Card-Not-Present Fraud resulting from Smishing Attacks: An Experimental Study

Sharad Agarwal
sharad.agarwal@ucl.ac.uk
Stop Scams UK & University College London (UCL)
London, UK

Marie Vasek
m.vasek@ucl.ac.uk
University College London (UCL)
London, UK

Abstract

Smishing or SMS phishing is a recent update to email-based phishing. This modern scam hinges upon the trust that users have in their bank or online service to steal users' personal details. While recent work examines these texts and the URLs sent, no work has empirically determined what happens after scammers obtain this credit card information. Card-not-present (CNP) fraud—where stolen card details are used to make purchases online without physical access to the card—has become a growing concern. While some investigate this indirectly using forum posts, the unavailability of credit card transaction data makes it tricky to study empirically. As smishing continues to rise, so does CNP fraud, resulting in more losses borne by consumers. To this end, we perform a proof-of-concept experiment towards understanding how criminals abuse stolen credit card details brought in from smishing. We collaborate with a mobile network operator and a financial institution to access live smishing URLs and test credit cards. We provide test credit cards to twelve different smishing URLs and observe 36 authorization attempts across 17 different online merchants. We analyze the ISO transaction messages to uncover scammers' transaction patterns and their cash-out mechanisms. Our insights into scammer behavior could help stakeholders develop effective mitigations to tackle CNP fraud towards eliminating the profitability of smishing.

CCS Concepts

• **Security and privacy** → *Economics of security and privacy*.

Keywords

card-not-present fraud, smishing, cybercrime, online financial fraud

ACM Reference Format:
Sharad Agarwal and Marie Vasek. 2025. Card-Not-Present Fraud resulting from Smishing Attacks: An Experimental Study. In *Proceedings of New Security Paradigms Workshop (NSPW '25).* ACM, New York, NY, USA, 13 pages. https://doi.org/XXXXXXX.XXXXXXX

1 Introduction

With the increasing adoption of SMS texts as a primary mode of communication between organizations and their customers, this medium has become a crucial tool for delivering timely and direct notifications to users. Banks, government organizations, and other service providers use this to deliver one-time passcodes (OTPs), alerts, and other substantial updates to individuals and businesses. However, criminals have begun exploiting users' trust in this channel by impersonating legitimate entities. This has started to impact the foundational trust between consumers and the organizations they interact with over SMS.

Recently there has been a surge in SMS scams [46], where scammers impersonate popularly known brands and send phishing URLs via SMS to lure victims into providing their personal or financial details, also known as smishing (SMS phishing). One in ten people have fallen for a scam in the UK [26], and seven in ten people reported receiving a suspicious text, making text messages the more common medium to propagate scams, as per Ofcom, the UK telecom regulator [85]. With users shifting from SMS to services like iMessage or RCS, criminals have similarly started to abuse these encrypted communication mediums for smishing [38].

There are six known types of SMS scams, with delivery impersonation scams targeting the largest number of individuals [5]. Despite the rise in conversational-style scams like "Hi mum" scams, attackers in the UK continue to prefer delivery-themed lures [39]. Similarly with other countries: delivery scams are the most prevalent form of smishing attack in several countries, including the US [15, 80] and Australia [120]. This trend contrasts with phishing emails, where delivery-themed messages are relatively uncommon, or at least uncommon in research datasets.

Unlike other types of SMS scams which seek to obtain login credentials or other personal information, delivery scams deceive victims into providing their credit card information. With the shift from physical payments to purchasing goods and paying for services online, criminals exploit user trust in online e-commerce to carry out these scams. One threat actor group that abuses iMessage/RCS to conduct smishing claims to harvest over 100k cards per day [84].

Scammers monetize stolen credit cards through card-not-present (CNP) fraud, using the card details to make purchases online or over the phone, without the physical card being present. Sometimes, rather than cashing out themselves, scammers carrying out SMS phishing will sell the stolen cards on underground forums. The card buyers or carders then use these details to commit CNP fraud. Since 2014, this has been the most common type of card fraud in the UK [114] and it has almost doubled in value and volume since 2012 [11]. UK Finance reported an increase of 11% of financial losses in the first half of 2024 (£193.7 million) due to remote card-not-present fraud [114]. The European Central Bank also reported

NSPW '25, Aerzen, Germany

ACM ISBN 978-1-4503-XXXX-X/2025/06
https://doi.org/XXXXXXX.XXXXXXX

that in H1 (first half) 2023, two-thirds of remote card fraud is due to card-not-present fraud [36].

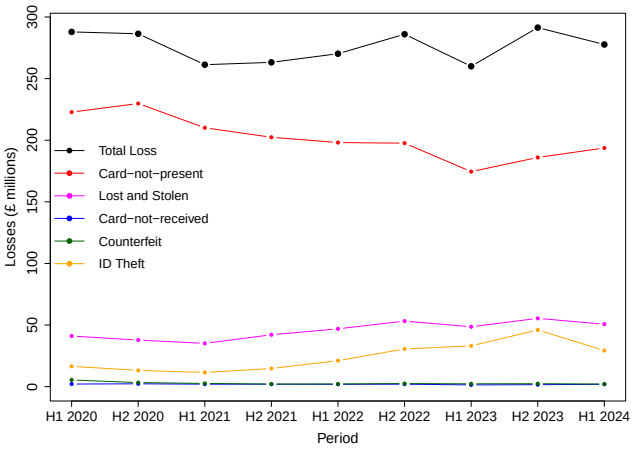


Figure 1: Amount of financial loss in the UK due to five types of card fraud over time [114]; Card-not-present fraud is the most prominent one.

Card-not-present fraud causes significantly more financial loss than any other unauthorized card fraud; see Fig. 1 for a detailed breakdown. While lost and stolen card loss has remained relatively constant over the last four years, CNP is increasing again as criminals find new ways to circumvent additional protections. These protections include the strong customer authentication (SCA) rules that require e-commerce to verify customers' identities for certain high-value purchases [41]. Two possible ways scammers thwart this are: (1) identifying online merchants that allow lower-value transactions without requiring identity verification, or (2) colluding with online payment merchants, allowing scammers to perform multiple transactions. While previous work has applied crime script analysis [18] and machine learning to detect CNP fraud [72, 94], there is little empirical research that directly examines scammer behavior in CNP fraud.

To address this research gap, our paper provides a proof-of-concept study to take a step forward in this direction. We propose a small-scale experiment in which we manually enter credit card details into confirmed smishing URLs and monitor the resulting authorization attempts to explore the types of activities scammers engage in with stolen cards. To this end, we collaborate with a mobile network operator and a financial institution based in the UK that provides us with blocked smishing texts and 12 test credit cards. We submit the cards to 12 smishing URLs: 10 identified as delivery scams, one entertainment streaming service scam, and one telecom payment scam. Our work introduces a novel methodology that enables understanding scammers' behavior to help stakeholders combat CNP fraud, contributing broadly to the literature examining how scammers exploit user trust in systems.

Our paper provides the following contributions:

(1) For the first time, we empirically investigate card-not-present (CNP) fraud using a proof-of-concept study.
(2) The analysis of the 36 authorization/transaction attempts ISO messages highlights scammers' transaction patterns.
(3) We identify scammers' preferred cash-out mechanisms, i.e., 17 different online merchants that criminals exploit to monetize stolen credit cards.

2 Background

Scammers lure victims via email, SMS, or calls, resulting in users providing their personal or financial details. Fraud accounts for 41% of all crime in England and Wales [87], leading to estimated losses of £6.8bn annually [83]. Similarly, the US Federal Trade Commission (FTC) reported that consumers lost $12.5bn to fraud in 2024 [40]. The increasing amount of financial losses highlights the necessity to study the uptick in scams.

Distinguishing benign websites from malicious ones remains challenging. Users continue to fall for phishing due to the inability to recognize online impersonation tactics [124]. They spend very little time gazing at security indicators compared to website content when making assessments [9]. Scammers have been exploiting the common trust indicators – logos, third-party endorsements, URLs, and padlock icons [57] to deceive victims. While users rely on a combination of at least three different strategies (most commonly - site information, design, and functionality) to differentiate phishing websites on a mobile phone [68], scammers use visual deception to create a false sense of trust [32]. As users' awareness of suspicious URLs grows, scammers shift towards abusing shortened URLs to hide phishing websites. Similarly in smishing, scammers exploit users' trust as they focus on the SMS content rather than the sender ID to decide the legitimacy of the text message [104].

In this section, we provide background on how scammers abuse users' trust in SMS by sending smishing texts, monetize the stolen details via card-not-present fraud, or sell those details on underground forums. We illustrate the stages with every step in Fig. 2.

2.1 Smishing

In the past few years, there has been an uptick in smishing [46, 85]. In order to carry these out, scammers set up a phishing website ❶, broadcast phishing text messages over SMS or online communication services (OCS) such as iMessage, rich communication service (RCS), or WhatsApp, providing a malicious URL ❷ and deceive users into taking an action ❸.

Previous work categorizes SMS scams into six unique types [5]. Some of these scams fall under Authorized Push Payment (APP) fraud, where customers intend to send money via bank transfer to a person or business, but end up sending the money to a scammer. For instance, 'Wrong number' scams start with a random text from the criminals, where they try to build a relationship after receiving a response from a user, and convert into a romance scam or fake cryptocurrency investment scam. Whereas in 'Hi Mum and Dad' scams, criminals pretend to be the victims' child in distress and request financial help [4].

