A Typology of Digital Scams: A Framework for Detection, Classification, and Prevention

The implementation of the project "Exposing scams: a Corporate and Civic Response" was possible thanks to the Civic Innovation Fund (CIF), a unique European pooled fund of THE CIVICS Innovation Hub. CIF is supported by the ERSTE Foundation

Title: A Typology of Digital Scams: A Framework for Detection, Classification, and Prevention

Date and Place of Publication: September 2025, Spain

Authors:

Pablo Hernández Escayola, Luisa Bernal Montoya, and Celia Ramos Vera. Fundación Maldita.es

Responsible Organizations:

This report was jointly produced by Fundación Maldita.es (Spain) and Faktograf (Croatia) as part of the project "Exposing Scams: A Corporate and Civic Response."

The implementation of the project was made possible thanks to the Civic Innovation Fund (CIF), a European pooled fund of The Civics Innovation Hub, supported by the ERSTE Foundation.

Localisation to Croatian:

Ivan Nekić and Ana Brakus. Croatian version available at: https://faktograf.hr/wp-content/uploads/2025/10/cif-scams-final-compressed.pdf

Content Index

INTRODUCTION

As nearly every aspect of our lives has become digitally connected, in recent years we have witnessed how the attack surface for cybercriminals has grown exponentially, and how, with today's technology, just a few keystrokes are enough to hijack networks, paralyze water supply systems, or even steal from virtual exchanges.

An illustrative case of this reality can be found in the data collected by the FBI's Internet Crime Complaint Center (IC3), the primary public reporting hub for scams and cyber threats in the United States. According to its 2024 Internet Crime Report, while IC3 initially received around 2,000 complaints per month, over the past five years it has averaged more than 2,000 complaints per day [1]. In the last year alone, the center registered 859,532 cybercrime complaints, with reported losses exceeding $16.6 billion (€14.225 million), representing a 33% increase from 2023 [1].

At the international level, the Global State of Scams Report 2024 by the Global Anti-Scam Alliance (GASA), based on a survey of 58,329 people worldwide, estimated that scams diverted over $1.03 trillion (€882.000 million) in just the past year —a sum that rivals the gross domestic product (GDP) of some nations [2]. For some countries, this has represented losses of more than 3% of their GDP, such as 4.2% in Pakistan and 3.6% in Kenya. The same report also highlighted the pervasiveness of the problem, noting that almost half of the global population encounters a scam at least once a week, while only 4% of victims manage to recover their money in full [2].

Moreover, the World Economic Forum's Global Cybersecurity Outlook 2025 identified technology-enabled cybercrime —including phishing, business email compromise (BEC), and vishing— as the second-highest organizational cyber risk for 2025 [3]. In fact, 42% of organizations reported experiencing phishing or social engineering attacks over the past 12 months. These campaigns have become increasingly sophisticated and scalable, for example, due to generative AI (GenAI) tools, which reduce the cost of attacks and allow cybercriminals to automate and personalize deceptive communications [3].

Beyond immediate financial losses, the spread of cyber fraud erodes citizens' trust in the digital ecosystem and jeopardizes the reputation of companies whose names and brands are exploited in fraudulent schemes.

In light of this reality, it is imperative to develop tools that enable the early identification of recurring patterns, the analysis of emerging trends, and the anticipation of new fraud dynamics. Based on this need, the present work is guided by a dual objective: **(1) to raise awareness among companies and monitoring agencies** about the social and economic impact of brand misuse, with an emphasis on transparency and ethical responsibility towards citizens harmed by these cyber frauds; and **(2) to equip professionals and citizens** with the knowledge required to detect and analyze how brands are exploited in scams designed to deceive users, extract personal data, and manipulate financial behavior. To this end, we propose the development of a **classification typology based on real cases**, conceived as a tool to support the **general public**, **media monitoring agencies** and **their clients** in identifying fraud patterns and enhancing financial awareness among citizens. The reasons for adopting this classification are as follows:

01

Expands knowledge of the problem and differentiates formats and data types more effectively

Cyber frauds display recurring patterns and formats that allow specialists to identify their key elements. These include, for example, message structures, fraudulent contact methods, and specific URL behaviors or social engineering techniques. Such differentiation facilitates classification, improves accuracy in incident identification, and deepens understanding of fraudsters' modus operandi across different contexts. Moreover, documenting these modalities functions as a historical record of cybercrime, useful for anticipating changes in the digital crime landscape.

02

Improves companies' response capacity

Enterprises and organisations need practical tools to identify when their brand is being misused in a fraud and to react quickly. Incident monitoring supported by a standardized typology will enable them to: more rapidly identify related incidents, design more specific internal response protocols and prevention campaigns, develop early-warning systems, and collaborate more effectively with other actors in the sector.

03

Reduces financial losses and reputational harm

A clear typology enables earlier detection and better classification, so that, by improving the identification and prevention of cyber fraud, it helps avoid financial losses for both consumers and companies while preserving brand value and customer trust (e.g., through proactive notifications and tailored communications when fraudsters misuse the brand), because when scammers use a brand to deceive, they can increase negative associations.

04

Fosters information and media literacy

By establishing a clear and specific classification of cyber frauds, this framework opens the door to information and media literacy programs—both external and internal—focused on cybersecurity and grounded in monitoring fraud by typology. For citizens, this means understanding how scams operate and recognizing their warning signs, thus

05

Ensures terminological consistency across organizations

Fragmentation in the way online scams are named and categorized hinders cooperation between companies, regulators, and civil society organizations. This typology is built on a carefully defined vocabulary subject to terminological control, ensuring that terms are used consistently and in alignment with other organizations. This, in turn, facilitates information future exchange and comparative trend analysis.

06

Benefits of effective public policies for consumer protection

In addition to its value for companies and organizations, the detailed classification and in-depth analysis of cyber frauds provide an invaluable resource for academic research and public policy development. In scientific contexts, it offers a solid empirical basis for studies in cybersecurity, digital criminology, and related fields. Furthermore, it enables longitudinal trend analyses capable of tracing the evolution of fraudsters' tactics and anticipating new fraud modalities—intelligence that is essential to inform the design of effective public policies on cybersecurity and consumer protection.

CONTEXT AND BACKGROUND

An **online scam or fraud** is a form of deliberate deception designed to obtain illicit gains at the expense of the victim. It is characterized by the use of fraudulent methods that appeal to the trust, ignorance, greed, or emotions of the affected person, in order to induce them to take action that benefits the scammer. The Australian federal police provide a more comprehensive definition of online fraud by defining the term as the **"any type of fraud scheme that uses email, web sites, chat rooms or message boards to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme."** [10]

Scams often use persuasion or psychological manipulation techniques to deceive victims, exploiting their good faith or taking advantage of their fears and desires. These actions may involve the use of convincing narratives, false promises, seemingly attractive offers, or identity theft.

The consequences of online fraud can range from financial losses to the loss of personal data (financial information, ID documents, and other relevant personal information), which cybercriminals can even use to impersonate the victim for criminal purposes. [33]

Cybercriminals and fraudsters are constantly refining their methods, using advanced technologies to increase the effectiveness and reach of their attacks.

- Use of Artificial Intelligence (AI) and Large Language Models (LLMs): Generative AI (GenAI) and LLMs are increasing the effectiveness of social-engineering techniques by enabling personalized communications and automating criminal processes [3, 6, 9].

They allow attackers to reduce the cost of phishing and social-engineering campaigns; convincingly mimic the communication styles of senior executives and organizations by leveraging contextual data from social networks, public statements, or leaked documents; and craft credible attacks in multiple languages simultaneously—thereby targeting more people across more countries at lower cost [3].

Recent studies show that phishing messages generated by LLMs achieve significantly higher click-through rates than those written by humans [7]. In addition, GenAI enables malicious actors to create convincing voice, video, and image deepfakes and to imitate corporate communication styles [6], which can be used to defraud both organisations (e.g., when such deepfakes are sustained during prolonged interactions with staff, they may help attackers gain access to corporate systems) and consumers. In this context, 47% of organizations surveyed by the WEF [3] expressed concern about adversarial capabilities powered by GenAI, and 55% of CISOs stated that deepfakes pose a moderate to significant cyber threat to their organization [3]. It is also worth noting that, although the rise of AI in scam tactics is a growing concern, 31% of respondents in GASA's 2024 survey were unsure whether the cyber scams they suffered involved AI [2].

- Common channels and platforms: Phone calls and text messages (SMS) remain the primary methods of initial contact, and platforms such as WhatsApp, Instagram, and Gmail are also frequently exploited by fraudsters [2].

- Increase in Ransomware attacks: Ransomware remains one of the top organizational risk concerns and a persistent, growing threat to organizations of all sizes [1, 8]. According to Verizon's 2025 Data Breach Investigations Report, ransomware was present in 44% of all analyzed breaches —marking a 37% increase from previous year [8]. In some good news, however, the median amount paid to ransomware groups fell to $115,000 (from $150,000 last year), and 64% of the victim organizations did not pay the ransoms, which was up from 50% two years ago [8].

- Social engineering: Cyber fraud (including phishing, BEC, vishing, etc.) is another of the highest risks [11], as illustrated by the fact that 42% of organizations surveyed by the WEF experienced a successful social engineering attack in 2024 [3]. Social engineering attacks involve the psychological compromise of a person that alters their behavior into taking an action or breaching confidentiality [8, 9]. Within this group, phishing and pretexting remain the primary tactics used to deceive employees [8, 11]. Phishing was found in 15% of all breaches, and the reporting rate for simulated phishing emails increased significantly after recent employee training [8].

Also notable is MFA prompt bombing—a tactic that floods users with multifactor authentication login requests in the hope they will relent just to make the prompts stop. It has been used successfully in more than 20% of social-engineering attacks in the public sector this year [8]. At the personal level, identity theft stands out as the leading perceived cyber risk (37%), followed by loss of access to utilities (24%), compromised personal data (20%), and cyber extortion (20%) [3].

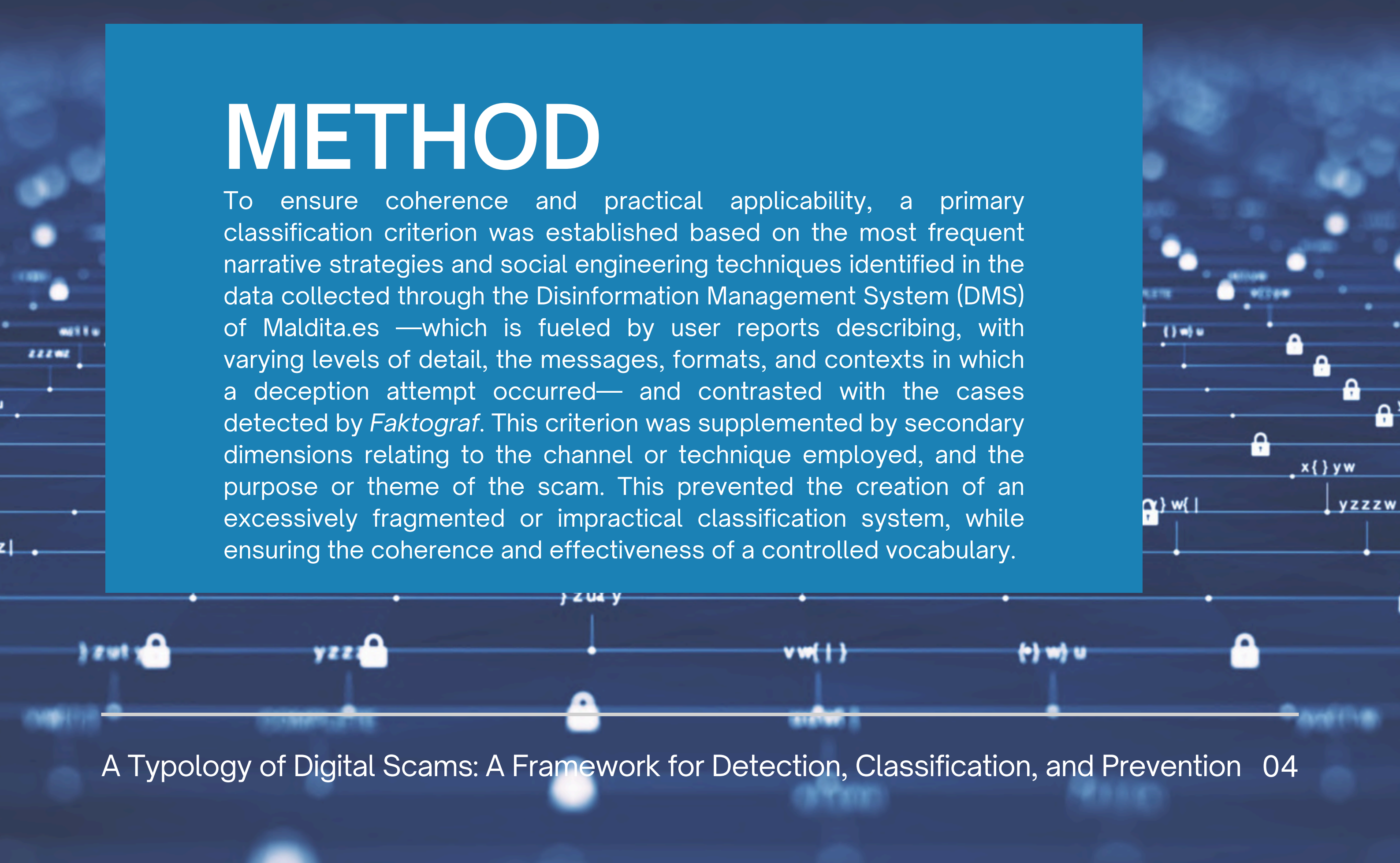
- Increase of charity scams leveraging emergency situations: This was visible during the COVID-19 pandemic, the Russian invasion of Ukraine, the earthquake in Türkiye and Syria, and the 2024 “DANA” Floods in Spain [11, 12]. Fraudsters show great versatility in modelling their narratives around current crises.

- Investment scams: especially those involving cryptocurrencies (also known as “pig butchering”), are the ones that report the highest losses, with a record $6.5 billion in 2024 and a 66% increase in cryptocurrency-related losses according to IC3 data [1].

- Crime-as-a-service (CaaS): This model remains dominant and fast-growing because it lets actors without technical expertise buy kits, infrastructure, and support to commit crimes—for example, to run ransomware campaigns or AI-enhanced phishing—thereby dramatically lowering the barrier to entry [3, 4]. To enable this, the CaaS ecosystem offers wide access to enablers and tools such as guides and tutorials on fraud methods in dark-web forums, phishing kits, remote administration tools (RATs), card dumps, and databases of personal data [11].

- Convergence with organized crime and “scam farms”: The rise and profitability of online fraud have attracted “traditionally” violent organized-crime groups to the cyber market. In Southeast Asia, more than 220,000 people have been documented as subjected to forced labor in “scam farms” that combine data collection, disinformation, and social engineering, acting as criminal service providers for third parties [5]. This culture of lower aversion to causing harm—including the impact on critical services—coupled with the scale enabled by CaaS platforms broadens the range of organizations exposed to attacks such as ransomware [3].

- Challenges in cyber resilience and the skills gap: Cyber inequality has worsened, creating a growing gap between large and small organizations, and between developed and emerging economies [3]. Only 15% of respondents in Europe and North America lack confidence in their country's ability to respond to major cyber incidents against critical infrastructure, while this proportion rises to 36% in Africa and 42% in Latin America [3]. The cyber skills gap has also widened, with two out of three organizations reporting moderate-to-critical deficiencies in this area, and only 14% of organizations saying that they have the necessary staff and skills [3].



METHOD

To ensure coherence and practical applicability, a primary classification criterion was established based on the most frequent narrative strategies and social engineering techniques identified in the data collected through the Disinformation Management System (DMS) of Maldita.es —which is fueled by user reports describing, with varying levels of detail, the messages, formats, and contexts in which a deception attempt occurred— and contrasted with the cases detected by *Faktograf*. This criterion was supplemented by secondary dimensions relating to the channel or technique employed, and the purpose or theme of the scam. This prevented the creation of an excessively fragmented or impractical classification system, while ensuring the coherence and effectiveness of a controlled vocabulary.

PRELIMINARY LIST OF TERMS AND SOURCE COLLECTION

Building on the Maldita.es team's prior expertise and references available in the cybersecurity field, a preliminary list of candidate terms was developed, partly inspired by the Cyberattack Guide of the Spanish National Cybersecurity Institute (INCIBE) [13], which served as a starting point for the typology.

This list was then expanded and refined using specialized sources, in order to ensure a solid and comprehensive classification and to minimize the risk of omitting relevant concepts. The sources reviewed included cybersecurity reports [4–6, 9, 14–17], academic and high-quality outreach articles [7, 9, 10, 18], prevention guides from recognized institutions (e.g., INCIBE [13, 19], Europol [11], Guardia Civil [20]), industry grey literature [21, 21, 22, 24] as well as bibliographic databases, existing classifications, taxonomies, thesauri, or controlled vocabularies available in specialized databases and repositories [25–32].

The process consisted of compiling the broadest possible repertoire of relevant terms, which were then provisionally grouped according to thematic similarity and affinity. This approach helped consolidate a robust set of terms, ensuring that no key element was omitted from the final classification.

DEFINITIONS AND TERMINOLOGICAL CONTROL

Once the candidate terms had been compiled, they were defined and subjected to terminological control, with the aim of ensuring a precise, coherent vocabulary adapted to the field of digital fraud. Defining the terms made it possible to delimit their meaning and, at the same time, facilitate the elimination of inconsistencies within the set. Given that classifications must function as controlled vocabularies, three properties were checked in this process:

- Homonymy: terms that coincided in form but referred to meanings outside the domain of digital fraud were discarded.
- Synonymy: when the same technique appeared under different names, the most precise and widely used term in specialized sources was selected. In cases where the terms were not strictly synonymous but were used interchangeably,

comprehensive definitions were developed to determine whether unification was appropriate or whether the concepts should be retained as distinct.

- Polysemy: in cases where terms had multiple meanings, a single criterion was applied, restricting each term to its sense related to digital scams.

STRUCTURAL CONSIDERATIONS

Once the candidate terms had been defined and non-relevant ones discarded, their relationships were analyzed to establish a coherent classification structure. The following types of relationships between terms can be identified:

- Hierarchical relationships (e.g., between impersonation techniques and their subtypes: phishing, smishing, vishing).

- Co-occurrence of terms (e.g., the same fraud that combines social engineering and malware).

- Strongly associated terms (e.g., “catfishing” and “impersonation of family or acquaintances” —a discarded term).

- Mutually exclusive terms.[1]

The result was a flexible and scalable typology, organized into two complementary dimensions, which are developed in the following section.

[1] We did not identify truly exclusive categories.In practice, attacks often span multiple dimensions —for example, a phishing attack may also deliver malware. Accordingly, the taxonomy is multi-label: analysts can select several options within the classification to categorise a single incident.

PROPOSED CATEGORIES OF SCAMS

The review of **specialized sources** —INCIBE's guides, academic articles, cybersecurity reports, and terminology databases— together with the analysis of data collected through *Maldita.es*'s DMS —which is fueled by user reports describing, with varying levels of detail, the messages, formats, and contexts in which a deception attempt occurred— and the experiences shared by *Faktograf* regarding its work in detecting and exposing scams has enabled the development of a typology for the structured classification of digital scams and frauds targeting the business environment.

