PRIVACY MYSTERY · CASE FILE 02

Blue Magpie

How does a billing notice with no link take over someone's whole account?

Type Privacy mystery, solo or 2–4 together
Time About 60–90 minutes
You need A pen, this file, and no hurry to do what you're told

anoni.net community · anoni.net/mystery/en
Feedback and case ideas: anoni.net/mystery/en/feedback/
This is fiction: the people, companies and events are not real. Content licensed CC BY 4.0.

> The last pages are the solution, printed upside down. Don't turn to the back until you've solved the case.

BRIEFING

How to play

You volunteer at the Mistport Privacy Aid. We help people who need to stay anonymous, and people who have been scammed, impersonated or tracked to take themselves back.

Tonight’s request

Office worker **Chou Chih-ning** got a notice that BeatBird’s “Sleep Analysis Premium Plan” would charge her 3,480 a month. The email had no link; it only told her to search for support. She did, scanned a QR code to “verify her membership”, and the next day her friend got a message from “her” asking for money.

What scares her most: the email knew her full name, her phone number, and that she has been sleeping 5 hours 12 minutes a night on average. A pro bono lawyer referred her to the aid station. Take the scam apart and find out **who leaked the member data**.

Your task

Stage one · take the scam apart Which tricks did the email and the fake site use? What did the QR code do?

Stage two · find Blue Magpie Where did the scammers’ list come from? Using only what’s in this file, narrow six people down to one. Write your answers on the answer sheet at the back.

Rules

- Everything you need is in files 01–10. No internet required.
- **Don’t scan the QR code in this file.** The investigator has read it with a tool that doesn’t open links; the result is in file 05.
- Back every conclusion with **evidence**. The person who looks most suspicious isn’t always the one who did it.
- If you’re stuck, the hints follow the answer sheet. Each one counts against your final rank.
- The solution is at the very back, behind a black “stop” page.

Files

01 Chih-ning’s encrypted messages
02 The billing notice (Chih-ning’s email)
03 BeatBird’s real newsletter
04 Search results and the “Member Centre”
05 The investigator’s lookups
06 Chih-ning’s phone
07 MaskMail aliases and breach checks
08 Anonymous forum thread
09 BeatBird’s data protection records
10 Appendix: what anyone can look up

FILE 01

Chih-ning’ s encrypted messages

Sent through an end-to-end encrypted messenger on the evening of Wednesday 9 December 2026.

— Safety number verified • messages disappear after 24 hours —

Hi, I’ m Chou Chih-ning. My pro bono lawyer said you could help with the technical side.
21:04

I got scammed… or nearly did.
21:05

Hi, I’ m the volunteer on duty tonight. Are you safe right now?
21:06

No money was taken. But someone else has been using my Ripple account.
21:06

On Monday night I got an email from BeatBird saying my “Sleep Analysis Premium” plan was active, at 3,480 a month.
21:07

I never signed up for it. The email told me to search for “BeatBird Member Centre Official” for details.
21:07

And you searched for it?
21:08

Yes. I clicked the top result, and the site looked exactly like BeatBird.
21:09

I pressed “Live support” and got an Agent Lin, who said I had to scan a QR code first to “verify my membership”.
21:09

After that he told me to open my online banking to “cancel the automatic payment”, but the screen said a transfer of 29,800. It felt wrong, so I hung up.
21:10

You did the right thing, stopping before the transfer.
21:10

But the next day my friend Che asked why I wanted him to buy me game credit.
21:11

I never sent anything like that.
21:12

And one more thing scares me: the email knew my full name, my phone number, and that I’ ve been sleeping 5 hours 12 minutes a night on average.
21:12

That comes from my BeatBird band. How would they know?
21:13

We’ ll find out together. Do you still have the email?
21:13

Yes. I’ ve put together the original email, my chat with Che and the screenshots I could take. I’ ve masked the middle of the phone number in the email.
21:14

Oh, and I use MaskMail, a different alias for each service. The list is in there too.
21:15

Chou Chih-ning sent from-chih-ning.zip (1.2 MB) · received

Got it. I’ ll look into it tonight.
21:15

Thank you. I’ ll stay online.
21:16

FILE 02

The billing notice

The email Chih-ning got on the evening of 12/7. Above, how her mail app showed it; below, the original headers.

