Tap, Pay, and Worry: Users' Perceptions of Contactless Payment Attacks versus Technical Feasibility

Mahshid Mehr Nezhad*, Maryam Mehrnezhad†, Timur Yunusov‡, Feng Hao§
*Secure Cyber Systems Research Group (SCSRG), WMG, University of Warwick, UK
†Information Security Department, Royal Holloway University of London, UK
‡Payment Village, UK
§Department of Computer Science, University of Warwick, UK

Abstract—**Contactless payment is one of the most popular payment methods, accessible through contactless cards, mobile phones, and wearable devices. However, there are several vulnerabilities associated with this payment method, leading to various attacks. While the technical aspects of these attacks have been extensively studied in the literature, the user perspective remains relatively under-explored. In this paper, we study users' perceptions about contactless payment attacks and vulnerabilities. We assess the technical feasibility of the existing attacks on contactless payment systems, and present a user survey involving 150 participants from the UK, examining their perceptions of contactless payment systems and attacks. We compare users' perceptions with our evaluation of the technical feasibility of contactless payment attacks and find that while users accurately interpret some attacks, they tend to overestimate certain attacks while underestimating others. Additionally, we find that despite available protective measures, users typically take only basic precautions. This highlights a gap between user perceptions and the technical feasibility of contactless payment attacks. We recommend improving contactless payment security and providing targeted user education.**

1. Introduction

Contactless payments have become increasingly prevalent in the UK, with 38% of all transactions utilizing contactless methods in 2023, with 85% of people now using this payment method on a regular basis [52]. This can be attributed to several factors, including the raised contactless payment limit to £100 in the UK, improved accessibility via acceptance devices, including credit and debit cards, smartphones with digital wallets (e.g., Apple Pay [3], Google Pay [22], Samsung Pay [44]), and wearable technology (e.g., smart watches), and growing consumer comfort and familiarity with this payment method. Despite these advantages, contactless payment systems are not immune to attacks. Previous research has identified various vulnerabilities within contactless payment systems, posing risks to overall security. While the technical aspects of contactless payment systems have been thoroughly researched, the perspective of the end user, those who ultimately utilize these systems remains relatively under-explored. This paper aims to explore this pivotal aspect of the contactless payment ecosystem by studying user behaviours, perceptions, and experiences.

In this paper, we employ six attack categories on contactless payment systems, including eavesdropping [14], [25], relay [8], [9], [11], [18], [24], [29], [31], [53], preplay [17], [20], [43], counterfeit card replica [17], [19], [38], contactless limit bypass [5]–[7], [20] and lock screen bypass [41], [50], [58], affecting the end user, to study the users' perspective on contactless payment attacks. To this end, we first evaluate the technical feasibility of these proposed attacks. Second, we study users' familiarity and adaptation to contactless payment systems, their concerns and perceptions of the feasibility of these attacks, as well as the protective actions they adopt to protect against such attacks. We then compare the users' perceived feasibility and concern regarding these attacks with our technical feasibility evaluation of attacks. Ultimately, this could strengthen the security of contactless payment systems. Essentially, this paper is structured around the following research questions:

- RQ1: What is the technical feasibility of contactless payment systems attacks?
- RQ2: What are the users' perceptions and understandings of these attacks?
- RQ3: How well do users' perceptions align with the technical feasibility of these attacks?

To address RQ1, using the mentioned six attack categories, we assess the technical feasibility of each of these categories based on our defined factors specified in Section 3.3. In response to RQ2, we conducted a user study with 150 participants, exploring user adoption patterns for contactless payment systems, their awareness of diverse attack types, their concerns and perceptions regarding the feasibility of these attacks, and the protective actions they deploy against such threats. Findings from this user study are showcased and analyzed in Section 5. For RQ3, we compare the users' perceptions and concerns about contactless payment attacks with our evaluation of the attacks' technical feasibility, further detailed in Section 6.1.

