

蓝鹊事件

一封没有链接的扣款通知，怎么把人的账号整个接走？

类型 隐私推理／单人或 2-4 人合作

时间 约 60-90 分钟

需要 笔、这份文件、不急着照做的耐心

anoni.net 匿名网络社群 · anoni.net/mystery/zh-cn

玩完的感想与案件的点子：anoni.net/mystery/zh-cn/feedback/

本作品为虚构，人物、公司与事件皆非真实。内容以 CC BY 4.0 授权。

最后几页是解答，上下颠倒印刷。破案之前，请不要翻到最后。

游戏说明

你是「雾港隐私互助站」的志愿者。我们帮助需要匿名的人，也帮被骗、被冒用、被追踪的人把自己拿回来。

今晚的委托

上班族周芷宁收到一封 BeatBird「睡眠分析高端方案」每月扣款 3,480 的通知。信里没有链接，只叫她自己搜索客服。她照做了，扫了一个「验证会员身份」的 QR code，隔天朋友就收到「她」传来的借钱消息。

更让她害怕的是：那封信知道她的全名、手机，还知道她最近平均只睡 5 小时 12 分。165 把她转介给互助站。你要拆穿这套诈骗，并找出是谁把会员数据流了出去。

你的任务

第一阶段·拆穿诈骗 这封信和假网站用了哪些手法？那个 QR code 做了什么？

第二阶段·找出蓝鹊 诈骗名单是从哪里来的？只靠文件里的信息，把六位下载者缩小到一人。答案写在后面的答题卡上。

规则

- 破案需要的信息都在文件 01-10 里，不需要上网。
- 不要扫描文件里的 QR code。** 调查员已经用不会打开链接的工具读过它，结果在文件 05。
- 每一条结论都要有**证据**支撑。看起来最可疑的人，不一定是做了这件事的人。
- 卡关时看答题卡后面的提示，每一条都会影响最后的自评。
- 解答在最后，前面有一页黑色的「停」。

文件

- | | |
|----------------------|-----------------|
| 01 芷宁的加密消息 | 02 扣款通知（芷宁收到的信） |
| 03 BeatBird 真的电子报 | 04 搜索结果与「会员中心」 |
| 05 调查员的查找记录 | 06 芷宁的手机 |
| 07 面具邮箱别名与泄露查找 | 08 匿名论坛讨论串 |
| 09 BeatBird 数据保护长的记录 | 10 附录：网络上查得到的数据 |

芷宁的加密消息

2026 年 12 月 9 日（三）晚上，通过端对端加密通信软件传来。

— 安全码已验证 · 消息 24 小时后自动销毁 —

你好，我是周芷宁，165 的人说可以找你们。

21:04

我被骗了……应该说，差一点被骗。

21:05

你好，我是今晚值班的志愿者。你现在安全吗？

21:06

钱没有被转走。可是我的涟漪账号被别人用了。

21:06

礼拜一晚上我收到一封 BeatBird 的信，说我的「睡眠分析高端方案」已经开通，每个月扣 3,480。

21:07

我根本没申请过。信里叫我自己去搜索「BeatBird 会员中心 官方」查看详情。

21:07

你照着搜索了？

21:08

对。点了最上面那个，网站跟 BeatBird 长得一模一样。

21:09

我按「在线客服」，有一位林专员，说要先扫一个 QR code「验证会员身份」。

21:09

扫完他叫我打开网银「解除自动扣款」，可是画面写的是转出 29,800。我觉得不对，就挂掉了。

21:10

你做得很对，停在转账前面。

21:10

可是隔天，我朋友阿哲问我为什么要他帮我买游戏点卡。

21:11

我没有传过那种消息。

21:12

还有一件事让我很怕：那封信知道我的全名、手机，还知道我最近平均只睡 5 小时 12 分。
21:12

那是 BeatBird 手环量的。他们怎么会知道？
21:13

我们会一起查。你手上有那封信吗？
21:13

有，我把原始信件、跟阿哲的对话、还有我能截的图都整理好了。
21:14

对了，我用面具邮箱，每个服务一个别名，清单也放进去了。
21:15

周芷宁发送了 芷宁给的资料.zip (1.2 MB) • 已接收

收到了。今晚就帮你查。
21:15

谢谢。我会一直在在线。
21:16

扣款通知

芷宁在 12/7 晚上收到的信。上面是邮件程序显示的样子，下面是原始邮件的邮件头。

周芷宁，睡眠分析高端方案 按月依约延续 3,480 NT

发件人 "BeatBird 会员中心" <notice@kq3fz.idv.tw>
回复给 <bb.member.care@mistmail.tw>
收件人 <bb.tidal-fern@maskmail.tw>
日期 Mon, 7 Dec 2026 20:11:58 +0800

