

# Staying Up-to-Date with SMS Scams: Building a Smishing Honeyypot

Sharad Agarwal and Marie Vasek

sharad.agarwal@ucl.ac.uk

The Honeynet Project Annual Workshop 2025

2nd June 2025





\whoami

 @shad1126

- Ph.D. Candidate at University College London (UCL)
- Related Publications:
  - Examining Newly Registered Phishing Domains at Scale. WEIS'25. (2025).
  - 'Hey mum, I dropped my phone down the toilet': Investigating Hi Mum and Dad SMS Scams in the United Kingdom. USENIX Security Symposium. (2025).
  - Poster: A Comprehensive Categorization of SMS Scams. ACM IMC'24. (2024)

\* Thanks to collaborators: E. Harvey, E. Mariconti, G. Suarez-Tangil, and M. Vasek



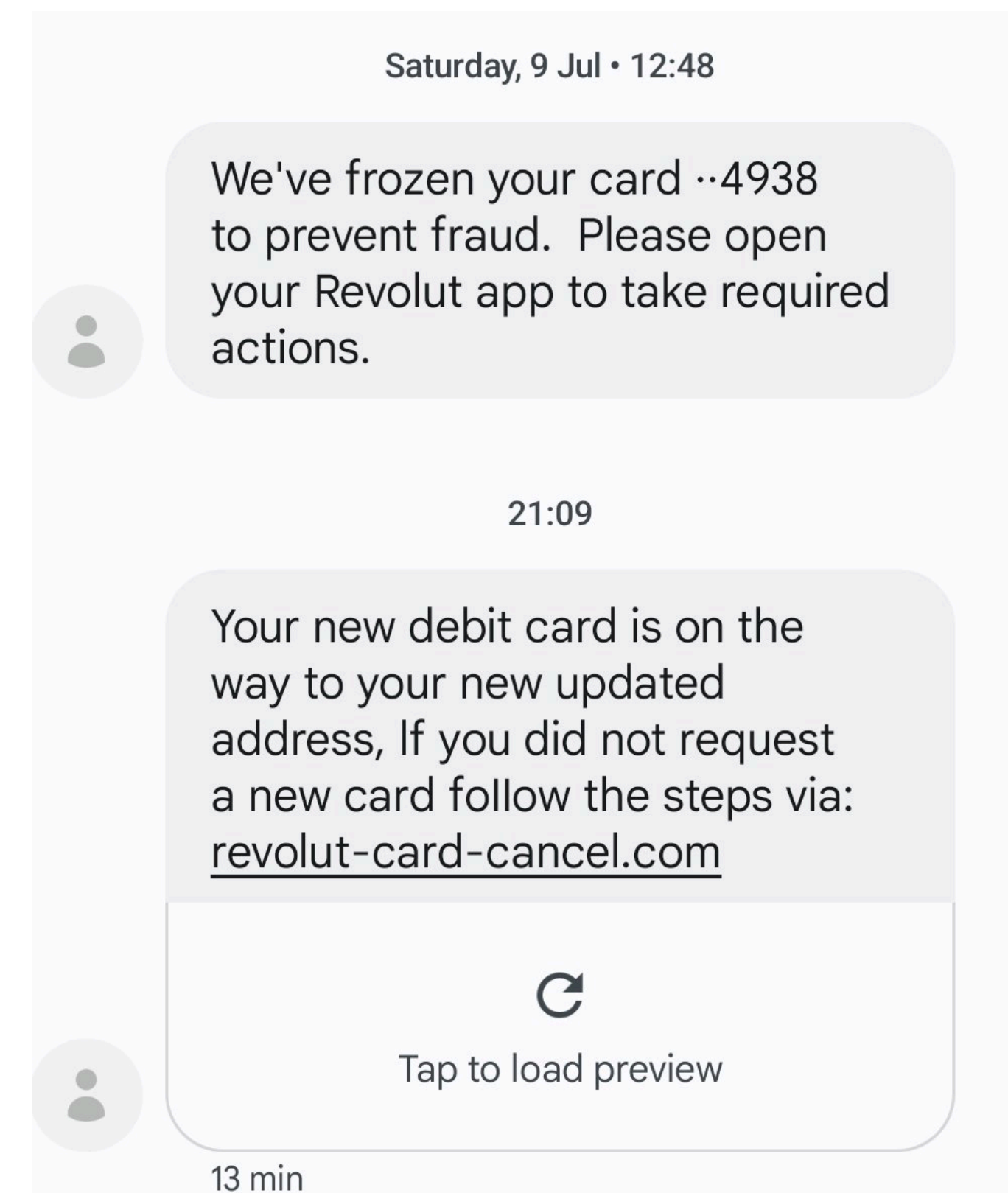
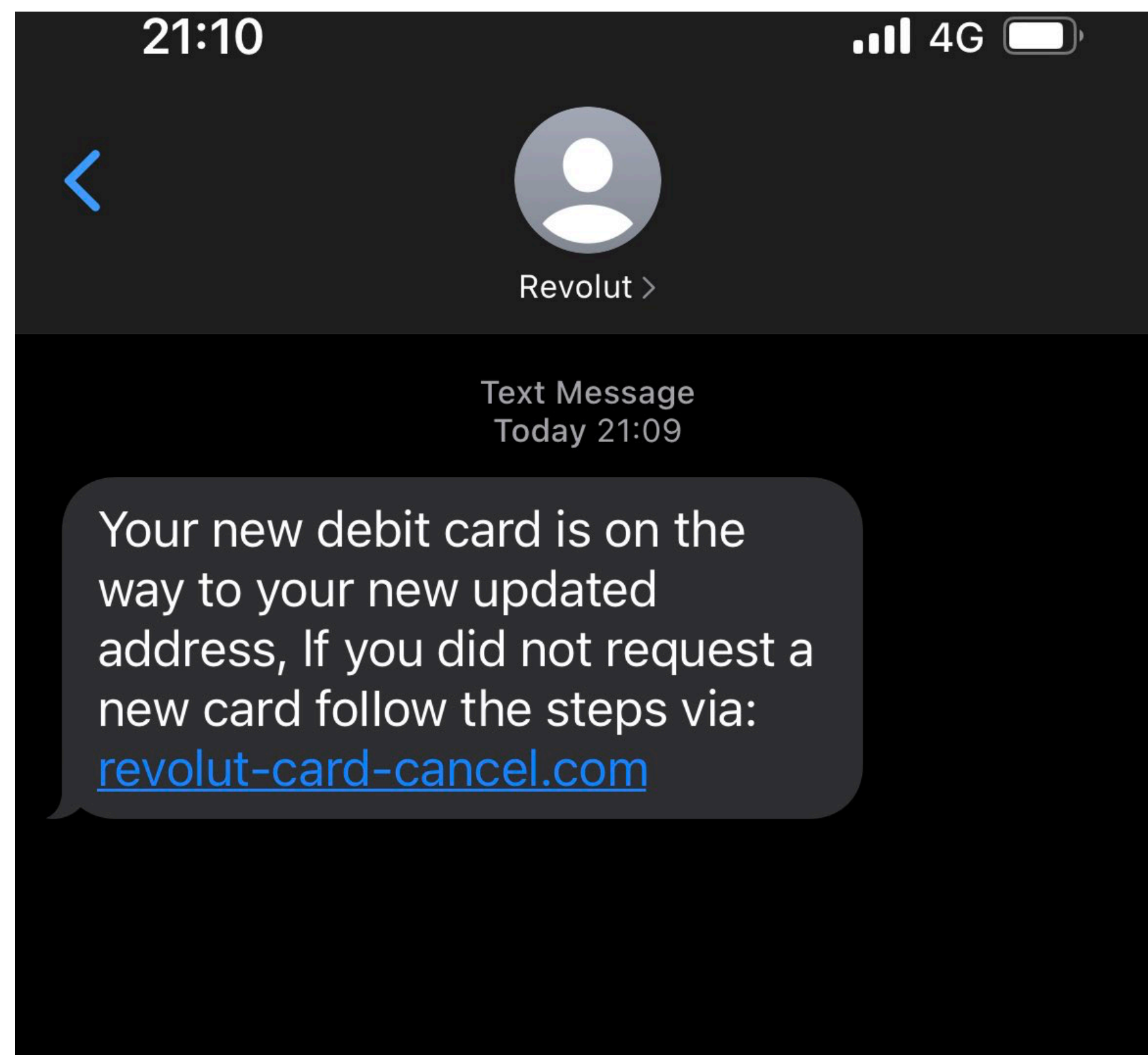