Our results show that users widely adopt contactless payment; meanwhile, they show varying levels of concern towards different attacks. While users have high concern levels for some attacks, they are less concerned about others. Users' concern level generally matches their perceptions of an attack's feasibility, with a few exceptions where, despite considering some attacks as less feasible, they still showed serious concern about them. This sug-

TABLE 1. Summary of Related Work.

Study	Year	Focus	Region	Participants	Methodology
Ismail et al. [27]	2022	Impact of COVID-19 on the perceived risk in contactless payment adoption	Malaysia	3	In-person Interview, Observation
Shishah & Alhelaly [46]	2021	Importance of health safety and hygiene in adopting contactless payments during COVID-19	Saudi Arabia	597	Online Survey
Vatsa & Agarwal [55]	2022	Role of perceived risk and usefulness in mobile payment adoption post-COVID-19	India	217	Online Survey
Lee & Pan [30]	2023	Factors affecting ongoing FRP use after COVID-19	China	321	Online Survey
Hillman et al. [26]	2014	User behaviours, motivations, and challenges with mobile payment systems	North America	21	In-person Interviews, Diary Entries
Dev et al. [10]	2024	Impact of UPI on spending behavior and financial practices	India	235 Surveys, 20 Interviews	Online Surveys, In-person Semi-structured Interviews
Mainwaring et al. [33]	2008	Impact of cultural and social factors in the adoption of FeliCa-based digital money systems	Japan	Not Specified	In-person Interviews, Observations
Lewis & Perry [32]	2019	Everyday spending behaviours and experiences with contactless payments	UK	12	Diaries Analysis, In-person Semi-structured Interviews
Pritchard et al. [39]	2015	Impact of cashless fares in the Transport for London (TFL) system	UK	20	In-person Interviews, Ethnographic Fieldwork, and Online Comment Analysis
Vines et al. [56]	2012	Banking experiences and perceptions of older adults regarding traditional payment methods	UK	23	In-person Interviews, Group Discussions
Aldag et al. [1]	2020	Risk perception of contactless debit cards	UK	56	Online Survey
This Study	**2024**	**Studying users' perceptions of contactless payment attacks and their technical feasibility**	**UK**	**150**	**Online Surveys**

gests complexity in user perception and attitude. Despite these concerns, our results show that users typically take few protective actions, although multiple protective actions are available to adopt. In order to close these gaps, we advocate better standardization and enforcement of contactless payment systems to improve their vulnerabilities, as well as user education and awareness.

The remainder of this paper is organized as follows: we review the related work in Sections 2. Section 3 provides an overview of contactless payment systems, attacks, and their technical feasibility. The methodology and results of our user study are presented in Sections 4 and 5, respectively. This is followed by our discussion in Section 6. Finally, we conclude the paper in Section 7.

2. Related Work

Several studies have explored this area. Table 1 summarizes a comparison between our study and related works. In terms of the adoption of contactless and mobile payment technologies during the COVID-19 pandemic, different studies have identified key factors influencing consumer behaviour. For instance, Ismail et al. [27] used in-person interviews and observations with a small sample of 3 participants in Malaysia to explore the impact of perceived risk on contactless payment adoption during the COVID-19 pandemic. Similarly, in Saudi Arabia, Shishah and Alhelaly [46] conducted a user study with 597 participants from Saudi Arabia, emphasizing the importance of health safety and hygiene considerations in adopting contactless payments during COVID-19. In India, Vatsa & Agarwal [55] surveyed 217 participants to investigate the roles of perceived trust and usefulness in mobile payment adoption after the pandemic. In China, Lee & Pan [30] examined the factors influencing the continuous usage intention of facial recognition payment (FRP) in the post-COVID-19 era. Their study, based on a survey of 321 users, found that attributes such as relative advantage, compatibility, user-interface attractiveness, and perceived security enhance the adoption of FRP. In addition to the pandemic-related studies, there have been research into the adoption of other means of contactless payments such as mobile payments, e-wallets, QR code, and facial recognition payments among consumers in different countries. Studies conducted in India [54], Pakistan [59], Malaysia [21], [37], and China [60] have examined factors such as perceived usefulness, perceived ease of use, and trust influencing consumer adoption of these technologies.