亲爱的会员您好：周芷宁

您的 BeatBird 睡眠分析高端方案已成功开通，相关配套服务皆已就绪。

- 会员账号：0937264118
 - 绑定设备：BeatBird Band 3
 - 近 30 日平均睡眠：5 小时 12 分
 - 服务方案：睡眠分析高端方案（月缴）
 - 生效日期：2026-12-07
 - 续期方式：按月依约延续
 - 每期共计：3,480 NT
-
- 浏览器搜索 [BeatBird 会员中心 官方] 查看详情或取消

感谢您的支持，祝您一夜好眠！

BeatBird 营运团队 敬上

公司地址：台北市内湖区瑞光路 588 号 8 楼

原始邮件头（节录）

```
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 203.0.113.47 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 会员中心" <notice@kq3fz.idv.tw>
Reply-To: <bb.member.care@mistmail.tw>
To: <bb.tidal-fern@maskmail.tw>
```

BeatBird 真的电子报

芷宁在 11/30 收到的 BeatBird 月报，拿来和扣款通知比一比。

你的 11 月睡眠报告出炉了

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

芷宁，你好：

你的 11 月睡眠报告已经在 App 里了。打开 BeatBird，点「报告」就能看到。

本月提醒

BeatBird 不会寄信要你搜索客服、不会要你扫 QR code，也不会要你到 ATM 或网银「解除扣款」。
订阅与付款请一律在 App 的「账号」订阅」查看。

心跳鸟科技股份有限公司
台北市内湖区洲子街 88 号 3 楼

原始邮件头（节录）

```
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>
```

搜索结果与「会员中心」

照信上说的，在雾搜查「BeatBird 会员中心 官方」。最上面三个是广告；点下去是一个「会员中心」网站。

雾搜：BeatBird 会员中心 官方

BeatBird 会员中心 官方

搜索

约 4 项结果

赞助 beatbird.app.member-care.com

BeatBird 会员中心 | 官方客服 24 小时

订阅查找、取消自动续约、退款申请，在线专员立即协助。

赞助 beatbird.app/member

BeatBird 会员中心 官方

扣款有疑问？登录会员中心，三分钟取消高端方案。

赞助 beatbird-help.app

BeatBird 取消订阅教学 | 官方协助

睡眠分析高端方案取消步骤，专人一对一处理。

beatbird.app

BeatBird 心跳鸟 | 睡得好，活得好

公告：近期有人冒用 BeatBird 名义寄送扣款通知。BeatBird 不会要你搜索客服或操作网银。

beatbird.app/notice

防诈公告 - BeatBird

订阅与付款请一律在 App 的「账号 > 订阅」查看。BeatBird 不会要求你扫描 QR code。

wuming.forum/t/90417

收到 BeatBird 扣款 3,480 是诈骗吗？ - 无名广场

我也收到！金额一样……最上面的「官方客服」叫我去 ATM 解除分期……

news.mist/beatbird-scam

BeatBird 用户接连收到假扣款信 公司：已报案、数据保护长调查中 | 科技新闻

诈骗信内含用户姓名与手机。BeatBird 表示已报案，并由新任数据保护长追查数据源。

会员中心首页 · beatbird.app.member-care.com

BeatBird 会员中心

[首页](#) [取消自动续约](#) [在线客服](#)

会员中心

订阅查找、取消自动续约、退款申请，一次完成。

[取消自动续约 →](#)

扣款有疑问？

近期系统升级，部分会员误开通「睡眠分析高端方案」，请于 24 小时内完成取消，以免持续扣款。

专人协助

[联系在线客服](#)，林专员一对一为您处理。

© 2026 贝特博德数字科技有限公司 统一编号
87654321
台北市内湖区瑞光路 588 号 8 楼 客服邮箱
bb.member.care@mistmail.tw

在线客服页 · beatbird.app.member-care.com/support

BeatBird 会员中心

[首页](#) [取消自动续约](#) [在线客服](#)