# Agenda

- SMS Phishing aka Smishing
- Current Landscape
- Motivation
- Smishing Honeypot
- Results
- Takeaways



# SMS Phishing aka Smishing



News Article





# Current Landscape

- Proofpoint's yearly report shows smishing attacks have significantly increased over the years.
- US FTC reports \$470 million loss to text scams with \$129k just towards Toll Scams in 2024.\*

\* <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2025/04/top-text-scams-2024>



# Current Landscape

- Proofpoint's yearly report shows smishing attacks have significantly increased over the years.
- US FTC reports \$470 million loss to text scams with \$129k just towards Toll Scams in 2024.\*
- The research community lacks open-access up-to-date smishing dataset that could help identify scammers' strategies.
- MNOs in limited countries like the UK have implemented spam filtering solutions, but are restricted to SMS.

\* <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2025/04/top-text-scams-2024>



# Current Landscape

- Proofpoint's yearly report shows smishing attacks have significantly increased over the years.
- US FTC reports \$470 million loss to text scams with \$129k just towards Toll Scams in 2024.\*
- The research community lacks open-access up-to-date smishing dataset that could help identify scammers' strategies.
- MNOs in limited countries like the UK have implemented spam filtering solutions, but are restricted to SMS.
- While certain MNOs and governments have rolled out user reporting services (7726/one-click reporting), the exponential increase in user reports has led to additional noise due to spam.

\* <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2025/04/top-text-scams-2024>



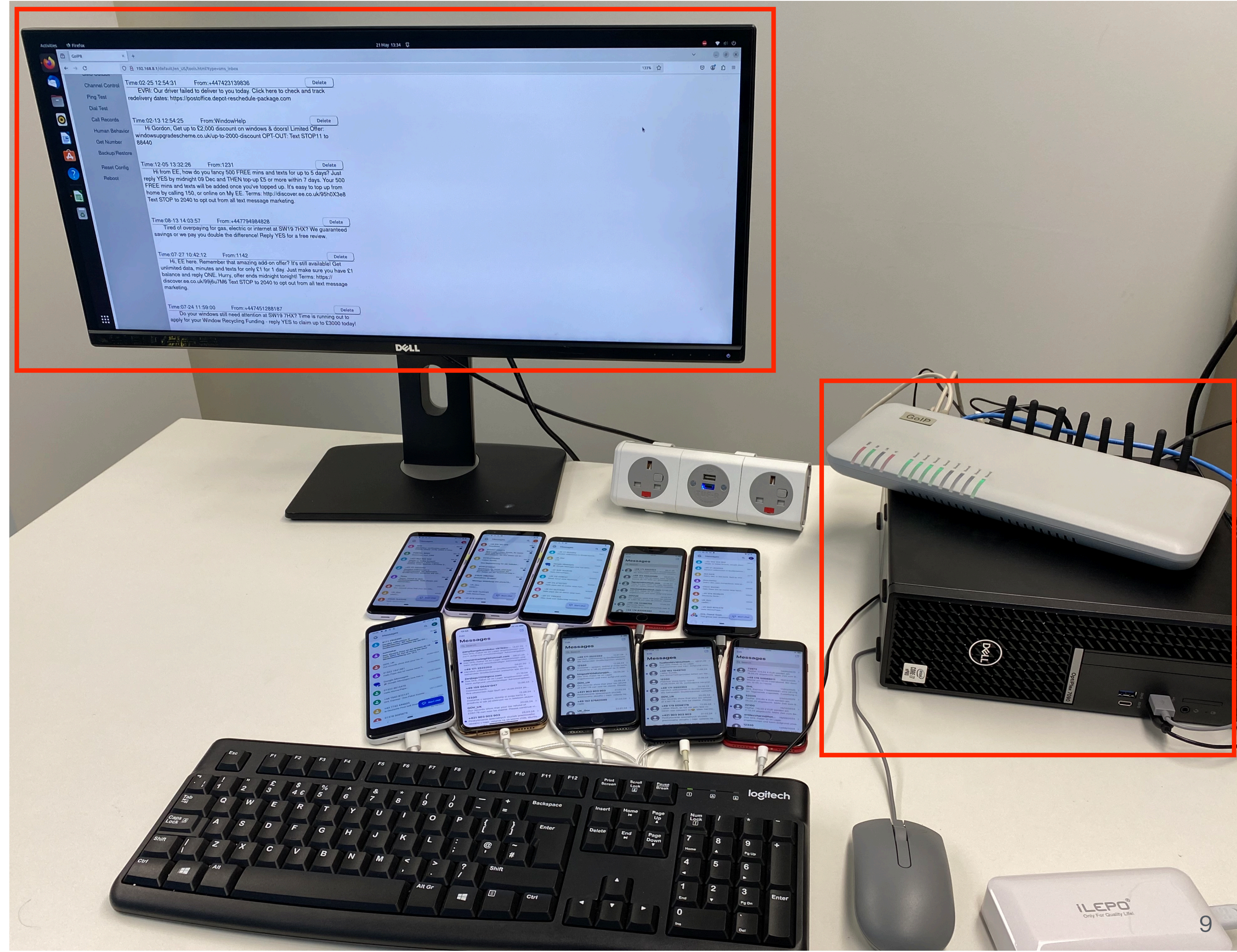
# Motivation

- Honeypots provide timely and accurate smishing data.
- Identify new smishing campaigns.
- Understand evolving scammer strategies.