While we are aware that digital scams may target password, connection or data and that malware can be used as a tool, the typology proposed here focuses specifically on those fraud schemes that rely on **social engineering techniques**. This focus reflects the nature of the cases reported to Maldita.es, which predominantly involve deception strategies aimed at manipulating users' trust, fear, or lack of awareness to achieve illicit gain, and for which we have accumulated the most data and experience. However, it is also recognized that it is important to include certain terms that reflect the specific objective or theme of the attack, such as financial fraud, attempts to steal personal data, or emotional scams, in order to ensure more comprehensive and contextualized coverage of the data.

Based on this, and to avoid an excessively fragmented or unmanageable classification, the typology has been organized around two main, non-exclusive dimensions: (1) t**he technical or channel-based**, which groups scams according to the social engineering techniques, the channels, or methods used to carry out the attack (e.g., phishing, smishing, QRshing, or vishing); and (2) **the thematic**, which classifies scams based on the narrative or pretext used to capture the victim's attention (such as investment promises, fake raffles, inheritances, romantic relationships, or false job offers). This approach emphasizes the thematic and discursive aspects of the content rather than its technical or structural characteristics, which makes the data more susceptible to identification and categorization within this typology.

In addition, it also allows for the detection of recurring patterns as well as the identification of emerging trends, which is particularly useful for generating alerts, designing prevention campaigns, or improving internal company protocols. Moreover, it is conceived as a flexible and scalable typology that can be adapted to evolving criminal tactics and incorporate new categories as they emerge

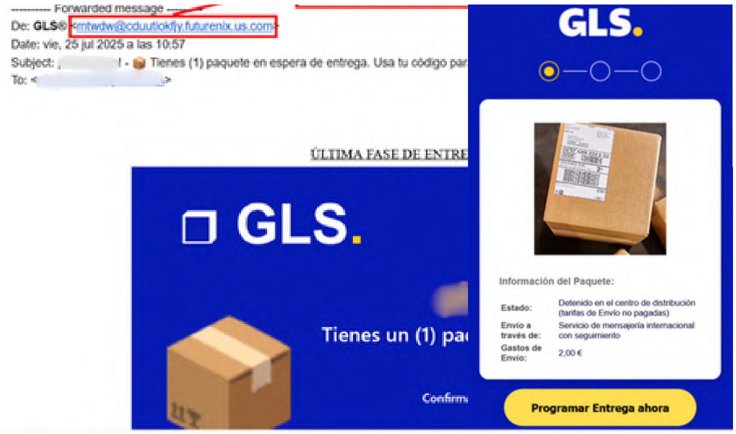
The following sections present the detailed classification, along with definitions, while representative examples illustrating each category can be found in the **Appendix.**

TYPOLOGY AND DEFINITIONS

Technical / Channel dimension

1. Social engineering attacks

These rely on a set of techniques aimed at users with the goal of getting them to reveal personal information or allow the attacker to take control of their devices. There are various types of attacks based on deception and manipulation:



---------- Forwarded message ---------
De: GLS® <mtwdw@cduutiokfly.futurenix.us.com>
Date: vie, 25 jul 2025 a las 10:57
Subject: [redacted] ! - 📦 Tienes (1) paquete en espera de entrega. Usa tu código par
To: <[redacted]>

ÚLTIMA FASE DE ENTRE

Tienes un (1) pa

Información del Paquete:

Estado:	Detenido en el centro de distribución (tarifas de Envío no pagadas)
Envío a través de:	Servicio de mensajería internacional con seguimiento
Gastos de Envío:	2,00 €

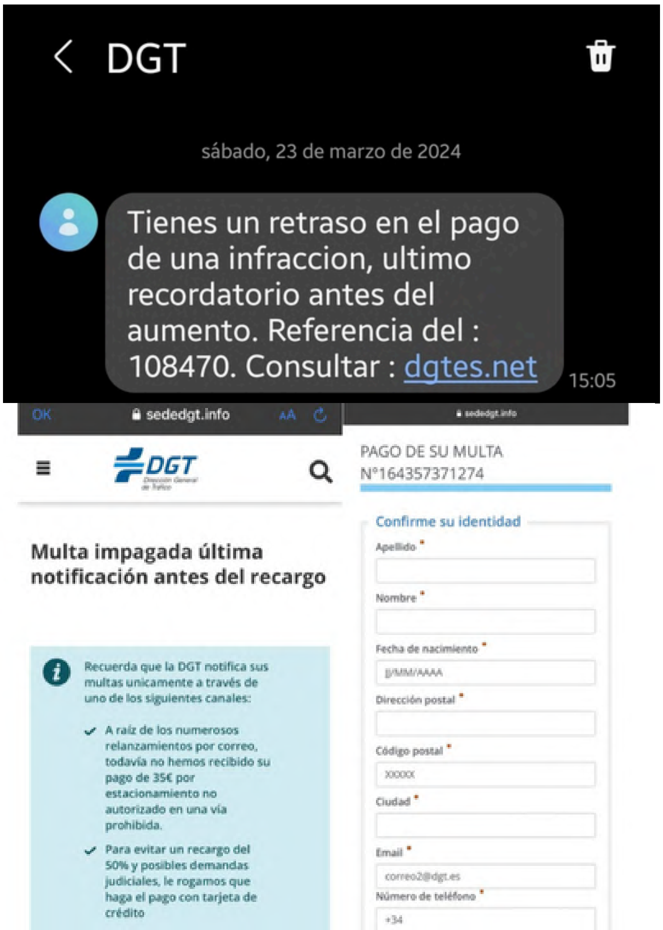
Figure 1. *Phishing scam impersonating GLS delivery service*
Note: *Fraudulent emails impersonating GLS inform users of a “pending delivery” and urge them to click on links leading to fake websites that request personal and banking data, demanding small payments as shipping fees. The brand identity is exploited to steal sensitive information and money.* ***Source:*** *Maldita.es*

1.1 Phishing

Sending a message via email, social media, or instant messaging while impersonating a legitimate entity—such as a bank, social network, tech support, or public institution—trusted by the user, in order to achieve the attacker's objective (Figure 1 and more examples in the Appendix: A1, A2, A3, A4, A17, A18).

1.2 Smishing

Sending a fraudulent SMS impersonating a trusted entity—such as a bank, social media platform, tech support, or public institution —to achieve the attacker’s goal (Figure 2).



DGT

sábado, 23 de marzo de 2024

Tienes un retraso en el pago de una infraccion, ultimo recordatorio antes del aumento. Referencia del : 108470. Consultar : dgtes.net 15:05

DGT Dirección General de Tráfico

Multa impagada última notificación antes del recargo

Recuerda que la DGT notifica sus multas unicamente a través de uno de los siguientes canales:

- ✓ A raíz de los numerosos relanzamientos por correo, todavía no hemos recibido su pago de 35€ por estacionamiento no autorizado en una vía prohibida.
- ✓ Para evitar un recargo del 50% y posibles demandas judiciales, le rogamos que haga el pago con tarjeta de crédito

PAGO DE SU MULTA
N°164357371274

Confirme su identidad

Apellido *

Nombre *

Fecha de nacimiento *
JJ/MM/AAAA

Dirección postal *

Código postal *
XXXXX

Ciudad *

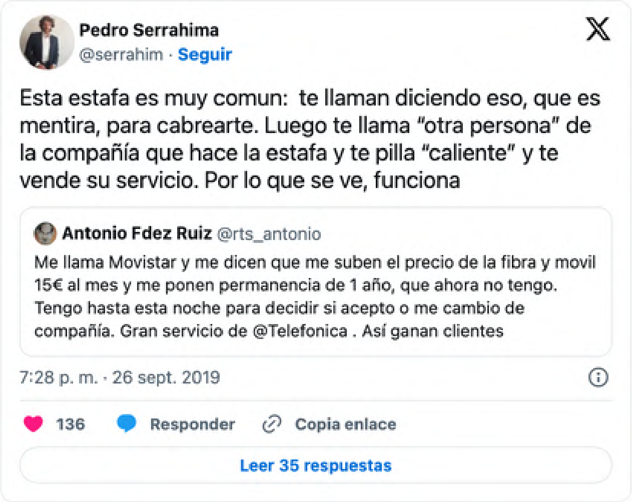
Email *
correo2@dgt.es

Número de teléfono *
+34

Figure A5. Smishing and false notifications from a service or institution

1.3 Vishing

A phone call (or video call) impersonating a legitimate entity —such as a bank, social network, technical service, or public entity—trusted by the user, in order to achieve their objective (Figure 3)).



Pedro Serrahima
@serrahim · Seguir

Esta estafa es muy comun: te llaman diciendo eso, que es mentira, para cabrearte. Luego te llama “otra persona” de la compañía que hace la estafa y te pilla “caliente” y te vende su servicio. Por lo que se ve, funciona

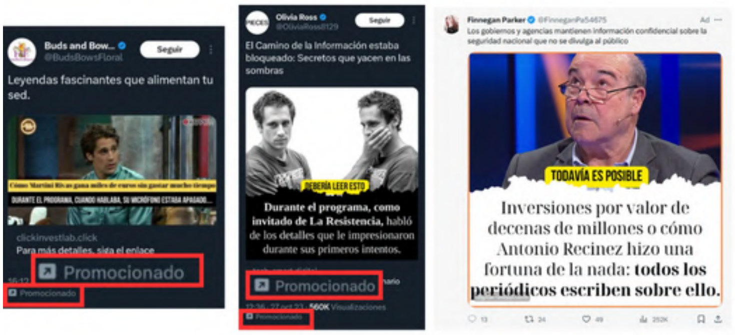
Antonio Fdez Ruiz @rts_antonio
Me llama Movistar y me dicen que me suben el precio de la fibra y movil 15€ al mes y me ponen permanencia de 1 año, que ahora no tengo. Tengo hasta esta noche para decidir si acepto o me cambio de compañía. Gran servicio de @Telefonica . Así ganan clientes

7:28 p. m. · 26 sept. 2019

Figure 3. Vishing and false notifications from a service or institution.
Note: *For more information, see Figure A6 in the Appendix.*

1.4 Baiting

Attackers use ads or websites that promote contests or prizes to lure users into sharing data or downloading malicious software. This can lead to theft of personal information, system takeover, network infection, or damage to devices (Figure 4, 5 and 6).



Buds and Bow... @BudsBowsFloral Seguir

Leyendas fascinantes que alimentan tu sed.

Cómo Martiñi Rivas gana miles de euros sin gastar mucho tiempo

DURANTE EL PROGRAMA, CUANDO HABLABA, SU MICRÓFONO ESTABA APAGADO...

clickinvestlab.click

Para más detalles, siga el enlace

Promocionado

16:12

Promocionado

Olivia Ross @OliviaRoss8129 Seguir

El Camino de la Información estaba bloqueado: Secretos que yacen en las sombras

DEBERÍA LEER ESTO

Durante el programa, como invitado de La Resistencia, habló de los detalles que le impresionaron durante sus primeros intentos.

Promocionado

12:36 · 27 oct 23 · 560K Visualizaciones

Promocionado

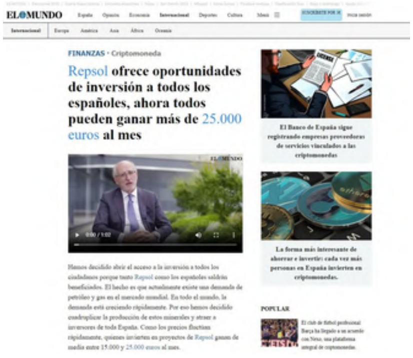
Finnegan Parker @FinneganPa54675 Ad

Los gobiernos y agencias mantienen información confidencial sobre la seguridad nacional que no se divulga al público

TODAVÍA ES POSIBLE

Inversiones por valor de decenas de millones o cómo Antonio Recinez hizo una fortuna de la nada: **todos los periódicos escriben sobre ello.**

13 24 49 252K



EL MUNDO España Opinión Economía Internacional Deportes Cultura Menú SUSCRÍBETE POR 1€ Iniciar sesión

Internacional Europa América Asia África Oceanía

FINANZAS · Criptomoneda

Repsol ofrece oportunidades de inversión a todos los españoles, ahora todos pueden ganar más de 25.000 euros al mes

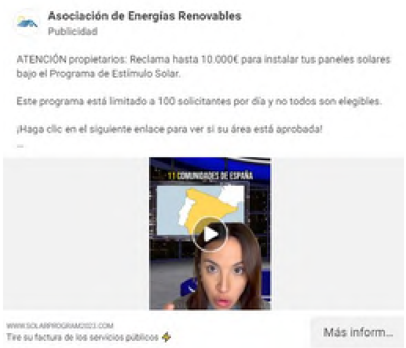
Hemos decidido abrir el acceso a la inversión a todos los ciudadanos porque tanto Repsol como los españoles saldrán beneficiados. El hecho es que actualmente existe una demanda de petróleo y gas en el mercado mundial. En todo el mundo, la demanda está creciendo rápidamente. Por eso hemos decidido cuadruplicar la producción de estos minerales y atraer a inversores de toda España. Como los precios fluctúan rápidamente, quienes invierten en proyectos de Repsol ganan de media entre 15.000 y 25.000 euros al mes.

El Banco de España sigue registrando empresas proveedoras de servicios vinculados a las criptomonedas

La forma más interesante de ahorrar e invertir: cada vez más personas en España invierten en criptomonedas.

POPULAR

El club de fútbol profesional Barça ha llegado a un acuerdo con Nexo, una plataforma integral de criptomonedas.



Asociación de Energías Renovables

Publicidad

ATENCIÓN propietarios: Reclama hasta 10.000€ para instalar tus paneles solares bajo el Programa de Estímulo Solar.

Este programa está limitado a 100 solicitantes por día y no todos son elegibles.

¡Haga clic en el siguiente enlace para ver si su área está aprobada!

WWW.SOLARPROGRAM2023.COM

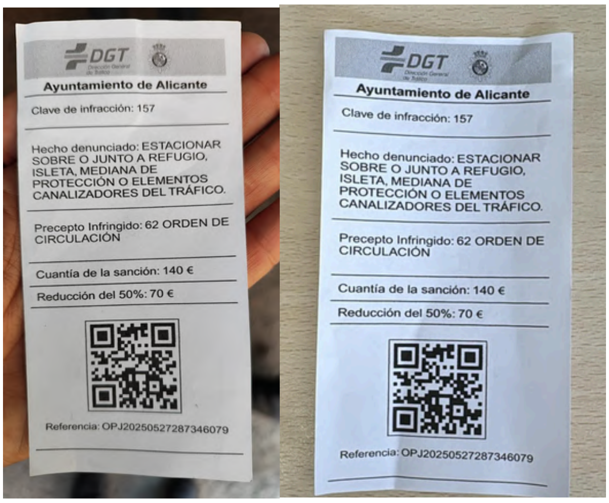
Tire su factura de los servicios públicos

Más inform...

Figure 4. Fraudulent ads on Twitter promoting fake cryptocurrency investments
Figure 5. Baiting and promotions or offers
Figure 6. Baiting, catfishing and investments
Note: *Fake ads on Twitter promote fabricated interviews with Spanish actors such as Martiño Rivas and Antonio Resines. The tweets redirect to websites impersonating media outlets, where the actors supposedly claim to earn "€128,000 extra each month" through crypto investments. These ads violate Twitter Ads' policies. Source: Maldita.es For more information, see Figure A7 in the Appendix.*

1.5 QRshing

Theft of data or money, or installation of malware, through the scanning of a malicious QR code (Figure 7).



DGT

Ayuntamiento de Alicante

Clave de infracción: 157

Hecho denunciado: ESTACIONAR SOBRE O JUNTO A REFUGIO, ISLETA, MEDIANA DE PROTECCIÓN O ELEMENTOS CANALIZADORES DEL TRÁFICO.

Precepto Infringido: 62 ORDEN DE CIRCULACIÓN

Cuantía de la sanción: 140 €

Reducción del 50%: 70 €

Referencia: OPJ20250527287346079

DGT

Ayuntamiento de Alicante

Clave de infracción: 157

Hecho denunciado: ESTACIONAR SOBRE O JUNTO A REFUGIO, ISLETA, MEDIANA DE PROTECCIÓN O ELEMENTOS CANALIZADORES DEL TRÁFICO.

Precepto Infringido: 62 ORDEN DE CIRCULACIÓN

Cuantía de la sanción: 140 €

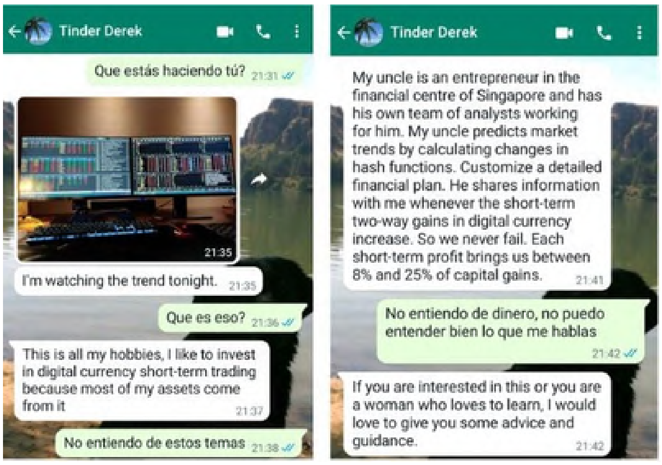
Reducción del 50%: 70 €

Referencia: OPJ20250527287346079

Figure 7. QRshing and notifications from a service or institution

1.6 Catfishing

Attackers impersonate someone else—such as a relative, acquaintance, or celebrity— or use a fake profile to deceive the victim and obtain personal information or money (Figure 8 and, more examples in the Appendix: A10)



Tinder Derek

Que estás haciendo tú? 21:31

21:35

I'm watching the trend tonight. 21:35

Que es eso? 21:36

This is all my hobbies, I like to invest in digital currency short-term trading because most of my assets come from it 21:37

No entiendo de estos temas 21:38

Tinder Derek

My uncle is an entrepreneur in the financial centre of Singapore and has his own team of analysts working for him. My uncle predicts market trends by calculating changes in hash functions. Customize a detailed financial plan. He shares information with me whenever the short-term two-way gains in digital currency increase. So we never fail. Each short-term profit brings us between 8% and 25% of capital gains. 21:41

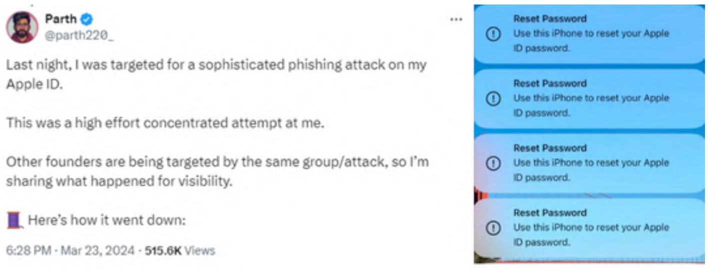
No entiendo de dinero, no puedo entender bien lo que me hablas 21:42

If you are interested in this or you are a woman who loves to learn, I would love to give you some advice and guidance. 21:42

Figure A8. Catfishing, investments and romantic relationship
Note: *For more information, see Figure A11 in the Appendix.*

2. Password attacks

Attempts to steal a user's credentials. Cybercriminals use techniques and tools to try to obtain our username and password. For example, they may use specialized software or try to guess it through trial and error, using information they have previously obtained. One of these attacks, MFA Bombing, combines social engineering and password-hacking techniques to try to steal our credentials (Figure 9).