Chou Chih-ning, Sleep Analysis Premium Plan renewal monthly as agreed 3,480 NT

From "BeatBird Member Centre" <notice@kq3fz.idv.tw>
Reply to <bb.member.care@mistmail.tw>
To <bb.tidal-fern@maskmail.tw>
Date Mon, 7 Dec 2026 20:11:58 +0800

Dear Valued Member: Chou Chih-ning

Your BeatBird Sleep Analysis Premium Plan has been successfully activated, all related services are now ready.

- Member account: 0937***118
- Linked device: BeatBird Band 3
- Average sleep, last 30 days: 5 hrs 12 min
- Service plan: Sleep Analysis Premium Plan (monthly)
- Effective date: 2026-12-07
- Renewal: monthly as agreed
- Total per period: 3,480 NT

- Search [BeatBird Member Centre Official] in your browser for details or to cancel

Thank you for your support and wish you a good night's sleep!
Sincerely, BeatBird Operations Team
Company address: 8F, No. 588, Wugang Rd, Neihu District, Taipei

Original headers (excerpt)

```
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 Member Centre" <notice@kq3fz.idv.tw>
Reply-To: <bb.member.care@mistmail.tw>
To: <bb.tidal-fern@maskmail.tw>
```

FILE 03

BeatBird’ s real newsletter

BeatBird’ s monthly email from 11/30, to compare with the billing notice.

Your November sleep report is ready

From "BeatBird" <news@beatbird.app>
To <bb.tidal-fern@maskmail.tw>
Date Mon, 30 Nov 2026 09:00:02 +0800

Hi Chih-ning,

Your November sleep report is waiting in the app. Open BeatBird and tap “Reports” to see it.

A reminder this month
BeatBird will never email you asking you to search for customer support, scan a QR code, or "cancel a payment" at an ATM or in online banking.
Check subscriptions and payments only in the app, under “Account › Subscription”.

BeatBird Technology Co., Ltd.
3F, No. 88, Wugang Rd, Neihu District, Taipei

Original headers (excerpt)

```
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

Search results and the “Member Centre”

Doing as the email says: MistSearch for “BeatBird Member Centre Official”. The top three results are ads; clicking one leads to a “Member Centre” site.

MistSearch: BeatBird Member Centre Official

BeatBird Member Centre Official Search

About 4 results

Sponsored beatbird.app.member-care.com

BeatBird Member Centre | Official support 24/7

Check your subscription, cancel auto-renewal, request a refund. Live agents ready to help.

Sponsored beatbird.app/member

BeatBird Member Centre Official

Questions about a charge? Log in and cancel your premium plan in three minutes.

Sponsored beatbird-help.app

How to cancel a BeatBird subscription | Official help

Steps to cancel the Sleep Analysis Premium Plan, handled one to one.

beatbird.app

BeatBird | Sleep well, live well

Notice: people are sending billing notices in BeatBird’s name. BeatBird will never ask you to search for support or use online banking.

beatbird.app/notice

Scam warning - BeatBird

Check subscriptions and payments only in the app, under “Account › Subscription”. BeatBird will never ask you to scan a QR code.

wuming.forum/t/90417

Got a BeatBird charge for 3,480: is it a scam? - Nameless Square

Me too! Same amount… The “official support” at the top told me to go to an ATM to cancel the instalments…

news.mist/beatbird-scam

BeatBird users hit by fake billing emails; company reports it to police, data protection officer investigating | Tech News

The scam emails include users’ names and phone numbers. BeatBird says it has reported them to the police and its new data protection officer is tracing where the data came from.

Member Centre home page · beatbird.app.member-care.com

BeatBird Member Centre

Home Cancel auto-renewal Live support

Member Centre

Check your subscription, cancel auto-renewal, request a refund, all in one place.

Cancel auto-renewal →

Questions about a charge?

During a recent system upgrade, some members were enrolled in the “Sleep Analysis Premium Plan” by mistake. Please cancel within 24 hours to avoid further charges.

Personal help

Contact live support and Agent Lin will sort it out with you one to one.

© 2026 Beatbyrd Digital Technology Ltd. Business No. 87654321
8F, No. 588, Wugang Rd, Neihu District, Taipei
Support: bb.member.care@mistmail.tw

Live support page · beatbird.app.member-care.com/support

BeatBird Member Centre

Home Cancel auto-renewal Live support

Live support • Agent Lin

To confirm you are the member, please **scan the QR code below with the Ripple app** to complete “member verification”. An agent will contact you as soon as you have scanned it.

Code valid for 10 minutes

beatbird_verify.png

If you can’t scan it, save the code image and choose it in Ripple under “Settings › Scan”.

© 2026 Beatbyrd Digital Technology Ltd. Business No. 87654321
8F, No. 588, Wugang Rd, Neihu District, Taipei
Support: bb.member.care@mistmail.tw

FILE 05

The investigator’s lookups

Domain registrations and DNS records the investigator looked up on their own computer, and the QR code’s contents, read with a tool that doesn’t open links.