# Smishing Honeypot: Infrastructure

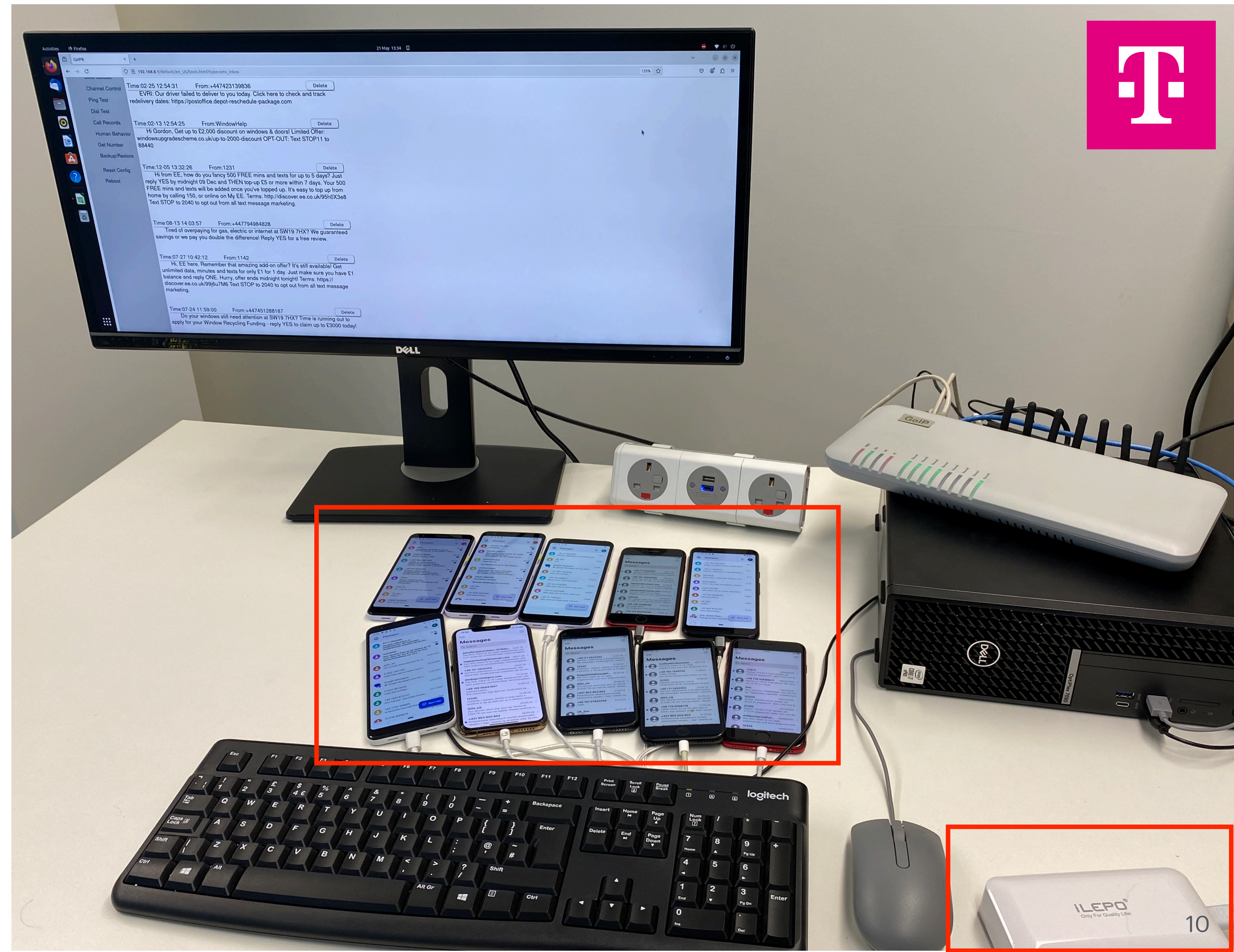
- GoIP-8 (GSM VoIP Gateway)
- Ubuntu OS installed in a commodity PC with a monitor





# Smishing Honeypot: Infrastructure

- GoIP-8 (GSM VoIP Gateway)
- Ubuntu OS installed in a Commodity PC with a monitor
- 10 Smartphones (Android and iOS)
- USB Power Supply (10 outlets - 40W)







# Smishing Honeyypot: Seeding

- Generate synthetic personas using an open-source Python package - Faker.\*

\* <https://github.com/joke2k/faker>



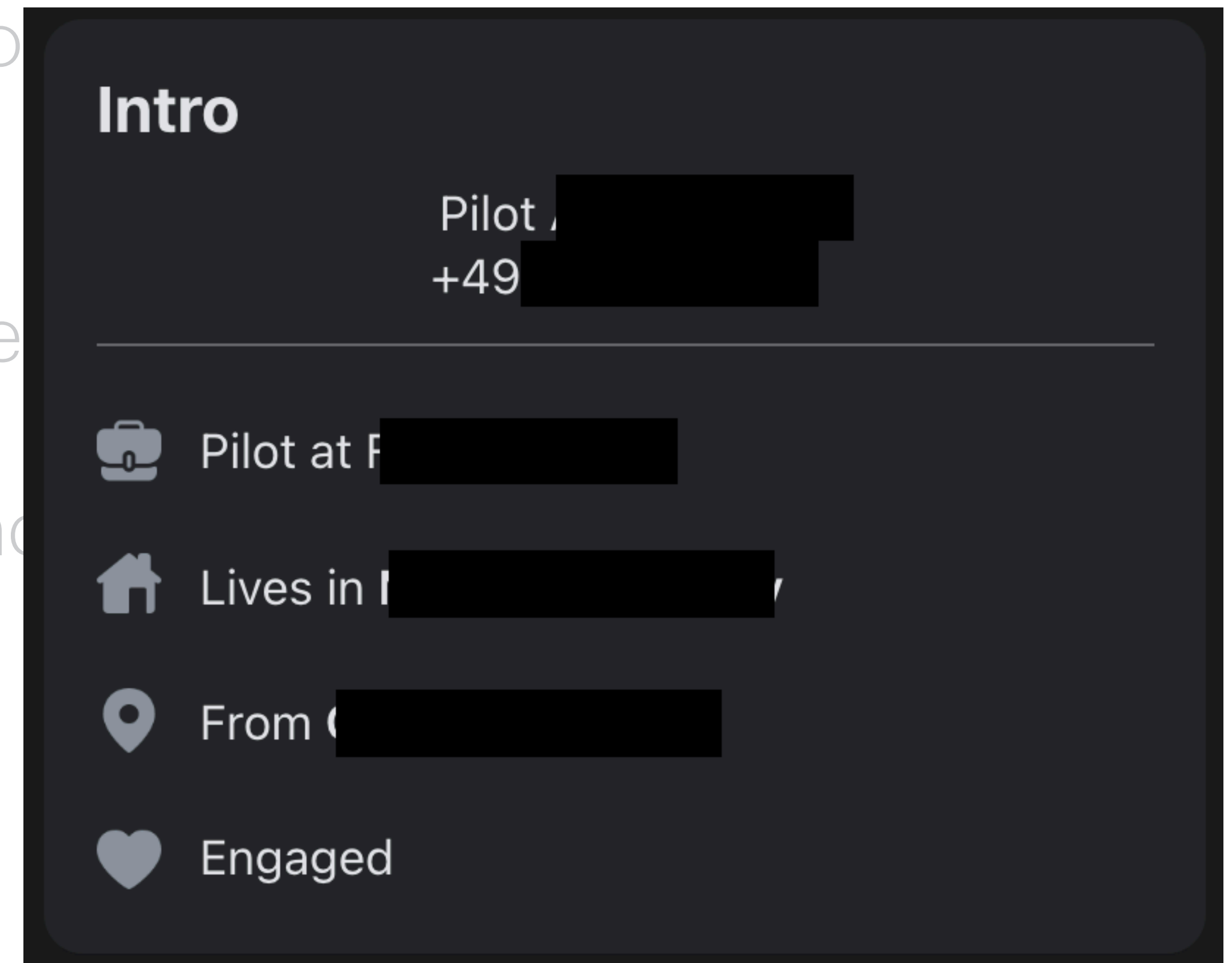
# Seeding: Creating Personas on Social Media

- Generate synthetic personas using an open-source Python package - Faker.\*
- Create social media accounts using the synthetic personas.  Meta 
  - Publicly display name, profession, address, and mobile numbers in the profile/bio information.

