PRIVACY MYSTERY · CASE FILE 02

藍鵲事件

一封沒有連結的扣款通知，怎麼把人的帳號整個接走？

類型　隱私推理／單人或 2–4 人合作
時間　約 60–90 分鐘
需要　筆、這份檔案、不急著照做的耐心

anoni.net 匿名網路社群 · anoni.net/mystery
玩完的感想與案件的點子：anoni.net/mystery/feedback/
本作品為虛構，人物、公司與事件皆非真實。內容以 CC BY 4.0 授權。

> 最後幾頁是解答，上下顛倒印刷。破案之前，請不要翻到最後。

BRIEFING

遊戲說明

你是「霧港隱私互助站」的志工。我們幫助需要匿名的人，也幫被騙、被冒用、被追蹤的人把自己拿回來。

今晚的委託

上班族**周芷寧**收到一封 BeatBird「睡眠分析進階方案」每月扣款 3,480 的通知。信裡沒有連結，只叫她自己搜尋客服。她照做了，掃了一個「驗證會員身分」的 QR code，隔天朋友就收到「她」傳來的借錢訊息。

更讓她害怕的是：那封信知道她的全名、手機，還知道她最近平均只睡 5 小時 12 分。義務律師把她轉介給互助站。你要拆穿這套詐騙，並找出**是誰把會員資料流了出去**。

你的任務

第一階段・拆穿詐騙　這封信和假網站用了哪些手法？那個 QR code 做了什麼？

第二階段・找出藍鵲　詐騙名單是從哪裡來的？只靠檔案裡的資訊，把六位下載者縮小到一人。答案寫在後面的答題卡上。

規則

- 破案需要的資訊都在檔案 01–10 裡，不需要上網。
- **不要掃描檔案裡的 QR code。**調查員已經用不會開啟連結的工具讀過它，結果在檔案 05。
- 每一條結論都要有**證據**支撐。看起來最可疑的人，不一定是做了這件事的人。
- 卡關時看答題卡後面的提示，每一條都會影響最後的自評。
- 解答在最後，前面有一頁黑色的「停」。

檔案

01　芷寧的加密訊息
02　扣款通知（芷寧收到的信）
03　BeatBird 真的電子報
04　搜尋結果與「會員中心」
05　調查員的查詢紀錄
06　芷寧的手機
07　面具信箱別名與外洩查詢
08　匿名論壇討論串
09　BeatBird 資料保護長的紀錄
10　附錄：網路上查得到的資料