In contrast, smishing texts deceive users into providing personal details via a malicious URL provided in the text message. Delivery, Government, and Telecom impersonation scams are three types of smishing scams. Here, scammers impersonate a parcel delivery

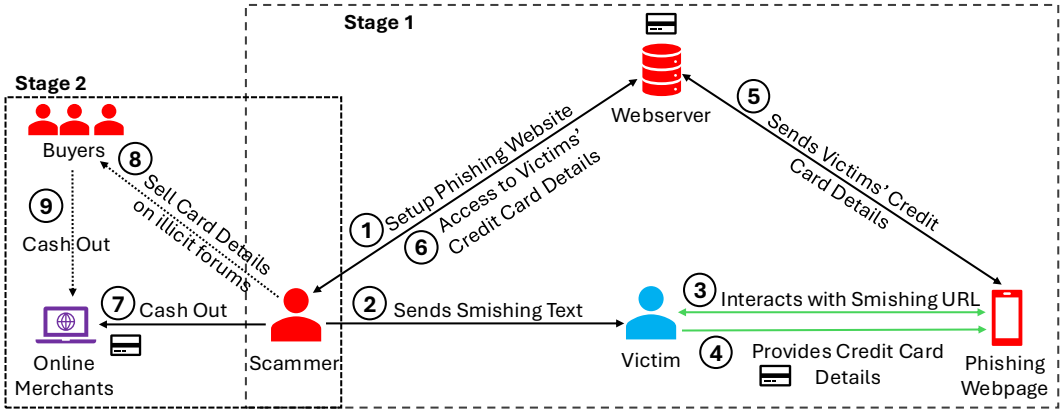


Figure 2: Scammers send smishing texts, steal credit card details, and commit card-not-present fraud. Stage 1: Scammers lure victims into opening a smishing URL and steal their credit card details. Stage 2: Scammers cash out or sell details on illicit forums.

company, government agency, or telecom provider with a text message tailored to impersonate the entity and provide a malicious URL. Scammers also impersonate other entities such as online streaming providers. These fall under the broader category of unauthorized fraud, where scammers steal victims' details through malicious URLs and abuse them for unauthorized access/payments or identity theft.

Delivery scams look similar to other smishing texts. They contain a malicious URL and impersonate a well-known company. For example:

> Evri-UK: Your parcel has a 1.45 (GBP) unpaid transit fee, you must pay the fee now for a redelivery via: [URL]

However, the difference lies in the information criminals steal from the victims. In banking or government impersonation scams, the phishing page exploits users' trust to steal their banking credentials. Similarly, they steal login credentials in scams that impersonate technical companies like Microsoft. But, the text message in delivery scams usually requests a small payment and provides an online form imitating a payment gateway (Fig. 4b). This phishing page exploits the user's trust as the individual assumes they are paying a fee to receive their parcel and end up providing their credit card details 4. Instead of authorizing the card, the phishing website steals the details – name, address, mobile number, and credit card details and stores them in a criminal database 5.

Even though delivery scams target individuals quite broadly [5], there is no empirical work done to study them on their own. Prior work broadly looks into smishing infrastructure using different datasets such as online public SMS gateways [79] or crowdsourced smishing reports [109]. Some work has focused on detection, e.g. via rule-based classifiers or machine learning to detect smishing texts [56, 58, 74, 75, 101]. Our work is the first to take an investigative approach to study impersonation scams requesting payments, such as delivery scams, by providing personal and credit card details to the malicious URLs.

2.2 Card-Not-Present (CNP) fraud

Criminals obtain victims' details through data compromise, including third-party data breaches, phishing emails, and scam text messages (smishing) 6 [53, 91, 98]. To cash out, criminals use the stolen card details to make a purchase online, over the phone, or via mail order, also known as Card-not-present (CNP) fraud 7. Bodker et al. use crime script analysis to present the various stages in the process of CNP fraud [18]. While this provides an understanding of the different stages involved in CNP fraud, our work focuses specifically on investigating the authorization attempts made by scammers when attempting to monetize compromised test credit cards.

Prior work on credit card fraud has primarily focused on detecting fraudulent transactions, often using private or limited publicly available datasets [1, 7, 19, 25, 35, 72, 76, 92, 107]. Abi Din et al. devised a model to detect card-not-present fraud for online applications where the merchants are supposed to request the users to provide their cards' scans [33]. While this could be an effective method, it introduces privacy concerns with uploading images of users' credit cards on a merchant's payment portal. Another proposal from Mannan and Oorschot posited that localized ID numbers could limit synthetic ID theft against card-not-present transactions [69]. Techniques such as identifying low-frequency transaction patterns [123], applying big data analytics [94], and geographic anomaly detection [6] have been explored. Our work does not aim to detect these transactions. Rather, we contribute insights into real world scammers' transaction behavior that could be used to improve previously devised models to better detect CNP fraud.

2.3 Underground forums

Cybercriminals use underground forums to interact with eachother, exchange knowledge, or trade products and services 8. These forums are generally closed and operate over TOR, providing pseudo-anonymity to the participants [21, 88]. Underground forums primarily provide a place for threat actors to interact with each other

and purchase services to conduct illicit activities. They can also serve as a training group for new people to gain skills or a place to meet new people to discuss further with them on private channels. Often cybercriminals specialize to sell narrowly attractive products or services to conduct cybercrime [117]. These include products and services like phishing kits [106], hosting malicious websites, fraudulent social media accounts [108], cashing out cards, and services to send bulk texts [4].

Previous work analyzed six closed forums and identified popular items criminals trade – online payments, game-related accounts, credit cards, and financial accounts [78]. Others analyzed the different types of goods sold longitudinally over 16 anonymous marketplaces [102]. More recently, criminals have started abusing platforms such as Telegram for easier access to new entrants [97]. This body of work relies on forum posts to understand the inner workings of criminal behavior. It is fundamentally tied to the availability of data both from the platform end but also relying on the criminals to use the platforms that they measure. While this allows us valuable insights into how cybercriminals operate, it is necessarily indirect.

Our work fits in the broader literature of understanding the illegitimate uses of stolen credit cards [8, 50, 53, 61, 91, 99, 121]. We do not investigate underground forums or collect data from them. Rather, we focus on directly understanding what happens after card information is (likely) sold ❾. We work to directly uncover their cash-out mechanisms, augmenting the literature understanding underground markets.

3 Methodology

This section describes our experimental approach for distributing test credit cards to scammers through smishing URLs. This helps us analyze the transaction/authorization attempts made by scammers to conduct card-not-present (CNP) fraud. Fig. 3 presents the overview of our methodology.

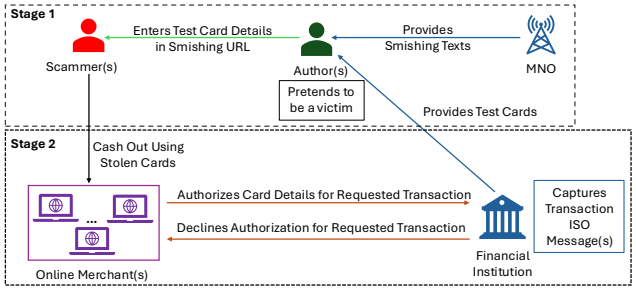


Figure 3: An overview of our methods. First, we provide test credit cards to scammers via smishing URLs and second, we receive the transaction ISO messages from our collaborator.

3.1 Accessing smishing URLs

Ofcom, the UK telecom regulator, works with the mobile network operators in the country to stop scam and spam text messages [86]. To this end, mobile network operators in the UK run an XDR detection system that utilizes machine learning and manually added rules to filter suspicious text messages [71]. These text messages are blocked and do not get delivered to their customers. We collaborate with a major UK mobile network operator that shares the feed of these blocked text messages with us daily (see stage 1 in Fig. 3).

For our experiment, we programmatically extract suspicious URLs from blocked text messages that impersonate delivery, telecom, or online entertainment services requesting users to pay unpaid bills between July 17 and July 25, 2024. Next, we manually confirm the malicious nature of pseudo-randomly selected URLs by opening them in a browser (see Fig. 4). Scammers create sophisticated phishing web pages and restrict them based on geographical locations and device types. To bypass these restrictions, we use a mobile user agent on our desktop browser and access the phishing website. We also use a virtual private network (VPN) to avoid providing our actual IP address to the scammers, as they are known to collect victims' device details.

3.2 Supplying test credit cards

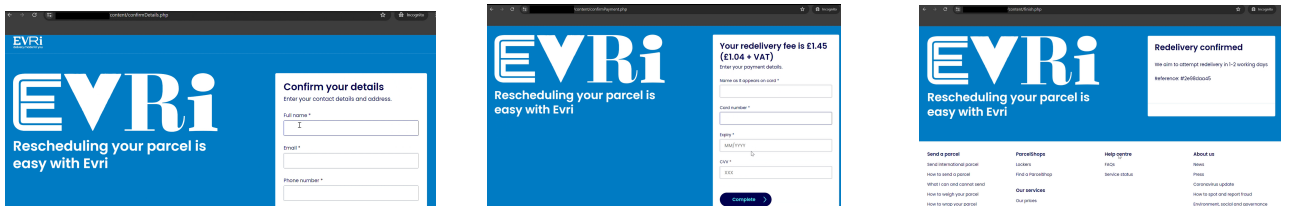
Our study aims to understand the transaction patterns scammers attempt using stolen cards, indicating their cash-out mechanisms. To this end, we collaborate with a UK-based financial institution that serves as a card issuer [89], which provides us with 12 test credit cards. Note that not all financial institutions have the authority to issue credit cards. We generate fake names and addresses using an open-source Python package – *Faker*.[1] We provide these synthetic identities to our collaborator to associate them with the test cards. Note: We do not impersonate any individual or known address for this purpose. In line with the ethical considerations, we need to ensure that no funds are transferred. This is achieved by declining all the transaction or authorization attempts made by the scammers. To this end, our collaborator provides us with an incorrect expiry date (MM/YYYY) combination for every test card. This ensures that scammers' every cash-out attempt is unsuccessful and avoids the bank-merchant chargeback process.

Next, we provide the 12 test credit card details in 12 confirmed live smishing URLs, with each card being entered into exactly one URL between July 17 and July 25, 2024 (see Fig. 3). The one-to-one URL-card relationship helps us track different scammer behaviors. We do this to attribute the observed transaction patterns or behaviors to a specific smishing URL. Using the same card across multiple URLs would make it challenging to trace it back to a particular scammer or group, reducing the precision of our behavioral analysis. The smishing URLs also request personal details before asking for a credit card, as shown in Fig. 4a. We use the fake identities created to supply this information and provide our working honeypot mobile numbers where the form requests one. Fig. 4 shows an example of an 'EVRI' smishing page where the first page asks victims' details, the second page requests the credit card details, and the last page shows a fake confirmation.