\* <https://github.com/joke2k/faker>

# Seeding: Creating Personas on Social Media



- Generate synthetic personas using an open source tool called **Faker**.\*
- Create social media accounts using the generated information
  - Display name, profession, address, and other bio information as public.



\* <https://github.com/joke2k/faker>

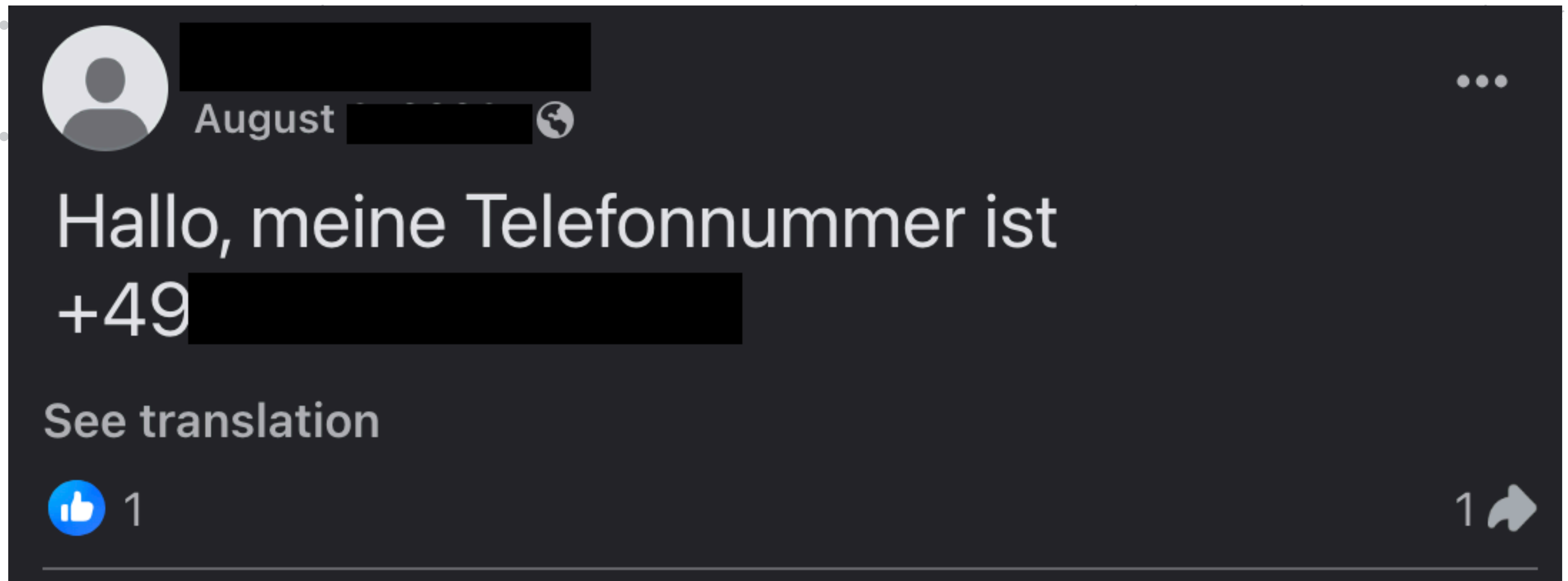


# Seeding: Posting on Social Media

- Generate synthetic personas using an open-source Python package - Faker.\*
- Create social media accounts using the synthetic personas.  Meta 
  - Display name, profession, address, and mobile numbers in the profile/bio information as public.
  - Regularly post in English/German (based on the persona): `Hi my name is ...` along with the mobile number and its country code.

\* <https://github.com/joke2k/faker>

# Seeding: Posting on Social Media





# Seeding: Sharing Mobile Numbers as Lists

- Post all mobile numbers as a list (paste) over online clipboards.



PASTEBIN

- Make the paste public and available for a year so it is accessible to scammers.



# Seeding: Replying to Identified URLs/Numbers

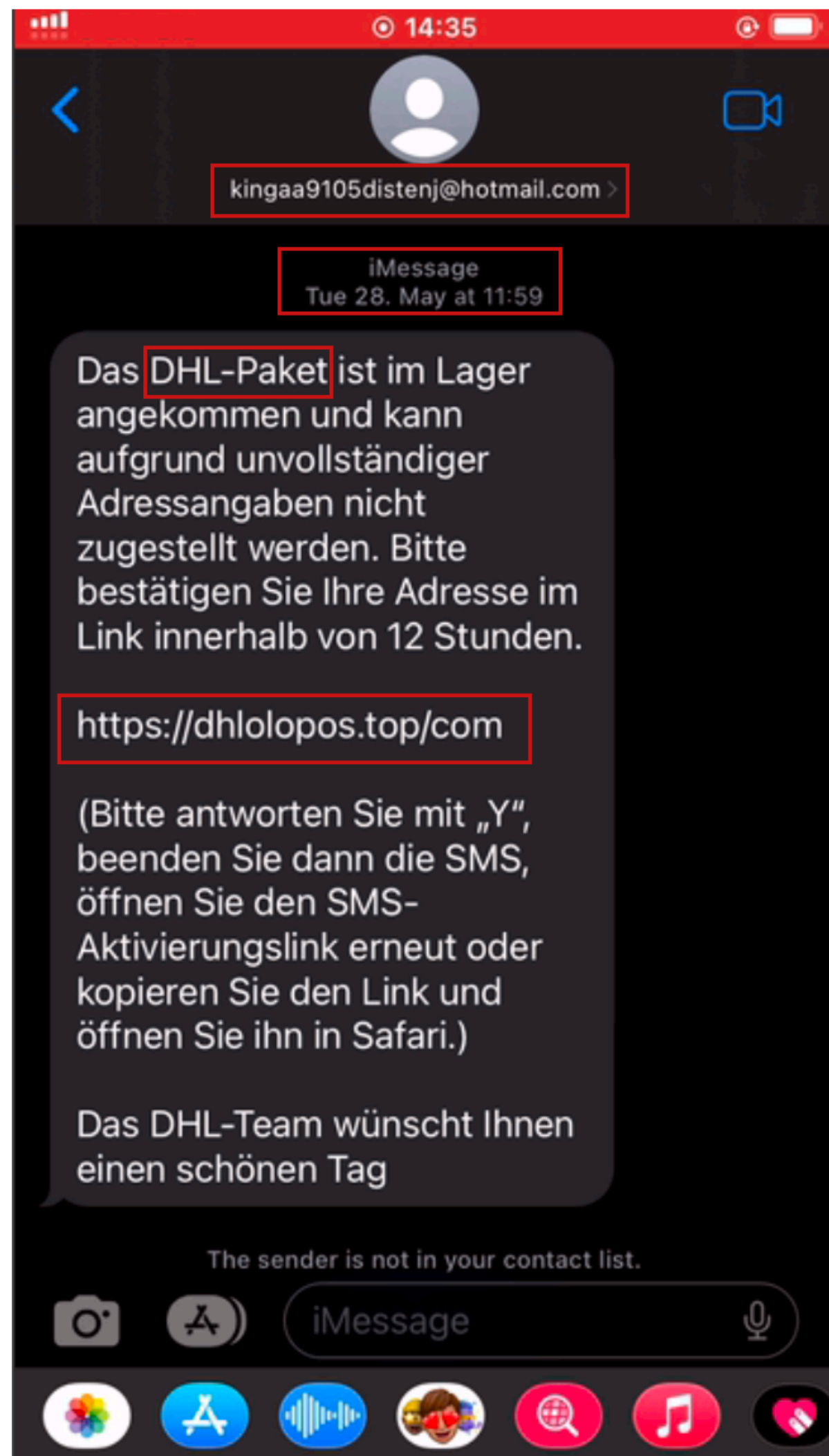
- Enter the honeypot mobile numbers into identified smishing URLs.
- Reply to identified smishing texts and mobile numbers.