在线客服 · 林专员

为确认是会员本人，请用**涟漪 App** 扫描下方二维码完成「会员身份验证」，扫描后专员会立即与您联系。



验证码 10 分钟内有效

beatbird_验证码.png

若无法扫描，请将验证码图片保存后于涟漪「设置」扫描」选择图片。

© 2026 贝特博德数字科技有限公司 统一编号
87654321
台北市内湖区瑞光路 588 号 8 楼 客服邮箱
bb.member.care@mistmail.tw

调查员的查找记录

调查员在自己电脑上查的域名注册数据、DNS 记录，以及用不会打开链接的工具读出的 QR code 内容。

```
$ whois beatbird.app
Domain Name           : beatbird.app
Creation Date         : 2019-03-11
Registrar            : TWNIC 认证注册商 HiDomain
Registrant Organization : 心跳鸟科技股份有限公司
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 (显示为 beatbird.app, 第二个字母是西里尔字母 e)
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 认证注册商 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 读取: beatbird_验证码.png

解出的内容: ripple://link-device?code=7F3Q-K2PX-9MZD&name=Chrome · Windows
类型: 不是网址。ripple:// 是涟漪 App 自己的命令。
动作: link-device, 把新设备关联到账号 (设备名称 Chrome · Windows)

芷宁的手机

涟漪「已关联的设备」截图（12/9 晚上），以及她和朋友阿哲的对话。



涟漪 · 与 阿哲 的对话（周芷宁导出）

周芷宁 12/08 13:05

在吗？可以帮我一个忙吗

周芷宁 12/08 13:05

我现在不方便刷卡，可以先帮我买 5 张 1000 的 GASH 点数吗？晚上还你

阿哲 12/08 13:07

你在哪？打给你都没接

周芷宁 12/08 13:07

在开会不方便讲电话，序号拍照传给我就好

阿哲 12/08 18:42

欸你中午那个是怎样？我差点就去买了

周芷宁 12/08 18:50

我中午没有传任何消息给你！！我一直在公司

阿哲 12/08 18:51

那你账号被盗了吧，快去处理

面具邮箱别名与泄露查找

芷宁的面具邮箱别名清单，以及在「泄了没」查两个邮箱的结果。

服务	别名	创建日期	备注
BeatBird	bb.tidal-fern@maskmail.tw	2025-03-02	只给 BeatBird 用
StreamBox	sb.quiet-moss@maskmail.tw	2025-06-11	
拾光读册	read.amber-cove@maskmail.tw	2025-09-20	
涟漪 Ripple	(用手机号码注册)		
好物团购网	zhining.chou@mistmail.tw	2023-11-05	用面具邮箱之前注册的，填的是主邮箱

※ 面具邮箱：每个别名收到的信都会转到主邮箱 zhining.chou@mistmail.tw，信件邮件头会注明是从哪个别名转来的。

泄了没：zhining.chou@mistmail.tw

来源	时间	泄露的字段
好物团购网	2024-04	姓名、电话、Email、收件地址
StreamBox 旧论坛	2021-10	Email、哈希过的密码

泄了没：bb.tidal-fern@maskmail.tw

没有出现在已知的公开泄露事件里。

匿名论坛讨论串

「无名广场」科技业板，12 月 6 日的讨论。

wuming.forum/t/90417

无名广场 科技业 › 闲聊

收到 BeatBird 扣款 3,480 是诈骗吗？

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

昨晚收到一封 BeatBird 的信，说我的睡眠分析高端方案开通了，每月 3,480。我根本没申请。信里没有链接，叫我自己搜索「BeatBird 会员中心 官方」。有人也收到吗？

回复

B1 · 12-06 09:30

我也收到！金额一样，但我根本没用过什么高端方案

B2 · 12-06 10:02