Further exploring the non-technical aspects of mobile payment systems; user behaviours, motivations, and challenges associated with mobile payment systems in North America were examined [26]. Their mixed-method approach, which included interviews and diary entries from 21 participants in the U.S. and Canada, provided a nuanced understanding of the factors driving mobile payment adoption in this region. This study, while insightful, is limited by its small sample size and the focus on non-technical aspects of mobile payment systems. In India, the impact of the Unified Payments Interface (UPI)[1], a smartphone-based platform launched by the National Payments Corporation of India, on spending behaviour among Indian users was examined [10]. The study, which used a mixed-methods approach involving 235 online survey responses and 20 semi-structured interviews, highlighted how UPI has transformed micro-level spending behaviours among diverse demographic groups. While the study provides valuable insights into the Indian context, it does not specifically discuss contactless payment systems and attacks. In Japan, the cultural and social factors influencing the adoption of digital money systems using Sony's FeliCa NFC technology were explored [33]. The study revealed that cultural concepts play a significant role in how users perceive and engage with digital money. While this research emphasizes the importance of designing payment systems that align with cultural norms and practices, it is limited by its focus on Sony's FeliCa system and does not address technical security attacks.

Despite global research, there is a notable gap in UK-focused studies on contactless payment systems, which have largely centred on everyday spending and specific contexts like public transport. Lewis & Perry [32] used diaries and interviews with 12 participants to explore

[1] https://www.npci.org.in/what-we-do/upi/product-overview

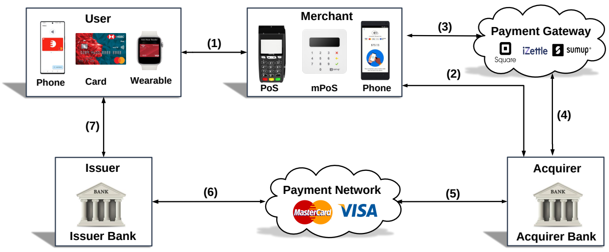

Figure 1. Contactless Payment System.

digital personal finance habits, while Pritchard et al. [39] examined cashless fare impacts on London bus drivers through mixed methods. Though insightful, these studies overlook technical attacks and broader security concerns. Vines et al. [56] explored older adults' banking experiences, highlighting trust in traditional payment methods, but did not address digital or contactless security. Aldag et al. [1] investigated fraud risk perceptions in a survey of 56 participants, but focused narrowly on a single scenario—purse theft. These limitations highlight the need for broader, in-depth research into diverse technical attack scenarios and user security perceptions in the UK context.

Given the limited UK-specific research, this paper fills a critical gap by conducting a comprehensive user study on technical attacks targeting contactless payment systems. According to the UK Finance 2024 report [51], contactless payment fraud losses are notably increasing, reaching £41.5 million—representing a 19% increase compared to 2022 and marking the highest total since records began in 2014. While users typically understand and can respond to straightforward threats like card theft, technical attacks—such as relay, pre-play, and counterfeit card exploits—are more subtle and often go unnoticed. These sophisticated attacks exploit technological vulnerabilities and pose significant challenges for user awareness and education. Understanding user perceptions of these hidden risks is key to closing the gap between perceived and actual threats, thereby improving both security measures and educational efforts in the contactless payment ecosystem.

3. Contactless Payment Systems

3.1. Background

Fig. 1 illustrates how a contactless payment system works. In this system, the user is presented with various options for payment devices, including credit/debit cards, Near Field Communication (NFC)-enabled mobile phones, and NFC-enabled wearable devices like smartwatches. Similarly, the accepting terminal on the merchant side also offers a range of options, such as traditional Point of Sale (PoS) terminals, which are stationary devices commonly found in retail settings, mobile PoS (mPoS) terminals, which are similar to traditional PoS terminals but integrate a third-party payment gateway (e.g., Sumup [49], Square [48], iZettle [28]) to process transactions, and mobile phones offering tap-to-phone (T2P) technology which enables merchants to accept contactless transactions using NFC-enabled mobile phones as terminals without requiring external physical devices.