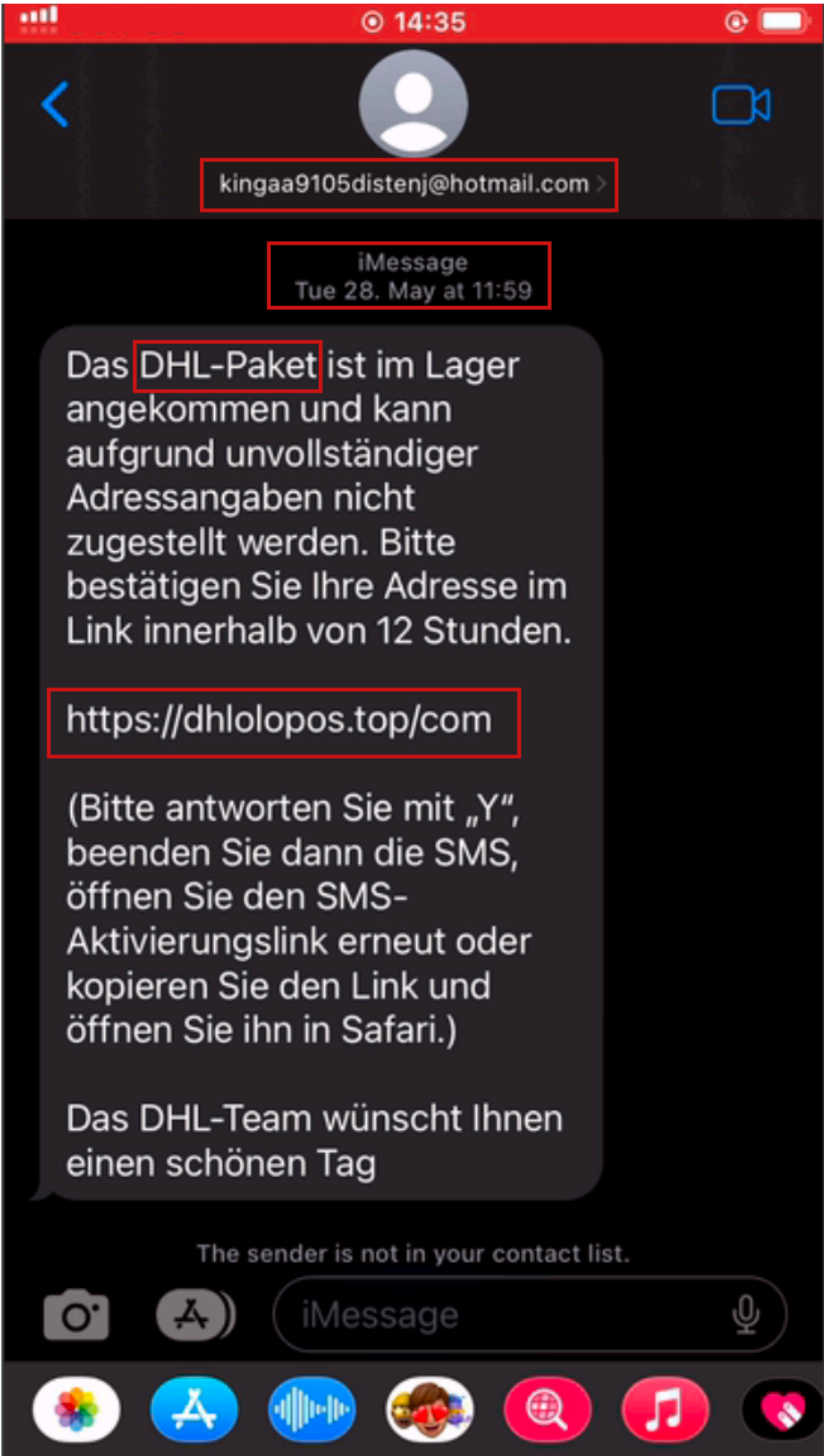
# Results: Overview

- As of May'25, we have collected more than 120 smishing texts over SMS and other encrypted medium - RCS/iMessage.
- We also receive 117 missed calls from plausible scammers.
- We observe various sender IDs - mobile numbers, emails and alphanumeric short-codes that scammers abuse to send smishing texts.
- We identify both conversational and non-conversational scams in our data. While conversational scams lead to APP fraud, non-conversational scams result in unauthorized fraud.



To evade detection, criminals send smishing texts over encrypted medium - **iMessage** and **RCS**.