3.3 Capturing transactions' ISO messages

After stealing credit card details through the smishing URLs, scammers either directly monetize by purchasing services/goods from online merchants (see transition from Stage 1 to Stage 2 in Fig. 3) or sell them to buyers on underground forums, who further monetize

[1] GitHub Repository for Faker Python Package - https://github.com/joke2k/faker



(a) First page requests victim's details. (b) Next page steals credit card details. (c) Last page shows redelivery confirmation.

Figure 4: Smishing webpage impersonating a delivery company stealing victim's personal and credit card information.

them. Monitoring underground forums for the sale of stolen credit cards is out of the scope of this paper. We aim to understand the transaction attempts made to conduct card-not-present fraud.

Our collaborating financial institution monitors all the cards they issue us for this research, declines any authorization/transaction attempt due to incorrect expiry date, and captures the ISO message for every transaction (see Stage 2 in Fig. 3). They provide us with the ISO messages for all the 36 transactions/authorizations attempted by scammers. ISO 8583 is an international standard for the interchange of electronic transactions initiated by cardholders [55, 110]. Every ISO 8583 message of a transaction supports up to 128 data elements, which are the key pieces of information. We receive 10 key data elements for every ISO message (see Table 1) from our collaborator that we analyze to understand scammer behavior in Section 4. As of December 2024, the scammers' last transaction was recorded on August 18, 2024. Note, we cannot make the (ISO messages) publicly available in compliance with the signed agreements.

Table 1: Key data elements received from our collaborator for all transactions' ISO messages scammers try using stolen credit cards.

Data Element	Explanation
DE 2	Card identifier token used to map the transaction to the card
DE 4	Transaction Amount (Original Currency)
DE 6	Transaction Amount (Converted Currency)
DE 7	Transaction date and time (MMDD HH:MM:SS)
DE 14	Expiration date (YYMM)
DE 18	Merchant category code
DE 19	Acquiring Institution (country code)
DE 43	Merchant name that will appear on statements
DE 49	Original currency identifier (country code)
DE 51	Card currency identifier (country code)

Enrichment of data elements. Before analyzing the ISO messages, we need to understand the meaning of each data element. While six data elements are straightforward to parse, four require additional queries to accurately interpret their values. The merchant category code (DE 18) provides the type of business category the merchant belongs to. We query this against the list of codes publicly available from Citibank to identify the merchant's categories in our data.[2] Three key data elements provide a country code to identify the country in which the acquirer bank is based (DE 19), the original currency's country (DE 49), and the card's currency (DE 51). We query these against the list of country codes publicly provided by Visa, a global payment network.[3]

3.4 Ethical considerations

The proposed methodology has some ethical concerns. Informed consent is not possible when providing test credit card details on known malicious URLs. Instead, we can view this work through the lens of the beneficence principle and perform a risk-benefit assessment. The use of deception in cybercrime research is discussed in the Menlo report [34] and considers deception for research purposes. Following the Belmont report [10, 73], we determine that there are negligible risks to the stakeholders and that it has broader societal benefits. As in our proof-of-concept, the test credit cards do not allow funds to be transferred. Instead, all authorizations fail because of the wrong expiry date provided. As a societal benefit, providing test credit cards to scammers helps waste their time and helps identify the merchants they abuse. Additionally, the research will help provide a much-needed understanding of the scammers' behavior, including transaction patterns, allowing stakeholders to better tackle this cybercrime.

We do not impersonate any entity or individual to issue test credit cards. The research for our case study was overseen by UK government agencies such as the National Crime Agency (NCA) and a global payment processor, in addition to our industry collaborators. We communicated our insights to our collaborating financial institution, law enforcement, and the payment processor. The department's research ethics committee evaluated our assessment and provided an exemption for this study.

Future work considerations. If future researchers were to scale out our work, it would be necessary to protect individuals' credit card information from criminals. We are also concerned about impact to banks involved – a heavy increase of test credit cards would need rigorous oversight to ensure that the benefit to the bank would exceed the overhead for providing them.

If future researchers were to create artificial datasets using existing credit card information, it would be important to use the best practices here to limit PII leakage. There is plenty of work in creating anonymized or synthetic datasets for everything from credit card fraud [22–24, 27–29, 59, 66, 67] to national security-related topics [31]. It has been possible to create something robustly private

[2]Merchant Category Codes - https://www.citibank.com/tts/solutions/commercial-cards/assets/docs/govt/Merchant-Category-Codes.pdf

[3]Supported Country Codes - https://developer.visa.com/capabilities/visa-b2b-payment-controls/docs-master-codes

yet usable given time and necessity [44] (albeit with potential harm if not done properly [81]).

4 Scammer behavior

Towards understanding scammers' transaction behavior and cash-out mechanism, we analyze the ISO messages of the transaction/authorization attempts they make. We find that scammers only try to authorize 8 out of 12 credit cards we enter in smishing URLs. As of December 2024, the remaining four cards have no transaction ISO message, per the data provided by our collaborator. This could be due to multiple reasons: (1) The scammers who stole these cards through the smishing URL only do so to sell the card details on illicit underground forums and did not manage to sell it; (2) The scammers were able to identify that the card details were not provided by a legitimate victim, or (3) The smishing URL was not able to collect/relay the stolen credit card detail to the scammers' database. While we achieve 66.7% (8/12 cards attempted) success in a small-scale experiment, this would differ based on the scale of a study. Previous scammer interaction studies have achieved a smaller success rate [3, 4]. If a large-scale study were conducted, the results would be more generalizable.

We provide a brief overview of the authorizations scammers attempt using the stolen cards in Table 2. Next, we focus on the broader findings from the table about scammers attempting multiple authentications and their monetary value. In this section, we describe the findings from our experiment about scammer transaction patterns and the cash-out mechanisms, followed by a discussion on how they continue to re-target victims.

Table 2: Distribution of transactions (n = 36) scammers try using stolen credit cards.

Card	Transactions (#)	Value (£)	Merchants (#)	Original Currencies
Card 4	18	302.07	4	ILS, USD, GBP, EUR
Card 1	7	54.97	5	USD, GBP
Card 2	3	1.00	2	GBP
Card 7	3	55.94	3	GBP, USD
Card 10	2	1.00	1	GBP
Card 5	1	1.99	1	GBP
Card 8	1	10.10	1	USD
Card 12	1	0.78	1	USD
Card 3	0	-	-	-
Card 6	0	-	-	-
Card 9	0	-	-	-
Card 11	0	-	-	-
Total	**36**	**427.85**	**18**	**4**

Scammers are unaware of authentication attempt errors. Scammers try multiple transactions using the stolen credit cards. Surprisingly, even after the first transaction fails, scammers do not try to change the card details when trying more than once. Instead, they keep using the same expiry date, name, and card number combination we provide. This indicates that they are unaware of the exact error that caused the transaction to fail. We find that scammers try multiple attempts with five cards and only one with the other three cards. In total, they try 36 transactions worth £427.85 at 18 online merchants.

Transaction values. Criminals often attempt to authorize stolen cards across multiple merchants using low-value transactions rather than high-value ones [116]. The results of our experiment also support these findings. This is likely intended to evade detection and bypass the implemented security mechanisms, such as strong customer authentication (SCA) rules that mandate online merchants to verify customers' identity for high-value purchases in the European Economic Area (EEA) and the UK [41, 119]. We also observe that scammers try to transact in currencies such as ILS (Israeli Shekel) and USD (Table 2), suggesting that the local currency of the acquirer bank or the source location of the transaction is outside regions where the SCA regulations apply. Scaling our experiment could further strengthen these observations.

4.1 Transaction timings

We explore the timings when the scammers attempt to authorize the stolen cards to understand transaction timing patterns, if any. We identify that all attempts are made between 07:55:59 and 18:53:46 BST (see Fig. 5). Timings of the transactions, even though online, are done during standard shopping hours based on the victim's location; BST in this case. Criminals use this as a measure to bypass the automated fraud detection systems to avoid getting flagged for manual reviews [54]. Researchers with access to CNP fraud datasets could verify this finding and also examine the distribution of attempts by day of the week. This could indicate if scammers prefer certain days of the week to cash out.

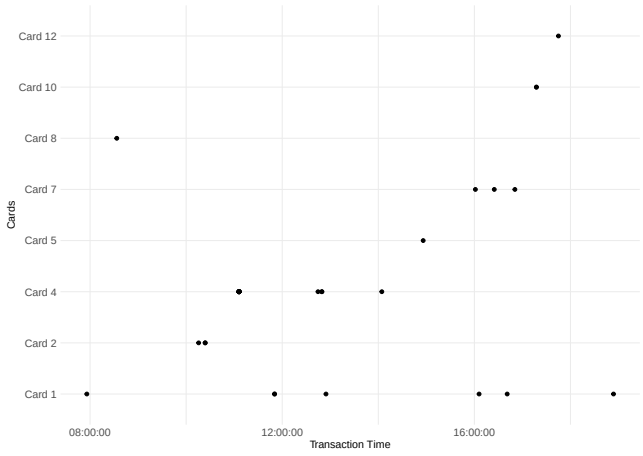


Figure 5: Time of the day when scammers try to transact using stolen cards (n = 36).

Even though every card was entered once in exactly one URL, Card 4 stands out. Surprisingly, we observe 18 authorization attempts on this card (see Table 2). On a closer investigation, we find that the scammer tried to authorize it 14 times at the same online merchant (see Table 3). From the ISO messages of these attempts, we observe that the scammer tried to authorize the card exactly at the same time (11:06) on 7 different days. This points out that the particular threat actor who has access to this card likely has an automated script that tries to authorize all stolen cards. Experimenting

on a larger scale or having access to fraudulent card transactions could highlight similar patterns.