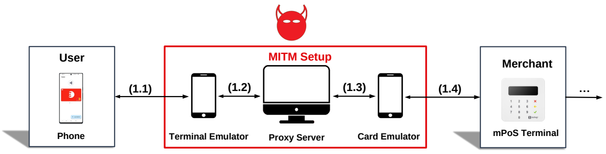

Figure 2. MITM Attack Setup.

As seen in Fig. 1, a contactless transaction is initiated by transmitting the transaction data between the payment device on the user side and the accepting terminal on the merchant side (1). Subsequently, the merchant analyzes the transaction, and depending on the setup, the transaction authorization may proceed directly to the acquirer bank (2) or be routed through a payment gateway (3) before reaching the acquirer bank (4) [42]. The acquirer bank communicates with the card association payment network, such as Visa [57] and Mastercard [34] to validate the transaction and verify fund availability (5) by connecting with the customer's issuing bank (6). Upon verification, the issuing bank sends an approval or decline response back to the payment network (6), which is then relayed to the acquirer bank (5). The acquirer bank subsequently notifies the merchant about the transaction outcome (4,3) or (2), and the merchant, in turn, informs the user's device (1). Upon receiving approval from the card issuer, the customer's account is charged, and the customer is notified accordingly (7).

However, the NFC communication channel (step 1 in Fig. 1) between the user and the merchant is the source of exploitation for attackers that leads to various attacks, as shown in Fig. 2. While this NFC communication is designed to work over a short range of a few centimetres, it can be extended over Bluetooth or the internet, thereby facilitating attacks beyond this limit. An attacker can use several devices to build up a Man-in-the-Middle (MITM) attack in such a compromised configuration, which allows them to intercept and alter transaction data for various attack purposes. In this scenario, rather than direct communication between the user and the merchant, the user interacts with a terminal emulator (1.1), while the merchant communicates with a card emulator (1.4). These emulators are connected and communicate through a proxy server (1.2 and 1.3) intermediating the transaction process [2]. In the following sections, we will discuss the categories of the attacks exploiting this setup, and evaluate their technical feasibility.

3.2. Contactless Payment Attacks

We study six distinct categories of attacks on contactless payment systems, including 1) eavesdropping, 2) relay, 3) pre-play, 4) counterfeit card replica, 5) contactless payment limit, and 6) lock-screen bypass, as discussed below.

Eavesdropping. Eavesdropping involves illicitly accessing sensitive information from contactless payment

[2] NFC emulators, readers, and mobile phones capable of reading NFC signals can be interchangeably used in attack configurations

TABLE 2. Feasibility Comparison of Contactless Payment Attacks: Evaluating the Complexity of Each Attack Category.

Attack Category	Replicability	Affected Devices	Required Equipment	Compromised Terminal	Required Time	Number of Crook(s)
Eavesdropping	Replicable	Cards	1 NFC Reader	No	Real-time	1
Relay	Replicable	Cards	2 NFC Readers	No	Real-time	2
Pre-play	Replicable	Card, Phone	NFC Reader	Some Yes	Real-time	1
Card Replica	Partially replicable	Card	NFC Reader, USB Card Reader, Card Writer, Blank Cards	No	Needs time	1
Limit Bypass	Partially Replicable	Card, Phone	2 NFC Readers	No	Real-time	2
Lock-screen Bypass	Partially Replicable	Phone	2 NFC Readers, Laptop	Some Yes	Need time or Real-time	2

cards by intercepting NFC communication. Attacks such as those described in [25] and [14] extract critical data like the Primary Account Number (PAN) and card expiry date via unprotected NFC channels using hidden NFC readers. Tools like [45] and [36] can also be employed to capture leaked data wirelessly from contactless credit/debit cards.