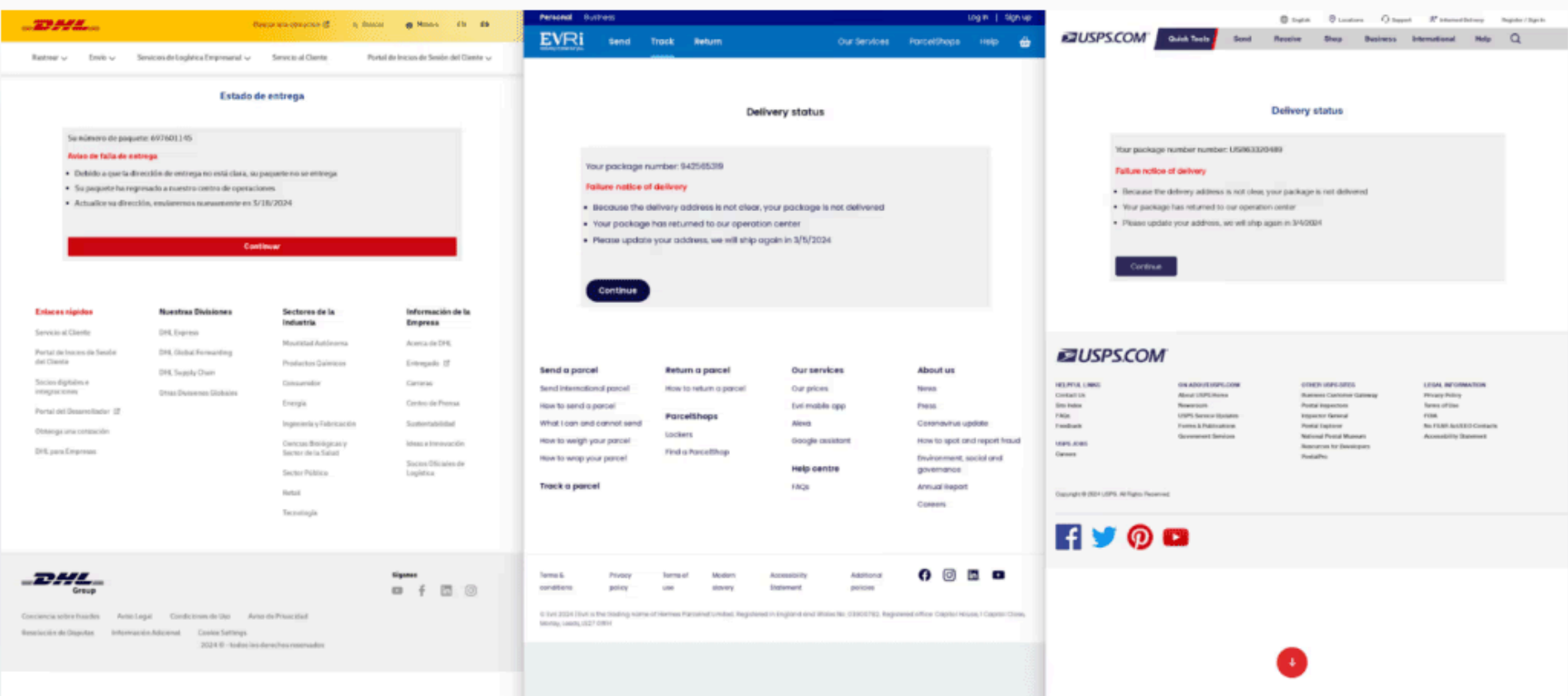




# What is darcula? Cybercrime-as-a-Service is a serious business

darcula is a Chinese-language PhaaS platform developed by a Telegram user sporting the same name, offering easy deployment of phishing sites with hundreds of templates targeting worldwide brands. Like other PhaaS actors, the darcula group offers a paid monthly subscription to other criminals.

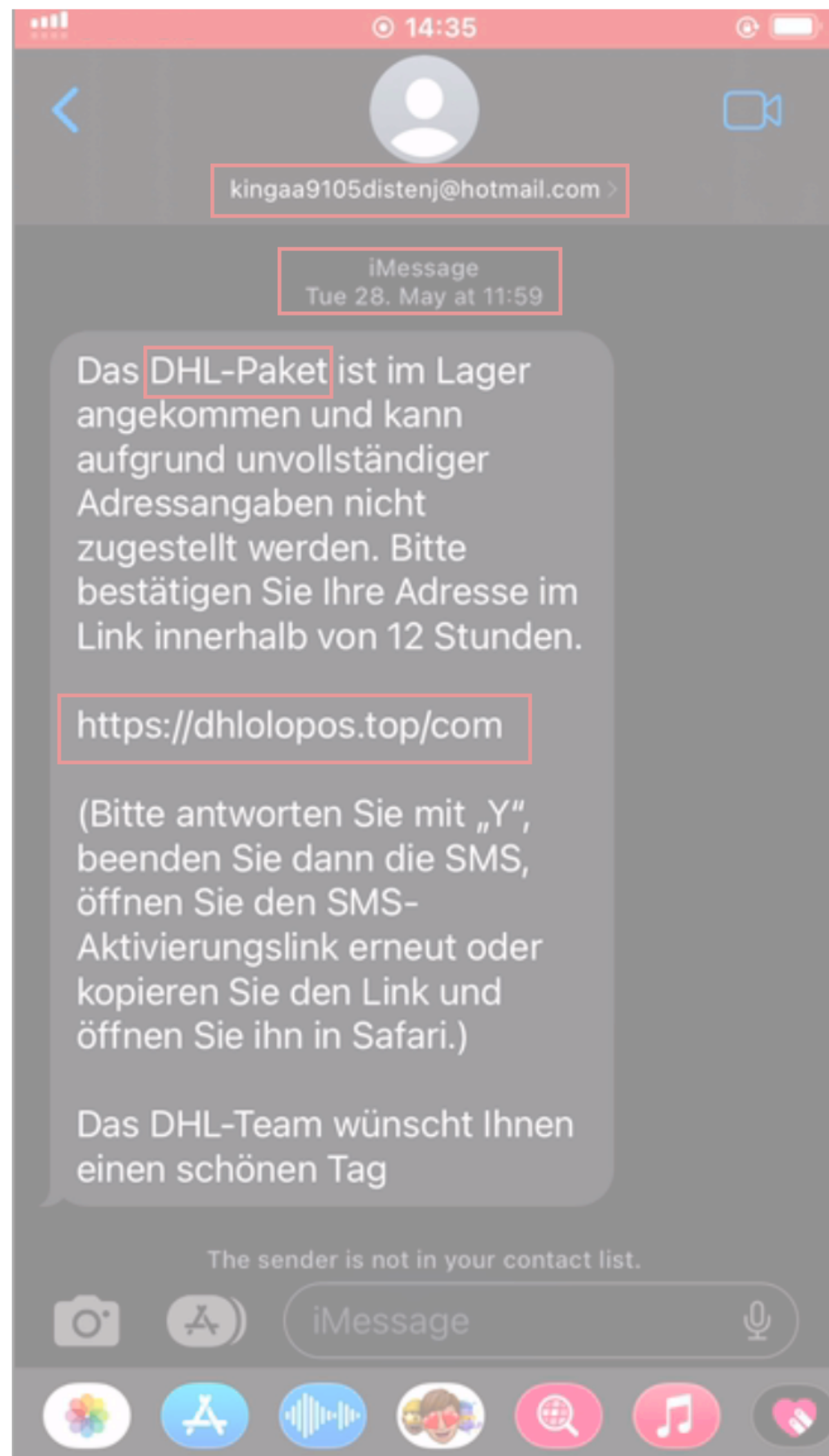
Unlike [more typical phishing kits](#), darcula phishing websites can update in place to add new features and anti-detection measures (that is, the kit does not need to be removed and then re-installed to benefit from new updates) functionality Netcraft has observed directly. For example, a recent darcula update changed the kit to make the malicious content available through a specific path (i.e. example.com/track), rather than the front page (example.com) to disguise the attack's location.



Complete Article







Smishing victims  
to steal credit  
card data,  
abused towards  
card-not-present  
(CNP) fraud.

Complete Article



## Inside the Scam Network

The scammers have tricked millions of people worldwide, including thousands of Norwegians, through text messages. Who are they and how do they scam us?

PUBLISERT 4. MAI KL. 06:38 | OPPDATERT 8. MAI KL. 11:39

[Martin Gundersen](#) +7 til  
Journalist

A stream of text messages is being sent to mobile users across the globe.

The messages are crafted to deceive us.





# Case Study 1

Law enforcement agencies send alerts to victims whose details have been identified in seized criminal databases.

# Case Study 1: Met Police

Law enforcement agencies send alerts to victims whose details have been identified in seized criminal databases.