FILE 01

芷寧的加密訊息

2026 年 12 月 9 日（三）晚上，通過端對端加密通訊軟體傳來。

— 安全碼已驗證 • 訊息 24 小時後自動銷毀 —

你好，我是周芷寧。幫我的義務律師說，技術上的事可以找你們。
21:04

我被騙了……應該說，差一點被騙。
21:05

你好，我是今晚值班的志工。你現在安全嗎？
21:06

錢沒有被轉走。可是我的漣漪帳號被別人用了。
21:06

禮拜一晚上我收到一封 BeatBird 的信，說我的「睡眠分析進階方案」已經開通，每個月扣 3,480。
21:07

我根本沒申請過。信裡叫我自己去搜尋「BeatBird 會員中心 官方」看詳情。
21:07

你照著搜尋了？
21:08

對。點了最上面那個，網站跟 BeatBird 長得一模一樣。
21:09

我按「線上客服」，有一位林專員，說要先掃一個 QR code「驗證會員身分」。
21:09

掃完他叫我打開網銀「解除自動扣款」，可是畫面寫的是轉出 29,800。我覺得不對，就掛掉了。
21:10

你做得很對，停在轉帳前面。
21:10

可是隔天，我朋友阿哲問我為什麼要他幫我買遊戲點數。
21:11

我沒有傳過那種訊息。
21:12

還有一件事讓我很怕：那封信知道我的全名、手機，還知道我最近平均只睡 5 小時 12 分。
21:12

那是 BeatBird 手環量的。他們怎麼會知道？
21:13

我們會一起查。你手上有那封信嗎？
21:13

有，我把原始信件、跟阿哲的對話、還有我能截的圖都整理好了。信裡的手機號碼我遮了中間三碼。
21:14

對了，我用面具信箱，每個服務一個別名，清單也放進去了。
21:15

周芷寧傳送了 芷寧給的資料.zip（1.2 MB）· 已接收

收到了。今晚就幫你查。
21:15

謝謝。我會一直在線上。
21:16

FILE 02

扣款通知

芷寧在 12/7 晚上收到的信。上面是郵件程式顯示的樣子，下面是原始郵件的標頭。

周芷寧，睡眠分析進階方案 按月依約延續 3,480 NT

寄件者　"BeatBird 會員中心" <notice@kq3fz.idv.tw>
回覆給　<bb.member.care@mistmail.tw>
收件者　<bb.tidal-fern@maskmail.tw>
日期　Mon, 7 Dec 2026 20:11:58 +0800

親愛的會員您好：周芷寧

您的 BeatBird 睡眠分析進階方案已成功開通，相關配套服務皆已就緒。

- 會員帳號：0937***118
- 綁定裝置：BeatBird Band 3
- 近 30 日平均睡眠：5 小時 12 分
- 服務方案：睡眠分析進階方案（月繳）
- 生效日期：2026-12-07
- 續期方式：按月依約延續
- 每期共計：3,480 NT

- 瀏覽器搜尋 [BeatBird 會員中心 官方] 查看詳情或取消

感謝您的支持，祝您一夜好眠！
BeatBird 營運團隊 敬上
公司地址：台北市內湖區霧港路 588 號 8 樓

原始郵件標頭（節錄）

```
Return-Path: <bounce-7f3a@kq3fz.idv.tw>
Received: from mta3.kq3fz.idv.tw (mta3.kq3fz.idv.tw [203.0.113.47])
        by mx1.maskmail.tw with ESMTPS id 4kTq8Rb2; Mon, 7 Dec 2026 20:12:05 +0800
Authentication-Results: mx1.maskmail.tw;
       spf=pass (mx1.maskmail.tw: domain of bounce-7f3a@kq3fz.idv.tw designates 203.0.11
3.47 as permitted sender) smtp.mailfrom=bounce-7f3a@kq3fz.idv.tw;
       dkim=pass header.d=kq3fz.idv.tw;
       dmarc=none (p=NONE) header.from=kq3fz.idv.tw
X-MaskMail-Alias: bb.tidal-fern@maskmail.tw → zhining.chou@mistmail.tw
From: "BeatBird 會員中心" <notice@kq3fz.idv.tw>
Reply-To: <bb.member.care@mistmail.tw>
To: <bb.tidal-fern@maskmail.tw>
```

FILE 03

BeatBird 真的電子報

芷寧在 11/30 收到的 BeatBird 月報，拿來和扣款通知比一比。

你的 11 月睡眠報告出爐了

寄件者　"BeatBird" <news@beatbird.app>
收件者　<bb.tidal-fern@maskmail.tw>
日期　Mon, 30 Nov 2026 09:00:02 +0800

芷寧，你好：

你的 11 月睡眠報告已經在 App 裡了。打開 BeatBird，點「報告」就能看到。

本月提醒
BeatBird 不會寄信要你搜尋客服、不會要你掃 QR code，也不會要你到 ATM 或網銀「解除扣款」。
訂閱與付款請一律在 App 的「帳號 › 訂閱」查看。