Delays in first transaction attempt. We find that scammers try to authorize five cards on the same day, one after a day (Card 2), one after three days (Card 4), and the last after nine days (Card 8). This indicates that while some scammers try to transact as soon as they receive the card details, others probably sell them on illicit underground forums instead of cashing out themselves directly [37, 50, 78]. This could be a possible reason for the delay in the first authorization in two cases where scammers try to authorize after three and nine days, respectively.

In four instances, we observe that criminals try to use the card as soon as possible. We recorded the time when we provided the card's details in a smishing URL. Three of these had the first authorization attempt on the same day, one of which was tried within 10 minutes, and the others within the first few hours. Criminals try to use the card before banks can block it based on the user's report. The red line in Fig. 6 shows the cumulative distribution for the days after which the scammers attempt to authorize the card for the first time (mean = 1.625 days).

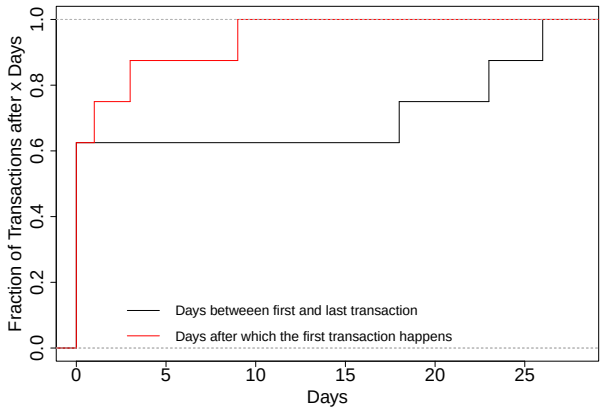


Figure 6: Cumulative distribution for the number of days scammers try to authorize the stolen credit cards (n = 8).

Lifetime of stolen cards. Previous research points out about the stolen cards going stale and provides a powerful incentive for scammers to sell cards as quickly as possible [90]. While we do not study the sale of stolen cards, we do look into how long the cards are abused before scammer gives it up. We analyze the ISO messages received from our collaborators to find the last timestamp when the scammer tries to authorize the stolen card. This helps us determine the lifetime of the stolen cards, i.e., the days between the first and last transaction. Out of the eight cards, three were only tried authorization once. To this end, we find a mean lifetime of 8.37 days with a median of 0 days. The black line in Fig. 6 represents the cumulative distribution for the lifetime of the stolen cards. While our findings are based on a proof-of-concept, a large-scale experiment using our methodology would produce more generalizable results.

4.2 Merchants

We investigate the 17 unique online merchants where scammers try to authorize the provided credit cards. Utilizing the acquirer bank country code (DE19 from Table 1), we identify that the scammers do not restrict the authorization attempts to merchants based in the UK. In addition to services in the UK, we identify that criminals try to authorize the cards with online merchants based in other countries – USA, Canada, Ireland, and the Netherlands (see Table 3 for merchant-wise breakdown). Scammers abuse both large and small entities to cash out using the cards obtained from smishing. This indicates that future studies on CNP fraud should include a broad range of merchants, as attackers target all kinds of services.

Services to fuel illicit activities. Some scammers use stolen credit cards to procure services that can be used to conduct further scams. We identify merchants such as mobile network operators (MNOs) (Merchant 3, 6 and 7), a large-language model (LLM) chat platform (Merchant 4), web hosting services (Merchant 17), and VPN (Merchant 5) where the scammers attempt to authorize the stolen cards. Purchasing SIM cards from MNOs could be use to conduct a range of scams including smishing and LLMs are used by scammers to create smishing text or better phishing emails [96].

Finding official websites for most merchants in our data was straightforward, except for Merchant 5. During our efforts to locate Merchant 5's website, we discovered a Reddit forum post in which a user reports receiving a fraudulent transaction alert from their bank, which was attributed to this merchant.[4] As the post on Reddit mention the transaction attempt from October 2023 and scammer tried to authorize our card in July 2024, the same threat actor may have been running multiple campaigns and targeting the same merchant since 2023 to procure VPN services from them. Alternatively, the merchant could be colluding with the scammers and helping them cash out. Researchers with access to real-world CNP fraud transactions datasets could help identify suspicious online merchants that collude with criminals to monetize stolen cards.

Services offering goods and subscription. Scammers also prefer to purchase goods (Merchant 9 and 10) or authenticate the cards with subscription services (Merchant 12). Criminals primarily target services related to physical goods where websites offer an easy returns/refunds process. To avoid getting tracked, criminals often use reshipping mules when they order physical goods [49]. Reshipping mules are people whose addresses criminals use for drops and reship the received goods to the criminals' addresses. If the websites do not allow returns, criminals resell the purchased products on online marketplaces like eBay [12]. Online platforms that allow the resale of purchased goods should verify the authenticity of the sellers during their onboarding process.

Targeting fundraising services. Recently, criminals have been known to conduct event or charity-related scams to steal funds from users [2, 17]. Surprisingly, we notice a transaction attempt (£98.67) that scammers try on one of the biggest crowdfunding platforms (Merchant 11). While platforms like these allow users to raise funds for life events and challenging circumstances, this transaction indicates that criminals create successful fraudulent fundraising

[4] https://www.reddit.com/r/PHCreditCards/comments/17dj4tl/citi_fraud_alert_letsgo_network/

Table 3: Description of unique merchants ($n = 17$) scammers abuse using stolen credit cards. (The transactions with £0 are zero-value authentication requests.)

Merchant	Merchant Category	Country	Transactions (#)	Value (£)	Offers Subscription	Offers Flat Price
Merchant 1	Computer Software Stores	US	14	172.38	Yes	No
Merchant 2	Eating Places & Restaurants	UK	4	2.00	Yes	Yes
Merchant 3	Telecommunication Services	UK	3	50.00	Yes	Yes
Merchant 4	Computer Software Stores	US	2	31.02	Yes	No
Merchant 5	Computer Network/Information Services	CA	1	0	Yes	No
Merchant 6	Telecommunication Services	US	1	0	Yes	Yes
Merchant 7	Telecommunication Services	US	1	4.97	Yes	Yes
Merchant 8	Recreation Services-Not Elsewhere Classified	NL	1	0	Yes	No
Merchant 9	Digital Goods	IE	1	0	No	Yes
Merchant 10	Miscellaneous House Furnishing Specialty Shops	UK	1	0	No	Yes
Merchant 11	Organizations, Charitable & Social Service	NL	1	98.67	No	Yes
Merchant 12	Direct Marketing-Continuity/Subscription	UK	1	1.99	Yes	No
Merchant 13	Grocery Stores, Supermarkets	US	1	0	Yes	Yes
Merchant 14	Business Services Not Elsewhere Classified	UK	1	0	Yes	No
Merchant 15	Eating Places & Restaurants	UK	1	55.94	No	Yes
Merchant 16	Department Store	US	1	10.10	No	Yes
Merchant 17	Computer Programming, Data Processing & Integrated System Design	US	1	0.78	Yes	No
Total		**5**	**36**	**427.85**	**12**	**10**

campaigns and use them for card-not-present fraud. As fundraisers are abused to cash out, there is a need to study fundraising platforms more broadly to identify possible cybercriminal activities.

Sophisticated methods to cash out. As the cat-and-mouse game between criminals and law enforcement continues, criminals find new ways to cash out using stolen card details. As they cannot create counterfeit cards with the textual information from smishing, they have started abusing mobile phone wallets such as Google Pay to link stolen cards [43, 63]. Recent research shows how the weaknesses in digital wallets can be exploited to add stolen cards and make unauthorized transactions. [13]. In our data, we also find two transactions where the criminal tried to link the provided credit card with two different online wallets (Merchant 8 and 14). Once the cards are added to the wallets, they are used to pay in person at POS machines (local shops or their own POS machines) or the phones with the linked cards are sold in illicit underground forums. This indicates how criminals continue to evolve and use sophisticated techniques to monetize stolen cards.

4.3 Re-victimizing users

Criminals continue to exploit victims' trust in communication mediums such as SMS by targeting them repeatedly [60, 70, 115]. Over 11% of fraud victims were victimized more than once in the UK [82]. Scam texts are generally broadcasted to multiple users, and threat actors do not know which recipients got lured into taking an action [4]. To gather victims' details, criminals develop phishing web pages that ask for users' details, as shown in Fig. 4a. While the name and address might be necessary to conduct card-not-present fraud through online merchants, attackers also collect contact information such as mobile numbers.

During our experiment, we entered mobile numbers along with the synthetic identity details into the phishing web page (see Fig. 4a) before providing the credit card details. Unexpectedly, two of the supplied mobile numbers later received targeted smishing texts, personally addressed using the names we had entered. We received one further delivery smishing message per month until four months later (Nov 29, 2024). After realizing that the card details have been stolen, victims would reach out to their banks to cancel their cards and get new cards issued [30]. The continuous smishing texts indicate that criminals perceive previous victims as easier targets and continue to re-target them to steal the new credit cards. Note that we did not engage with these messages in line with the protocol of our study. Two examples where scammers address us by the provided names are:

> [First Name] , a c t o n y o u r p u r c h a s e i m m e d i a t e l y : [URL]
> [First Name] , y o u r n e e d s a c t i o n : [URL]

Unlike conversational scams, where criminals continue to contact victims to groom or convince them to invest more money, the targeted smishing texts in our case simply try to steal more credit cards, causing victims more financial and psychological harm. This suggests an urgent need for proactive intervention approaches and user awareness.

5 Discussion and implications

We discuss the limitations of our methodology and other issues that limit researchers from studying card-not-present fraud. We further discuss implications of our work to trust, regulation, traditional crime, and further work.

5.1 Limitations

Data limitations. Our experiment has a few limitations. Our collaborator provided us with limited cards for a short period of time. While the limited cards and time period allowed us to enter the card details in only 12 malicious smishing URLs, our work is an important first step in the direction of empirically studying card-not-present (CNP) fraud. No prior work has been able to study scammers' transaction behavior by providing and monitoring test cards.