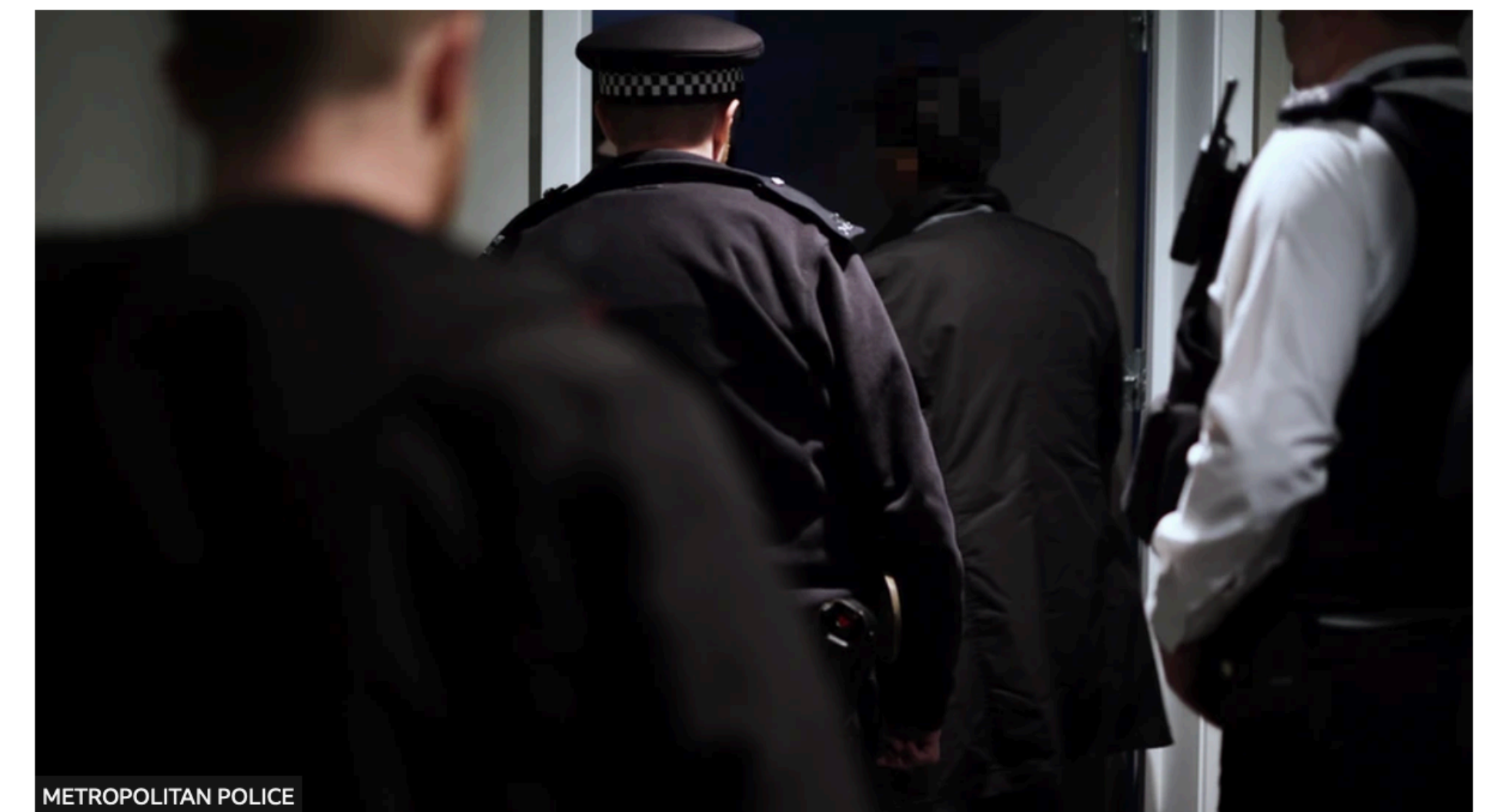
News Article



## NEWS

### Police text 70,000 victims in UK's biggest anti-fraud operation

🕒 24 November 2022



METROPOLITAN POLICE

Police raid a property in connection with suspected fraudsters



# Case Study 1: Our Honeypot Results

	Parts	Cost(p)	CC	Message
				<p>The Met Police has accessed a criminal service impersonating companies to obtain people's data.</p> <p>Your data has been accessed through this platform and we advise you to change any passwords that you use for your (Apple Pay) account.</p> <p>Please be reassured that we have taken action to disrupt the platform, safeguarded your personal details and reported to Action Fraud on your behalf.</p> <p>We understand this may be worrying but for further advice and support please go to the homepage of the Met Police website.</p>

# Case Study 1: Our Honeyypot Results

This text from the Metropolitan Police in the UK verifies the success of our mobile number seeding methodology.

Sent	Recd	From	To	Message
17 Apr 2024				
16:40:58		MetPolice	+447 [REDACTED]	The Met Police has accessed a criminal service impersonating companies to obtain people's data. Your data has been accessed through this platform and we advise you to change any passwords that you use for your (Apple Pay) account. Please be reassured that we have taken action to disrupt the platform, safeguarded your personal details and reported to Action Fraud on your behalf. We understand this may be worrying but for further advice and support please go to the homepage of the Met Police website.



# Case Study 2

Criminals abuse SMS blasters/Fake Base Stations/ IMSI\* catchers to broadcast smishing texts.

\* IMSI - International Mobile Subscriber Identity

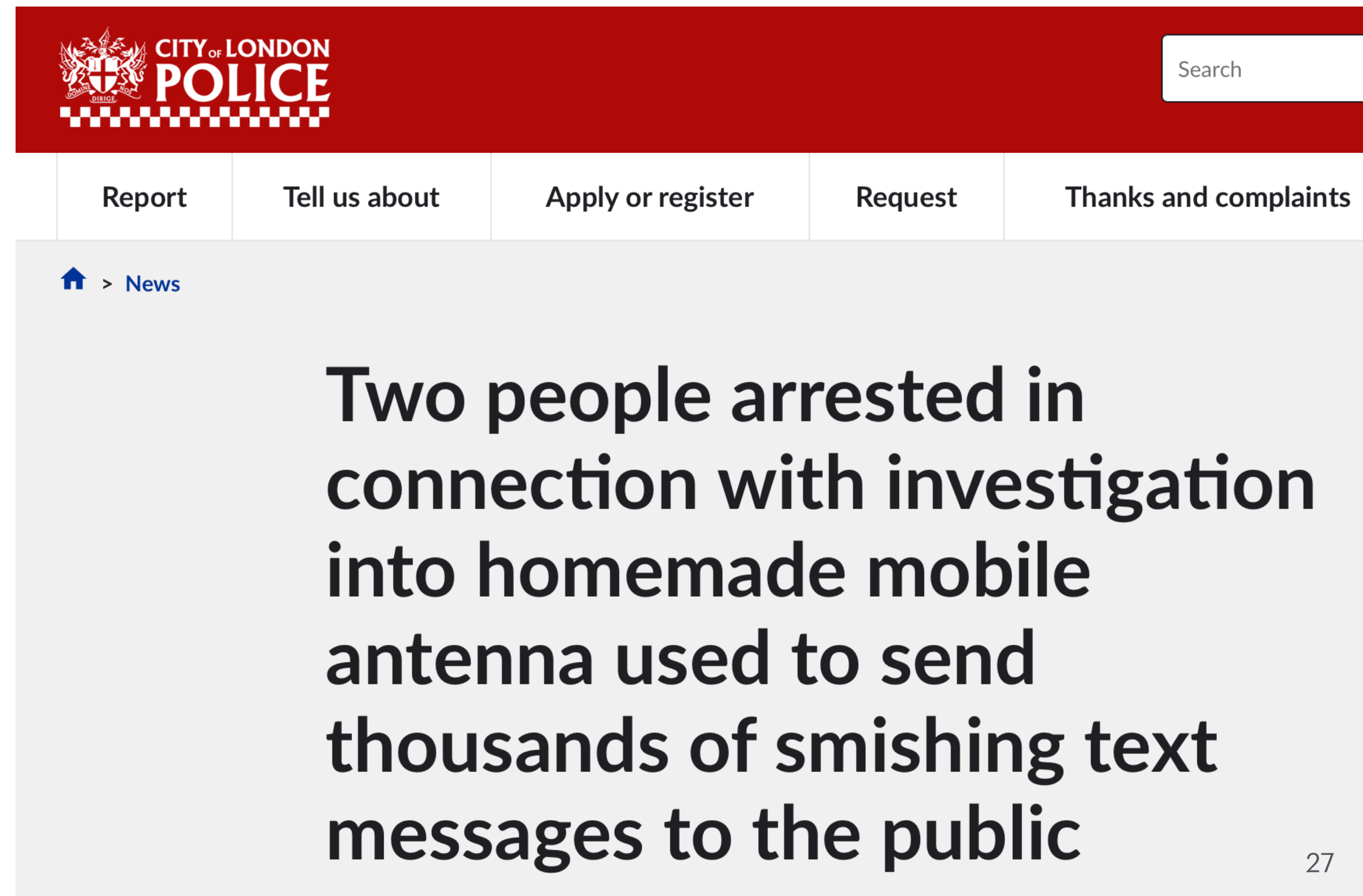
# Case Study 2: Incidence of SMS Blasters