```
$ whois beatbird.app
Domain Name              : beatbird.app
Creation Date            : 2019-03-11
Registrar                : HiDomain (TWNIC accredited)
Registrant Organization  : BeatBird Technology Co., Ltd.
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 (shown as beatbird.app; the second letter i
s a Cyrillic 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                : QuickReg (TWNIC accredited)
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"
```

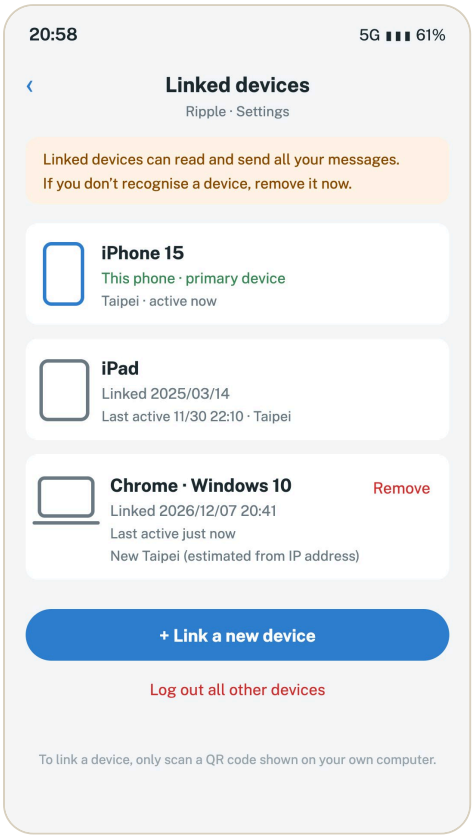
QR reader: beatbird_verify.png