Parth
@parth220_

Last night, I was targeted for a sophisticated phishing attack on my Apple ID.

This was a high effort concentrated attempt at me.

Other founders are being targeted by the same group/attack, so I'm sharing what happened for visibility.

🧵 Here's how it went down:

6:28 PM · Mar 23, 2024 · **515.6K** Views

Reset Password
Use this iPhone to reset your Apple ID password.

Reset Password
Use this iPhone to reset your Apple ID password.

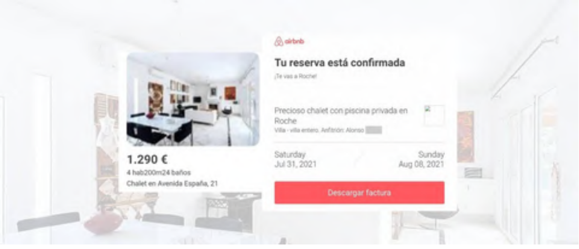
Reset Password
Use this iPhone to reset your Apple ID password.

Reset Password
Use this iPhone to reset your Apple ID password.

Figure 9. MFA bombing against Apple ID: notification flood + spoofed Apple Support call
Note: *The attack abuses the Apple ID password-reset flow to flood the iPhone with prompts, making the device hard to use (MFA fatigue). Minutes later, scammers call with caller-ID spoofing, impersonate Apple Support, and request the verification code "to stop the attack." If the victim shares it, the attackers take over the account, change the password, and access sensitive data. Source: Maldita.es*

3. Connection attacks

Interception of data exchanged between a user and a web service to monitor and steal information.



airbnb

Tu reserva está confirmada

¡Te vas a Roche!

Precioso chalet con piscina privada en Roche

Villa - villa entero. Anfitrión: Alonso [redacted]

Saturday
Jul 31, 2021

Sunday
Aug 08, 2021

Descargar factura

1.290 €

4 hab200m24 baños

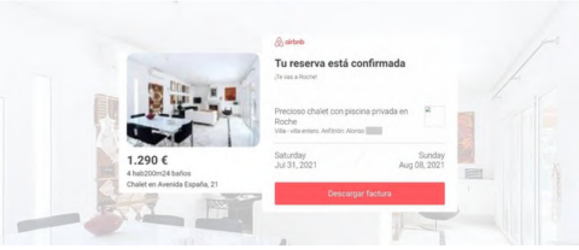
Chalet en Avenida España, 21

Figure 10. Web spoofing and property rentals or reservations
Note: *For more information, see Figure A12 in the Appendix.*

3.1 Spoofing

An attack that involves the malicious use of hacking techniques to impersonate a user's identity.

- **IP spoofing:** Falsifying an IP address to make it appear as a different one.
- **Web spoofing:** Creating a fake website that imitates a legitimate one (Figure 10)
- **Email spoofing:** Faking a trusted email address to deceive the recipient (Figure 10 and 11).
- **DNS spoofing:** Manipulating a legitimate domain (URL) to redirect users to a fraudulent website.
- **SMS spoofing** (see Appendix: A13)
- **Caller ID spoofing** (see Appendix: A14)



airbnb

Tu reserva está confirmada

¡Te vas a Roche!

Precioso chalet con piscina privada en Roche

Villa - villa entero. Anfitrión: Alonso [redacted]

1.290 €

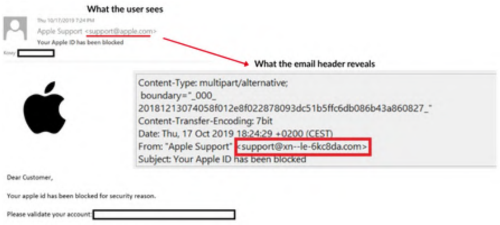
4 hab200m24 baños

Chalet en Avenida España, 21

Saturday
Jul 31, 2021

Sunday
Aug 08, 2021

Figure 10. Web spoofing and property rentals or reservations
Note: *For more information, see Figure A12 in the Appendix.*



Thu 10/17/2019 7:24 PM
Apple Support <support@apple.com>
Your Apple ID has been blocked
Kinvy: [redacted]

```
Content-Type: multipart/alternative;
 boundary="_000_
20181213074058f012e8f022878093dc51b5ffc6db086b43a860827_"
Content-Transfer-Encoding: 7bit
Date: Thu, 17 Oct 2019 18:24:29 +0200 (CEST)
From: "Apple Support" <support@xn--le-6kc8da.com>
Subject: Your Apple ID has been blocked
```

Dear Customer,

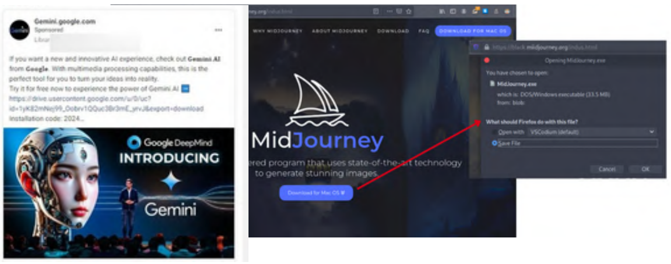
Your apple id has been blocked for security reason.

Please validate your account: [redacted]

Figure 11. Email spoofing example. Fake Apple Support message
Note:The sender appears to be "Apple Support" with a convincing layout and brand identity, but the underlying email is fraudulent, designed to deceive recipients and prompt unsafe actions. While the email client displays support@apple.com, the technical header reveals the true origin: support@xn--le-6kc8da.com. Source: Kaspersky

4. Malware attacks

Use of malicious software to perform harmful actions, such as stealing data, taking control of the system, or causing damage Figure 12



Gemini.google.com
Sponsored
Librar [redacted]

If you want a new and innovative AI experience, check out **Gemini AI** from **Google**. With multimedia processing capabilities, this is the perfect tool for you to turn your ideas into reality.
Try it for free now to experience the power of Gemini AI ➡
https://drive.usercontent.google.com/u/0/uc?id=1yK82mNej99_0obrv1QQuc3Br3mE_yrvJ&export=download
Installation code: 2024...

...ered program that uses state-of-the-art technology to generate stunning images.

https://black.midjourney.org/index.html

Opening MidJourney.exe

You have chosen to open:

MidJourney.exe

which is: DOS/Windows executable (33.5 MB)
from: blob:

What should Firefox do with this file?

○ Open with VSCodium (default)

● Save File

Figure 12. Fake generative A tool used to deliver malware
Note: *Cybercriminals are promoting free generative artificial intelligence tools on social media to redirect users to fraudulent websites. Instead of an AI program, victims download malware onto their computers that allows attackers to access confidential information such as passwords or bank details. Source: Maldita.es*

Thematic dimension

Promotions or offers

Scammers present a highly attractive fake offer, usually adding a time limit to take advantage of it, in an attempt to make the recipient act as quickly as possible (Figure 13).

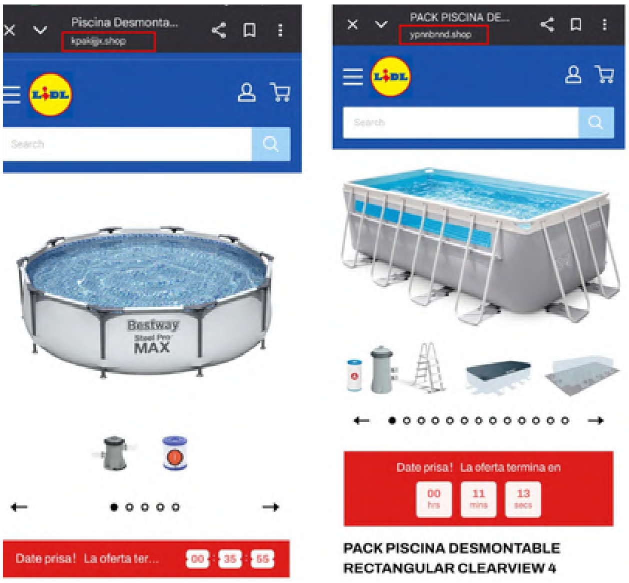
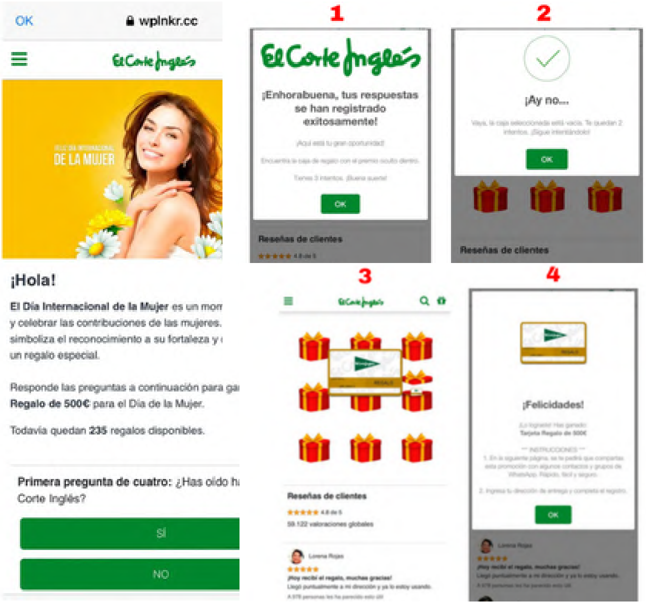


Figure 13. Phishing and promotions or offers
Note: *For more information, see Figure A1 in the Appendix.)*

Contests, raffles, or prizes

A prize or lottery opportunity is presented, and people are asked to provide their personal information in order to participate (Figure 14 and more examples in the Appendix: A7).



¡Hola!

El Día Internacional de la Mujer es un mom
y celebrar las contribuciones de las mujeres.
simboliza el reconocimiento a su fortaleza y
un regalo especial.

Responde las preguntas a continuación para ga
Regalo de 500€ para el Día de la Mujer.

Todavía quedan **235** regalos disponibles.

Primera pregunta de cuatro: ¿Has oído h
Corte Inglés?

¡Enhorabuena, tus respuestas se han registrado exitosamente!

¡Aquí está tu gran oportunidad!

Encuentra la caja de regalo con el premio oculto dentro.

Tienes 3 intentos. ¡Buena suerte!

¡Ay no...

Vaya, la caja seleccionada está vacía. Te quedan 2 intentos. ¡Sigue intentándolo!

59.122 valoraciones globales

¡Hoy recibí el regalo, muchas gracias!
Llegó puntualmente a mi dirección y ya lo estoy usando.
A 978 personas les ha parecido esto útil

¡Felicidades!

¡Lo lograste! Has ganado:
Tarjeta Regalo de 500€

** INSTRUCCIONES **

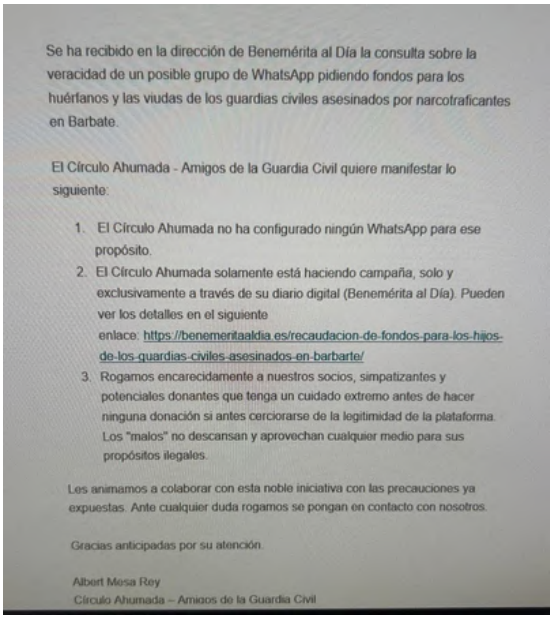
1. En la siguiente página, se te pedirá que compartas esta promoción con algunos contactos y grupos de WhatsApp. Rápido, fácil y seguro.

2. Ingresa tu dirección de entrega y completa el registro.

Figure 14. Phishing and false contests, raffles, or prizes

Inheritance, donations, or lottery

Scammers contact someone to inform them that they are entitled to a large sum of money, and that only the completion of a few paperwork is needed for it to be delivered, (Figure 15)



Se ha recibido en la dirección de Benemérita al Día la consulta sobre la veracidad de un posible grupo de WhatsApp pidiendo fondos para los huérfanos y las viudas de los guardias civiles asesinados por narcotraficantes en Barbate.

El Círculo Ahumada - Amigos de la Guardia Civil quiere manifestar lo siguiente:

1. El Círculo Ahumada no ha configurado ningún WhatsApp para ese propósito.
2. El Círculo Ahumada solamente está haciendo campaña, solo y exclusivamente a través de su diario digital (Benemérita al Día). Pueden ver los detalles en el siguiente enlace: https://benemeritaaldia.es/recaudacion-de-fondos-para-los-hijos-de-los-guardias-civiles-asesinados-en-barbarte/
3. Rogamos encarecidamente a nuestros socios, simpatizantes y potenciales donantes que tenga un cuidado extremo antes de hacer ninguna donación si antes cerciorarse de la legitimidad de la plataforma. Los "malos" no descansan y aprovechan cualquier medio para sus propósitos ilegales.

Les animamos a colaborar con esta noble iniciativa con las precauciones ya expuestas. Ante cualquier duda rogamos se pongan en contacto con nosotros.

Gracias anticipadas por su atención.

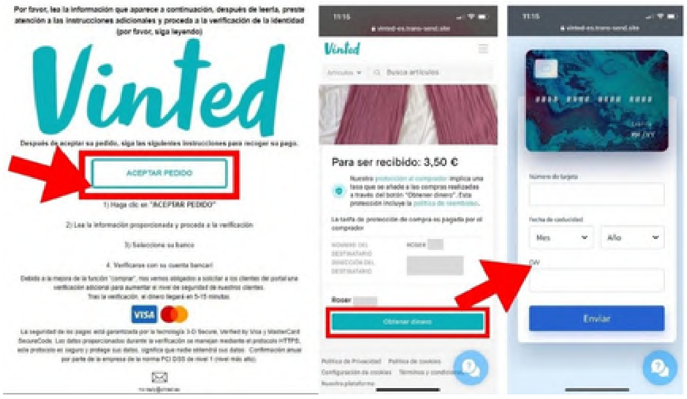
Albert Mesa Rey
Círculo Ahumada – Amigos de la Guardia Civil

Figure 15. Phishing and inheritance, donations, or lottery
Note: *For more information, see Figure A2 in the Appendix.*

Purchase or sale of products and services

cammers present a supposed platform to sell various products or provide some type of services (Figure 12)**. The most common formats are:**

- Medical or health-related products
- Online store
- Buying and selling platform (Figure. 16)



Por favor, lea la información que aparece a continuación, después de leerla, preste atención a las instrucciones adicionales y proceda a la verificación de la identidad (por favor, siga leyendo)

Después de aceptar su pedido, siga las siguientes instrucciones para recoger su pago.

ACEPTAR PEDIDO

1) Haga clic en "ACEPTAR PEDIDO"

2) Lea la información proporcionada y proceda a la verificación

3) Seleccione su Banco

4. Verificarse con su cuenta bancari

Debido a la mejora de la función "comprar", nos vemos obligados a solicitar a los clientes del portal una verificación adicional para aumentar el nivel de seguridad de nuestros clientes. Tras la verificación, el dinero llegará en 5-15 minutos.

La seguridad de los pagos está garantizada por la tecnología 3-D Secure, Verified by Visa y MasterCard SecureCode. Los datos proporcionados durante la verificación se manejan mediante el protocolo HTTPS, este protocolo es seguro y protege sus datos, significa que nadie obtendrá sus datos. Confirmación anual por parte de la empresa de la norma PCI DSS de nivel 1 (nivel más alto).

11:15
vinted-es.trans-send.site

Para ser recibido: 3,50 €

Nuestra protección al comprador implica una tasa que se añade a las compras realizadas a través del botón "Obtener dinero". Esta protección incluye la política de reembolso.

La tarifa de protección de compra es pagada por el comprador

NOMBRE DEL DESTINATARIO ROSER [redacted]
DIRECCIÓN DEL DESTINATARIO [redacted]

Roser [redacted]

Obtener dinero

11:15
vinted-es.trans-send.site

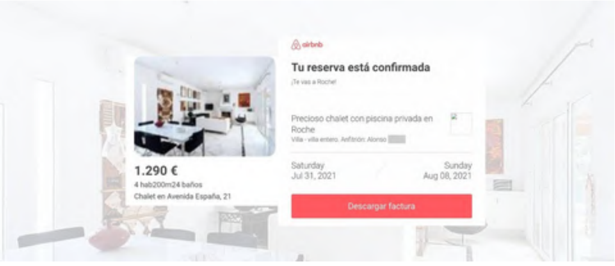
Número de tarjeta
Fecha de caducidad
Mes
Año
CVV

Enviar

Figure 16. Spoofed Vinted website used to steal banking data
Note: *Fraudsters sent sellers a deceptive "Accept order" email that redirected to a fake "Vinted" site mimicking its design but hosted on a fraudulent domain. Source: Maldita.es*

Property rentals or reservations

By simulating real estate offers, scammers can not only collect personal data but also request money in the form of advance payments or fees to reserve a house or an apartment. (Figure 17)



1.290 €
4 hab200m24 baños
Chalet en Avenida España, 21

Tu reserva está confirmada
¡Te vas a Roche!