Relay. Malicious actors exploit the extended range of NFC technology to execute relay attacks, intercepting payment information between a card and a distant terminal. This typically involves using a terminal emulator near a victim's contactless payment device to initiate a transaction, then wirelessly transmitting the data to another remote NFC reader (card emulator) positioned near a legitimate terminal to complete the transaction covertly. Various relay attacks documented in literature [8], [9], [11], [18], [24], [29], [31], [53] employ different device combinations. Notably, attacks like the one described in [35] integrate essential equipment into a compact device (mPoS terminals), facilitating relay attacks in a more convenient way such as digital pickpocketing.

Pre-play. Pre-play attacks involve prerecording transaction data for future use under specific conditions, primarily targeting the magnetic stripe (mag-stripe) mode of transactions in credit and debit cards, in contrast to the EMV mode. These attacks [17], [20], [43] often entail downgrade attacks, wherein attackers modify EMV messages to downgrade a transaction to mag-stripe mode. Once downgraded, attackers can pre-record genuine transactions, clone them, and later re-play them on compromised terminals.

Counterfeit Card Replica. Counterfeit card replica attacks involve fraudsters creating fake copies of legitimate payment cards to conduct unauthorized transactions. They acquire cardholder information through methods like skimming devices and data breaches, exploiting the mag-stripe mode of transactions to produce replicas of mag-stripe card clones. Contactless mag-stripe cards are vulnerable to such attacks, as demonstrated in [17], [19], [38], where attackers use NFC readers to intercept and extract card numbers for cloning onto functional mag-stripe cards.

Limit Bypass. Contactless limit bypass attacks enable unauthorized users to surpass transaction limits on contactless payments. For example, the UK imposes a £100 limit on contactless transactions [23], which attackers circumvent through various means, such as exploiting transaction currency vulnerabilities [12] or deceiving payment terminals into falsely verifying transactions [5], [6], [20]. Recent research [7] has uncovered additional methods of bypassing this limit by exploiting vulnerabilities in payment terminals during offline card validation.

Lock-screen Bypass. Lock-screen bypass attacks involve exploiting vulnerabilities in mobile devices, particularly those using digital wallets like Apple Pay [3], Google Pay [22], and Samsung Pay [44]. Despite the convenience of these digital wallets for contactless transactions, they typically require the device to be unlocked, a security aspect exploited in this attack category. Researchers have identified various methods to bypass lock screens [41], [50], [58] for different combinations of digital wallets and card brands. Public transport schemes like Apple Pay [2] and Samsung Pay [47] "Express Transit" mode, introduced in 2019, have also been targeted in some attacks within this category. These schemes, for example, in the case of Apple Pay, employ security features such as the "magic string", a specific byte sequence from ticket-gate readers.

3.3. Feasibility of Contactless Payment Attacks

Using the attack categories explained in Section 3.2, here, we evaluate the technical feasibility of each of these attack categories as shown in Table 2 and based on the following factors:

Replicability: The replicability of an attack is defined as the ability to repeat an attack and achieve the same results, falling into three categories: "fully replicable" if all attacks in a category are currently executable; "partially replicable" if some attacks have been mitigated but others persist; and "non-replicable" if all known methods of attack have been effectively addressed.

Affected Devices: Among the available payment devices discussed shown in Fig. 1, credit/debit cards and mobile phones are typically the main targets. While some attacks exclusively target cards, others focus on NFC-enabled mobile phones, and a subset can affect both types of devices.

Required Equipment: This factor denotes the bare minimum hardware, excluding the victim's device and the payment terminal, needed to perform an attack. This can be improved to perform the attack with less equipment; however, we report the equipment that attackers deploy to perform the attack reported in their research.

Compromised Terminal: While certain attacks may function with a standard terminal, others necessitate modifications that compromise its integrity. Such compromises can occur through either physical alterations or firmware modifications. It is important to recognize that compromising a terminal is widely regarded as challenging.

Required Time: The required time for an attack denotes the duration necessary to successfully execute it,

TABLE 3. Attack Example Scenarios for Contactless Payment.