我照信上搜索，最上面的「官方客服」叫我去 ATM 解除分期，挂掉了

B3 · 12-06 12:47

好笑的是我收到的那封连睡眠时数都没填好，直接写「近 30 日平均睡眠：{avg_sleep_30d}」，这种大括号是模板没套好吧

B4 · 12-06 15:21

它知道我的名字跟手机，BeatBird 是不是泄露了？

B5 · 12-06 22:08

听说浪花行销有个做数据的最近到处在问信贷，不知道有没有关系

B6 · 12-07 00:15

不要乱猜人。有问题打 165，官方只会叫你去 App 里看订阅

BeatBird 数据保护长的记录

阿雾查到诈骗信寄到只给 BeatBird 的别名之后，联系了 BeatBird 数据保护长唐启文。他传来以下数据，并要求在证据确定之前不要对外讲任何名字。

唐启文（BeatBird 数据保护长）给雾港互助站的说明 2026-12-09

1. 11 月 24 日，公司依合作合约把三份试办数据放上文件分享系统：
F-01 给衡准精算（鼎岳保险委托的外部精算顾问）
F-02 给浪花行销（BeatBird Plus 推广活动）
F-03 给云杉数据（App 使用分析）
各份的字段见「数据提供记录.csv」。

2. 我到任后要求：每一次下载，系统都会在那一份文件里多埋一条「陷阱数据」。
陷阱数据是不存在的假用户，只会出现在那一次下载的文件里。
有邮箱的陷阱数据，邮箱由我们自己监看。哪个陷阱邮箱收到信，就代表那一次下载的文件被拿去用了。
哪一笔陷阱属于哪一次下载，见「陷阱名单.csv」；每一次下载是谁、什么时候，见「下载记录.csv」。

3. 11 月 28 日浪花行销照合约发出 BeatBird Plus 体验活动信，用的是项目经理那一份。那封信属于合约内的正常使用。

4. 请在证据确定之前，不要对外提任何人的名字。

数据提供记录.csv

文件	提供对象	用途	字段
F-01	衡准精算	保费精算试算（鼎岳保险委托）	user_hash / birth_ym / postcode / device_model / sleep_avg_30 / resting_hr
F-02	浪花行销	BeatBird Plus 推广活动	user_hash / name / email / phone / device_model / plan_tier
F-03	云杉数据	App 使用分析	user_hash / avg_sleep_30d / sleep_score / app_sessions / device_model

※ user_hash 是把会员编号哈希后的代号，三份文件用的是同一套。

下载记录.csv

下载编号	时间	文件	下载者	单位	连接位置
D-01	2026-11-25 10:12	F-02	罗美君	浪花行销	浪花行销办公室
D-02	2026-11-25 10:40	F-01	谢明哲	衡准精算	衡准精算办公室
D-03	2026-11-25 14:05	F-03	戴宇翔	云杉数据	云杉数据办公室

D-04	2026-11-25 14:31	F-02	江柏宇	浪花行销	浪花行销办公室
D-05	2026-11-25 16:02	F-02	何佳颖	浪花行销	浪花行销办公室
D-06	2026-11-26 09:55	F-03	刘怡君	云杉数据	云杉数据办公室
D-07	2026-11-26 23:48	F-03	江柏宇	浪花行销	住家宽带（经分享链接 S-1）
D-08	2026-11-27 13:20	F-03	何佳颖	浪花行销	浪花行销办公室（经分享链接 S-1）

※ 分享链接 S-1：云杉数据的戴宇翔在 11/26 创建，提供浪花行销依睡眠分群规划活动。

陷阱名单.csv

陷阱编号	下载编号	假名	邮箱
C-01	D-01	林雨萱	yuxuan.lin.k7@maskmail.tw
C-02	D-02	(F-01 没有姓名字段)	(F-01 没有邮箱字段)
C-03	D-03	(F-03 没有姓名字段)	(F-03 没有邮箱字段)
C-04	D-04	陈品妤	pinyu.chen.q2@maskmail.tw
C-05	D-05	许书豪	shuhao.hsu.m9@maskmail.tw
C-06	D-06	(F-03 没有姓名字段)	(F-03 没有邮箱字段)
C-07	D-07	(F-03 没有姓名字段)	(F-03 没有邮箱字段)
C-08	D-08	(F-03 没有姓名字段)	(F-03 没有邮箱字段)

※ 没有邮箱的陷阱数据只能靠 user_hash 追，目前没有发现被使用。

陷阱邮箱收件记录.txt