心跳鳥科技股份有限公司
台北市內湖區霧港路 88 號 3 樓

原始郵件標頭（節錄）

```
Return-Path: <bounce@mail.beatbird.app>
Received: from out2.mail.beatbird.app (out2.mail.beatbird.app [198.51.100.20])
        by mx1.maskmail.tw with ESMTPS id 3pQa77Lz; Mon, 30 Nov 2026 09:00:14 +0800
Authentication-Results: mx1.maskmail.tw;
       spf=pass (mx1.maskmail.tw: domain of bounce@mail.beatbird.app designates 198.51.10
0.20 as permitted sender) smtp.mailfrom=bounce@mail.beatbird.app;
       dkim=pass header.d=beatbird.app;
       dmarc=pass (p=REJECT) header.from=beatbird.app
X-MaskMail-Alias: bb.tidal-fern@maskmail.tw → zhining.chou@mistmail.tw
From: "BeatBird" <news@beatbird.app>
To: <bb.tidal-fern@maskmail.tw>
```

FILE 04

搜尋結果與「會員中心」

照信上說的，在霧搜查「BeatBird 會員中心 官方」。最上面三個是廣告；點下去是一個「會員中心」網站。

霧搜：BeatBird 會員中心 官方

BeatBird 會員中心 官方　搜尋

約 4 項結果

贊助 beatbird.app.member-care.com

BeatBird 會員中心｜官方客服 24 小時

訂閱查詢、取消自動續約、退款申請，線上專員立即協助。

贊助 beatbird.app/member

BeatBird 會員中心 官方

扣款有疑問？登入會員中心，三分鐘取消進階方案。

贊助 beatbird-help.app

BeatBird 取消訂閱教學｜官方協助

睡眠分析進階方案取消步驟，專人一對一處理。

beatbird.app

BeatBird 心跳鳥｜睡得好，活得好

公告：近期有人冒用 BeatBird 名義寄送扣款通知。BeatBird 不會要你搜尋客服或操作網銀。

beatbird.app/notice

防詐公告 - BeatBird

訂閱與付款請一律在 App 的「帳號 › 訂閱」查看。BeatBird 不會要求你掃描 QR code。

wuming.forum/t/90417

收到 BeatBird 扣款 3,480 是詐騙嗎？ - 無名廣場

我也收到！金額一樣……最上面的「官方客服」叫我去 ATM 解除分期……

news.mist/beatbird-scam

BeatBird 用戶接連收到假扣款信　公司：已報案、資料保護長調查中｜科技新聞

詐騙信內含用戶姓名與手機。BeatBird 表示已報案，並由新任資料保護長追查資料來源。

會員中心首頁 · beatbird.app.member-care.com

BeatBird 會員中心

首頁　取消自動續約　線上客服

會員中心

訂閱查詢、取消自動續約、退款申請，一次完成。

取消自動續約 →

扣款有疑問？

近期系統升級，部分會員誤開通「睡眠分析進階方案」，請於 24 小時內完成取消，以免持續扣款。

專人協助

聯絡線上客服，林專員一對一為您處理。

© 2026 貝特博德數位科技有限公司　統一編號 87654321
台北市內湖區霧港路 588 號 8 樓　客服信箱 bb.member.care@mistmail.tw

線上客服頁 · beatbird.app.member-care.com/support

BeatBird 會員中心

首頁　取消自動續約　線上客服

線上客服 · 林專員

為確認是會員本人，請用**漣漪 App 掃描**下方 QR code 完成「會員身分驗證」，掃描後專員會立即與您聯繫。

驗證碼 10 分鐘內有效

beatbird_驗證碼.png

若無法掃描，請將驗證碼圖片儲存後於漣漪「設定 › 掃描」選擇圖片。

© 2026 貝特博德數位科技有限公司　統一編號 87654321
台北市內湖區霧港路 588 號 8 樓　客服信箱 bb.member.care@mistmail.tw