Precioso chalet con piscina privada en Roche
Villa - villa entero. Anfitrión: Alonso [redacted]

Saturday
Jul 31, 2021

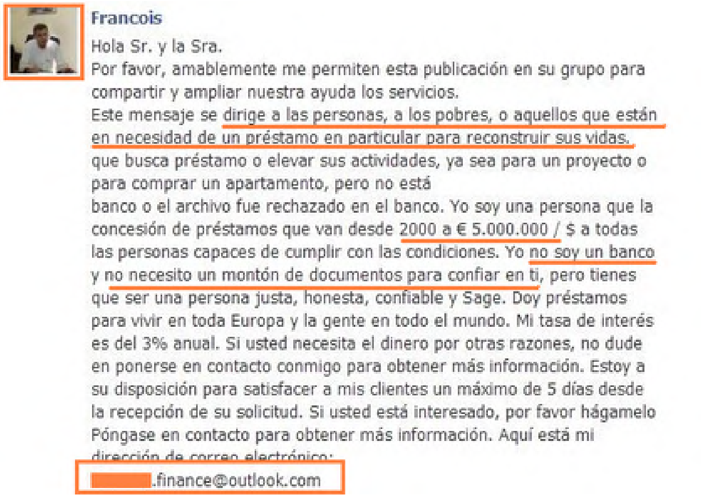
Sunday
Aug 08, 2021

Descargar factura

Figure 17. Web spoofing and property rentals or reservations
Note: *For more information, see Figure A12 in the Appendix.*

Loans

The scammer offers supposed loans on very favorable terms, better than what could be obtained from a bank. (Figure 18)



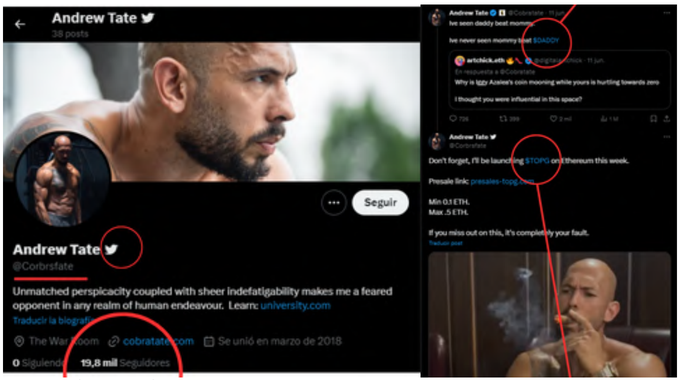
Francois

Hola Sr. y la Sra.
Por favor, amablemente me permiten esta publicación en su grupo para compartir y ampliar nuestra ayuda los servicios.
Este mensaje se dirige a las personas, a los pobres, o aquellos que están en necesidad de un préstamo en particular para reconstruir sus vidas. que busca préstamo o elevar sus actividades, ya sea para un proyecto o para comprar un apartamento, pero no está banco o el archivo fue rechazado en el banco. Yo soy una persona que la concesión de préstamos que van desde 2000 a € 5.000.000 / $ a todas las personas capaces de cumplir con las condiciones. Yo no soy un banco y no necesito un montón de documentos para confiar en ti, pero tienes que ser una persona justa, honesta, confiable y Sage. Doy préstamos para vivir en toda Europa y la gente en todo el mundo. Mi tasa de interés es del 3% anual. Si usted necesita el dinero por otras razones, no dude en ponerse en contacto conmigo para obtener más información. Estoy a su disposición para satisfacer a mis clientes un máximo de 5 días desde la recepción de su solicitud. Si usted está interesado, por favor hágamelo Póngase en contacto para obtener más información. Aquí está mi dirección de correo electrónico:
[redacted].finance@outlook.com

Figure 18. Catfishing and loans
Note: *For more information, see Figure A15 in the Appendix.*

Investments

A supposed investment is presented, promising a very high return in a short period of time. The use of cryptocurrencies as a lure is common. (Figures 4, 6 and 19)



Andrew Tate
38 posts

Seguir

Andrew Tate
@Corbrsfate
Unmatched perspicacity coupled with sheer indefatigability makes me a feared opponent in any realm of human endeavour. Learn: university.com
Traducir la biografía
The War Room cobratate.com Se unió en marzo de 2018
0 Siguiendo 19,8 mil Seguidores

Andrew Tate @Cobratate · 11 jun.
Ive seen daddy beat mommy.
Ive never seen mommy beat $DADDY

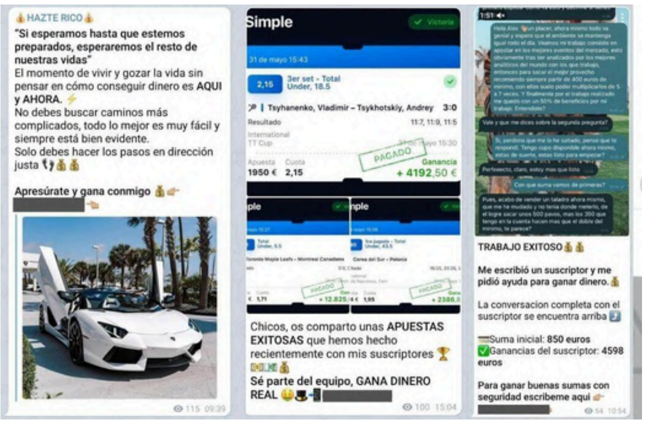
artchick.eth @digitalartchick · 11 jun.
En respuesta a @Cobratate
Why is Iggy Azalea's coin mooning while yours is hurtling towards zero
I thought you were influential in this space?

Andrew Tate
@Corbrsfate
Don't forget, I'll be launching $TOPG on Ethereum this week.
Presale link: presales-topg.com
Min 0.1 ETH.
Max .5 ETH.
If you miss out on this, it's completely your fault.
Traducir post

Figure 19. Catfishing and investments
Note: *For more information, see Figure A10 in the Appendix*

Gambling (Fig. A16)

The popularization of online gaming makes it easier for scammers to pose as betting companies or specialized websites. (Figure 20)



💰HAZTE RICO💰
"Si esperamos hasta que estemos preparados, esperaremos el resto de nuestras vidas"
El momento de vivir y gozar la vida sin pensar en cómo conseguir dinero es **AQUI y AHORA.** ⚡
No debes buscar caminos más complicados, todo lo mejor es muy fácil y siempre está bien evidente.
Solo debes hacer los pasos en dirección justa 👣💰💰

Apresúrate y gana conmigo 💰👉
[redacted] 👈

115 09:39

Simple ✓ Victoria
31 de mayo 15:43
2,15 3er set - Total Under, 18.5
Tsyhanenko, Vladimir – Tsykhotskiy, Andrey 3:0
Resultado 11:7, 11:9, 11:5
International TT Cup 31 de mayo 15:30
PAGADO
Apuesta 1950 € Cuota 2,15 Ganancia + 4192,50 €

Toronto Maple Leafs - Montreal Canadiens PAGADO + 12.825
Corea del Sur - Polonia PAGADO + 2386

Chicos, os comparto unas **APUESTAS EXITOSAS** que hemos hecho recientemente con mis suscriptores 🏆💵💰
Sé parte del equipo, GANA DINERO REAL 🤑🎩➡️[redacted]

100 15:04

1:51

Hola Alex 👋 un placer, ahora mismo todo va genial y espero que el ambiente se mantenga igual todo el día. Veamos mi trabajo consiste en apostar en los mejores eventos del mercado, esto obviamente tras ser analizados por los mejores analíticos del mundo con los que trabajo, entonces para sacar el mejor provecho recomiendo siempre partir de 400 euros de mínimo, con ellos suelo poder multiplicarlos de 5 a 7 veces. Y finalmente por el trabajo realizado me quedo con un 50% de beneficios por mi trabajo. Entendiste?

Vale y que me dices sobre la segunda pregunta?

Si, perdona que me lo he saltado, pensé que te respondí. Tengo cupo disponible ahora mismo, estas de suerte, estas listo para empezar?

Perfeeecto, claro, estoy mas que listo

Con que suma vamos de primeras?

Pues, acabo de vender un taladro ahora mismo, que me he mudado y no tenia donde meterlo, de el logre sacar unos 500 pavos, mas los 350 que tengo en la cuenta hacen mas que el doble del mínimo, te parece?

TRABAJO EXITOSO💰💰

Me escribió un suscriptor y me pidió ayuda para ganar dinero.💰

La conversacion completa con el suscriptor se encuentra arriba ⤴️

💳Suma inicial: **850 euros**
✅Ganancias del suscriptor: **4598 euros**

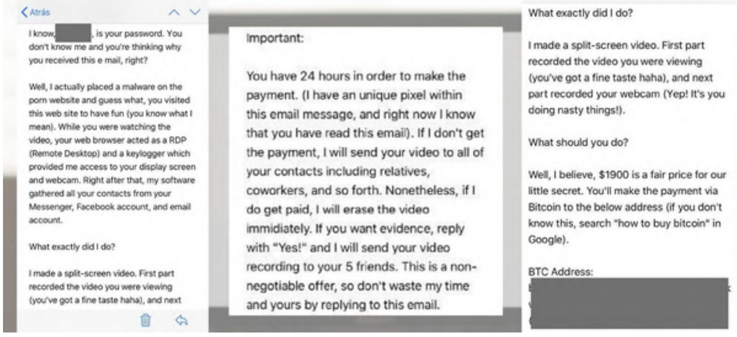
Para ganar buenas sumas con seguridad escribeme aqui 👉
[redacted]

54 10:54

Figure 20 Catfishing and gambling
Note: *For more information, see Figure A16 in the Appendix.*

Threats and extortion

The scammer directly threatens the victim to demand money. One way of doing this is by threatening to release compromising sexual videos or images. This is known as sextortion. (Figure 21)



Atrás

I know, [redacted], is your password. You don't know me and you're thinking why you received this e mail, right?

Well, I actually placed a malware on the porn website and guess what, you visited this web site to have fun (you know what I mean). While you were watching the video, your web browser acted as a RDP (Remote Desktop) and a keylogger which provided me access to your display screen and webcam. Right after that, my software gathered all your contacts from your Messenger, Facebook account, and email account.

What exactly did I do?

I made a split-screen video. First part recorded the video you were viewing (you've got a fine taste haha), and next

Important:

You have 24 hours in order to make the payment. (I have an unique pixel within this email message, and right now I know that you have read this email). If I don't get the payment, I will send your video to all of your contacts including relatives, coworkers, and so forth. Nonetheless, if I do get paid, I will erase the video immidiately. If you want evidence, reply with "Yes!" and I will send your video recording to your 5 friends. This is a non-negotiable offer, so don't waste my time and yours by replying to this email.

What exactly did I do?

I made a split-screen video. First part recorded the video you were viewing (you've got a fine taste haha), and next part recorded your webcam (Yep! It's you doing nasty things!).

What should you do?

Well, I believe, $1900 is a fair price for our little secret. You'll make the payment via Bitcoin to the below address (if you don't know this, search "how to buy bitcoin" in Google).

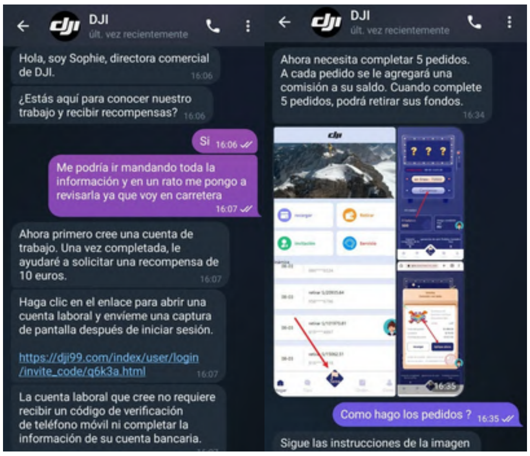
BTC Address:

[redacted]

Figure 21. Sextortion email scam demanding Bitcoin payments
Note: *Fraudulent emails threaten users with the release of supposed intimate videos (which do not actually exist) unless a Bitcoin payment is made. Source: Maldita.es*

Job offers

By pretending to offer a job, scammers can ask potential candidates for all kinds of personal information and, on some occasions, also request a fee to participate in the selection process. (Figure 22)



DJI
últ. vez recientemente

Hola, soy Sophie, directora comercial de DJI. 16:06

¿Estás aquí para conocer nuestro trabajo y recibir recompensas? 16:06

Si 16:06

Me podría ir mandando toda la información y en un rato me pongo a revisarla ya que voy en carretera 16:07

Ahora primero cree una cuenta de trabajo. Una vez completada, le ayudaré a solicitar una recompensa de 10 euros. 16:07

Haga clic en el enlace para abrir una cuenta laboral y envíeme una captura de pantalla después de iniciar sesión.

https://dji99.com/index/user/login/invite_code/q6k3a.html 16:07

La cuenta laboral que cree no requiere recibir un código de verificación de teléfono móvil ni completar la información de su cuenta bancaria.

DJI
últ. vez recientemente

Ahora necesita completar 5 pedidos. A cada pedido se le agregará una comisión a su saldo. Cuando complete 5 pedidos, podrá retirar sus fondos. 16:34

16:35

Como hago los pedidos ? 16:35

Sigue las instrucciones de la imagen

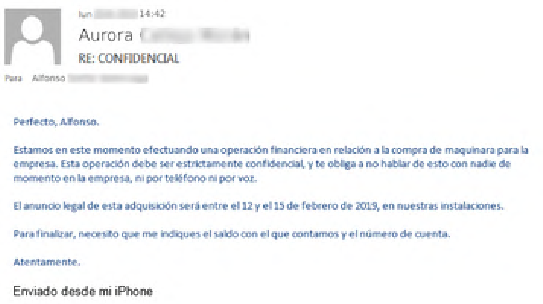
Figure 22. Phishing and false jobs offers
Note: *For more information, see Figure A4 in the Appendix.*

Romantic relationship

Scammers pose as someone who has fallen in love with the person they are trying to defraud. They use fake images and pretend to urgently need money. (Figure 8)

Work environment (Fig. A17)

The scammer poses as a coworker or a boss and takes advantage of trust or hierarchy to request information or something else. (Figure 23 and more examples in the Appendix: A18)



lun [redacted] 14:42

Aurora [redacted]

RE: CONFIDENCIAL

Para Alfonso [redacted]

Perfecto, Alfonso.

Estamos en este momento efectuando una operación financiera en relación a la compra de maquinara para la empresa. Esta operación debe ser estricktamente confidencial, y te obliga a no hablar de esto con nadie de momento en la empresa, ni por teléfono ni por voz.

El anuncio legal de esta adquisición será entre el 12 y el 15 de febrero de 2019, en nuestras instalaciones.

Para finalizar, necesito que me indiques el saldo con el que contamos y el número de cuenta.

Atentamente.

Enviado desde mi iPhone

Figure 23. Phishing and work environment: CEO fraud
Note: *For more information, see Figure A17 in the Appendix.*

Notifications from a service or institution

The potential victim is contacted by someone pretending to be a trustworthy organization or institution, in an attempt to obtain their personal information and money. (Figures 1, 2,7, 24 and more examples in the Appendix: A13)

"They took all my money from the bank by pretending to be La Caixa, and I checked myself that it was a CaixaBank number"

Figure 24. Caller ID spoofing and notifications from a service or institution
Note: For more information, see Figure A14 in the Appendix.

Other topics

Scammers adapt their messages to the changing habits and customs of the time, as well as to the cultural characteristics of each region, so that different types of themes may appear at specific times and places.

The categories are not mutually exclusive; in other words, some scams may fall under more than one technique and thematic category. For example, a phone call in which fraudsters impersonate a bank while also spoofing its number should be categorized both as vishing and as a connection attack. Another illustrative case is the fake Microsoft technical support scam, in which cybercriminals call victims, claiming their computer is infected (vishing), and ultimately attempt to install a malicious remote-control program (malware).

APPLICATIONS

CORPORATE AND ORGANIZATIONAL USE

The typology can be integrated into brand protection and risk management strategies. For example:

- Integration into monitoring tools: Media monitoring agencies or cybersecurity providers can map scam reports according to the typology, allowing companies to visualize which categories of fraud most frequently exploit their brand. This facilitates prioritization (for instance, if phishing and fake sweepstakes dominate, resources can be allocated to those areas).

- Internal training: The typology can be translated into training modules for staff, enabling, for example, customer service teams to recognize fraud patterns and guide customers who report suspicious contacts.

- Crisis response: When a new scam emerges, companies can quickly classify it according to the typology, link it to previous cases, and generate pre-drafted customer alerts. This shortens response times and ensures consistency in communication.

PUBLIC SECTOR AND REGULATORY USE

For regulators and supervisory bodies, the typology standardizes a reporting and analysis language. Among the possible applications, we can distinguish:

- Incident databases: Fraud reports can be systematically coded using the typology, enabling data comparison across agencies and over time.

- Cross-sector and transnational cooperation: A shared typology allows institutions from different countries to harmonize terminology and exchange useful, easily comparable information.

- Trend monitoring: Regulators can track which categories of scams are gaining prevalence and use this information to issue public alerts or take coercive/inhibitory measures.

EDUCATIONAL AND CITIZEN-FACING USE

The typology has strong pedagogical potential:

- Literacy for professionals: Journalists, educators, and other stakeholders can use the typology as a reference to report accurately and teach about fraud dynamics.

- Awareness campaigns: Public institutions and civil society organizations can design campaigns around specific scam categories (“romance scams,” “lottery frauds”), showing citizens real examples from the typology.

- Verification flow for citizens: The typology can be adapted into a verification flow that guides users in identifying whether they are facing a scam: Does the message include urgent claims? Does it request an advance payment? Is the contact impersonating a public institution? Each critical question could correspond directly to a scam category, serving as a reference framework to help users make informed decisions.

Recommendations

Recommendations are strategically tailored to the characteristics and needs of the target audiences, ensuring that applications are easier to implement, easier to use, and ultimately more effective.

01 For Companies

02 For Citizens

03 For Authorities

04 For Online Services

05 For Fact-checking Organisations

For companies

Internal Training. Develop continuous cybersecurity training programs for employees guided by expert organizations in scams and financial literacy, reinforced by regular phishing and social engineering drills. It is advisable to make use of publicly available national and European resources (guidelines, training programs, and digital tools) to foster a culture of cybersecurity within the organization.

Protection and Security Protocols. Implement advanced technical measures (two-factor authentication, email filtering, access monitoring, encryption of sensitive data) and establish official communication channels with clients and suppliers to reduce the risk of impersonation.

Regulatory Compliance and Cyber Resilience. Ensure compliance with European cybersecurity regulations (NIS2, DORA, Cyber Resilience Act, among others) as part of the corporate strategy. Additionally, promote cyber resilience, understood as the capacity to guarantee operational continuity in the face of incidents.

Cooperation and Early Warning. Maintain direct contact with specialized organizations and promote collaboration with companies and sectoral associations, sharing information on fraud attempts to anticipate patterns and emerging threats.

Social Responsibility and Transparency. Assume corporate responsibility for protecting citizens from cyber risks by ensuring transparent incident reporting and disseminating preventive alerts. This practice contributes to curbing the spread of cyber scams and strengthening trust in the brand. It can be included as part of the company’s responsible communication with its clients, reinforcing trust and demonstrating a commitment to transparency and accountability

For citizens

Critical Attitude and Verification. Be cautious of urgent messages or those promising significant discounts or benefits, and always verify the authenticity of emails, URLs, and social media profiles. Learn to recognize when a message triggers a strong emotional reaction—whether alarm or excitement. Developing this awareness helps prevent impulsive responses and encourages taking the necessary steps to verify information before acting. It is important to incorporate the practice of conducting your own search as a standard habit, ensuring it becomes an integrated and natural part of the process.

Contact specialized organizations. If you have doubts that something might be a scam attempt, contact organizations specialized in scam detection. Not only will their experts help you clear up your doubts, but also, if it is indeed a scam attempt, your alert will help warn other citizens. Follow the advice of these organizations to improve your ability to detect possible fraud

Reporting and Collaboration. Report fraud attempts to the platforms involved through their dedicated channels to flag illegal content. Likewise, share such information with family and contacts, thereby helping to break the chain of deception. Maintaining open conversations about these issues can help prevent potential risks and also ensure that clear communication channels are in place, enabling timely reporting and effective response when challenges arise.

Personal Protection and Prevention. Use strong passwords, enable two-factor authentication, keep software updated, and consult reliable sources to stay informed about new types of fraud.

For authorities

Educational Campaigns. Disseminate clear and regular messages on new types of cyber fraud through both traditional and digital media. Ensure that campaigns are kept up to date and respond to new developments and techniques.

Law enforcement. Apply existing regulation (i.e. EU's Digital Services Act) on illegal content online, which includes scams, to ensure platforms are complying with their obligations on removal and mitigation of this risk.

Efficient Reporting Channels. Simplify procedures for citizens and companies to report online fraud. Ensure that there are effective and user-friendly communication channels in place, with the capacity to efficiently direct citizens to the appropriate services. This approach enhances accessibility, improves service delivery, and strengthens trust between the organization and its stakeholders.