```
Decoded: ripple://link-device?code=7F3Q-K2PX-9MZD&name=Chrome · Windows
Type: not a web address. ripple:// is a command for the Ripple app.
Action: link-device, link a new device to your account (device name Chrome · Windows)
```

FILE 06

Chih-ning’ s phone

Ripple’ s “Linked devices” screen (evening of 12/9), and her chat with her friend Che.



Ripple · chat with Che (exported by Chou Chih-ning)

Chou Chih-ning 12/08 13:05
you there? can you do me a favour

Chou Chih-ning 12/08 13:05
I can't use my card right now, could you buy me 5 GASH cards of 1000 each? I'll pay you back tonight

Che 12/08 13:07
where are you? I called and you didn't pick up

Chou Chih-ning 12/08 13:07
in a meeting, can't talk. just send me a photo of the codes

Che 12/08 18:42
hey what was that at lunch? I nearly went and bought them

Chou Chih-ning 12/08 18:50
I didn't send you ANY messages at lunch!! I was at work all day

Che 12/08 18:51
then your account's been hacked, sort it out

FILE 07

MaskMail aliases and breach checks

Chih-ning’s list of MaskMail aliases, and what “Leaked Yet?” says about two of her addresses.

service	alias	created	note
BeatBird	bb.tidal-fern@maskmail.tw	2025-03-02	only for BeatBird
StreamBox	sb.quiet-moss@maskmail.tw	2025-06-11	
Timelight Books	read.amber-cove@maskmail.tw	2025-09-20	
Ripple	(signed up with phone number)		
GoodDeals group-buying	zhining.chou@mistmail.tw	2023-11-05	signed up before MaskMail; uses the main address

※ MaskMail: mail to every alias is forwarded to the main address zhining.chou@mistmail.tw, and the headers say which alias it came through.

Leaked Yet?: zhining.chou@mistmail.tw

Source	Date	Fields leaked
GoodDeals group-buying	2024-04	name, phone, email, delivery address
StreamBox old forum	2021-10	email, hashed password

Leaked Yet?: bb.tidal-fern@maskmail.tw

Doesn’t appear in any known public breach.

FILE 08

Anonymous forum thread

Nameless Square, Tech board, 6 December.

wuming.forum/t/90417

Nameless Square Tech › Chat

Got a BeatBird charge for 3,480: is it a scam?

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

Last night I got an email from BeatBird saying my Sleep Analysis Premium Plan was active, at 3,480 a month. I never signed up. There's no link in it; it tells me to search for "BeatBird Member Centre Official" myself. Anyone else get one?

Replies

B1 · 12-06 09:30

Me too! Same amount, and I've never used any premium plan

B2 · 12-06 10:02

I searched like the email said. The "official support" at the top told me to go to an ATM to cancel the instalments. Hung up.

B3 · 12-06 12:47

Funny thing, mine didn't even fill in the sleep hours. It literally said "Average sleep, last 30 days: {avg_sleep_30d}". Curly brackets like that mean the template didn't get filled, right?

B4 · 12-06 15:21

It knew my name and my phone number. Did BeatBird get breached?

B5 · 12-06 22:08

Heard some data guy at Langhua Marketing has been asking around about personal loans lately. No idea if it's related.

B6 · 12-07 00:15

Don’ t go guessing about people. If in doubt call 165. The real company will only ever tell you to check your subscription in the app.

FILE 09

BeatBird’ s data protection records