FILE 05

調查員的查詢紀錄

調查員在自己電腦上查的網域註冊資料、DNS 紀錄，以及用不會開啟連結的工具讀出的 QR code 內容。

```
$ whois beatbird.app
Domain Name             : beatbird.app
Creation Date           : 2019-03-11
Registrar               : TWNIC 認證註冊商 HiDomain
Registrant Organization : 心跳鳥科技股份有限公司
Registrant Country      : TW
Name Server             : ns1.beatbird.app

$ whois member-care.com
Domain Name             : member-care.com
Creation Date           : 2026-12-02
Registrar               : NameDrop Ltd.
Registrant              : REDACTED FOR PRIVACY
Registrant Country      : REDACTED
Name Server             : ns1.fastparkdns.net

$ whois beatbird-help.app
Domain Name             : beatbird-help.app
Creation Date           : 2026-12-03
Registrar               : NameDrop Ltd.
Registrant              : REDACTED FOR PRIVACY
Registrant Country      : REDACTED
Name Server             : ns1.fastparkdns.net

$ whois xn--batbird-7gg.app
Domain Name             : xn--batbird-7gg.app（顯示為 beatbird.app，第二個字母是西里爾字母 е）
Creation Date           : 2026-12-02
Registrar               : NameDrop Ltd.
Registrant              : REDACTED FOR PRIVACY
Registrant Country      : REDACTED
Name Server             : ns1.fastparkdns.net

$ whois kq3fz.idv.tw
Domain Name             : kq3fz.idv.tw
Creation Date           : 2026-12-01
Registrar               : TWNIC 認證註冊商 QuickReg
Registrant              : REDACTED FOR PRIVACY
Name Server             : ns1.fastparkdns.net
```

```
$ dig txt kq3fz.idv.tw
kq3fz.idv.tw.  300  IN  TXT  "v=spf1 ip4:203.0.113.47 -all"
```

```
$ dig txt beatbird.app
beatbird.app.  300  IN  TXT  "v=spf1 include:_spf.mail.beatbird.app -all"
beatbird.app.  300  IN  TXT  "google-site-verification=0x3bA…"

$ dig txt _dmarc.beatbird.app
_dmarc.beatbird.app.  300  IN  TXT  "v=DMARC1; p=reject; rua=mailto:dmarc@beatbird.app"
```

QR 讀取：beatbird_驗證碼.png

```
解出的內容：ripple://link-device?code=7F3Q-K2PX-9MZD&name=Chrome · Windows
類型：不是網址。ripple:// 是漣漪 App 自己的指令。
動作：link-device，把新裝置連結到帳號（裝置名稱 Chrome · Windows）
```

FILE 06

芷寧的手機

漣漪「已連結的裝置」截圖（12/9 晚上），以及她和朋友阿哲的對話。

漣漪 · 與 阿哲 的對話（周芷寧匯出）

周芷寧 12/08 13:05
在嗎？可以幫我一個忙嗎

周芷寧 12/08 13:05
我現在不方便刷卡，可以先幫我買 5 張 1000 的 GASH 點數嗎？晚上還你

阿哲 12/08 13:07
你在哪？打給你都沒接

周芷寧 12/08 13:07
在開會不方便講電話，序號拍照傳給我就好

阿哲 12/08 18:42
欸你中午那個是怎樣？我差點就去買了

周芷寧 12/08 18:50
我中午沒有傳任何訊息給你！！我一直在公司

阿哲 12/08 18:51
那你帳號被盜了吧，快去處理

FILE 07

面具信箱別名與外洩查詢

芷寧的面具信箱別名清單，以及在「洩了沒」查兩個信箱的結果。

服務	別名	建立日期	備註
BeatBird	bb.tidal-fern@maskmail.tw	2025-03-02	只給 BeatBird 用
StreamBox	sb.quiet-moss@maskmail.tw	2025-06-11	
拾光讀冊	read.amber-cove@maskmail.tw	2025-09-20	
漣漪 Ripple	（用手機號碼註冊）		
好物團購網	zhining.chou@mistmail.tw	2023-11-05	用面具信箱之前註冊的，填的是主信箱