International Cooperation. Strengthen networks for police and judicial information exchange, given that many online frauds cross borders.

Data Transparency. Publish regular reports with statistics and examples of detected fraud. Include specific practical and preventive recommendations in reports. In addition, incorporate an impact-oriented strategy to ensure that findings and conclusions are actionable, effectively guiding decision-making and improving the overall effectiveness of reports.

For online services

Law compliance. Act in accordance to existing law (i.e. Digital Services Act) to counter illegal content online, including establishing reporting channels and acting on flags as well as, for Very Large Services, assess and mitigate the risks of platforms being exploited for illegal scamming campaigns.

Better detection. Continuously update detection methods to prevent this type of content being disseminated in online services, attending to the limitations of automated scanning.

Cooperation. Work closely with specialized organisations and authorities in order to exchange knowledge on new patterns and tactics in order to better protect users.

For fact-checking organizations

Systematic Monitoring. Track recurring narratives and tactics used in online scamming campaigns to identify variations. Deactivating the narratives takes longer, but it allows us to understand the logic and strategy behind the fraud and prevent possible variations of the same modus operandi.

Partnerships with Platforms. Establish sustainable cooperation schemes that allow swifter detection and removal of fraudulent ads or posts, and make use of existing channels of removal. Have protocols in place to actively report fraudulent content on the platform and also communicate about it clearly through secure channels, expanding existing prebunking content.

Accessible Language. Produce clear, visual, and easily shareable debunking materials, tailored to different levels of digital literacy. Ensure that these materials are accessible on the channels used by the target audiences of the frauds.

Impact Assessment. Measure the reach of issued alerts to improve the effectiveness of preventive communication.

Engagement with Key Stakeholders. Establish open communication channels to alert affected companies and authorities about detected scam campaigns.

CONCLUSIONS

The rapid evolution of digital fraud, fueled by advances such as generative AI, demands frameworks that provide clarity and consistency in classification. The typology presented here responds to this need, offering a curated vocabulary and practical categorization that can support prevention, awareness-raising, and coordinated responses across sectors.

Coordination among the various actors combating digital fraud is essential to minimize its effects. Efficiently categorizing the different types of scams is a basic step to improve the effectiveness of the measures taken against them. The typology proposed here covers almost all the scams and frauds currently circulating on social media.

Although the recent emergence of artificial intelligence tools has boosted this type of fraudulent practices, this new technology has not, so far, brought any innovations in terms of the techniques or themes of deception. Scammers have begun to use artificial intelligence to enhance, systematize, and expand the impact of the scams they were already using, but new-generation AI-based frauds have not emerged. Therefore, although the landscape of digital scams is changing, we believe that the typology we propose is completely current and useful for monitoring and analyzing online fraud attempts.

The emergence of artificial intelligence is an example of how scammers adapt to technological advances to update their fraud attempts. That is why it is important for authorities and companies to take responsibility for remaining vigilant against these phenomena and to implement the necessary tools to protect citizens and prevent them from becoming victims of scams.

But it is also essential to focus on the citizens who fall victim to scams.

Media and financial literacy is an indispensable tool to make people harder to deceive and more capable of detecting possible fraud attempts. These training programs should also be renewed and updated regularly to be as effective as possible in such a rapidly changing landscape as online scams.

Collaboration between organizations specialized in scam detection is another area that should be actively strengthened. Joint efforts provide a broader understanding of scammers' activities, facilitate the detection of international fraud operations, and allow the sharing of experiences in combating these criminal practices. A notable example of the benefits of collaboration is the investigation led by Maldita.es into a network of Facebook pages impersonating public transportation services. More than a dozen fact-checkers from different countries, including Faktograf, participated in the investigation, which uncovered over 1,000 fraudulent pages attempting to scam citizens across 60 countries.

It is essential to maintain and reinforce this type of collective and collaborative work to share expertise among different organizations in this field. For instance, existing structures such as the European Fact-Checking Standards Network (EFCSN) could be leveraged to conduct a survey on the most prevalent types of scams in each country, thereby enabling more effective and targeted responses.

At the same time, certain limitations must be recognized. Complex fraud schemes that combine advanced technical components with social engineering may not be fully captured by a single category. Furthermore, the fact that the classification is primarily centered on social engineering techniques could imply the omission of widely used cybersecurity terms. However, the typology's multi-label design ensures flexibility, allowing analysts to classify scams across multiple dimensions when necessary. And while prioritizing social engineering attacks represents a limitation in terms of coverage, it provides a gain in operability and coherence.

The typology should therefore not be considered a static or exhaustive model, but rather a flexible, scalable, and practical tool. Its adoption can improve the early detection of fraud patterns, enhance crisis response and prevention strategies, help avoid financial losses and reputational costs, be used to promote literacy in the field both externally and internally, and facilitate the adoption of a curated vocabulary.

REFERENCES

1. FBI’s Internet Crime Complaint Center. (2025). *Internet Crime Report 2024*. https://tinyurl.com/bjx965ab

2. Global Anti-Scam Alliance (GASA). (2024). *Global State of Scams Report 2024*. https://tinyurl.com/5yefneky

3. World Economic Forum (WEF). (2025, January). *Global Cybersecurity Outlook 2025. Insight Report.* https://tinyurl.com/ycyjwk7b

4. Europol. (2024, April 18). International investigation disrupts phishing-as-a-service platform LabHost. https://tinyurl.com/5fmmwhx4.

5. United Nations Office on Drugs and Crime. (2023, September). Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia. https://tinyurl.com/y6fjvw3d

6. Internet Organised Crime Threat Assessment (IOCTA). (2025). *Steal, deal and repeat: How cybercriminals trade and exploit your data*. https://tinyurl.com/48nfcc48

7. Heiding, F., Lermen, S., Kao, A., Schneier, B., & Vishwanath, A. (2024). Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects. arXiv preprint arXiv:2412.00586. https://doi.org/10.48550/arXiv.2412.00586

8. Verizon. (2025). *2025 Data Breach Investigations Report*. https://www.verizon.com/business/resources/Tbf6/reports/2025-dbir-data-breach-investigations-report.pdf

9. Rathod, T., Jadav, N. K., Tanwar, S., Alabdulatif, A., Garg, D., & Singh, A. (2025). A comprehensive survey on social engineering attacks, countermeasures, case study, and research challenges. *Information Processing & Management*, *62*(1), 103928. https://doi.org/10.1016/j.ipm.2024.103928

10. Kävrestad, J., & Nohlberg, M. (2018, September). Defining and Modelling the Online Fraud Process. In HAISA (pp. 203-213).

11. Europol. (2023). *Europol Spotlight - Online Fraud Schemes: A Web Of Deceit*. https://tinyurl.com/mea6ux7h

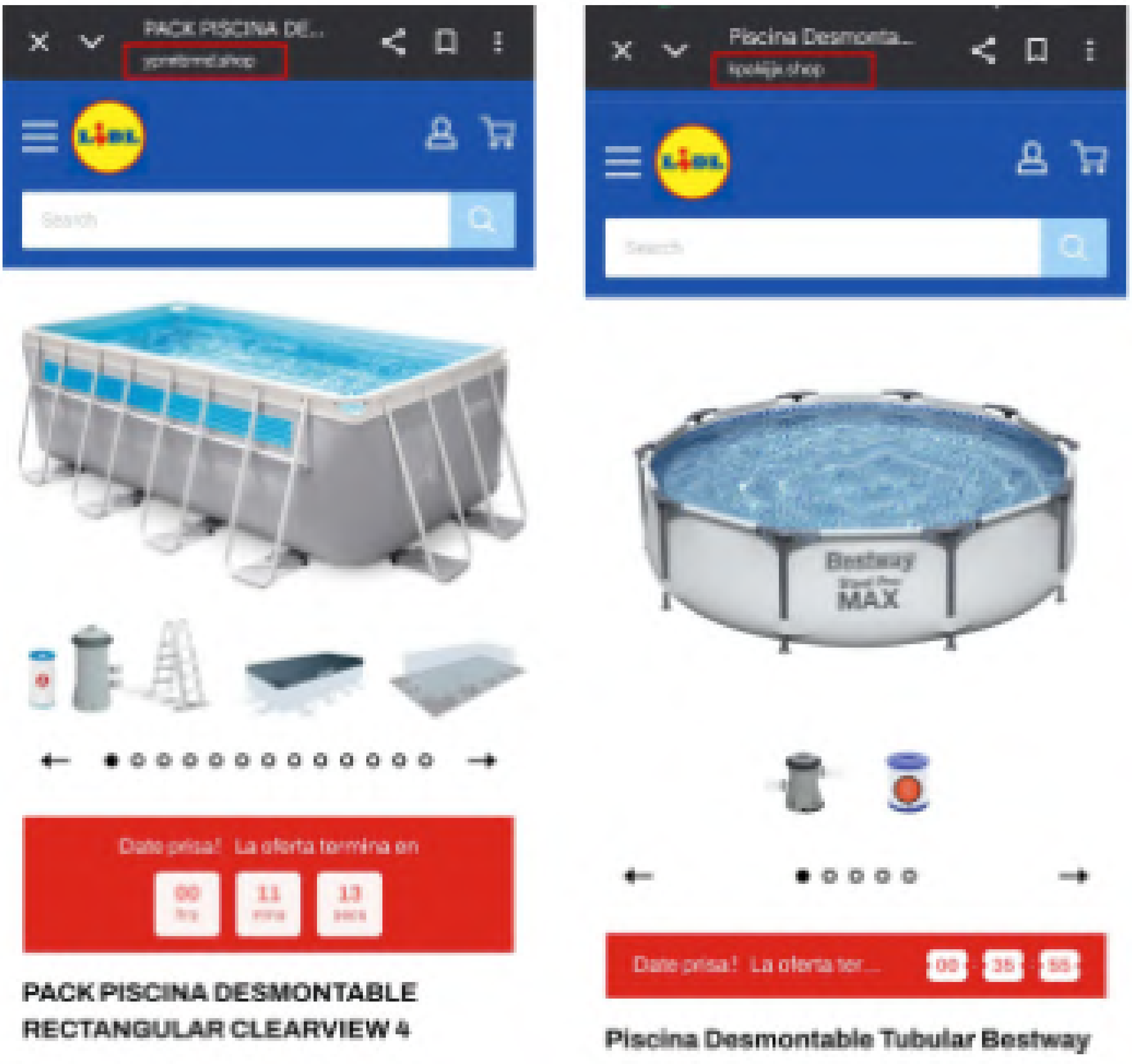
12. Maldita.es. (2024, November 1). Cuidado con los supuestos voluntarios de la Cruz Roja que piden dinero por la DANA: el Ayuntamiento de Sueca dice que es una “estafa”. https://tinyurl.com/2xh9r3u5

13. Instituto Nacional de Ciberseguridad (INCIBE). (2020). Guía de ciberataques: Todo lo que debes saber a nivel usuario. https://tinyurl.com/3877ryme

14. Instituto Nacional de Ciberseguridad (INCIBE). (2024). Balance de ciberseguridad 2022. https://tinyurl.com/4fmrbwc9
15. Instituto Nacional de Ciberseguridad (INCIBE). (2022). Balance de ciberseguridad 2022. https://tinyurl.com/bdfdvd7n
16. Ministerio del Interior. (2023). *Informe sobre la cibercriminalidad en España 2023*. Dirección General de Coordinación y Estudios, Secretaría de Estado de Seguridad. https://tinyurl.com/42fv3h3a
17. Ministerio del Interior. (2022). *Informe sobre la cibercriminalidad en España 2022*. Dirección General de Coordinación y Estudios, Secretaría de Estado de Seguridad. https://tinyurl.com/mtturvn7
18. Arroyo, D., Gayoso, V., and Hernández, L. (2020). *¿Qué sabemos de? Ciberseguridad*. Editorial CSIC.
19.INCIBE-CERT. (2020). *Guía nacional de notificación y gestión de ciberincidentes*. https://tinyurl.com/yfxu9def
20. Guardia Civil. (n.d.). *Consejos de seguridad para no ser víctima de estafa*. https://web.guardiacivil.es/es/colaboracion/consejos/estafa/index.html
21. Kaspersky. (n.d). *¿Qué es el cibercrimen? Cómo protegerte*. https://latam.kaspersky.com/resource-center/threats/what-is-cybercrime
22. Panda Mediacenter. (2023, March 22). *Tipos de cibercrimen*. https://www.pandasecurity.com/es/mediacenter/tipos-de-cibercrimen/
23. Cano Teruel, Q. (2020, December 04). *Ciberdelincuencia en el Código Penal*. Cibercrim. https://cibercrim.com/ciberdelincuencia-en-el-codigo-penal/
24. e-Legales. (n.d.). *Clasificación de los ciberdelitos según la víctima*. e-Legales. https://tinyurl.com/33hv59nv
25. European Union Agency for Network and Information Security (ENISA). (2018). *Reference Incident Classification Taxonomy. Task Force Status and Way Forward.* https://tinyurl.com/4fsp2uk3
26. Feature Space. (2023). *SCAMS. La guía completa. Identificación y prevención de fraude autorizado de tarjetas y pagos*. https://tinyurl.com/4fp6k48f
27. F-Secure. (s.f.). *Scam Taxonomy.* https://www.f-secure.com/en/partners/scam-protection/scam-taxonomy
28. Instituto Nacional de Ciberseguridad (INCIBE). (2021). *Glosario de términos de ciberseguridad: Una guía de aproximación para el empresario*. https://tinyurl.com/mrrfp4wv
29. Instituto Nacional de Ciberseguridad (INCIBE). (n.d.). *Taxonomía*. INCIBE-CERT. https://tinyurl.com/ynuprzvh
30. Instituto Nacional de Ciberseguridad (INCIBE). (n.d.). *Ciudadanía*. https://www.incibe.es/ciudadania
31. Mestre Delgado, E. (2023, June 16). *Delitos en internet: ciberestafas*. Abogacía Española. https://tinyurl.com/yfyah5cp
32. Observatorio Español de Delitos Informáticos (OEDI). (n.d.). *Ciberdelitos*. https://oedi.es/ciberdelitos/

APPENDIX

Figure A1. Phishing and promotions or offers



Date prisa! La oferta termina en

00 hrs 11 mins 13 secs

PACK PISCINA DESMONTABLE RECTANGULAR CLEARVIEW 4

Date prisa! La oferta ter... 00 : 35 : 55

Piscina Desmontable Tubular Bestway

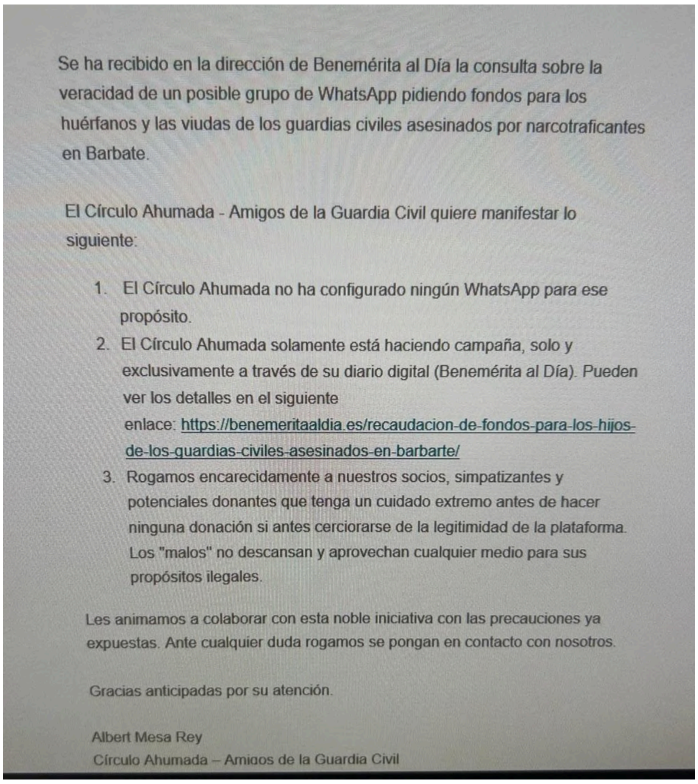
Lidl offers swimming pools on its website at discounted prices

Technique: Phishing

Thematic: Promotions or offers

Article URL: https://tinyurl.com/mws4c9ea

Figure A2. Phishing and inheritance, donations, or lottery



Se ha recibido en la dirección de Benemérita al Día la consulta sobre la veracidad de un posible grupo de WhatsApp pidiendo fondos para los huérfanos y las viudas de los guardias civiles asesinados por narcotraficantes en Barbate.

El Círculo Ahumada - Amigos de la Guardia Civil quiere manifestar lo siguiente:

1. El Círculo Ahumada no ha configurado ningún WhatsApp para ese propósito.
2. El Círculo Ahumada solamente está haciendo campaña, solo y exclusivamente a través de su diario digital (Benemérita al Día). Pueden ver los detalles en el siguiente enlace: https://benemeritaaldia.es/recaudacion-de-fondos-para-los-hijos-de-los-guardias-civiles-asesinados-en-barbarte/
3. Rogamos encarecidamente a nuestros socios, simpatizantes y potenciales donantes que tenga un cuidado extremo antes de hacer ninguna donación si antes cerciorarse de la legitimidad de la plataforma. Los "malos" no descansan y aprovechan cualquier medio para sus propósitos ilegales.

Les animamos a colaborar con esta noble iniciativa con las precauciones ya expuestas. Ante cualquier duda rogamos se pongan en contacto con nosotros.

Gracias anticipadas por su atención.

Albert Mesa Rey
Círculo Ahumada – Amigos de la Guardia Civil

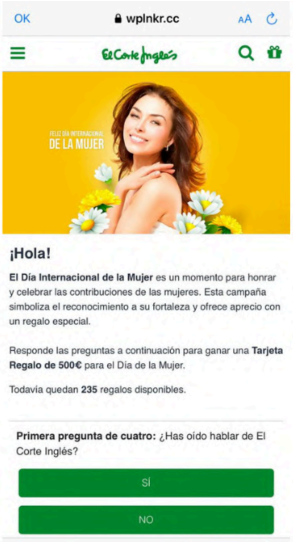
The Civil Guard is asking for donations for the orphans and widows of the two civil guards killed in Barbate

Technique: Phishing

Thematic: False inheritance, donations, or lottery

Article URL: https://tinyurl.com/3vm2n982

Figure A3. Phishing and false contests, raffles, or prizes



¡Hola!

El Día Internacional de la Mujer es un momento para honrar y celebrar las contribuciones de las mujeres. Esta campaña simboliza el reconocimiento a su fortaleza y ofrece aprecio con un regalo especial.

Responde las preguntas a continuación para ganar una **Tarjeta Regalo de 500€** para el Día de la Mujer.

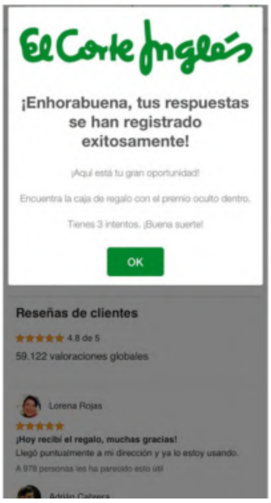
Todavia quedan **235** regalos disponibles.

Primera pregunta de cuatro: ¿Has oído hablar de El Corte Inglés?

SÍ

NO

1



¡Enhorabuena, tus respuestas se han registrado exitosamente!