Criminals abuse SMS blasters/Fake Base Stations/ IMSI\* catchers to broadcast smishing texts.

Complete Article



\* IMSI - International Mobile Subscriber Identity



The screenshot shows the City of London Police website. The header is red with the police crest and 'CITY OF LONDON POLICE' text. A search bar is on the right. Below the header is a navigation bar with links: 'Report', 'Tell us about', 'Apply or register', 'Request', and 'Thanks and complaints'. The main content area shows a breadcrumb trail 'Home > News' and a large headline: 'Two people arrested in connection with investigation into homemade mobile antenna used to send thousands of smishing text messages to the public'.

**Two people arrested in connection with investigation into homemade mobile antenna used to send thousands of smishing text messages to the public**



# Case Study 2: SMS Blasters in a Moving Van



Source Article

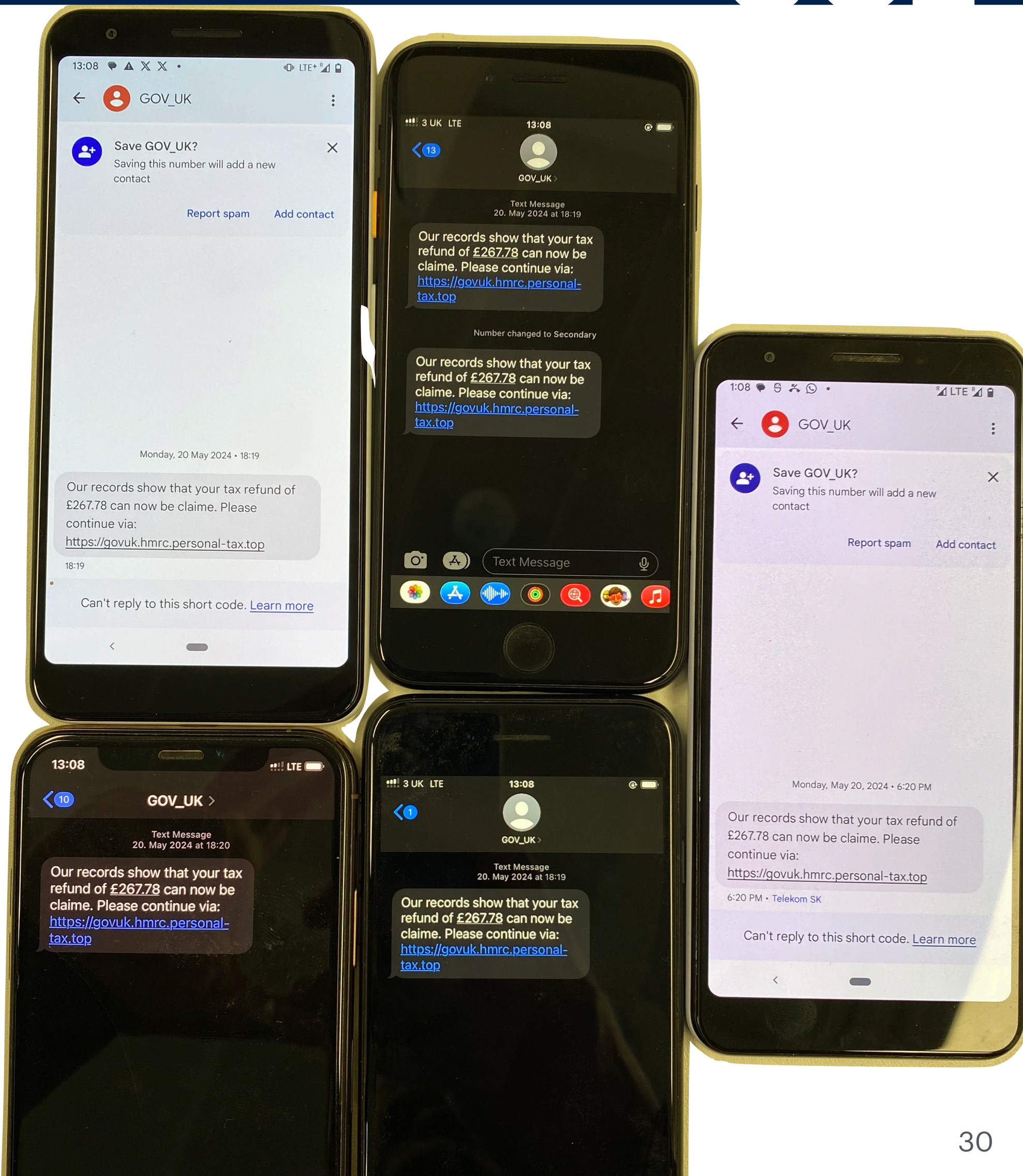




# Our Honeyypot Results

Smishing texts impersonating UK Government using **GOV\_UK** sender ID received on **German** mobile numbers at the same time indicates **SMS blaster** abuse.

Timestamp	Sender ID	Text
20/05/2024 18:19	GOV_UK	Our records show that your tax refund of £267.78 can now be claime. Please continue via: <a href="https://govuk.hmrc.personal-tax.top">https://govuk.hmrc.personal-tax.top</a>





# Our Honeyypot Results

We notice a similar campaign with a different domain on **German** mobile numbers that we spotted on Jan, 21 2024 also indicating abuse of **SMS blaster**.





# Key Takeaways

- Smishing is a continuously evolving cybercrime affecting users worldwide.
- There is a lack of up-to-date publicly available datasets to study this threat.
- Our smishing honeypot provides timely, accurate and complete smish.
- It is possible to reproduce or/and scale the current infrastructure.
- The results support the efficiency of our seeding mechanisms.