※ 面具信箱：每個別名收到的信都會轉到主信箱 zhining.chou@mistmail.tw，信件標頭會註明是從哪個別名轉來的。

洩了沒：zhining.chou@mistmail.tw

來源	時間	外洩的欄位
好物團購網	2024-04	姓名、電話、Email、收件地址
StreamBox 舊論壇	2021-10	Email、雜湊過的密碼

洩了沒：bb.tidal-fern@maskmail.tw

沒有出現在已知的公開外洩事件裡。

FILE 08

匿名論壇討論串

「無名廣場」科技業板，12 月 6 日的討論。

wuming.forum/t/90417

無名廣場 科技業 › 閒聊

收到 BeatBird 扣款 3,480 是詐騙嗎？

sleepless_dev · 2026-12-06 09:14 · 回覆 318

昨晚收到一封 BeatBird 的信，說我的睡眠分析進階方案開通了，每月 3,480。我根本沒申請。信裡沒有連結，叫我自己搜尋「BeatBird 會員中心 官方」。有人也收到嗎？

回覆

B1 · 12-06 09:30

我也收到！金額一樣，但我根本沒用過什麼進階方案

B2 · 12-06 10:02

我照信上搜尋，最上面的「官方客服」叫我去 ATM 解除分期，掛掉了

B3 · 12-06 12:47

好笑的是我收到的那封連睡眠時數都沒填好，直接寫「近 30 日平均睡眠：{avg_sleep_30d}」，這種大括號是範本沒套好吧

B4 · 12-06 15:21

它知道我的名字跟手機，BeatBird 是不是外洩了？

B5 · 12-06 22:08

聽說浪花行銷有個做數據的最近到處在問信貸，不知道有沒有關係

B6 · 12-07 00:15

不要亂猜人。有問題打 165，官方只會叫你去 App 裡看訂閱

FILE 09

BeatBird 資料保護長的紀錄

阿霧查到詐騙信寄到只給 BeatBird 的別名之後，聯絡了 BeatBird 資料保護長唐啟文。他傳來以下資料，並要求在證據確定之前不要對外講任何名字。

唐啟文（BeatBird 資料保護長）給霧港互助站的說明　2026-12-09

1. 11 月 24 日，公司依合作合約把三份試辦資料放上檔案分享系統：
   F-01 給衡準精算（鼎岳保險委託的外部精算顧問）
   F-02 給浪花行銷（BeatBird Plus 推廣活動）
   F-03 給雲杉數據（App 使用分析）
   各份的欄位見「資料提供紀錄.csv」。

2. 我到任後要求：每一次下載，系統都會在那一份檔案裡多埋一筆「陷阱資料」。
   陷阱資料是不存在的假使用者，只會出現在那一次下載的檔案裡。
   有信箱的陷阱資料，信箱由我們自己監看。哪個陷阱信箱收到信，就代表那一次下載的檔案被拿去用了。
   哪一筆陷阱屬於哪一次下載，見「陷阱名單.csv」；每一次下載是誰、什麼時候，見「下載紀錄.csv」。

3. 11 月 28 日浪花行銷照合約寄出 BeatBird Plus 體驗活動信，用的是專案經理那一份。那封信屬於合約內的正常使用。

4. 請在證據確定之前，不要對外提任何人的名字。

資料提供紀錄.csv

檔案	提供對象	用途	欄位
F-01	衡準精算	保費精算試算（鼎岳保險委託）	user_hash / birth_ym / postcode / device_model / sleep_avg_30 / resting_hr
F-02	浪花行銷	BeatBird Plus 推廣活動	user_hash / name / email / phone / device_model / plan_tier
F-03	雲杉數據	App 使用分析	user_hash / avg_sleep_30d / sleep_score / app_sessions / device_model

※ user_hash 是把會員編號雜湊後的代號，三份檔案用的是同一套。

下載紀錄.csv

下載編號	時間	檔案	下載者	單位	連線位置
D-01	2026-11-25 10:12	F-02	羅美君	浪花行銷	浪花行銷辦公室
D-02	2026-11-25 10:40	F-01	謝明哲	衡準精算	衡準精算辦公室
D-03	2026-11-25 14:05	F-03	戴宇翔	雲杉數據	雲杉數據辦公室