Our collaborator provided us with incorrect expiry dates to ensure that the transactions scammers try to authorize fail and no payments could be made. While this is one way to ensure the authorizations are unsuccessful, it might have alerted attentive fraudsters and stopped them from authenticating and then using or selling the stolen card details. If more resources were available, our collaborator could have allowed authorization attempts but denied transactions with an error message mentioning unavailable funds instead of an incorrect expiry date. This would help scammers gain confidence in the card details and attempt further transactions.

We collect the malicious URLs from a collaborating mobile network operator that provides us with live blocked text messages along with the URLs. This experiment is biased towards scammers that target individuals in a specific country through smishing texts, a similar caveat as related work which rely on telecom data [4, 5], Having access to smishing data targeting users in multiple countries could have helped study different scammers or threat actor groups, shedding light on some new insights into their transaction patterns. However, this would necessitate international, significant levels of cooperation for a type of industry that is notably not set up for data sharing with academics. This is often due to legal or logistical issues, like complex contracts, more so than reluctance to work with academics. More work needs to be done for academics to interface with mobile network operators and other telecom intermediaries to find solutions to share data while protecting consumer privacy [65].

More recently, criminals have started abusing online payment gateway APIs to validate stolen credit card details [112]. While we are not aware of any instance where scammers tried validating the test cards we provided (aka card cycling), it is possible that the single authorization attempts in our study were done for similar reasons. Card cycling is inherently valuable for both sellers of card information to ensure they are selling a high quality product as well as buyers who want to test the card works before making high value purchases. We do not have the data to test this empirically – more data is necessary to study this distinction.

Unavailability of data more broadly. Card-not-present (CNP) fraud is the most significant type of card fraud [36, 114]. While this has been increasing over the years [11], the unavailability of real fraudulent transactions makes it challenging for the academic researchers to study this scam. While recent work has devised machine learning models to detect CNP fraud [72, 94], the lack of real-world transaction data restricts the understanding of the scammers' behavior patterns. Furthermore, most CNP fraud is viewed alone, rather than in the context of knowing where the cards came from. This greatly impacts, e.g., the understanding of cash out mechanisms, which is a major limitation of our work and strongly motivates why there needs to be more work done here. Our methodology can be utilized by researchers and industry stakeholders to conduct studies on a significantly larger scale. This would result in new, updated datasets to study CNP fraud.

We also suggest that the stakeholders (payment processors, financial institutions, and other intermediaries) should publish anonymized, up-to-date datasets of CNP fraudulent transactions. This would enable researchers to empirically analyze scammers' transactions and help devise better detection models.

5.2 Criminals exploit users' trust

Scammers exploit users' trust in text communication channels which cannot be fully, safely monitored [100]. Trust is a crucial factor in the relationship between users and technology. When compromised, it can fundamentally alter users' behavior and perception of security. Without establishing trust, interactions cannot be completed. SMS as a communication medium involves multiple stakeholders such as aggregators that cannot be monitored completely by the mobile network operators. In case of RCS and iMessage, end-to-end encryption hides the plain text of the message, making it harder for stakeholders to detect and stop scam texts. While these factors introduce barriers to stopping scams, scammers misuse these technologies to enter into the ecosystem. Fraudsters exploit the trusted communication channels to send smishing texts by impersonating authoritative entities such as banks, government agencies, and logistics providers [38, 43]. Users trust that the sender is reliable while the scammers abuse this by impersonating a trusted entity [42]. While users rely on their mobile network operator to tackle scam texts and calls, scammers use sophisticated techniques such as sender ID impersonation to evade detection [5, 111].

Alongside smishing which exploits trust in communication channels, sophisticated phishing websites abuse users' trust in e-commerce and online payment services [64]. A phishing web page uses visual deception, imitating the authentic website of the brand being impersonated to make the user believe that they are providing their details to a legitimate entity. For example, Fig. 4 shows how scammers deceive users into providing their personal and credit card details on a phishing website imitating a parcel delivery company. The stolen details are then monetized by scammers through card-not-present fraud.

Smishing texts leading to CNP fraud result in direct financial loss and undermine users' long-term trust in online services [20]. Impersonating brands also affects businesses' reputation and people's trust in them, impacting their revenue generation. As a protective response to scams, some times users reduce or completely stop their use of digital platforms [45]. This changes the ways in which users interact with businesses and could significantly impact both users and brands. Trust exploitations across communication and transactional vectors suggest the need to design more resilient trust and security mechanisms in digital platforms.

Quantitatively measuring CNP fraud resulting from smishing could allow researchers to measure the negative financial impact of trust in institutions. Without the trust in the system, these scams would not be possible [105]. However, without trust in the system, legitimate use resulting in billions upon billions of dollars of profit would also not be possible. It is important to weigh costs here –

how much fraud is worth an additional dollar of revenue? While others [52, 93, 122] provide insight into the profits generated by online services (particularly online delivery services like UPS and Amazon), we work to quantify the risks here.

5.3 Criminals bypass regulations to cash out

Criminals strategically select target merchants; the Strong Customer Authentication (SCA) rules in the EU affect their decisions to conduct card-not-present (CNP) fraud. To avoid authorizing stolen cards on online merchants that may have 3D Secure authentication enabled [118], fraudsters often target merchants that offer products with low-values/zero value authorization requests or have an acquirer bank (the receiving bank of the merchant) based outside the European Economic Area (EEA) [119]. We find multiple low-value transaction attempts and zero-value authentication requests subscribing to online services (see Table 3) as well as merchants whose acquirer banks are based outside the EEA and UK. We additionally found authorization attempts in four different currencies, USD being the most common (see Table 2). These trends, while not conclusive, add weight to this theory. While we have limited transaction data, researchers with access to real-world CNP fraud data should use our initial insights to further explore such patterns and uncover scammer cash-out strategies.

Scammers have identified new techniques such as authorizing stolen credit card details with digital wallets [63]. Our findings support this: we identify two authorization attempts to two different merchants that offer digital wallet services. While previous work (from 8 years before our data collection) outlines various methods criminals employ to launder money [116], we find little evidence of these techniques, indicating that criminals' methods likely evolve over time. This indicates an urgent need to update the current regulations. We suggest that the payment security mechanisms on online gateways should challenge the user to detect CNP fraud, even for small-value transactions. For services providing digital goods that offer instant value and anonymity, such as gift cards, merchants should perform more due diligence before issuing them. As fraud has no boundaries, fighting this battle needs international cooperation. Implementing something more global than regional SCA rules would stop scammers from attempting transactions to merchants whose acquiring bank is based outside the regions where the rules apply.

5.4 Cash-out strategies similar to physical crime

Traditionally, criminals monetize stolen physical cards and counterfeit cards at point-of-sale (PoS) retailers to purchase physical goods or gift cards, often resold to cash out. Since the transition to card-not-present (CNP) fraud, the cash-out mechanisms have largely remained the same; only the medium has shifted. Online services (such as Merchant 15) sell gift cards that could be easily resold to cash out. Other services that provide refunds of purchased services/goods with in-platform credits are also abused as cash out mechanisms (e.g. Merchant 1). Criminals take advantage of these available and flexible options by abusing online services to monetize stolen credit card details, conducting card-not-present (CNP) fraud. We identify 17 online merchants in Section 4.2 that criminals abuse to authorize stolen credit cards.

Rather than physically stealing or cloning cards to create counterfeit ones, cybercriminals steal card details through social engineering techniques such as smishing. This shift has altered the technical skill requirements and eliminated the need for physical presence, enabling them to operate remotely with a reduced risk of detection [16]. In addition to targeting physical retailers, fraudsters purchase products through online merchants (see Section 4.2), but continue to leverage drop shipping mules to receive and redistribute the goods [49]. Others also monetize by selling credit card details to buyers on underground forums (Fig. 2).

Online merchants need to effectively stop CNP fraud transactions. We find transaction attempts where criminals use stolen cards to purchase services such as virtual private network (VPN) or web hosting, allowing them to continue running their illicit activities. All these cash-out mechanisms closely mirror the techniques used in physical card fraud. Despite the shift from physical cards to CNP fraud, the fundamental strategy to convert stolen credentials into monetary value remains unchanged. While scammers evolve with users' trends, the cash-out mechanisms more or less remain the same. We suggest that online merchants should implement better fraud detection systems to tackle CNP fraud [62, 103]. Some ways towards this could include understanding abnormal refund patterns and multiple small-value transactions [18, 113].

5.5 Experiments to study cybercrime help in seeding data for future cybercrime research

The unavailability of data is an issue that often makes it challenging to study cybercrime [51, 77, 88, 95]. Our study indicates how controlled experiments can be used not only to study one fraudulent activity, but also to help seed honeypot infrastructure that passively collects further data to study other cybercriminal activities. For example, the phishing webpage shown in Fig. 4 requests the victims to provide personal details, including contact information that criminals use to re-target the victims. We observe in Section 4.3 that criminals send smishing texts to the mobile numbers we provide in the phishing page. While this is done to re-victimize the users, it creates an opportunity to establish effective global telephony honeypots. This could allow researchers to collect data on scam texts and calls - another cybercrime that lacks updated real-world datasets.

Building datasets using effective honeypots could significantly contribute to the community [47, 48]. This would not only help researchers but also enable stakeholders, such as mobile network operators, to keep up-to-date with scam trends. It could also help to identify malware that is spread using SMS [45] and stop threats from affecting their users. While previous work on developing telephony honeypots is a good start [14, 48], our method contributes by suggesting a more effective seeding approach. However, such methodologies require careful ethical considerations before deployment. This is particularly important for early researchers in this space, where data providers are extremely hesitant to share with academics. Bad examples for data sharing privacy violations could limit progress for all researchers.

6 Conclusion

We present a new experimental proof-of-concept study that enables us to empirically study card-not-present (CNP) fraud transactions. While previous work has devised machine learning models to detect fraudulent transactions, our work provides a new method that enables researchers to understand scammers' transaction behavior patterns in this continuously evolving cybercrime.

We contribute broadly to the literature studying card-not-found fraud as well as profits of cybercrime. Often, work analyzing credit card reselling focuses on underground markets. This is frequently under the assumption that these cards are taken from data breaches. It is hard to know transparently where the cards are from. We propose a method to be able to detect when cards are coming from delivery scams and other smishing attacks. We hope our work will help bridge the gap between underground markets and cybercrime that happens before goods/services are sold.