```
陷阱邮箱收件记录（BeatBird 数据保护室监看） 导出时间 2026-12-09 20:30

[2026-11-28 10:00] 收件: yuxuan.lin.k7@maskmail.tw
发件: BeatBird Plus <plus@beatbird.app>
主题: BeatBird Plus 免费体验 30 天，送给睡不好的你

[2026-12-05 21:44] 收件: shuhao.hsu.m9@maskmail.tw
发件: "BeatBird 会员中心" <notice@kq3fz.idv.tw>
主题: 许书豪，睡眠分析高端方案 按月依约延续 3,480 NT
内文节录：
  亲爱的会员您好：许书豪
  • 会员账号：0912558107
  • 绑定设备：BeatBird Band 2
  • 近 30 日平均睡眠：{avg_sleep_30d}
  • 浏览器搜索 [BeatBird 会员中心 官方] 查看详情或取消

（其他陷阱邮箱：没有收到任何信）
```

附录：网络上查得到的数据

调查员查得到的公开信息。

BeatBird 防诈公告（2026-12-07 更新）

近期部分会员收到「睡眠分析高端方案 按月依约延续 3,480 NT」的信件。这不是 BeatBird 发出的，我们没有这个方案。BeatBird 的信只会从 @beatbird.app 发出；我们不会要你搜索「官方客服」、加入专员的聊天账号、扫描 QR code，也不会要你到 ATM 或网银「解除扣款」。

公司登记查找

统一编号	结果
53018827	心跳鸟科技股份有限公司，台北市内湖区洲子街 88 号 3 楼，2018-11-02 核准设立
87654321	查无登记数据

165 反诈骗专线：假冒 App 扣款、解除分期

- 收到「已开通」「按月扣款」的通知，先不要照信上说的去搜索客服。自己打开 App，或拨原本就知道的官方电话确认。
- 官方不会要你到 ATM 或网银「解除扣款」，也不会要你扫 QR code「验证身份」。
- 通信软件被接上陌生设备：到「已关联的设备」移除它，打开两步骤验证，并通知亲友。

网址怎么看

网址的「注册域名」是顶级域名（.com、.app）前面那一段，例如 mail.beatbird.app 的注册域名是 beatbird.app。注册域名前面的部分是子域名，域名所有者想取什么名字都可以。有些字母看起来和英文一样，其实是其他文本（例如西里尔字母 e），那就是另一个域名。

答题卡

每题都要写下证据来自哪个文件。

第一阶段・拆穿诈骗

1. 这封扣款通知用了哪些手法？

- ☐ 不放链接，叫你自己去搜索
- ☐ 宣称已经开始扣款，制造急迫感
- ☐ 用真实的姓名、手机与睡眠数据取得信任
- ☐ 伪造成 beatbird.app 发出
- ☐ 附件夹带恶意程序

2. 假客服要芷宁扫的 QR code 做了什么？

- ☐ 把她的涟漪账号关联到诈骗者的电脑
- ☐ 在她手机上安装监控程序
- ☐ 授权信用卡自动扣款
- ☐ 让网站取得她的涟漪密码

3. 诈骗名单是用哪两份数据拼起来的？

- ☐ F-01（衡准精算）
- ☐ F-02（浪花行销）
- ☐ F-03（云杉数据）
- ☐ 2024 年好物团购网泄露名单

第二阶段・找出蓝鹊

符合打 ○，排除打 ×。

线索	罗美君	何佳颖	江柏宇	戴宇翔	刘怡君	谢明哲
下载了 F-02（有姓名）						
下载了 F-03（有睡眠数据）						
陷阱邮箱收到诈骗信						

4. 是谁把数据流出去的？列出至少三条独立证据。

加分题

B1. 诈骗信的 SPF 和 DKIM 都通过了，为什么还是假的？

B2. 芷宁的主邮箱 2024 年泄露过，里面也有姓名和手机。为什么诈骗名单不是从那里来的？

提示

真的卡住再看。用纸遮住，一次只露出一条，并记下看了几条。

提示 1 • 信本身

文件 02 的信里有没有链接？它要芷宁做什么？为什么「没有链接」反而让人放心？

提示 2 • 发件人

看文件 02 的 From 和 Authentication-Results，再和文件 03 真的电子报比一比。验证通过的是哪个域名？

提示 3 • 广告

文件 04 的三个广告，网址看起来都有 beatbird。用附录「网址怎么看」找出它们真正的注册域名。

提示 4 • 域名的年纪

文件 05 的 whois：真的 beatbird.app 是什么时候注册的？假网站的域名呢？

提示 5 • QR code

文件 05 的 QR 读取结果，对照文件 06 的已关联设备截图，看那台陌生设备是什么时候接上的。

