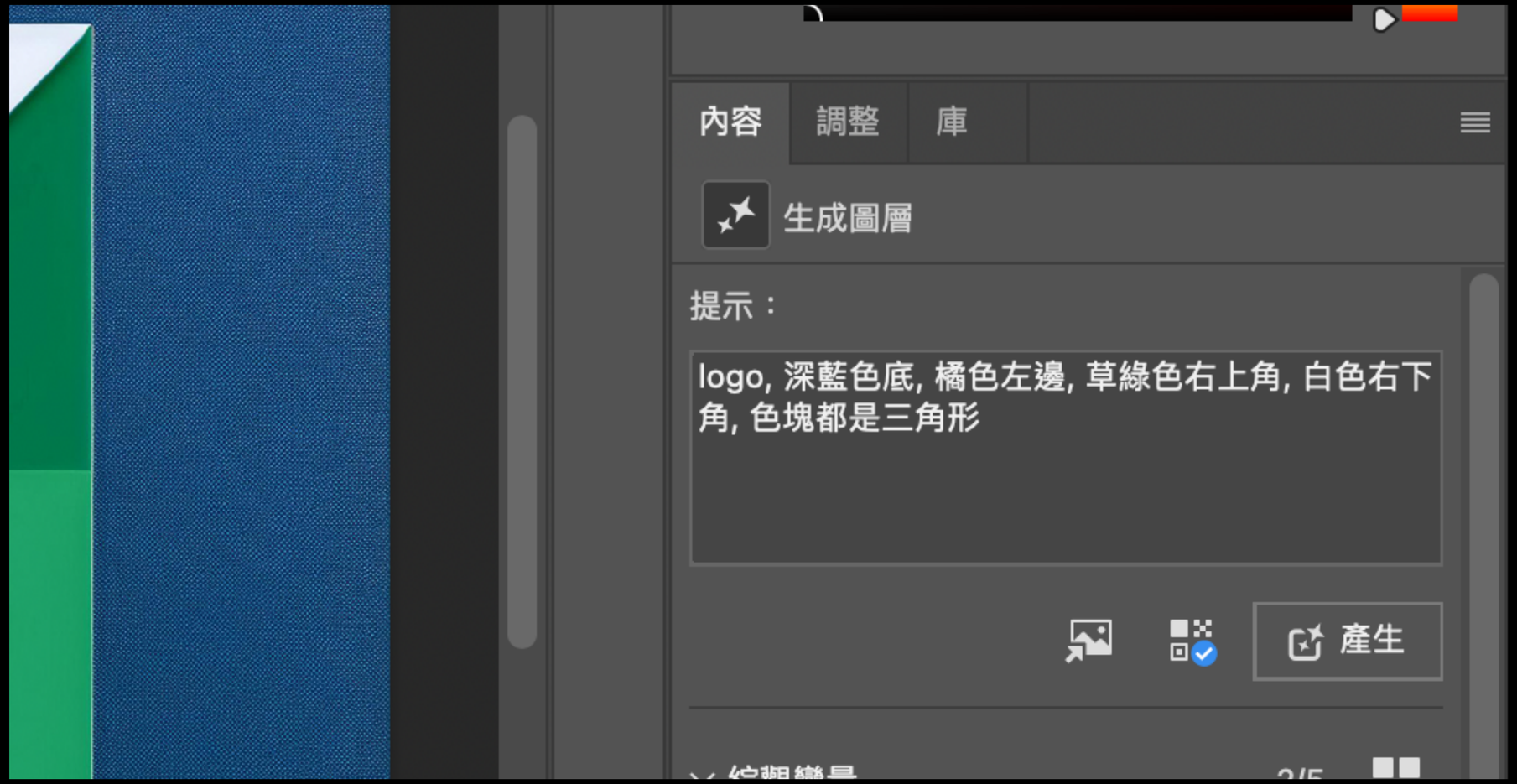
手刻 HTML 與 CSS

懶人版銀行網站誕生

所有連結都沒有用，騙不到人

怕被告，所以...