Once Fog found the scam went to an alias only BeatBird had, the aid station contacted Tang Chi-wen, BeatBird’ s data protection officer. Tang sent the following, and asked that no names be made public until the evidence is solid.

From Tang Chi-wen (Data Protection Officer, BeatBird) to the Mistport Privacy Aid 2026-12-09

1. On 24 November, under our partnership contracts, we put three pilot files on our file-sharing system:
F-01 for Hengzhun Actuarial (outside actuarial consultants hired by Dingyue Insurance)
F-02 for Langhua Marketing (the BeatBird Plus campaign)
F-03 for Yunshan Data (app usage analytics)
The fields in each file are listed in data-provided.csv.

2. Since I took up the post, every download plants one extra "canary" record in that copy of the file.
A canary is a fake user that appears only in the copy from that one download.
For canaries with an email address, we watch the mailbox ourselves. If a canary's mailbox gets mail, the copy from that download has been used.
Which canary belongs to which download is in canaries.csv; who downloaded each copy, and when, is in downloads.csv.

3. On 28 November Langhua Marketing sent the BeatBird Plus trial email, as the contract allows, using the project manager's copy. That email was normal use under the contract.

4. Please do not mention anyone's name in public until the evidence is solid.

data-provided.csv

file	provided to	purpose	fields
F-01	Hengzhun Actuarial	premium modelling (for Dingyue Insurance)	user_hash / birth_ym / postcode / device_model / sleep_avg_30 / resting_hr
F-02	Langhua Marketing	BeatBird Plus campaign	user_hash / name / email / phone / device_model / plan_tier
F-03	Yunshan Data	app usage analytics	user_hash / avg_sleep_30d / sleep_score / app_sessions / device_model

※ user_hash is a hash of the member number; all three files use the same one.

downloads.csv

download	time	file	downloaded by	company	connected from
D-01	2026-11-25 10:12	F-02	Lo Mei-chun	Langhua Marketing	Langhua Marketing office

D-02	2026-11-25 10:40	F-01	Hsieh Ming-che	Hengzhun Actuarial	Hengzhun Actuarial office
D-03	2026-11-25 14:05	F-03	Tai Yu-hsiang	Yunshan Data	Yunshan Data office
D-04	2026-11-25 14:31	F-02	Chiang Po-yu	Langhua Marketing	Langhua Marketing office
D-05	2026-11-25 16:02	F-02	Ho Chia-ying	Langhua Marketing	Langhua Marketing office
D-06	2026-11-26 09:55	F-03	Liu Yi-chun	Yunshan Data	Yunshan Data office
D-07	2026-11-26 23:48	F-03	Chiang Po-yu	Langhua Marketing	home broadband (via share link S-1)
D-08	2026-11-27 13:20	F-03	Ho Chia-ying	Langhua Marketing	Langhua Marketing office (via share link S-1)

※ Share link S-1: created on 11/26 by Tai Yu-hsiang of Yunshan Data, so Langhua Marketing could plan campaigns by sleep segment.

canaries.csv

canary	download	fake name	email
C-01	D-01	Lin Yu-hsuan	yuxuan.lin.k7@maskmail.tw
C-02	D-02	(F-01 has no name field)	(F-01 has no email field)
C-03	D-03	(F-03 has no name field)	(F-03 has no email field)
C-04	D-04	Chen Pin-yu	pinyu.chen.q2@maskmail.tw
C-05	D-05	Hsu Shu-hao	shuhao.hsu.m9@maskmail.tw
C-06	D-06	(F-03 has no name field)	(F-03 has no email field)
C-07	D-07	(F-03 has no name field)	(F-03 has no email field)
C-08	D-08	(F-03 has no name field)	(F-03 has no email field)

※ Canaries without an email can only be traced by user_hash; none has been seen in use so far.

canary-inbox.txt