Acknowledgments

We want to thank Stop Scams UK and Paymentology for supporting this project. Many thanks for the anonymous reviewers as well as the shepherd for their feedback on this paper.

References

[1] Youness Abakarim, Mohamed Lahby, and Abdelbaki Attioui. 2018. An Efficient Real Time Model For Credit Card Fraud Detection Based On Deep Learning. In *12th International Conference on Intelligent Systems: Theories and Applications* (Rabat, Morocco) *(SITA'18)*. Association for Computing Machinery, New York, NY, USA, Article 30, 7 pages. doi:10.1145/3289402.3289530

[2] Bhupendra Acharya, Dario Lazzaro, Antonio Emanuele Cinà, and Thorsten Holz. 2025. Pirates of Charity: Exploring Donation-based Abuses in Social Media Platforms. In *The Web Conference 2025 (WWW '25)*. Association for Computing Machinery, New York, NY, USA, 3968–3981.

[3] Bhupendra Acharya, Muhammad Saad, Antonio Emanuele Cinà, Lea Schönherr, Hoang Dai Nguyen, Adam Oest, Phani Vadrevu, and Thorsten Holz. 2024. Conning the Crypto Conman: End-to-End Analysis of Cryptocurrency-based Technical Support Scams. In *IEEE Symposium on Security and Privacy*. IEEE Computer Society, Los Alamitos, CA, USA, 17–35.

[4] Sharad Agarwal, Emma Harvey, Enrico Mariconti, Guillermo Suarez-Tangil, and Marie Vasek. 2025. 'Hi Mum, my phone went down the toilet': Investigating Hi Mum and Dad SMS Scams in the UK. In *34th USENIX Security Symposium (USENIX Security 25)*. USENIX Association, Berkeley, CA, USA.

[5] Sharad Agarwal, Emma Harvey, and Marie Vasek. 2024. Poster: A Comprehensive Categorization of SMS Scams. In *Internet Measurement Conference (IMC '24)*. Association for Computing Machinery, New York, NY, USA, 755–756.

[6] John Akhilomen. 2013. Data Mining Application for Cyber Credit-Card Fraud Detection System. In *Advances in Data Mining. Applications and Theoretical Aspects*, Petra Perner (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 218–228.

[7] Yara Alghofaili, Albatul Albattah, and Murad A Rassam. 2020. A financial fraud detection model based on LSTM deep learning technique. *Journal of Applied Security Research* 15, 4 (2020), 498–516.

[8] Maxwell Aliapoulios, Cameron Ballard, Rasika Bhalerao, Tobias Lauinger, and Damon McCoy. 2021. Swiped: Analyzing Ground-truth Data of a Marketplace for Stolen Debit and Credit Cards. In *30th USENIX Security Symposium (USENIX Security 21)*. USENIX Association, Berkeley, CA, USA, 4151–4168.

[9] Mohamed Alsharnouby, Furkan Alaca, and Sonia Chiasson. 2015. Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies* 82 (2015), 69–82.

[10] Icy Fresno Anabo, Iciar Elexpuru-Albizuri, and Lourdes Villardón-Gallego. 2019. Revisiting the Belmont Report's ethical principles in internet-mediated research: Perspectives from disciplinary associations in the social sciences. *Ethics and Information Technology* 21, 2 (2019), 137–149.

[11] Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Carlos Gañán, Tom Grasso, Michael Levi, Tyler Moore, and Marie Vasek. 2019. Measuring the Changing Cost of Cybercrime. *The 18th Annual Workshop on the Economics of Information Security (WEIS 2019)* (2019).

[12] Sara Aniello and Stefano Caneppele. 2018. Selling stolen goods on the online markets: An explorative study. *Global Crime* 19, 1 (2018), 42–62.

[13] Raja Hasnain Anwar, Syed Rafiul Hussain, and Muhammad Taqi Raza. 2024. In Wallet We Trust: Bypassing the Digital Wallets Payment Security for Free Shopping. In *33rd USENIX Security Symposium (USENIX Security 24)*. USENIX Association, Berkeley, CA, USA, 541–558.

[14] Marco Balduzzi, Payas Gupta, Lion Gu, Debin Gao, and Mustaque Ahamad. 2016. Mobipot: Understanding mobile telephony threats with honeycards. In *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*. Association for Computing Machinery, New York, NY, USA, 723–734.

[15] Better Business Bureau (BBB). 2025. BBB Scam Alert: Don't click on that text! 5 ways to avoid delivery scams. https://www.bbb.org/article/scams/16460-scam-alert-fake-text-delivery-scam.

[16] Tej Paul Bhatla, Vikram Prabhu, Amit Dua, et al. 2003. Understanding credit card frauds. *Cards business review* 1, 6 (2003), 1–15.

[17] Marzieh Bitaab, Haehyun Cho, Adam Oest, Penghui Zhang, Zhibo Sun, Rana Pourmohamad, Doowon Kim, Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili, et al. 2020. Scam pandemic: How attackers exploit public fear through phishing. In *2020 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, Boston, MA, USA, 1–10.

[18] Amanda Bodker, Phil Connolly, Oliver Sing, Benjamin Hutchins, Michael Townsley, and Jacqueline Drew. 2022. Card-not-present fraud: Using crime scripts to inform crime prevention initiatives. *Security Journal* 36 (2022), 693–711.

[19] Bernardo Branco, Pedro Abreu, Ana Sofia Gomes, Mariana SC Almeida, João Tiago Ascensão, and Pedro Bizarro. 2020. Interleaved sequence RNNs for fraud detection. In *Proceedings of the 26th ACM SIGKDD international conference on knowledge discovery & data mining*. Association for Computing Machinery, New York, NY, USA, 3101–3109.

[20] Mark Button, Chris Lewis, and Jacki Tapley. 2014. Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal* 27, 1 (2014), 36–54.

[21] Michele Campobasso and Luca Allodi. 2022. THREAT/crawl: a Trainable, Highly-Reusable, and Extensible Automated Method and Tool to Crawl Criminal Underground Forums. In *2022 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, Boston, MA, USA, 1–13.

[22] Fabrizio Carcillo, Andrea Dal Pozzolo, Yann-Aël Le Borgne, Olivier Caelen, Yannis Mazzer, and Gianluca Bontempi. 2018. Scarff: a scalable framework for streaming credit card fraud detection with spark. *Information Fusion* 41 (2018), 182–194.

[23] Fabrizio Carcillo, Yann-Aël Le Borgne, Olivier Caelen, and Gianluca Bontempi. 2018. Streaming active learning strategies for real-life credit card fraud detection: assessment and visualization. *International Journal of Data Science and Analytics* 5 (2018), 285–300.

[24] Fabrizio Carcillo, Yann-Aël Le Borgne, Olivier Caelen, Yacine Kessaci, Frédéric Oblé, and Gianluca Bontempi. 2021. Combining unsupervised and supervised learning in credit card fraud detection. *Information sciences* 557 (2021), 317–331.

[25] Asma Cherif, Arwa Badhib, Heyfa Ammar, Suhair Alshehri, Manal Kalkatawi, and Abdessamad Imine. 2023. Credit card fraud detection in the era of disruptive technologies: A systematic review. *Journal of King Saud University - Computer and Information Sciences* 35, 1 (2023), 145–174.

[26] CIFAS. 2023. £7.5 billion stolen as 1 in 10 Britons fall victim to scams in 12 months. https://www.cifas.org.uk/newsroom/stateofscams.

[27] Andrea Dal Pozzolo, Giacomo Boracchi, Olivier Caelen, Cesare Alippi, and Gianluca Bontempi. 2017. Credit card fraud detection: a realistic modeling and a novel learning strategy. *IEEE Transactions on Neural Networks and Learning Systems* 29, 8 (2017), 3784–3797.

[28] Andrea Dal Pozzolo, Olivier Caelen, Reid A Johnson, and Gianluca Bontempi. 2015. Calibrating probability with undersampling for unbalanced classification. In *2015 IEEE Symposium Series on Computational Intelligence*. IEEE, 159–166.

[29] Andrea Dal Pozzolo, Olivier Caelen, Yann-Ael Le Borgne, Serge Waterschoot, and Gianluca Bontempi. 2014. Learned lessons in credit card fraud detection from a practitioner perspective. *Expert Systems with Applications* 41, 10 (2014), 4915–4928.

[30] Partha Das Chowdhury, Karen Renaud, and Awais Rashid. 2024. When Data Breaches Happen, Where Does the Buck Stop?... and where should it stop?. In *Proceedings of the New Security Paradigms Workshop (NSPW '24)*. Association for Computing Machinery, New York, NY, USA, 106–125.

[31] Harry Deng. 2023. Exploring Synthetic Data for Artificial Intelligence and Autonomous Systems: A Primer. https://unidir.org/wp-content/uploads/2023/11/UNIDIR_Exploring_Synthetic_Data_for_Artificial_Intelligence_and_Autonomous_Systems_A_Primer.pdf.

[32] Rachna Dhamija, J Doug Tygar, and Marti Hearst. 2006. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*. Association for Computing Machinery, New York, NY, USA, 581–590.

[33] Zainul Abi Din, Hari Venugopalan, Jaime Park, Andy Li, Weisu Yin, HaoHui Mai, Yong Jae Lee, Steven Liu, and Samuel T. King. 2020. Boxer: Preventing fraud by scanning credit cards. In *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Berkeley, CA, USA, 1571–1588.

[34] David Dittrich and Erin Kenneally. 2012. *The Menlo Report: Ethical principles guiding information and communication technology research.* Technical Report. US Department of Homeland Security.

[35] Vaishnavi Nath Dornadula and Sa Geetha. 2019. Credit card fraud detection using machine learning algorithms. *Procedia computer science* 165 (2019), 631–641.

[36] European Banking Authority. 2024. 2024 Report On Payment Fraud. https://www.ecb.europa.eu/press/intro/publications/pdf/ecb.ebaecb202408.en.pdf.