Attacks	Example Scenario
Eavesdropping	Imagine you're standing in the payment queue at a coffee shop, completely unaware that an attacker nearby or the malicious coffee shop owner may exploit the situation. Once you proceed to make a contactless payment, they could utilize a skimming device to gather your payment information, including your account number.
Relay	Imagine you're waiting in a shop line, and an attacker in close proximity to you gain access to your card by using a phone to interact with it, hidden in a pocket or bag. This phone then relays the obtained data to a second device located in a jewellery shop in real-time, where a purchase is made using your card information.
Pre-play	Imagine you're at a store, all set to make a contactless payment with your card or smartphone. Little do you know that the payment terminal has been compromised by attackers. They intercept your payment information, which is then used later to conduct multiple fraudulent transactions. You may not notice anything suspicious during the legitimate transaction.
Card Replica	Imagine you are on a bus, and someone uncomfortably leans close to you. Alternatively, imagine being at a shop where the merchant insists on swiping your card, claiming they only accept magnetic stripe (mag-stripe) payments (on a terminal that is compromised). In all such cases, the necessary card data is collected through data interception, to be later encoded onto a counterfeit mag-stripe card.
Limit Bypass	Imagine you have lost your card. In this scenario, as criminals lack knowledge of your PIN, their only way to steal money from you is by utilizing your card for a contactless transaction up to the £100 limit in the UK. However, using the mentioned equipment, they can bypass this limit and make transactions of higher amounts, such as £1000 if available in your account.
Lock-screen Bypass	Imagine you are in a restaurant, and you leave your phone on the table unattended for a few seconds, or you are in a crowded place and put your phone in your bag, assuming that it is locked. The attacker gets fairly close to your locked phone, initiates a contactless payment with a terminal near it, and by using special equipment such as additional smartphones that run malicious codes, changes the payment information and convinces your phone that it is making a payment to a transit operator, so it does not need to unlock.

with some attacks occurring in real-time, while others demand additional time for preparation and execution.

Number of Crook(s): This refer to the number of attackers involved in the attack, depending on the attack type and the threat model. The analysis of these factors for each attack category is explained below.

Eavesdropping is categorized as "replicable". Although encryption and tokenization measures are in place, our experiments indicate that certain data can still be accessed from cards. Attacks reported in the literature [14], [25] primarily target cards and only require one NFC reader, without the need to compromise the terminal. This NFC reader could be conveniently positioned at a checkout counter, enabling data to be read in real-time without requiring an active crook, or data can be read with one active crook approaching a victim that has a card.

Relay attacks [8], [9], [11], [18], [24], [29] are fully "replicable" as relay attacks are still feasible, regardless of the relay protection measures, as shown in [41]. As previously mentioned, these attacks necessitate the use of two emulators in real time, indicating the need for two present crooks. The attacks aim at cards and can be executed without the user's knowledge or the need to compromise the terminal.

Pre-play attacks [17], [20], [43] are considered "replicable". Although researchers in [7] have reported that the attack in [43] have been patched, our experimental results show that this attack can still be replicated. While other attacks in this category [17], [43] do not require a compromised terminal, the attack in [20] can affect both cards and phones when the terminal is compromised. One present crook is required to capture such information.

Card Replica attacks are also "partially replicable". While our experimental results show that attacks in [19] and [38] are still replicable, Visa's decision to remove the old mag-stripe mode affects the applicability of the attack in [17]. The recent replicable attack in 2019 [19] involves one active crook who reads data from two interfaces (EMV and magstripe) and later transcribes it onto a blank card, a process that requires time. These attacks can be executed without compromising the terminal.

Limit Bypass is considered "partially replicable", with the attack in [5] being patched and the attack in [13] being impossible to replicate (due to the removing of the offline PIN verification in contactless payment), while [6], [7], [12], [20] are still replicable. These active threats can target both cards and phones, require two NFC readers, and can be executed without compromising terminals. The attack can occur in real time and requires two present crooks when the card is in possession of the victim.