```
Canary mailboxes: received mail (watched by BeatBird's data protection office)    exporte
d 2026-12-09 20:30

[2026-11-28 10:00] To: yuxuan.lin.k7@maskmail.tw
  From: BeatBird Plus <plus@beatbird.app>
  Subject: 30 days of BeatBird Plus, free, for when you can't sleep
```

```
[2026-12-05 21:44] To: shuhao.hsu.m9@maskmail.tw
  From: "BeatBird Member Centre" <notice@kq3fz.idv.tw>
  Subject: Hsu Shu-hao, Sleep Analysis Premium Plan renewal monthly as agreed 3,480 NT
  Excerpt:
    Dear Valued Member: Hsu Shu-hao
    • Member account: 0912***107
    • Linked device: BeatBird Band 2
    • Average sleep, last 30 days: {avg_sleep_30d}
    • Search [BeatBird Member Centre Official] in your browser for details or to cancel

(Other canary mailboxes: no mail received)
```

FILE 10

Appendix: what anyone can look up

Public information the investigator found.

BeatBird scam warning (updated 2026-12-07)

Some members have received emails titled “Sleep Analysis Premium Plan renewal monthly as agreed 3,480 NT”. BeatBird did not send them, and we have no such plan. BeatBird only ever emails from @beatbird.app. We will never ask you to search for “official support”, add an agent’s chat account, scan a QR code, or “cancel a payment” at an ATM or in online banking.

Company registry lookup

Business number	Result
53018827	BeatBird Technology Co., Ltd., 3F, No. 88, Wugang Rd, Neihu District, Taipei; registered 2018-11-02
87654321	No company registered

165 Anti-Fraud Hotline: fake app charges and “cancelling instalments”

- If a notice says a plan is “now active” or “billed monthly”, don’t search for the support it points you to. Open the app yourself, or call a number you already know is official.
- Real companies never ask you to “cancel a payment” at an ATM or in online banking, or to scan a QR code to “verify your identity”.
- If an unknown device has joined your messaging app, remove it under “Linked devices”, turn on two-step verification and tell your friends and family.

How to read a web address

An address’s “registered domain” is the part just before the top-level domain (.com, .app): the registered domain of mail.beatbird.app is beatbird.app. Anything before the registered domain is a subdomain, and the domain’s owner can call it whatever they like. Some letters look like English ones but come from another alphabet (such as the Cyrillic e); then it is a different domain.

ANSWER SHEET

Answer sheet

For every answer, note which file your evidence comes from.

Stage one · take the scam apart

1. Which tricks did the billing notice use?

☐ No link: it tells you to search for yourself ☐ Claims you are already being charged, to rush you ☐ Uses her real name, phone and sleep data to win trust ☐ Forged to come from beatbird.app ☐ Carries malware in an attachment

2. What did the QR code the fake agent asked Chih-ning to scan do?

○ Linked her Ripple account to the scammer's computer ○ Installed spyware on her phone ○ Authorised automatic card payments ○ Gave the site her Ripple password

3. Which two files were combined to make the scammers' list?

☐ F-01 (Hengzhun Actuarial) ☐ F-02 (Langhua Marketing) ☐ F-03 (Yunshan Data) ☐ The 2024 GoodDeals group-buying breach

Stage two · find Blue Magpie

○ if they fit, × to rule them out.

Clue	Lo Mei-chun	Ho Chia-ying	Chiang Po-yu	Tai Yu-hsiang	Liu Yi-chun	Hsieh Ming-che
Downloaded F-02 (names)						
Downloaded F-03 (sleep data)						
Canary got the scam						

4. Who leaked the data? List at least three independent pieces of evidence.

Bonus questions

B1. The scam email passed SPF and DKIM. Why is it still fake?

B2. Chih-ning's main address leaked in 2024, with her name and phone number. Why didn't the scammers' list come from there?

HINTS

Hints

Only when you’ re really stuck. Cover them with paper, reveal one at a time, and keep count.

> Hint 1 · The email
> Is there a link in the email in file 02? What does it ask Chih-ning to do? Why might “no link” make people trust it more?

> Hint 2 · The sender
> Read From and Authentication-Results in file 02, then compare with the real newsletter in file 03. Which domain did authentication pass for?

> Hint 3 · The ads
> All three ads in file 04 have “beatbird” in their address. Use “How to read a web address” in the appendix to find their real registered domains.

> Hint 4 · Domain ages
> The whois records in file 05: when was the real beatbird.app registered? And the fake sites’ domains?

> Hint 5 · The QR code
> Compare the QR reader result in file 05 with the linked-devices screenshot in file 06. When did the unknown device join?

> Hint 6 · Where the list came from
> Which address did the email in file 02 go to? Check the aliases and breach checks in file 07.

> Hint 7 · Two files
> In file 09’ s data-provided list: which file has names? Which has avg_sleep_30d? In the download log, who downloaded both?