D-04	2026-11-25 14:31	F-02	江柏宇	浪花行銷	浪花行銷辦公室
D-05	2026-11-25 16:02	F-02	何佳穎	浪花行銷	浪花行銷辦公室
D-06	2026-11-26 09:55	F-03	劉怡君	雲杉數據	雲杉數據辦公室
D-07	2026-11-26 23:48	F-03	江柏宇	浪花行銷	住家寬頻（經分享連結 S-1）
D-08	2026-11-27 13:20	F-03	何佳穎	浪花行銷	浪花行銷辦公室（經分享連結 S-1）

※ 分享連結 S-1：雲杉數據的戴宇翔在 11/26 建立，提供浪花行銷依睡眠分群規劃活動。

陷阱名單.csv

陷阱編號	下載編號	假名	信箱
C-01	D-01	林雨萱	yuxuan.lin.k7@maskmail.tw
C-02	D-02	（F-01 沒有姓名欄位）	（F-01 沒有信箱欄位）
C-03	D-03	（F-03 沒有姓名欄位）	（F-03 沒有信箱欄位）
C-04	D-04	陳品妤	pinyu.chen.q2@maskmail.tw
C-05	D-05	許書豪	shuhao.hsu.m9@maskmail.tw
C-06	D-06	（F-03 沒有姓名欄位）	（F-03 沒有信箱欄位）
C-07	D-07	（F-03 沒有姓名欄位）	（F-03 沒有信箱欄位）
C-08	D-08	（F-03 沒有姓名欄位）	（F-03 沒有信箱欄位）

※ 沒有信箱的陷阱資料只能靠 user_hash 追，目前沒有發現被使用。

陷阱信箱收件紀錄.txt

```
陷阱信箱收件紀錄（BeatBird 資料保護室監看） 匯出時間 2026-12-09 20:30

[2026-11-28 10:00] 收件：yuxuan.lin.k7@maskmail.tw
  寄件：BeatBird Plus <plus@beatbird.app>
  主旨：BeatBird Plus 免費體驗 30 天，送給睡不好的你

[2026-12-05 21:44] 收件：shuhao.hsu.m9@maskmail.tw
  寄件："BeatBird 會員中心" <notice@kq3fz.idv.tw>
  主旨：許書豪，睡眠分析進階方案 按月依約延續 3,480 NT
  內文節錄：
    親愛的會員您好：許書豪
    • 會員帳號：0912***107
    • 綁定裝置：BeatBird Band 2
    • 近 30 日平均睡眠：{avg_sleep_30d}
    • 瀏覽器搜尋 [BeatBird 會員中心 官方] 查看詳情或取消

（其他陷阱信箱：沒有收到任何信）
```

FILE 10

附錄：網路上查得到的資料

調查員查得到的公開資訊。

BeatBird 防詐公告（2026-12-07 更新）

近期部分會員收到「睡眠分析進階方案 按月依約延續 3,480 NT」的信件。這不是 BeatBird 寄出的，我們沒有這個方案。BeatBird 的信只會從 @beatbird.app 寄出；我們不會要你搜尋「官方客服」、加入專員的聊天帳號、掃描 QR code，也不會要你到 ATM 或網銀「解除扣款」。

公司登記查詢

統一編號	結果
53018827	心跳鳥科技股份有限公司，台北市內湖區霧港路 88 號 3 樓，2018-11-02 核准設立
87654321	查無登記資料

165 反詐騙專線：假冒 App 扣款、解除分期

- 收到「已開通」「按月扣款」的通知，先不要照信上說的去搜尋客服。自己打開 App，或撥原本就知道的官方電話確認。
- 官方不會要你到 ATM 或網銀「解除扣款」，也不會要你掃 QR code「驗證身分」。
- 通訊軟體被接上陌生裝置：到「已連結的裝置」移除它，開啟兩步驟驗證，並通知親友。