¡Aquí está tu gran oportunidad!

Encuentra la caja de regalo con el premio oculto dentro.

Tienes 3 intentos. ¡Buena suerte!

OK

Reseñas de clientes

★★★★★ 4.8 de 5

59.122 valoraciones globales

Lorena Rojas

★★★★★

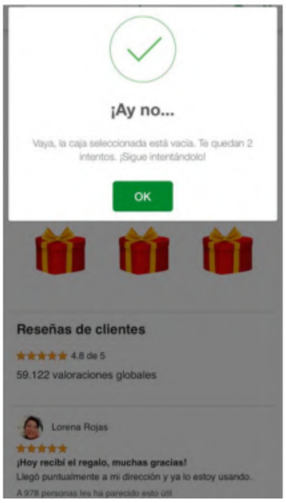
¡Hoy recibí el regalo, muchas gracias!

Llegó puntualmente a mi dirección y ya lo estoy usando.

A 978 personas les ha parecido esto útil

Adrián Cabrera

2



¡Ay no...

Vaya, la caja seleccionada está vacía. Te quedan 2 intentos. ¡Sigue intentándolo!

OK

Reseñas de clientes

★★★★★ 4.8 de 5

59.122 valoraciones globales

Lorena Rojas

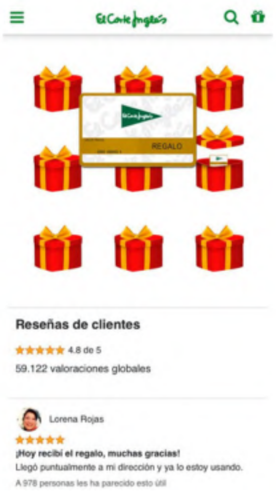
★★★★★

¡Hoy recibí el regalo, muchas gracias!

Llegó puntualmente a mi dirección y ya lo estoy usando.

A 978 personas les ha parecido esto útil

3



Reseñas de clientes

★★★★★ 4.8 de 5

59.122 valoraciones globales

Lorena Rojas

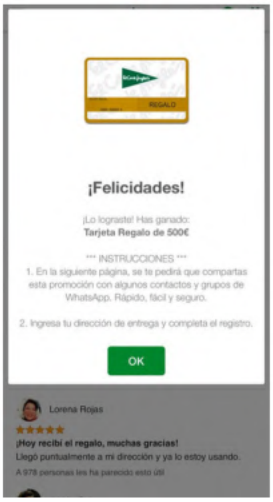
★★★★★

¡Hoy recibí el regalo, muchas gracias!

Llegó puntualmente a mi dirección y ya lo estoy usando.

A 978 personas les ha parecido esto útil

4



¡Felicidades!

¡Lo lograste! Has ganado:
Tarjeta Regalo de 500€

*** INSTRUCCIONES ***
1. En la siguiente página, se te pedirá que compartas esta promoción con algunos contactos y grupos de WhatsApp. Rápido, fácil y seguro.

2. Ingresa tu dirección de entrega y completa el registro.

OK

Lorena Rojas

★★★★★

¡Hoy recibí el regalo, muchas gracias!

Llegó puntualmente a mi dirección y ya lo estoy usando.

A 978 personas les ha parecido esto útil

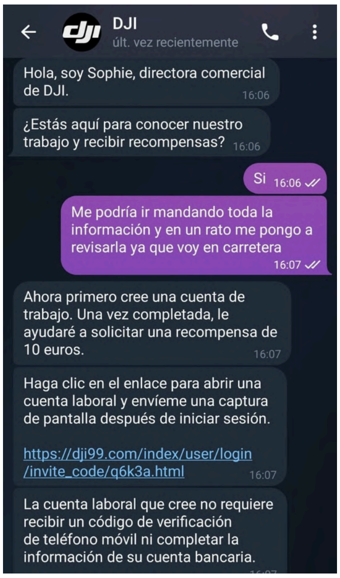
El Corte Inglés offers a gift card for Women's Day

Technique: Phishing

Thematic: False false contests, raffles, or prizes

Article URL: https://tinyurl.com/2ddzmfu6

Figure A4. Phishing and false jobs offers



DJI
últ. vez recientemente

Hola, soy Sophie, directora comercial de DJI. 16:06

¿Estás aquí para conocer nuestro trabajo y recibir recompensas? 16:06

Si 16:06

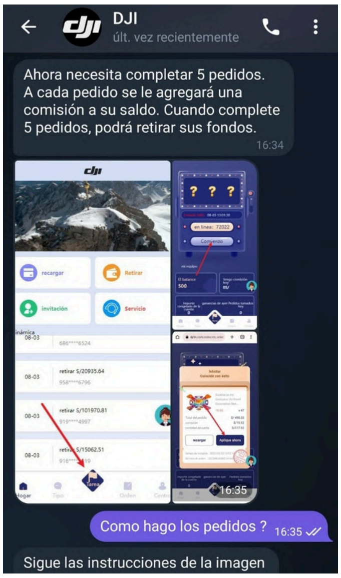
Me podría ir mandando toda la información y en un rato me pongo a revisarla ya que voy en carretera 16:07

Ahora primero cree una cuenta de trabajo. Una vez completada, le ayudaré a solicitar una recompensa de 10 euros. 16:07

Haga clic en el enlace para abrir una cuenta laboral y envíeme una captura de pantalla después de iniciar sesión.

https://dji99.com/index/user/login/invite_code/q6k3a.html 16:07

La cuenta laboral que cree no requiere recibir un código de verificación de teléfono móvil ni completar la información de su cuenta bancaria.



DJI
últ. vez recientemente

Ahora necesita completar 5 pedidos. A cada pedido se le agregará una comisión a su saldo. Cuando complete 5 pedidos, podrá retirar sus fondos. 16:34

16:35

Como hago los pedidos ? 16:35

Sigue las instrucciones de la imagen

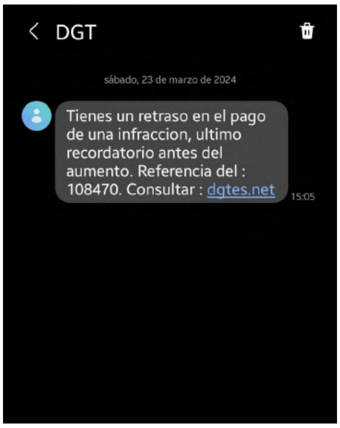
DJI is offering a lot of money for completing online tasks

Technique: Phishing

Thematic: False job offers

Article URL: https://tinyurl.com/3np9kcfe

Figure A5. Smishing and false notifications from a service or institution

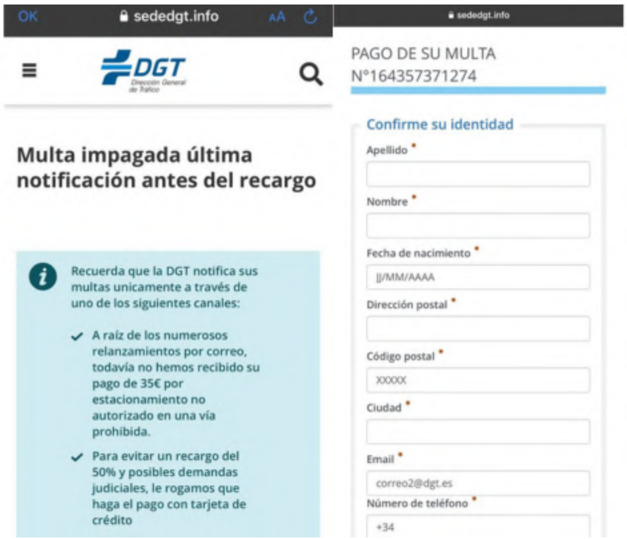


DGT

sábado, 23 de marzo de 2024

Tienes un retraso en el pago de una infraccion, ultimo recordatorio antes del aumento. Referencia del : 108470. Consultar : dgtes.net

15:05



Multa impagada última notificación antes del recargo

Recuerda que la DGT notifica sus multas unicamente a través de uno de los siguientes canales:

- ✓ A raíz de los numerosos relanzamientos por correo, todavía no hemos recibido su pago de 35€ por estacionamiento no autorizado en una vía prohibida.
- ✓ Para evitar un recargo del 50% y posibles demandas judiciales, le rogamos que haga el pago con tarjeta de crédito

PAGO DE SU MULTA
N°164357371274

Confirme su identidad

Apellido *

Nombre *

Fecha de nacimiento *
JJ/MM/AAAA

Dirección postal *

Código postal *
XXXXX

Ciudad *

Email *
correo2@dgt.es

Número de teléfono *
+34

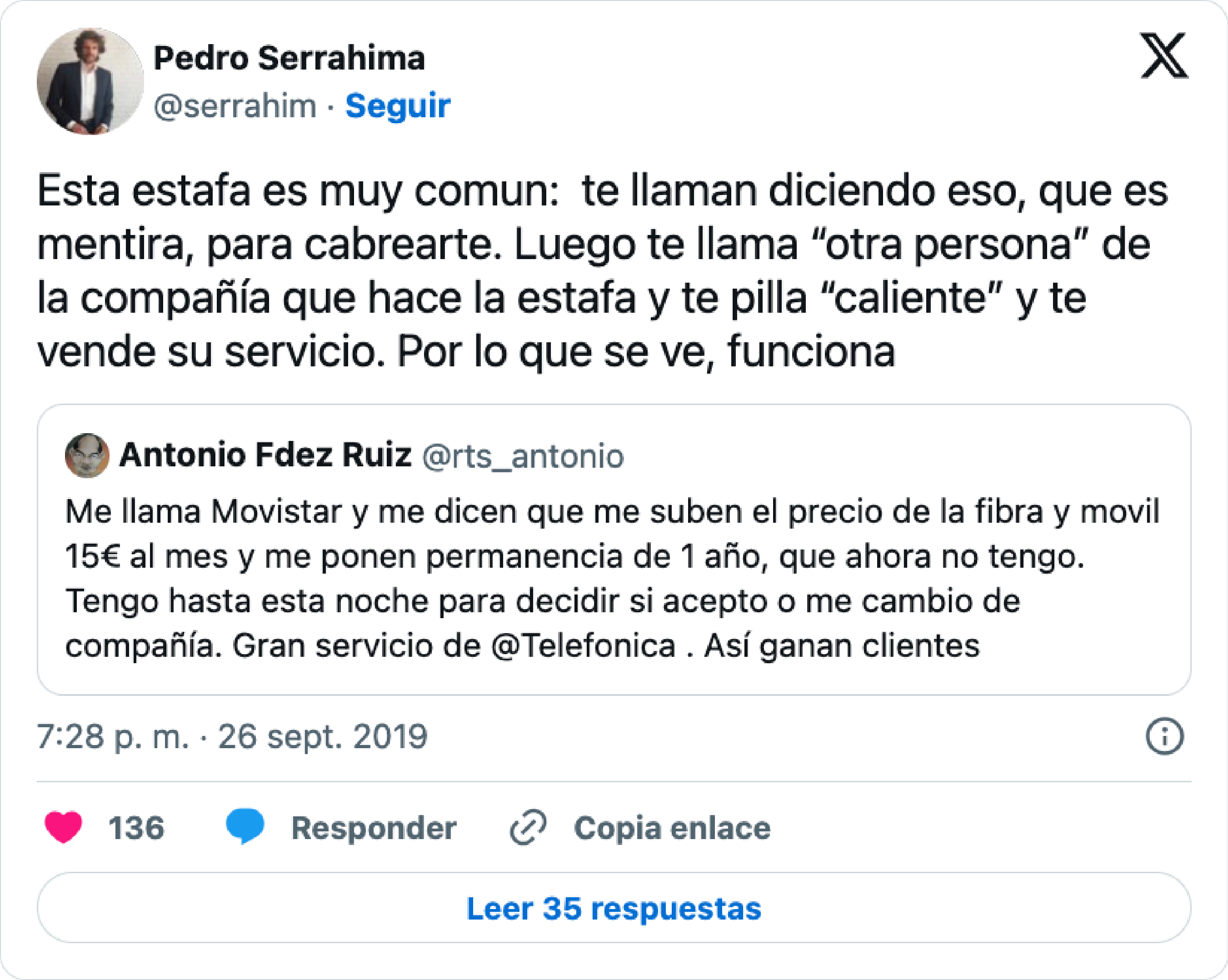
Notification from the DGT warning of a delay in payment for a traffic offence

Technique: Smishing

Thematic: False notifications from a service or institution

Article URL: https://tinyurl.com/2p9mkap6

Figure A6. Vishing and false notifications from a service or institution



Pedro Serrahima
@serrahim · Seguir

Esta estafa es muy comun: te llaman diciendo eso, que es mentira, para cabrearte. Luego te llama “otra persona” de la compañía que hace la estafa y te pilla “caliente” y te vende su servicio. Por lo que se ve, funciona

Antonio Fdez Ruiz @rts_antonio

Me llama Movistar y me dicen que me suben el precio de la fibra y movil 15€ al mes y me ponen permanencia de 1 año, que ahora no tengo. Tengo hasta esta noche para decidir si acepto o me cambio de compañía. Gran servicio de @Telefonica . Así ganan clientes

7:28 p. m. · 26 sept. 2019

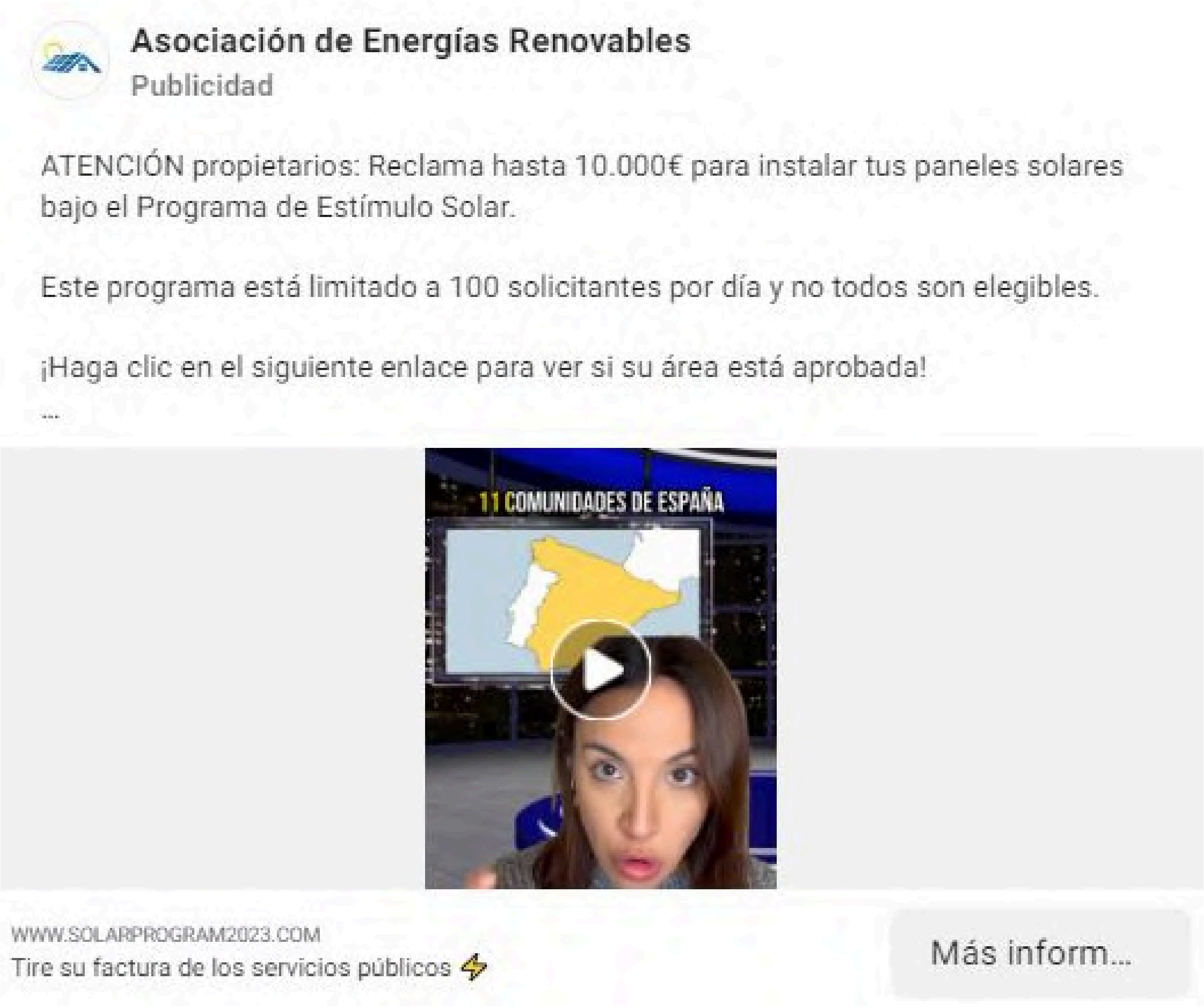
Call from a supposed telephone company to increase the service rate

Technique: Vishing

Thematic: Purchase or sale of products and services

Article URL: https://tinyurl.com/ycx29dau

Figure A7. Baiting and promotions or offers



Asociación de Energías Renovables

Publicidad

ATENCIÓN propietarios: Reclama hasta 10.000€ para instalar tus paneles solares bajo el Programa de Estímulo Solar.

Este programa está limitado a 100 solicitantes por día y no todos son elegibles.

¡Haga clic en el siguiente enlace para ver si su área está aprobada!

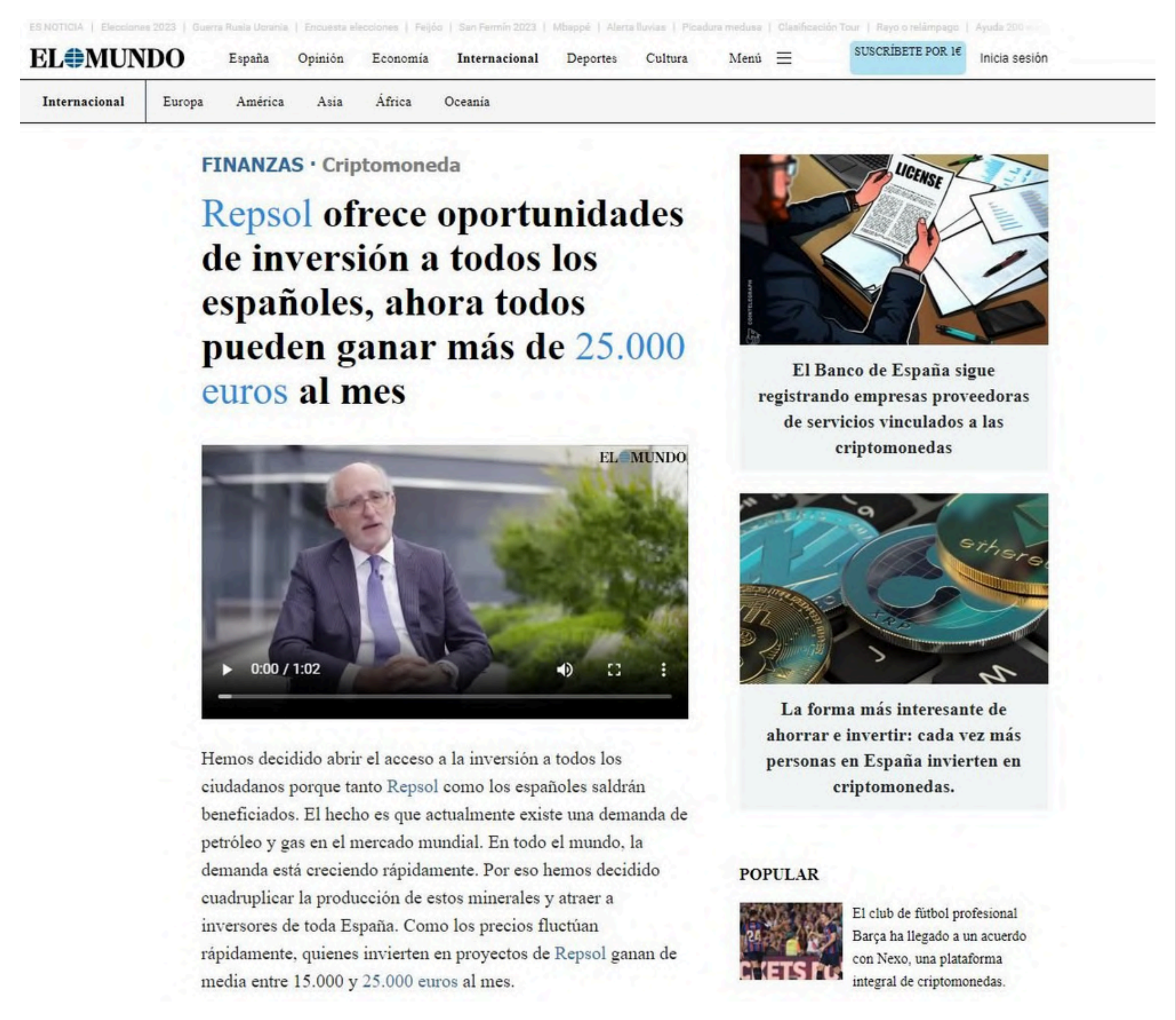
...