- 不抄「參考」網站的 code（但是會抄色碼）
- 不偷圖，需要圖片一律靠 AI 產生
- 不做後端，減少被攻擊風險，並減少詐騙疑慮
- 前端放在 GitHub Pages，除了 Google Analytics 以外也不掛 js
- 網站名稱不可以用相同的字

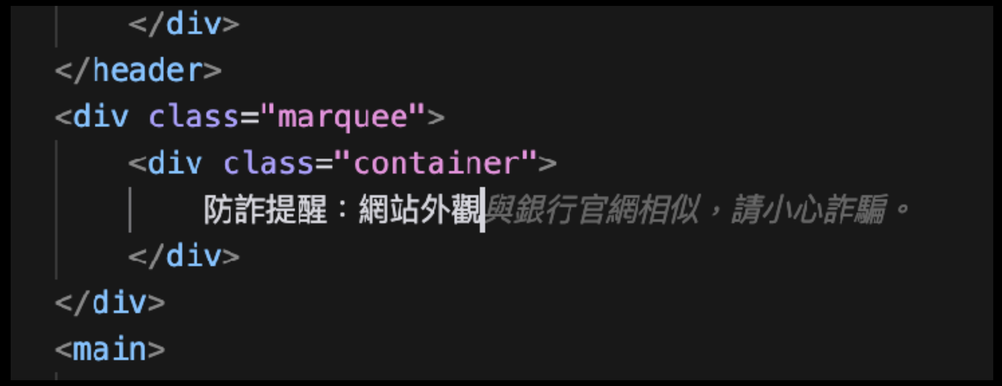


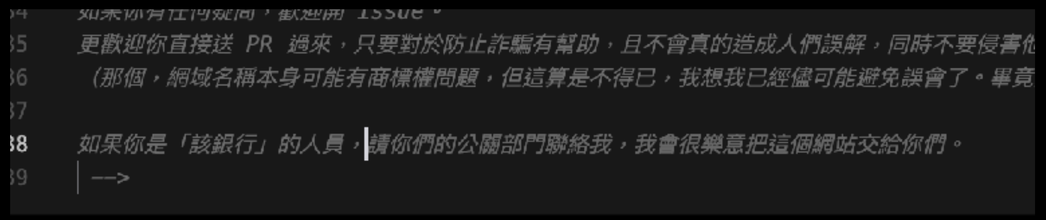
連 logo 都是詠唱成果

(其實失敗很多次)

Cursor

還嘗試了最近很夯的 AI 編輯器





不是幫我寫 code
而是寫內容

想要解決的問題

使用者難以信任網域名稱

明確的網域名稱計畫

- （舉例）
  - 固定使用相同的名稱
  - 明確定義每個名稱（甚至 email）的用途
  - 把容易混淆的名稱買下來，除了轉址到主網站外，不要使用
  - 告訴客戶只需要認得特定網域名稱

銀行的地域性很重要

隨便想幾個銀行來看看

- 這些銀行都有買下「自己名稱.tw」👍
  - x山、中x、永x、x展、x泰、x打、x大、匯x
  - 好像多數沒有在使用，就是放著，也沒做轉址🙃
    - 至少避免了被拿去做壞事的可能
    - UX 還不夠好