網址怎麼看

網址的「註冊網域」是頂級網域（.com、.app）前面那一段，例如 mail.beatbird.app 的註冊網域是 beatbird.app。註冊網域前面的部分是子網域，網域擁有者想取什麼名字都可以。有些字母看起來和英文一樣，其實是其他文字（例如西里爾字母 е），那就是另一個網域。

ANSWER SHEET

答題卡

每題都要寫下證據來自哪個檔案。

第一階段・拆穿詐騙

1. 這封扣款通知用了哪些手法？

☐ 不放連結，叫你自己去搜尋　☐ 宣稱已經開始扣款，製造急迫感　☐ 用真實的姓名、手機與睡眠資料取得信任　☐ 偽造成 beatbird.app 寄出　☐ 附件夾帶惡意程式

---

2. 假客服要芷寧掃的 QR code 做了什麼？

○ 把她的漣漪帳號連結到詐騙者的電腦　○ 在她手機上安裝監控程式　○ 授權信用卡自動扣款　○ 讓網站取得她的漣漪密碼

---

3. 詐騙名單是用哪兩份資料拼起來的？

☐ F-01（衡準精算）　☐ F-02（浪花行銷）　☐ F-03（雲杉數據）　☐ 2024 年好物團購網外洩名單

第二階段・找出藍鵲

符合打 ○，排除打 ×。

線索	羅美君	何佳穎	江柏宇	戴宇翔	劉怡君	謝明哲
下載了 F-02（有姓名）						
下載了 F-03（有睡眠資料）						
陷阱信箱收到詐騙信						

4. 是誰把資料流出去的？列出至少三條獨立證據。

加分題

B1. 詐騙信的 SPF 和 DKIM 都通過了，為什麼還是假的？

B2. 芷寧的主信箱 2024 年外洩過，裡面也有姓名和手機。為什麼詐騙名單不是從那裡來的？

HINTS

提示

真的卡住再看。用紙遮住，一次只露出一條，並記下看了幾條。

提示 1・信本身
檔案 02 的信裡有沒有連結？它要芷寧做什麼？為什麼「沒有連結」反而讓人放心？

提示 2・寄件人
看檔案 02 的 From 和 Authentication-Results，再和檔案 03 真的電子報比一比。驗證通過的是哪個網域？

提示 3・廣告
檔案 04 的三個廣告，網址看起來都有 beatbird。用附錄「網址怎麼看」找出它們真正的註冊網域。

提示 4・網域的年紀
檔案 05 的 whois：真的 beatbird.app 是什麼時候註冊的？假網站的網域呢？

提示 5・QR code
檔案 05 的 QR 讀取結果，對照檔案 06 的已連結裝置截圖，看那台陌生裝置是什麼時候接上的。

提示 6・名單從哪來
檔案 02 的信寄到哪個信箱？對照檔案 07 的別名清單與外洩查詢。

提示 7・兩份資料
檔案 09 的資料提供紀錄：哪一份有姓名？哪一份有 avg_sleep_30d？下載紀錄裡誰兩份都下載過？

提示 8・陷阱
陷阱信箱收件紀錄裡，哪個陷阱收到的是詐騙信？用陷阱名單對到下載編號，再對到下載紀錄。

停

破案了嗎？

翻過這頁就是真相。還沒寫完答題卡的話，請回到前面。

接下來的解答頁上下顛倒印刷，把整份檔案轉過來就能閱讀。

CASE FILE 02 · SOLVED

真相

藍鵲是何佳穎。浪花行銷的企劃。她把工作上拿到的兩份 BeatBird 試辦資料對在一起，賣給了詐騙集團。

事件經過

11 月 25 日，何佳穎從分享系統下載了 F-02（有姓名、信箱、手機的行銷名單），27 日又透過雲杉數據開給浪花的分享連結，下載了 F-03（有睡眠資料的使用分析）。兩份檔案用的是同一套 user_hash，對起來就得到一份「誰、怎麼聯絡、最近睡多少」的名單。