> Hint 8 · The canaries
> In the canary inbox, which canary received the scam? Match it to a download in the canary list, then to a person in the download log.

S T O P

Have you solved it?
The truth is on the other side of this page. If your answer sheet isn’ t finished, go back.

The solution pages are printed upside down: turn the whole file round to read them.

CASE FILE 02 · SOLVED

The truth

Blue Magpie is Ho Chia-ying.A campaign planner at Langhua Marketing. She matched up two of BeatBird’ s pilot files she had access to at work and sold the result to a scam ring.

What happened

On 25 November, Ho Chia-ying downloaded F-02 (the marketing list with names, emails and phone numbers) from the file-sharing system. On the 27th, through the share link Yunshan Data had made for Langhua, she also downloaded F-03 (the usage analytics with sleep data). Both files use the same user_hash, so joining them gives a list of who people are, how to reach them and how much they have been sleeping.

From 1 December the scam ring registered the sending domain kq3fz.idv.tw and three domains posing as BeatBird, and on 5 December the emails started going out. Chih-ning got hers on 7 December. She searched as told, clicked an ad and scanned the “verification” QR code, and her Ripple account was linked to the scammers’ computer.

How the scam works

- **An email with no link**: with no link, it slips past mail filters and seems “not like a scam”. It only tells you to search for support yourself.
- **Paid ads**: the top three “official support” results are all ads, using the brand as a subdomain (beatbird.app.member-care.com), extra words next to the brand (beatbird-help.app), and a Cyrillic e in place of e (beatbird.app). All three domains were registered a few days before the emails went out.
- **Real personal data**: name, phone number, band model and hours of sleep. Real data makes people believe BeatBird sent it.
- **The QR code**: the “member verification” decodes to ripple://link-device, Ripple’ s “link a new device”. Scanning it made the scammers’ computer part of Chih-ning’ s account: they could read her new messages and ask her friends for money in her name.
- **The sender**: SPF and DKIM both pass, but for kq3fz.idv.tw itself. Authentication only proves the mail really came from that domain, not that the domain is BeatBird.

Ruling people out

Suspect	F-02 (names)	F-03 (sleep)	Canary got the scam
Lo Mei-chun	D-01	×	C-01 got only the normal trial email
Ho Chia-ying	D-05	D-08	C-05 ✓
Chiang Po-yu	D-04	D-07	C-04 got nothing
Tai Yu-hsiang	×	D-03	—
Liu Yi-chun	×	D-06	—
Hsieh Ming-che	×	× (F-01)	—

The scam uses both names (F-02) and avg_sleep_30d (only in F-03), and only Ho Chia-ying and Chiang Po-yu downloaded both. Canary mailbox C-05 received the scam, and C-05 was planted only in download D-05: the F-02 that Ho Chia-ying downloaded.

Traps

- **Chiang Po-yu**: downloaded F-03 late at night from home, and someone on the forum says he has been asking about loans. He looks the most suspicious, but the canary in his copy of F-02, C-04, never received a scam email.
- **The GoodDeals breach**: Chih-ning's main address really did leak in 2024, with her name and phone number. But the scam went to an alias she gave only to BeatBird, and that alias is not in the group-buying site's list.
- **The fake site's form**: when you check a fake site, look but never fill in or send anything. Even fake details tell them someone bit.

Next time you get an email like this

- A plan that is "now active" or "billed monthly": open the app yourself, or call a number you already know, to check. Don't search for the support the email points you to.
- Read the registered domain of every address. A brand in a subdomain, extra words next to it, or letters from another alphabet all make a different domain.
- Never scan a QR code someone sends you with a messaging app to "verify your identity". Check "Linked devices" now and then, remove any you don't recognise, and turn on two-step verification.
- Use a different email alias for each service, so when something leaks you can tell where it came from.
- If money has already gone, call 165 at once.

Further reading: What an ordinary person should actually do · Email aliases, and who you hand your trust to · anoni.net utilities

Answer key
1. No link, a claim she was already being charged, and her real data (not forged as beatbird.app; no attachment) 2. Linked her Ripple account to the scammer's computer 3. F-02 and F-03
Bonus B1: SPF and DKIM only prove the mail really came from kq3fz.idv.tw, and that domain isn't BeatBird's. Bonus B2: the scam went to an alias only BeatBird had; the group-buying breach leaked her main address.
Rate yourself No hints, right first time: Chief Onion Investigator · Three hints or fewer: Senior Privacy Volunteer · Otherwise: Trainee Investigator