提示 6 • 名单从哪来

文件 02 的信寄到哪个邮箱？对照文件 07 的别名清单与泄露查找。

提示 7 • 两份数据

文件 09 的数据提供记录：哪一份有姓名？哪一份有 avg_sleep_30d？下载记录里谁两份都下载过？

提示 8 • 陷阱

陷阱邮箱收件记录里，哪个陷阱收到的是诈骗信？用陷阱名单对到下载编号，再对到下载记录。

停

破案了吗？

翻过这页就是真相。还没写完答题卡的话，请回到前面。

接下来的解答页上下颠倒印刷，把整份文件转过来就能阅读。

真相

蓝荫是何佳颖。浪花行销的企划。她把工作上拿到的两份 BeatBird 试办数据对在一起，卖给了诈骗集团。

事件经过

11 月 25 日，何佳颖从分享系统下载了 F-02（有姓名、邮箱、手机的行销名单），27 日又通过云杉数据开始浪花的分享链接，下载了 F-03（有睡眠数据的使用分析）。两份文件用的是同一套 user_hash，对起来就得到一份「谁、怎么联系、最近睡多少」的名单。

12 月 1 日起，诈骗集团注册了发件域名 kq3tz.idv.tw 与三个假冒 BeatBird 的域名，12 月 5 日开始寄信。芷宁在 12 月 7 日收到，照着搜索、点了广告、扫了「验证身份」的 QR code，涟漪账号就被接到对方的电脑上。

诈骗怎么运行

- **没有链接的信**：信里不放链接，躲得过邮件过滤，也让人觉得「不像诈骗」。它只叫你自己去搜索客服。
- **买来的广告**：搜索结果最上面三个「官方客服」都是广告：品牌放在子域名 (beatbird.app.member-care.com)、品牌旁边加字 (beatbird-help.app)、把 e 换成西里尔字母 e (beatbird.app)。三个域名都在诈骗信发出前几天才注册。
- **真实的个资**：姓名、手机、手环型号、睡眠时数，用真数据让人相信「这是 BeatBird 寄的」。
- **QR code**：「验证会员身份」解出来是 ripple://link-device，是涟漪的关联新设备。扫了它，对方的电脑就成了芷宁账号的一部分，可以读她的新消息、用她的名义跟朋友借钱。
- **发件人**：SPF、DKIM 都通过，但通过的是 kq3tz.idv.tw 自己。验证只能证明「信真的从这个域名发出」，不能证明这个域名是 BeatBird。

逐条排除

嫌疑人	F-02 (姓名)	F-03 (睡眠)	陷阱收到诈骗信
罗美君	D-01	×	C-01 只收到正常的体验信
何佳颖	D-05	D-08	C-05 ✓
江柏宇	D-04	D-07	C-04 没有收到
戴宇翔	×	D-03	—
刘怡君	×	D-06	—
谢明哲	×	×	(F-01)

诈骗信同时用到姓名 (F-02) 与 avg_sleep_30d (只在 F-03)，两份都下载过的只有何佳颖与江柏宇。陷阱邮箱 C-05 收到了诈骗信，而 C-05 只埋在 D-05 那一份，也就是何佳颖下载的 F-02。

陷阱

- **江柏宇**：深夜从住家下载 F-03，论坛上还有人说他在问信贷，看起来最可疑。可是他那份 F-02 的陷阱 C-04 从来没收过诈骗信。
- **好物团购网泄露**：芷宁的主邮箱确实在 2024 年泄露过，里面也有姓名和手机。但诈骗信寄到的是只给过 BeatBird 的别名，团购网那份名单里没有这个别名。
- **假网站的表单**：查假网站只看、不填、不送出。真假数据一样会让对方知道有人上钩。

下次收到这种信

- 「已开通」按月扣款」的通知：自己打开 App 或拨原本就知道的电话确认，不要照信上说的搜索客服。
- 看网址先看注册域名，品牌名放在子域名、旁边加字、混用其他字母，都是另一个域名。
- 不要用通信软件给别人给的 QR code 「验证身份」。定期打开「已关联的设备」，移除不认得的设备，打开两步验证验证。
- 每个服务用不同的 email 别名，泄露时才追得到是从哪里流出去的。
- 钱已经导出去：立刻拨 165。

延伸阅读：一般人平常该做到什么 • 邮件别名怎么用，以及它把信任交给谁 • anonini.net 小工具

答题卡对答案

1. 不放链接、宣称已开始扣款制造急迫感、用真实个资取得信任（不是伪造 beatbird.app，也没有附件） 2. 把滴滴账号关联到诈骗者的电脑 3. F-02 与 F-03 加分 B1：SPF、DKIM 只证明信真的从 kq3tz.idv.tw 发出，那个域名不是 BeatBird 的。加分 B2：诈骗信寄到只给过 BeatBird 的别名，团购网泄露的是主邮箱。
自评 没看提示、一次指认正确：洋葱首席调查员 • 看了 3 条以内提示：资深隐私志愿者 • 其他：见习调查员