[37] Europol. 2025. European Union Serious and Organised Crime Threat Assessment - The changing DNA of serious and organised crime. https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

[38] Harry Everett. 2024. Out of the shadows – 'darcula' iMessage and RCS smishing attacks target USPS and global postal services. https://www.netcraft.com/blog/darcula-smishing-attacks-target-usps-and-global-postal-services/.

[39] Kasra Farhadpour. 2023. Cybercriminals continue to target UK mobile users with smishing attempts.... https://www.proofpoint.com/uk/blog/email-and-cloud-threats/cybercriminals-continue-target-uk-mobile-users-smishing-attempts.

[40] Federal Trade Commission (FTC). 2025. New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024. https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.

[41] Financial Conduct Authority (FCA). 2021. Changes to the SCA-RTS and to the guidance in 'Payment Services and Electronic Money – Our Approach' and the Perimeter Guidance Manual. https://www.fca.org.uk/publication/policy/ps21-19.pdf.

[42] Ivan Flechais, Jens Riegelsberger, and M. Angela Sasse. 2005. Divide and conquer: the role of trust and assurance in the design of secure socio-technical systems. In *Proceedings of the 2005 Workshop on New Security Paradigms (NSPW '05)*. Association for Computing Machinery, New York, NY, USA, 33–41.

[43] Harry Freeborough. 2025. The Bleeding Edge of Phishing: darcula-suite 3.0 Enables DIY Phishing of Any Brand. https://www.netcraft.com/blog/darcula-v3-phishing-kits-targeting-any-brand/.

[44] Andrea Gadotti, Luc Rocher, Florimond Houssiau, Ana-Maria Creţu, and Yves-Alexandre de Montjoye. 2024. Anonymization: The imperfect science of using data while preserving privacy. *Science Advances* 10, 29 (2024), eadn7053.

[45] Artur Geers, Aaron Ding, Carlos Hernandez Gañán, and Simon Parkin. 2023. Lessons in Prevention and Cure: A User Study of Recovery from Flubot Smartphone Malware. In *Proceedings of the 2023 European Symposium on Usable Security (EuroUSEC '23)*. Association for Computing Machinery, New York, NY, USA, 126–142.

[46] Global Anti-Scam Alliance (GASA). 2024. The State of Scams in the United Kingdom 2024. https://www.gasa.org/_files/ugd/7bdaac_bc34e713c6434551a9c8f25207e1be9d.pdf.

[47] Payas Gupta, Mustaque Ahamad, Jonathan Curtis, Vijay Balasubramaniyan, and Alex Bobotek. 2014. *M3AAWG Telephony Honeypots: Benefits and Deployment Options.* Technical Report. Technical report.

[48] Payas Gupta, Bharat Srinivasan, Vijay Balasubramaniyan, and Mustaque Ahamad. 2015. Phoneypot: Data-driven understanding of telephony threats.. In *NDSS*, Vol. 107. NDSS, 108.

[49] Shuang Hao, Kevin Borgolte, Nick Nikiforakis, Gianluca Stringhini, Manuel Egele, Michael Eubanks, Brian Krebs, and Giovanni Vigna. 2015. Drops for stuff: An analysis of reshipping mule scams. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. Association for Computing Machinery, New York, NY, USA, 1081–1092.

[50] Andreas Haslebacher, Jeremiah Onaolapo, and Gianluca Stringhini. 2017. All your cards are belong to us: Understanding online carding forums. In *2017 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, Scottsdale, AZ, USA, 41–51.

[51] Thomas J Holt and Adam M Bossler. 2014. An assessment of the current state of cybercrime scholarship. *Deviant behavior* 35, 1 (2014), 20–40.

[52] Christian Homburg, Nicole Koschate, and Wayne D Hoyer. 2005. Do satisfied customers really pay more? A study of the relationship between customer satisfaction and willingness to pay. *Journal of marketing* 69, 2 (2005), 84–96.

[53] Alice Hutchings and Thomas J. Holt. 2014. A Crime Script Analysis of the Online Stolen Data Market. *The British Journal of Criminology* 55, 3 (12 2014), 596–614.

[54] Alice Hutchings, Sergio Pastrana, and Richard Clayton. 2019. Displacing big data: How criminals cheat the system. *The Human Factor of Cybercrime* (2019), 408–424.

[55] ISO 8583:2023(E). 2023. Financial-transaction-card-originated messages — Interchange message specifications. https://www.iso.org/standard/79451.html

[56] Ankit Kumar Jain and BB Gupta. 2018. Rule-based framework for detection of smishing messages in mobile environment. *Procedia Computer Science* 125 (2018), 617–623.

[57] Markus Jakobsson, Alex Tsow, Ankur Shah, Eli Blevis, and Youn-Kyung Lim. 2007. What Instills Trust? A Qualitative Study of Phishing. In *Financial Cryptography and Data Security*. Springer-Verlag, Berlin, Heidelberg, 356–361.

[58] Jae Woong Joo, Seo Yeon Moon, Saurabh Singh, and Jong Hyuk Park. 2017. S-Detector: an enhanced security model for detecting Smishing attack for mobile computing. *Telecommunication Systems* 66 (2017), 29–38.

[59] Kaggle. 2018. Credit Card Fraud Detection. https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud.

[60] Kent R Kerley and Heith Copes. 2002. Personal fraud victims and their official responses to victimization. *Journal of Police and Criminal Psychology* 17, 1 (2002), 19–35.

[61] Alex Kigerl. 2022. Behind the scenes of the underworld: hierarchical clustering of two leaked carding forum databases. *Social Science Computer Review* 40, 3 (2022), 618–640.

[62] Tobias Knuth and Dennis C Ahrholdt. 2022. Consumer fraud in online shopping: Detecting risk indicators through data mining. *International Journal of Electronic Commerce* 26, 3 (2022), 388–411.

[63] Brian Krebs. 2025. How Phished Data Turns into Apple & Google Wallets. https://krebsonsecurity.com/2025/02/how-phished-data-turns-into-apple-google-wallets/.

[64] Ponnurangam Kumaraguru, Alessandro Acquisti, and Lorrie Faith Cranor. 2006. Trust modelling for online transactions: a phishing scenario. In *Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services* (Markham, Ontario, Canada) *(PST '06)*. Association for Computing Machinery, New York, NY, USA, Article 11, 9 pages.

[65] Stefan Laube and Rainer Böhme. 2017. Strategic Aspects of Cyber Risk Information Sharing. *ACM Comput. Surv.* 50, 5, Article 77 (Nov. 2017), 36 pages.

[66] Bertrand Lebichot, Yann-Aël Le Borgne, Liyun He-Guelton, Frederic Oblé, and Gianluca Bontempi. 2020. Deep-learning domain adaptation techniques for credit cards fraud detection. In *Recent Advances in Big Data and Deep Learning*. Springer International Publishing, Cham, 78–88.

[67] Bertrand Lebichot, Gian Marco Paldino, Wissam Siblini, Liyun He-Guelton, Frédéric Oblé, and Gianluca Bontempi. 2021. Incremental learning strategies for credit cards fraud detection. *International Journal of Data Science and Analytics* 12, 2 (2021), 165–174.

[68] Joakim Loxdal, Måns Andersson, Simon Hacks, and Robert Lagerström. 2021. Why phishing works on smartphones: A preliminary study. In *54th Annual Hawaii International Conference on System Sciences, HICSS 2021*. ScholarSpace, 7173–7182.

[69] Mohammad Mannan and P. C. van Oorschot. 2008. Localization of credential information to address increasingly inevitable data breaches. In *Proceedings of the 2008 New Security Paradigms Workshop (NSPW '08)*. Association for Computing Machinery, New York, NY, USA, 13–21.

[70] Daniel Brannock Marguerite DeLiema, Lynn Langton and Edward Preble. 2024. Fraud victimization across the lifespan: evidence on repeat victimization using perpetrator data. *Journal of Elder Abuse & Neglect* 36, 3 (2024), 227–250.

[71] Mavenir. 2024. SpamShield MESSAGING FRAUD. https://www.mavenir.com/portfolio/mavapps/fraud-security/spamshield-messaging-fraud/.

[72] Igor Mekterović, Mladen Karan, Damir Pintar, and Ljiljana Brkić. 2021. Credit card fraud detection in card-not-present transactions: Where to invest? *Applied Sciences* 11, 15 (2021), 6766.

[73] Vickie A Miracle. 2016. The Belmont Report: The triple crown of research ethics. *Dimensions of critical care nursing* 35, 4 (2016), 223–228.

[74] Sandhya Mishra and Devpriya Soni. 2020. Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis. *Future Generation Computer Systems* 108 (2020), 803–815.

[75] Sandhya Mishra and Devpriya Soni. 2023. DSmishSMS–A system to detect smishing SMS. *Neural Computing and Applications* 35, 7 (2023), 1–18.

[76] Krishna Modi and Reshma Dayma. 2017. Review on fraud detection methods in credit card transactions. In *2017 International Conference on Intelligent Computing and Control (I2C2)*. Coimbatore, India, 1–5.

[77] Tyler Moore and Richard Clayton. 2008. The consequence of non-cooperation in the fight against phishing. In *2008 eCrime Researchers Summit*. IEEE, Atlanta, GA, USA, 1–14.

[78] Marti Motoyama, Damon McCoy, Kirill Levchenko, Stefan Savage, and Geoffrey M. Voelker. 2011. An analysis of underground forums. In *Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement Conference (IMC '11)*. Association for Computing Machinery, New York, NY, USA, 71–80.

[79] Aleksandr Nahapetyan, Sathvik Prasad, Kevin Childs, Adam Oest, Yeganeh Ladwig, Alexandros Kapravelos, and Brad Reaves. 2024. On SMS Phishing Tactics and Infrastructure. In *IEEE Symposium on Security and Privacy*. IEEE, San Francisco, CA, USA, 169–169.

[80] Kate Nalepinski. 2025. Warning Issued for USPS Scam Text: What to Look Out For. https://www.newsweek.com/usps-scam-text-warning-package-delivery-post-fraud-2040890.