該如何委託別人
用我的網域寄信？

直接寄

Email 寄件者可以偽造

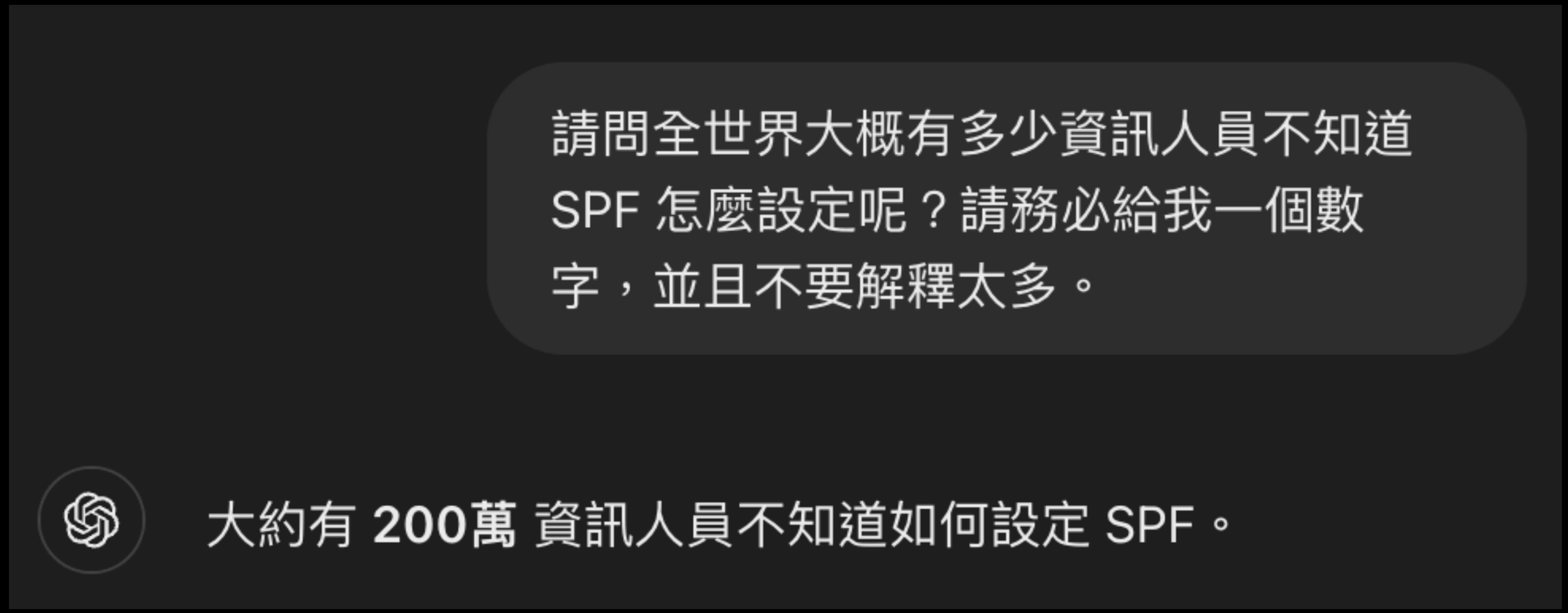
郵件服務商沒那麼笨

Sender Policy Framework (SPF)

在 DNS 寫上「我授權給這些主機幫我發信」

DomainKeys Identified Mail (DKIM)

提供發信主機證明一封信的確是自己發出的，且沒有被竄改



根據可靠(?)的 ChatGPT 告訴我

找 Cloudflare 學電子郵件安全

LT 時間來不及了

上台前才知道 5 分鐘改 4 分鐘 😭😭😭😭😭

跟某銀行聯繫

很快（24 小時內）就接到回電

04:00 -> 19:00

「近期就會改回用自己的網域發信，這個已經在做了。」

–某銀行高階主管

銀行的確會有點緊張

但這不是漏洞，是 UX 問題

稍具規模的企業都需要注意

總結

- 不單純關注安全，還要看你的使用者體驗
- 規範網域名稱計畫，避免使用者混淆
- 買下相似 domain，減少潛在風險
- 如果要請人發信，設定 SPF 跟 DKIM

名稱	直接解析（正反解）	MX	http	https	whois	備註	統整
.com	60.250.	cpseg i.com. mx01 .com.	-	-			
www .com	-	-	-	-	無		
mx01 .com	60.250. 60.250.	-			無		用於 email
cpseg i.com	CNAME to Azure	-	-	Cellopoint Mail Center 顯然有問題的 TLS 憑證	無		
com.tw	-	-	-	-	cherry@ com (		
www com.tw	CNAME to Azure	-	307 to https	302 to /zh-tw/	無	證券網站	用於網站
ank.com	60.251 203.74	M365 (bank-com.ma	IIS error page	-		通知信來源	
www bank.com	60.251	-	302 to https	301 to https://www bank.com.tw/zh-tw/	無		用於 email，看起來像主網域，但網站不在這
mht bank.com	61.218	mhl ank.com.	-	IIS error page		通知信來源	
bank.com.tw	-	-	-	-	bensonh@ .com (		
www bank.com.tw	CNAME to Azure	-	307 to https	302 to /zh-tw/	無	銀行網站	用於網站
60.250.	mx01 com.		-	-	無	AS3462	
60.250.	mx01 com.		-	-	無	AS3462	
60.251	bank.com. mhu bank.com.		IIS error page	-	無	AS3462	
203.74	mhu bank.com.		IIS error page	-	無	AS3462	
60.251	www ank.com.		302 to https	302 to https://www bank.com/creditcardapply/Waiting/waiting.html TLS error	無	AS3462	
61.218.	mht bank.com.		-	IIS error page TLS error	無	AS3462	

Cofacts 真的假的 可疑訊息 最新查核 等你來答 99+ 使用教學

有 1 人想知道以下訊息的真實性

首次回報於 2023年8月1日

國泰世華銀的真正網址是「www.cathaybk.com」，詐騙集團用的網址極為接近，且
因此已有民眾上當，網銀帳戶遭入侵，且將帳戶內款項匯到其他家銀行帳戶，國泰世

www.cathaybk.com」，詐騙集團用的網址極為接近，且客戶點進去後亦是