WWW.SOLARPROGRAM2023.COM

Tire su factura de los servicios públicos ⚡

False ads promote a new government program that provides funding for solar panel installation
Technique: Baiting
Thematic: False contests, raffles, or prizes
Article URL: https://tinyurl.com/mr22785h

Figure A8. Baiting and promotions or offers


ES NOTICIA | Elecciones 2023 | Guerra Rusia Ucrania | Encuesta elecciones | Feijóo | San Fermín 2023 | Mbappé | Alerta lluvias | Picadura medusa | Clasificación Tour | Rayo o relámpago | Ayuda 200
EL MUNDO
España
Opinión
Economía
Internacional
Deportes
Cultura
Menú
SUSCRÍBETE POR 1€
Inicia sesión
Internacional
Europa
América
Asia
África
Oceanía
EL MUNDO
0:00 / 1:02
LICENSE

FINANZAS · Criptomoneda

Repsol ofrece oportunidades de inversión a todos los españoles, ahora todos pueden ganar más de 25.000 euros al mes

Hemos decidido abrir el acceso a la inversión a todos los ciudadanos porque tanto Repsol como los españoles saldrán beneficiados. El hecho es que actualmente existe una demanda de petróleo y gas en el mercado mundial. En todo el mundo, la demanda está creciendo rápidamente. Por eso hemos decidido cuadruplicar la producción de estos minerales y atraer a inversores de toda España. Como los precios fluctúan rápidamente, quienes invierten en proyectos de Repsol ganan de media entre 15.000 y 25.000 euros al mes.

El Banco de España sigue registrando empresas proveedoras de servicios vinculados a las criptomonedas

La forma más interesante de ahorrar e invertir: cada vez más personas en España invierten en criptomonedas.

POPULAR

El club de fútbol profesional Barça ha llegado a un acuerdo con Nexo, una plataforma integral de criptomonedas.

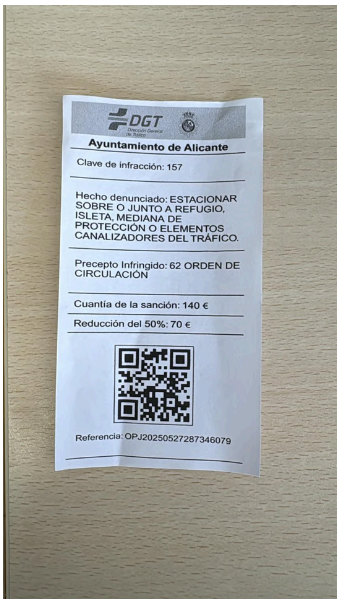
Carlos Franganillo announces investments in Repsol shares

Technique: Baiting and catfishing

Thematic: False investments

Article URL: https://tinyurl.com/4stktkjh

Figure A9. QRshing and notifications from a service or institution



DGT

Ayuntamiento de Alicante

Clave de infracción: 157

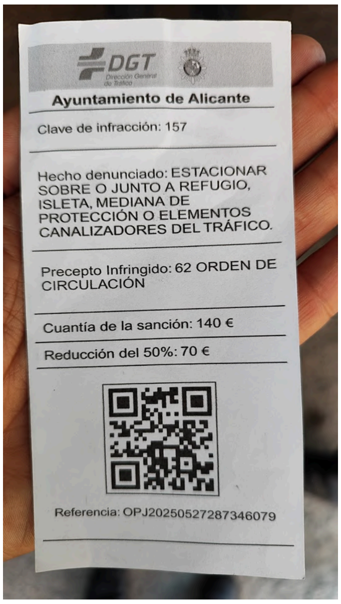
Hecho denunciado: ESTACIONAR SOBRE O JUNTO A REFUGIO, ISLETA, MEDIANA DE PROTECCIÓN O ELEMENTOS CANALIZADORES DEL TRÁFICO.

Precepto Infringido: 62 ORDEN DE CIRCULACIÓN

Cuantía de la sanción: 140 €

Reducción del 50%: 70 €

Referencia: OPJ20250527287346079



DGT

Ayuntamiento de Alicante

Clave de infracción: 157

Hecho denunciado: ESTACIONAR SOBRE O JUNTO A REFUGIO, ISLETA, MEDIANA DE PROTECCIÓN O ELEMENTOS CANALIZADORES DEL TRÁFICO.

Precepto Infringido: 62 ORDEN DE CIRCULACIÓN

Cuantía de la sanción: 140 €

Reducción del 50%: 70 €

Referencia: OPJ20250527287346079

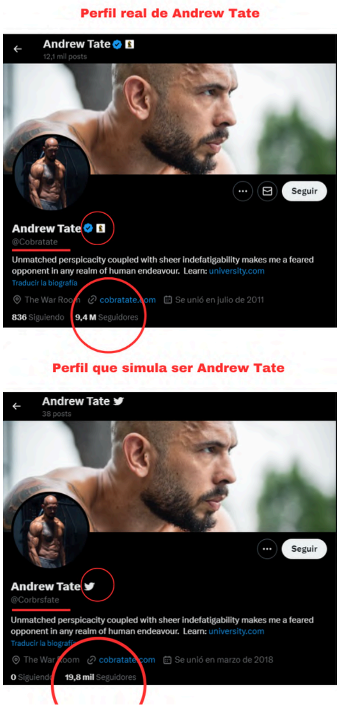
Fake DGT fines use QR codes to steal banking data

Technique: QRshing

Thematic: Notification from a service or institution

Article URL: https://tinyurl.com/y9vsb83k

Figure A10. Catfishing and investments



Perfil real de Andrew Tate

Andrew Tate
12,1 mil posts

Andrew Tate
@Cobratate

Unmatched perspicacity coupled with sheer indefatigability makes me a feared opponent in any realm of human endeavour. Learn: university.com
Traducir la biografía

The War Room cobratate.com Se unió en julio de 2011

836 Siguiendo 9,4 M Seguidores

Perfil que simula ser Andrew Tate

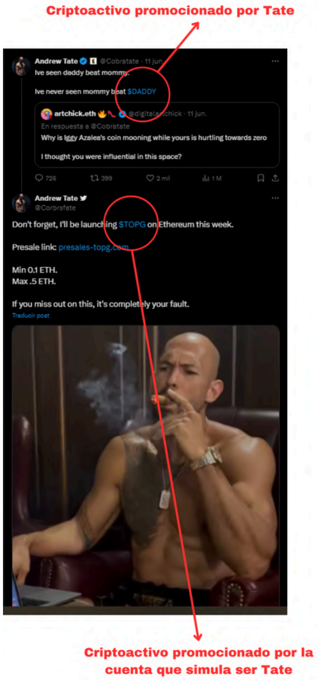
Andrew Tate
38 posts

Andrew Tate
@Corbrsfate

Unmatched perspicacity coupled with sheer indefatigability makes me a feared opponent in any realm of human endeavour. Learn: university.com
Traducir la biografía

The War Room cobratate.com Se unió en marzo de 2018

0 Siguiendo 19,8 mil Seguidores



Criptoactivo promocionado por Tate

Andrew Tate @Cobratate · 11 jun.
Ive seen daddy beat mommy.

Ive never seen mommy beat $DADDY

artchick.eth 🔥 @digitalartchick · 11 jun.
En respuesta a @Cobratate
Why is Iggy Azalea's coin mooning while yours is hurtling towards zero

I thought you were influential in this space?

Andrew Tate
@Corbrsfate

Don't forget, I'll be launching $TOPG on Ethereum this week.

Presale link: presales-topg.com

Min 0.1 ETH.
Max .5 ETH.

If you miss out on this, it's completely your fault.
Traducir post

Criptoactivo promocionado por la cuenta que simula ser Tate

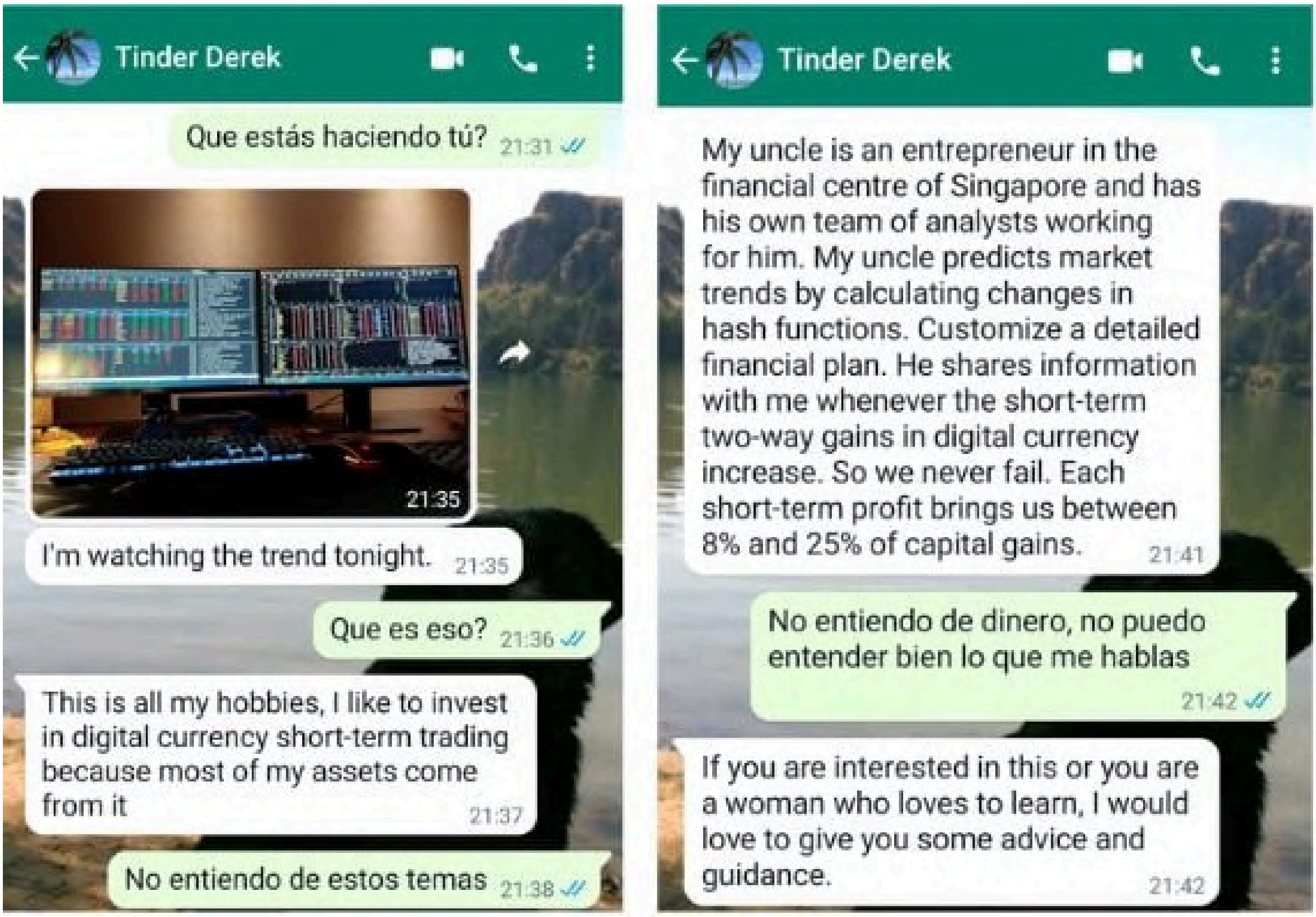
Andrew Tate's X profile promotes cryptocurrencies

Technique: Catfishing

Thematic: False investments

Article URL: https://tinyurl.com/msshbnwj

Figure A11. Catfishing, investments and romantic relationship



Que estás haciendo tú? 21:31

21:35

I'm watching the trend tonight. 21:35

Que es eso? 21:36

This is all my hobbies, I like to invest in digital currency short-term trading because most of my assets come from it 21:37

No entiendo de estos temas 21:38

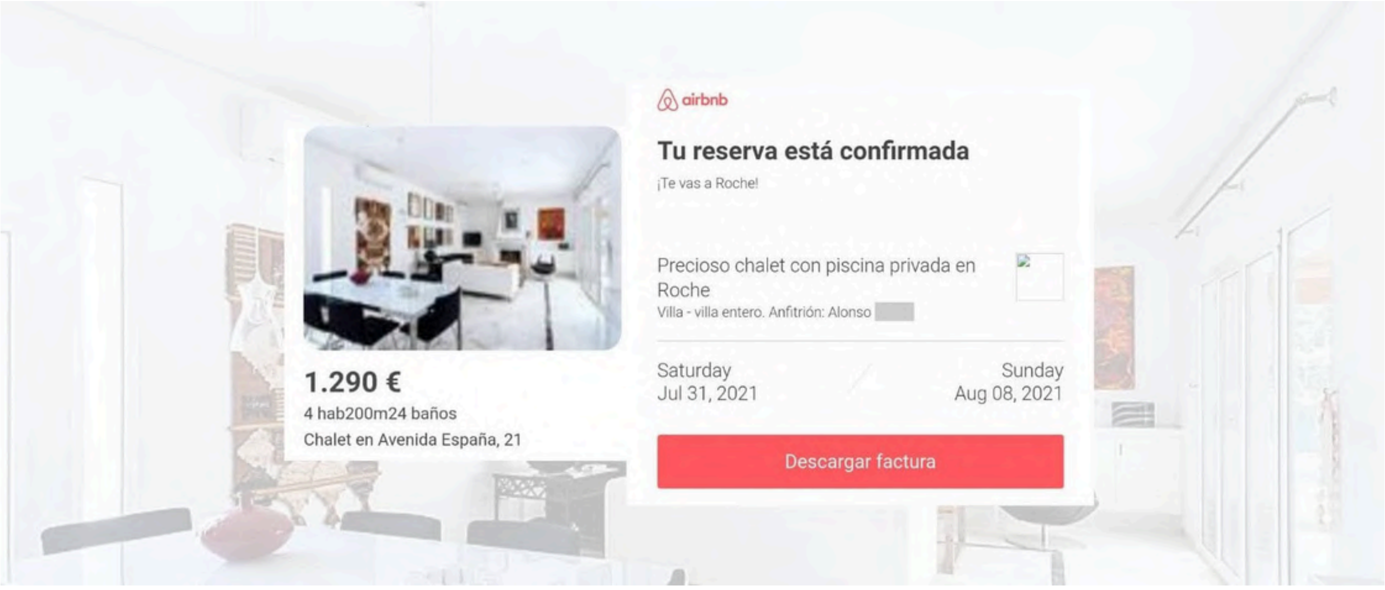
My uncle is an entrepreneur in the financial centre of Singapore and has his own team of analysts working for him. My uncle predicts market trends by calculating changes in hash functions. Customize a detailed financial plan. He shares information with me whenever the short-term two-way gains in digital currency increase. So we never fail. Each short-term profit brings us between 8% and 25% of capital gains. 21:41

No entiendo de dinero, no puedo entender bien lo que me hablas 21:42

If you are interested in this or you are a woman who loves to learn, I would love to give you some advice and guidance. 21:42

Fake Tinder profiles promoting crypto investments
Technique: Catfishing
Thematic: False investments, romantic relationship
Article URL: https://tinyurl.com/4a7yutc9/

Figure A12. Web spoofing and property rentals or reservations



1.290 €

4 hab200m24 baños

Chalet en Avenida España, 21

airbnb

Tu reserva está confirmada

¡Te vas a Roche!

Precioso chalet con piscina privada en Roche

Villa - villa entero. Anfitrión: Alonso [redacted]

Saturday
Jul 31, 2021

Sunday
Aug 08, 2021

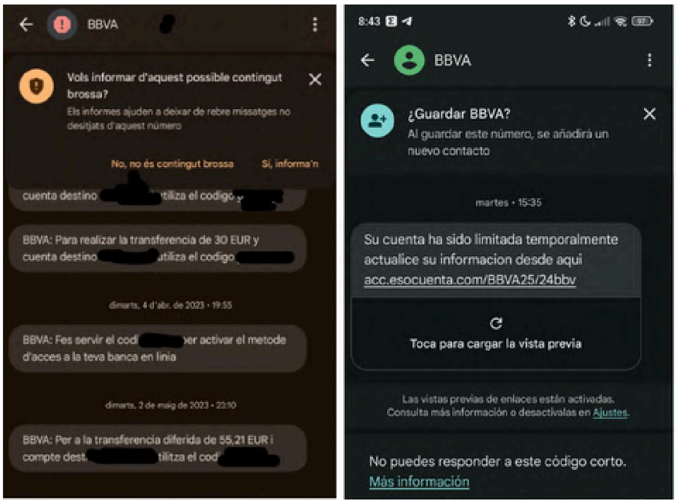
Advertisement for a house on Fotocasa and impersonation of Airbnb's website and email address

Technique: Web and email spoofing

Thematic: Property rentals or reservations

Article URL: https://tinyurl.com/y24846tn/

Figure A13. SMS spoofing and notifications from a service or institution



BBVA [redacted]

Vols informar d'aquest possible contingut brossa?

Els informes ajuden a deixar de rebre missatges no desitjats d'aquest número

cuenta destino [redacted] tiliza el codigo y [redacted]

BBVA: Para realizar la transferencia de 30 EUR y cuenta destino [redacted] utiliza el codigo [redacted]

dimarts, 4 d'abr. de 2023 · 19:55

BBVA: Fes servir el codi [redacted] per activar el metode d'acces a la teva banca en linia

dimarts, 2 de maig de 2023 · 23:10

BBVA: Per a la transferencia diferida de 55,21 EUR i compte dest. [redacted] tilitza el codi [redacted]

8:43

BBVA

¿Guardar BBVA?