[81] Arvind Narayanan and Vitaly Shmatikov. 2008. Robust De-anonymization of Large Sparse Datasets. In *2008 IEEE Symposium on Security and Privacy*. 111–125.

[82] National Crime Agency (NCA). 2024. Fraud remains the most common crime type experienced by victims in England and Wales. https://www.nationalcrimeagency.gov.uk/threats/nsa-fraud-2024.

[83] NCA. 2025. Operation Henhouse: 433 arrests and £7.5m seized in national crackdown on fraud. https://www.nationalcrimeagency.gov.uk/news/operation-henhouse-422-arrests-and-7-5m-seized-in-national-crackdown-on-fraud.

[84] Nate Nelson. 2025. 'Lucid' Phishing-as-a-Service Exploits Faults in iMessage, Android RCS. https://www.darkreading.com/threat-intelligence/lucid-phishing-exploits-imessage-android-rcs.

[85] Ofcom. 2021. 45 million people targeted by scam calls and texts this summer. https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/45-million-people-targeted-by-scams/.

[86] Ofcom. 2024. Tackling scam calls and texts. https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/tackling-scam-calls-and-texts/.

[87] ONS. 2022. Crime in England and Wales: Appendix tables. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesappendixtables.

[88] Sergio Pastrana, Daniel R. Thomas, Alice Hutchings, and Richard Clayton. 2018. CrimeBB: Enabling Cybercrime Research on Underground Forums at Scale. In *Proceedings of the 2018 World Wide Web Conference (WWW '18)*. International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 1845–1854.

[89] Payment Systems Regulator (PSR). 2025. Card payments. https://www.psr.org.uk/our-work/card-payments/.

[90] Timothy Peacock and Allan Friedman. 2010. Automation and disruption in stolen payment card markets. *Criminal Justice Studies* 23, 1 (2010), 33–50.

[91] Kimberly Kiefer Peretti. 2008. Data breaches: What the underground world of "carding" reveals. *Santa Clara Computer & High Tech. LJ* 25 (2008), 375.

[92] Utkarsh Porwal and Smruthi Mukund. 2019. Credit Card Fraud Detection in E-Commerce. In *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, Rotorua, New Zealand, 280–287.

[93] Subramanian Rangan and Ron Adner. 2001. Profits and the Internet: Seven misconceptions. *MIT Sloan Management Review* (2001).

[94] Abdul Razaque, Mohamed Ben Haj Frej, Gulnara Bektemyssova, Fathi Amsaad, Muder Almiani, Aziz Alotaibi, NZ Jhanjhi, Saule Amanzholova, and Majid Alshammari. 2022. Credit card-not-present fraud detection and prevention using big data analytics algorithms. *Applied Sciences* 13, 1 (2022), 57.

[95] Markus Riek and Rainer Böhme. 2018. The costs of consumer-facing cybercrime: An empirical exploration of measurement issues and estimates. *Journal of Cybersecurity* 4, 1 (2018), tyy004.

[96] Sayak Saha Roy, Poojitha Thota, Krishna Vamsi Naragam, and Shirin Nilizadeh. 2024. From chatbots to phishbots?: Phishing scam generation in commercial large language models. In *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, USA, 36–54.

[97] Sayak Saha Roy, Elham Pourabbas Vafa, Kobra Khanmohammadi, and Shirin Nilizadeh. 2025. DarkGram: Exploring and Mitigating Cybercriminal content shared in Telegram channels. In *34th USENIX Security Symposium (USENIX Security 25)*. USENIX Association, Berkeley, CA, USA.

[98] Irina Sakharova. 2012. Payment card fraud: Challenges and solutions. In *2012 IEEE International Conference on Intelligence and Security Informatics*. IEEE, Washington, DC, USA, 227–234.

[99] Amichai Shulman. 2010. The underground credentials market. *Computer Fraud & Security* 2010, 3 (2010), 5–8.

[100] Abe Singer and Matt Bishop. 2021. Trust-Based Security; Or, Trust Considered Harmful. In *Proceedings of the New Security Paradigms Workshop 2020 (NSPW '20)*. Association for Computing Machinery, New York, NY, USA, 76–89.

[101] Gunikhan Sonowal and KS Kuppusamy. 2018. SmiDCA: an anti-smishing model with machine learning approach. *Comput. J.* 61, 8 (2018), 1143–1157.

[102] Kyle Soska and Nicolas Christin. 2015. Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In *24th USENIX security symposium (USENIX security 15)*. USENIX Association, Berkeley, CA, USA, 33–48.

[103] Stripe. 2023. Carding and how businesses can prevent it. https://stripe.com/in/resources/more/what-is-carding-how-this-type-of-fraud-works-and-how-businesses-can-prevent-it#how-businesses-can-protect-themselves-against-carding.

[104] Sarah Tabassum, Cori Faklaris, and Heather Richter Lipford. 2024. What Drives SMiShing Susceptibility? A U.S. Interview Study of How and Why Mobile Phone Users Judge Text Messages to be Real or Fake. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. USENIX Association, Berkeley, CA, USA, 393–411.

[105] Alain Claude Tambe Ebot, Mikko Siponen, and Volkan Topalli. 2024. Towards a cybercontextual transmission model for online scamming. *European Journal of Information Systems* 33, 4 (2024), 571–596.

[106] Bhaskar Tejaswi, Nayanamana Samarasinghe, Sajjad Pourali, Mohammad Mannan, and Amr Youssef. 2022. Leaky Kits: The Increased Risk of Data Exposure from Phishing Kits. In *2022 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE, Boston, MA, USA, 1–13.

[107] Anuruddha Thennakoon, Chee Bhagyani, Sasitha Premadasa, Shalitha Mihiranga, and Nuwan Kuruwitaarachchi. 2019. Real-time Credit Card Fraud Detection Using Machine Learning. In *2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. IEEE, Noida, India, 488–493.

[108] Kurt Thomas, Damon McCoy, Chris Grier, Alek Kolcz, and Vern Paxson. 2013. Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse. In *22nd USENIX Security Symposium (USENIX Security 13)*. USENIX Association, Berkeley, CA, USA, 195–210.

[109] Daniel Timko and Muhammad Lutfor Rahman. 2024. Smishing Dataset I: Phishing SMS Dataset from Smishtank.com. In *ACM Conference on Data and Application Security and Privacy (CODASPY '24)*. Association for Computing Machinery, New York, NY, USA, 289–294.

[110] Dmitrij Titarenko. 2025. ISO 8583: The Essential Standard For Credit Card Transactions. https://dashdevs.com/blog/iso-8583/.

[111] Bill Toulas. 2022. Revolut hack exposes data of 50,000 users, fuels new phishing wave. https://www.bleepingcomputer.com/news/security/revolut-hack-exposes-data-of-50-000-users-fuels-new-phishing-wave/.

[112] Bill Toulas. 2025. Carding tool abusing WooCommerce API downloaded 34K times on PyPI. https://www.bleepingcomputer.com/news/security/carding-tool-abusing-woocommerce-api-downloaded-34k-times-on-pypi/.

[113] Michael Townsley and Benjamin Hutchins. 2021. Loss prevention in a time of accelerated change: How can loss prevention future-proof the businesses they protect. In *Griffith Criminology Institute/Profit Protection Future Forum*.

[114] UK Finance. 2024. Half Year Fraud Report. https://www.ukfinance.org.uk/system/files/2024-10/HalfYearFraudReport2024.pdf.

[115] UK Home Office. 2025. Experiences of victims of fraud and cyber crime. https://www.gov.uk/government/publications/experiences-of-victims-of-fraud-and-cyber-crime/experiences-of-victims-of-fraud-and-cyber-crime.

[116] Gert Jan van Hardeveld, Craig Webber, and Kieron O'Hara. 2016. Discovering credit card fraud methods in online tutorials. In *Proceedings of the 1st International Workshop on Online Safety, Trust and Fraud Prevention (OnSt '16)*. Association for Computing Machinery, New York, NY, USA, Article 1, 5 pages.

[117] Rolf van Wegberg, Samaneh Tajalizadehkhoob, Kyle Soska, Ugur Akyazi, Carlos Hernandez Ganan, Bram Klievink, Nicolas Christin, and Michel van Eeten. 2018. Plug and Prey? Measuring the Commoditization of Cybercrime via Online Anonymous Markets. In *27th USENIX Security Symposium (USENIX Security 18)*. USENIX Association, Baltimore, MD, 1009–1026.

[118] VISA. 2019. Strong Customer Authentication. https://www.visa.co.uk/partner-with-us/payment-technology/strong-customer-authentication.html.

[119] VISA. 2020. PSD2 SCA Regulatory Guide. https://www.visa.co.uk/dam/VCOM/regional/ve/unitedkingdom/PDF/sca/visa-psd2-sca-regulatory-guide-v1-december-2020.pdf.

[120] Richard Wood. 2024. Almost three-quarters of Australians targeted by package and delivery scams. https://www.9news.com.au/national/delivery-scams-in-australia-the-most-popular-swindle/480235f1-8ddc-42c3-8dc3-a09100412aa8.

[121] Michael Yip, Nigel Shadbolt, and Craig Webber. 2013. Why forums? an empirical analysis into the facilitating factors of carding forums. In *Proceedings of the 5th Annual ACM Web Science Conference (WebSci '13)*. Association for Computing Machinery, New York, NY, USA, 453–462.

[122] Sha Zhang, Koen Pauwels, and Chenming Peng. 2019. The impact of adding online-to-offline service platform channels on firms' offline and total sales and profits. *Journal of Interactive Marketing* 47, 1 (2019), 115–128.

[123] Zhaohui Zhang, Ligong Chen, Qiuwen Liu, and Pengwei Wang. 2020. A fraud detection method for low-frequency transaction. *IEEE Access* 8 (2020), 25210–25220.

[124] Sarah Zheng and Ingolf Becker. 2022. Presenting Suspicious Details in User-Facing E-mail Headers Does Not Improve Phishing Detection. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. USENIX Association, Berkeley, CA, USA, 253–271.