12 月 1 日起，詐騙集團註冊了寄件網域 kq3fz.idv.tw 與三個假冒 BeatBird 的網域，12 月 5 日開始寄信。芷寧在 12 月 7 日收到，照著搜尋、點了廣告、掃了「驗證身分」的 QR code，漣漪帳號就被接到對方的電腦上。

詐騙怎麼運作

- **沒有連結的信**：信裡不放連結，躲得過郵件過濾，也讓人覺得「不像詐騙」。它只叫你自己去搜尋客服。
- **買來的廣告**：搜尋結果最上面三個「官方客服」都是廣告：品牌放在子網域（beatbird.app.member-care.com）、品牌旁邊加字（beatbird-help.app）、把 e 換成西里爾字母 е（beatbird.app）。三個網域都在詐騙信寄出前幾天才註冊。
- **真實的個資**：姓名、手機、手環型號、睡眠時數，用真資料讓人相信「這是 BeatBird 寄的」。
- **QR code**：「驗證會員身分」解出來是 ripple://link-device，是漣漪的連結新裝置。掃了它，對方的電腦就成了芷寧帳號的一部分，可以讀她的新訊息、用她的名義跟朋友借錢。
- **寄件人**：SPF、DKIM 都通過，但通過的是 kq3fz.idv.tw 自己。驗證只能證明「信真的從這個網域寄出」，不能證明這個網域是 BeatBird。

逐條排除

嫌疑人	F-02（姓名）	F-03（睡眠）	陷阱收到詐騙信
羅美君	D-01	×	C-01 只收到正常的體驗信
何佳穎	D-05	D-08	C-05 ✓
江柏宇	D-04	D-07	C-04 沒有收到
戴宇翔	×	D-03	—
劉怡君	×	D-06	—
謝明哲	×	×（F-01）	—

詐騙信同時用到姓名（F-02）與 avg_sleep_30d（只在 F-03），兩份都下載過的只有何佳穎與江柏宇。陷阱信箱 C-05 收到了詐騙信，而 C-05 只埋在 D-05 那一份，也就是何佳穎下載的 F-02。

陷阱

- **江柏宇**：深夜從住家下載 F-03，論壇上還有人說他在問信貸，看起來最可疑。可是他那份 F-02 的陷阱 C-04 從來沒收過詐騙信。
- **好物團購網外洩**：芷寧的主信箱確實在 2024 年外洩過，裡面也有姓名和手機。但詐騙信寄到的是只給過 BeatBird 的別名，團購網那份名單裡沒有這個別名。
- **假網站的表單**：查假網站只看、不填、不送出。填假資料一樣會讓對方知道有人上鉤。

下次收到這種信

- 「已開通」「按月扣款」的通知：自己打開 App 或撥原本就知道的電話確認，不要照信上說的搜尋客服。
- 看網址先看註冊網域，品牌名放在子網域、旁邊加字、混用其他字母，都是另一個網域。
- 不要用通訊軟體掃別人給的 QR code「驗證身分」。定期打開「已連結的裝置」，移除不認得的裝置，開啟兩步驟驗證。
- 每個服務用不同的 email 別名，外洩時才追得到是從哪裡流出去的。
- 錢已經匯出去：立刻撥 165。

延伸閱讀：一般人平常該做到什麼　・　郵件別名怎麼用，以及它把信任交給誰　・　anoni.net 小工具

答題卡對答案
1. 不放連結、宣稱已開始扣款製造急迫感、用真實個資取得信任（不是偽造 beatbird.app，也沒有附件）　2. 把漣漪帳號連結到詐騙者的電腦　3. F-02 與 F-03
加分 B1：SPF、DKIM 只證明信真的從 kq3fz.idv.tw 寄出，那個網域不是 BeatBird 的。加分 B2：詐騙信寄到只給過 BeatBird 的別名，團購網外洩的是主信箱。
自評　沒看提示、一次指認正確：洋蔥首席調查員　・　看了 3 條以內提示：資深隱私志工　・　其他：見習調查員