Al guardar este número, se añadirá un nuevo contacto

martes · 15:35

Su cuenta ha sido limitada temporalmente actualice su informacion desde aqui acc.esocuenta.com/BBVA25/24bbv

Las vistas previas de enlaces están activadas. Consulta más información o desactívalas en Ajustes.

No puedes responder a este código corto. Más información

SMS from BBVA warning that our account has been temporarily restricted

Technique: SMS spoofing

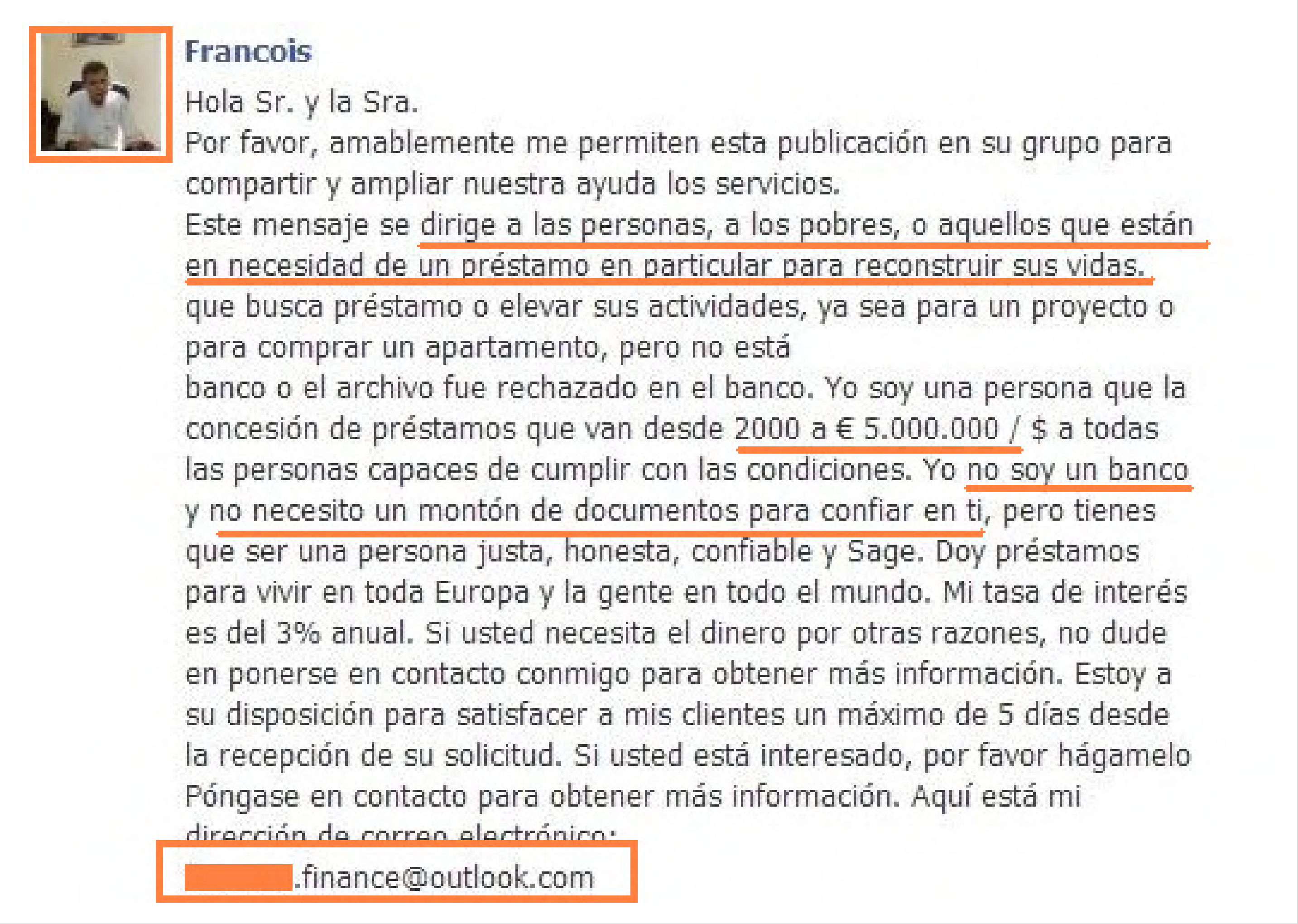
Thematic: Property rentals or reservations

Article URL: https://tinyurl.com/mvfbneu9

Figure A14. Caller ID spoofing and notifications from a service or institution

 “They took all my money from the bank by pretending to be La Caixa, and I checked myself that it was a CaixaBank number“
Spoofed calls display the bank’s official number and cite a ‘fraudulent transaction
Technique: Caller ID spoofing
Thematic: Notifications from a service or institution
Article URL: https://tinyurl.com/bczhs3b6

Figure A15. Catfishing and loans



Francois

Hola Sr. y la Sra.

Por favor, amablemente me permiten esta publicación en su grupo para compartir y ampliar nuestra ayuda los servicios.

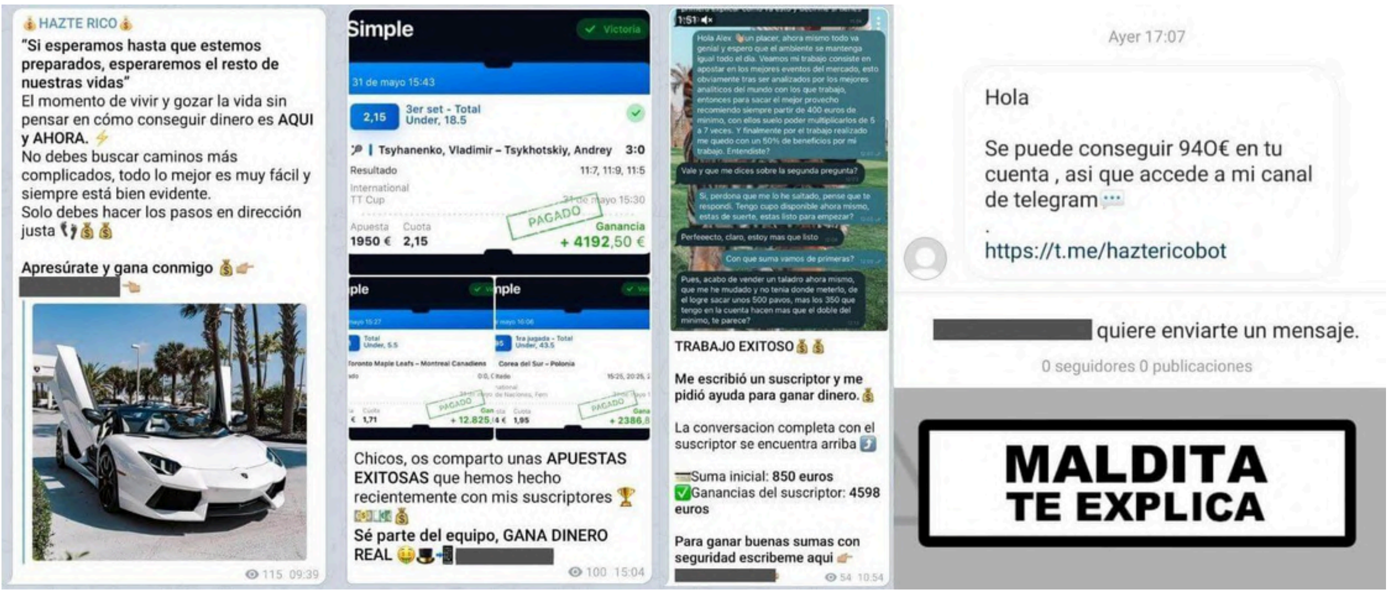
Este mensaje se dirige a las personas, a los pobres, o aquellos que están en necesidad de un préstamo en particular para reconstruir sus vidas. que busca préstamo o elevar sus actividades, ya sea para un proyecto o para comprar un apartamento, pero no está

banco o el archivo fue rechazado en el banco. Yo soy una persona que la concesión de préstamos que van desde 2000 a € 5.000.000 / $ a todas las personas capaces de cumplir con las condiciones. Yo no soy un banco y no necesito un montón de documentos para confiar en ti, pero tienes que ser una persona justa, honesta, confiable y Sage. Doy préstamos para vivir en toda Europa y la gente en todo el mundo. Mi tasa de interés es del 3% anual. Si usted necesita el dinero por otras razones, no dude en ponerse en contacto conmigo para obtener más información. Estoy a su disposición para satisfacer a mis clientes un máximo de 5 días desde la recepción de su solicitud. Si usted está interesado, por favor hágamelo Póngase en contacto para obtener más información. Aquí está mi dirección de correo electrónico:

[redacted].finance@outlook.com

Fraudulent loan ads posing as legitimate lenders
Technique: Catfishing
Thematic: Loans
Article URL: https://tinyurl.com/4rm22rsk

Figure A16. Catfishing and gambling



💰HAZTE RICO💰

"Si esperamos hasta que estemos preparados, esperaremos el resto de nuestras vidas"

El momento de vivir y gozar la vida sin pensar en cómo conseguir dinero es **AQUI y AHORA.** ⚡

No debes buscar caminos más complicados, todo lo mejor es muy fácil y siempre está bien evidente.

Solo debes hacer los pasos en dirección justa 👣💰💰

Apresúrate y gana conmigo 💰👉

[redacted] 👈

115 09:39

Simple ✓ Victoria

31 de mayo 15:43

2,15 3er set - Total Under, 18.5 ✓

Tsyhanenko, Vladimir – Tsykhotskiy, Andrey 3:0

Resultado 11:7, 11:9, 11:5

International TT Cup 31 de mayo 15:30

PAGADO

Apuesta 1950 € Cuota 2,15 Ganancia + 4192,50 €

Total Under, 5.5 Toronto Maple Leafs – Montreal Canadiens Cuota 1,71 PAGADO + 12.825

1ra jugada - Total Under, 43.5 Corea del Sur – Polonia Cuota 1,95 PAGADO + 2386,8

Chicos, os comparto unas **APUESTAS EXITOSAS** que hemos hecho recientemente con mis suscriptores 🏆💵💶💰

Sé parte del equipo, GANA DINERO REAL 🤑🎩➡📱[redacted]

100 15:04

Hola Alex 👋un placer, ahora mismo todo va genial y espero que el ambiente se mantenga igual todo el dia. Veamos mi trabajo consiste en apostar en los mejores eventos del mercado, esto obviamente tras ser analizados por los mejores analiticos del mundo con los que trabajo, entonces para sacar el mejor provecho recomiendo siempre partir de 400 euros de minimo, con ellos suelo poder multiplicarlos de 5 a 7 veces. Y finalmente por el trabajo realizado me quedo con un 50% de beneficios por mi trabajo. Entendiste?

Vale y que me dices sobre la segunda pregunta?

Si, perdona que me lo he saltado, pense que te respondi. Tengo cupo disponible ahora mismo, estas de suerte, estas listo para empezar?

Perfeeecto, claro, estoy mas que listo

Con que suma vamos de primeras?

Pues, acabo de vender un taladro ahora mismo, que me he mudado y no tenia donde meterlo, de el logre sacar unos 500 pavos, mas los 350 que tengo en la cuenta hacen mas que el doble del minimo, te parece?

TRABAJO EXITOSO💰💰

Me escribió un suscriptor y me pidió ayuda para ganar dinero.💰

La conversacion completa con el suscriptor se encuentra arriba ⤴

💳Suma inicial: 850 euros

✅Ganancias del suscriptor: 4598 euros

Para ganar buenas sumas con seguridad escribeme aqui 👉

[redacted]

54 10:54

Ayer 17:07

Hola

Se puede conseguir 940€ en tu cuenta , asi que accede a mi canal de telegram💬

.

https://t.me/haztericobot

[redacted] quiere enviarte un mensaje.

0 seguidores 0 publicaciones

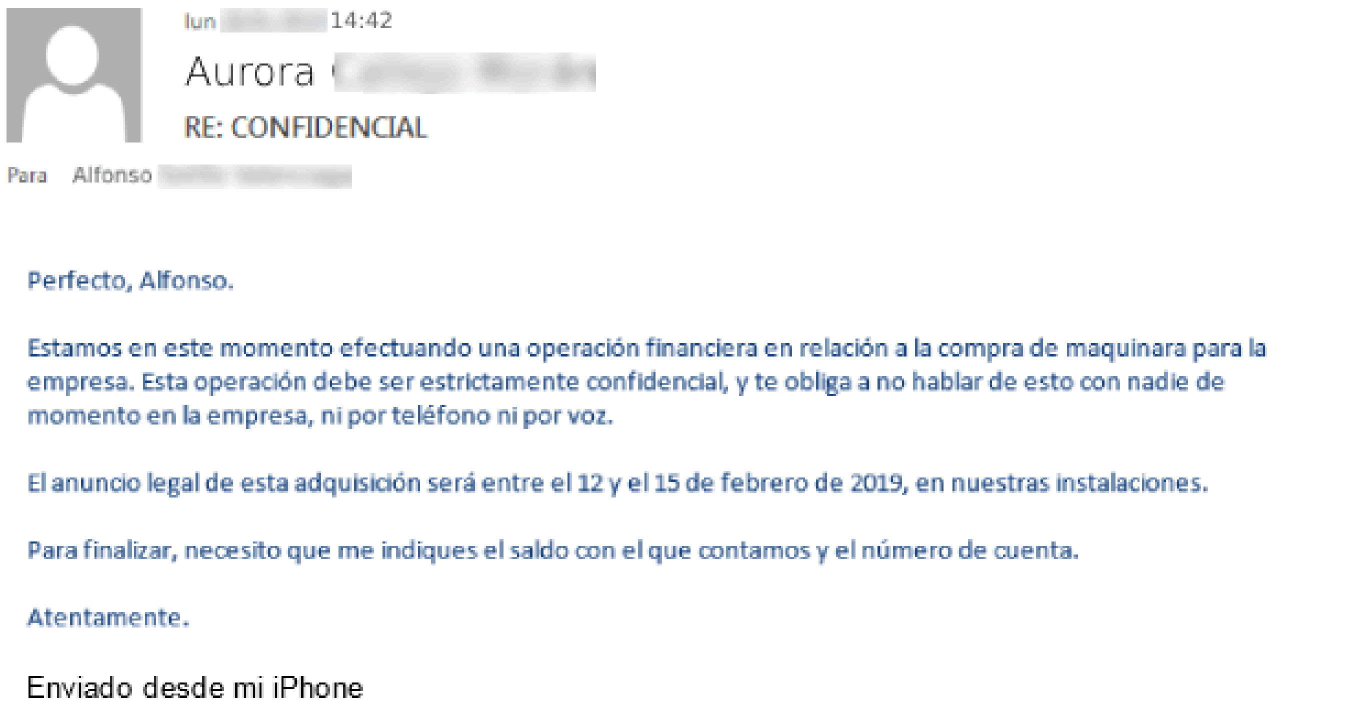
Telegram channels posing as bookmaker tipsters

Technique: Catfishing

Thematic: Gambling

Article URL: https://tinyurl.com/5f8svuyv

Figure A17. Phishing and work environment: CEO fraud



lun [redacted] 14:42

Aurora [redacted]

RE: CONFIDENCIAL

Para Alfonso [redacted]

Perfecto, Alfonso.

Estamos en este momento efectuando una operación financiera en relación a la compra de maquinara para la empresa. Esta operación debe ser estrictamente confidencial, y te obliga a no hablar de esto con nadie de momento en la empresa, ni por teléfono ni por voz.

El anuncio legal de esta adquisición será entre el 12 y el 15 de febrero de 2019, en nuestras instalaciones.

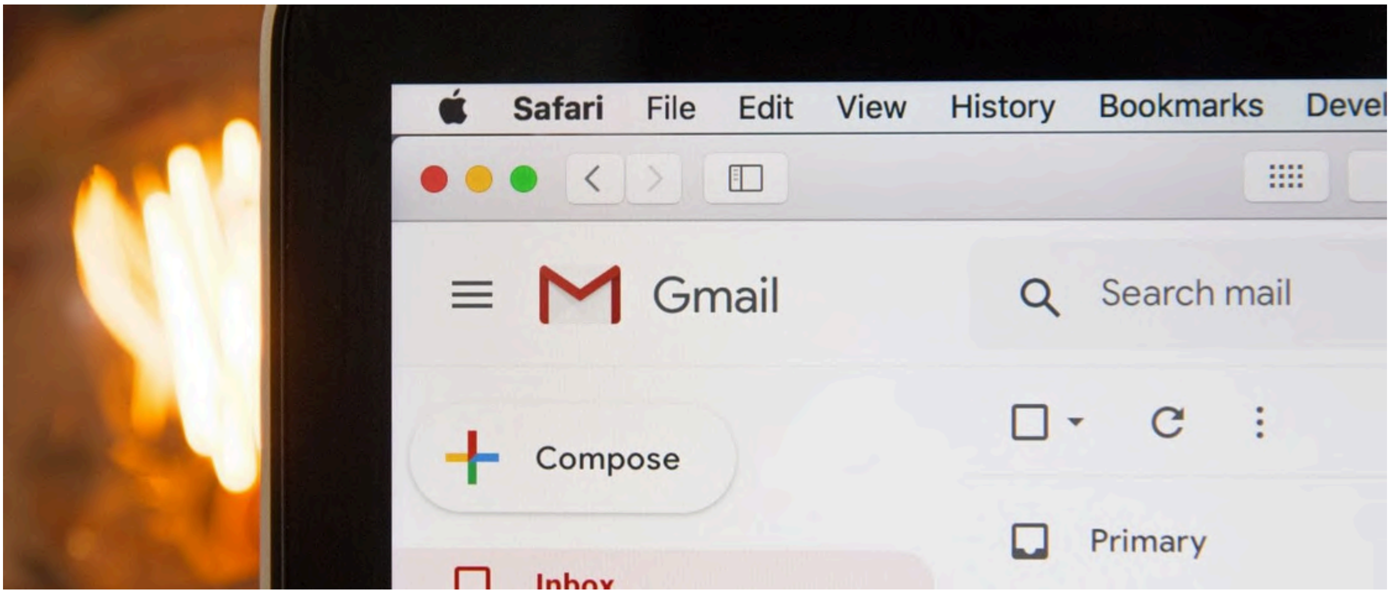
Para finalizar, necesito que me indiques el saldo con el que contamos y el número de cuenta.

Atentamente.

Enviado desde mi iPhone

Email from “CEO” requesting bank account details for a “confidential” transfer
Technique: Phishing
Thematic: Work environment
Article URL: https://tinyurl.com/ycys9fyn

Figure A18. Phishing and work environment: BEC fraud

 Safari File Edit View History Bookmarks Devel Gmail Search mail Compose Primary Inbox
Fraudsters hack corporate emails and change the account number on invoices
Technique: Phishing
Thematic: Work environment
Article URL: https://tinyurl.com/2x9dd57f

A Typology of Digital Scams: A Framework for Detection, Classification, and Prevention

The implementation of the project "Exposing scams: a Corporate and Civic Response" was possible thanks to the Civic Innovation Fund (CIF), a unique European pooled fund of THE CIVICS Innovation Hub. CIF is supported by the ERSTE Foundation