Locks-screen Bypass attacks are also "partially replicable" due to the replicability of some combinations (e.g., applePay-Visa) as well as some others being patched (e.g., Mastercard attacks that require the modification of the Merchant Category code (MCC)). They primarily target phones with lock screens and necessitate two NFC readers and a laptop acting as a proxy server. Some scenarios, such as ApplePay Visa bypass, do not require a compromised terminal and can happen in real-time, while others, like GooglePay-Mastercard [50], demand the terminal to be compromised and require time (50 attempts for a success rate of 22%). Finally, two present crooks are required for this attack.

4. Methodology

4.1. Survey Design

The survey consists of the following main sections. Further details regarding each section can be found in Section 8.1.

Introduction and Consent: This section marks the initiation of the survey and provides participants with a summary of the study's objectives and procedures. We ensure to clarify that participation is entirely voluntary and that the data collection is anonymous, following ethical guidelines. Then, participants are asked to give their informed consent before proceeding further.

General Knowledge and Preferences: In this section, we aim to understand the participant's technology usage patterns and preferences. Hence, participants are inquired about their familiarity with contactless payment, their usage frequency, the payment devices that they use for contactless payment, as well as their preferences, likes, and dislikes linked to this method of payment.

Perception on Contactless Payment Security: This section begins by exploring participants' general perceptions of contactless payment and device security. It then

TABLE 4. USER STUDY PARTICIPANT DEMOGRAPHICS (N=150).

Demographic	Participants(%)
Gender	
Male	72 (48%)
Female	76 (50.7%)
Non-binary/Third gender	1 (0.7%)
Prefer not to say	1 (0.7%)
Age	
18-24	21 (14%)
25-34	52 (34.7%)
35-44	41 (27.3%)
45-54	15 (10%)
55-64	12 (8%)
65 years or older	8 (5.3%)
Prefer not to say	1 (0.7%)
Highest Level of Education	
High school diploma or equivalent	26 (17.3%)
Some college or associate degree	39 (26%)
Bachelor's degree	54 (36%)
Master's degree	24 (16%)
PhD or higher	6 (4%)
Prefer not to say	1 (0.7%)

introduces six attack categories, asking participants to evaluate each in terms of feasibility and concern. Example scenarios are provided in Table 3.

Protective Actions: This section aims to gauge the participants' proactive steps toward protecting against unauthorized payments. Questions are framed around their account monitoring habits in response to unauthorized transactions. Further, we ask participants to choose their preferred protective actions from a list of twelve options to counteract the vulnerabilities of contactless payment attacks.

Demographics: Participants are asked to provide demographic information, including age, gender, and the highest level of education.

4.2. Data Collection and Analysis

We designed our survey utilizing Google Forms and ran a series of pilot studies to verify the comprehensibility and consistency of the attack descriptions, especially ensuring that technical terms were understandable to participants. The first pilot study asked feedback from five experts on the study's design, with subsequent second and third pilot studies focusing on testing the survey's clarity among a broader audience. These pilot studies facilitated the identification and rectification of minor errors, informed necessary structural adjustments based on received feedback, and provided a benchmark for the time required to complete the questionnaire. Data collection was streamlined through Prolific [40], an online platform dedicated to simplifying participant recruitment and management for research. This platform allowed us to recruit 150 UK-based participants. Details regarding participant demographics are shown in Table. 4. Participants were compensated for their involvement in the study.

In the process of analyzing the collected data, we employed a range of techniques to facilitate an understanding of the survey results. Our initial approach involved a descriptive analysis to examine the survey responses in each category, providing insights into technology usage patterns, concerns about attacks, and participants' protective actions. Through this analysis, we could generate an overview of the central tendencies within the data, understanding the common behaviours and perceptions amongst our diverse sample of participants. Furthermore, we implemented a pre-post analysis to evaluate how the presentation of detailed information about various types of contactless payment attacks influenced the participants' perceptions of security.

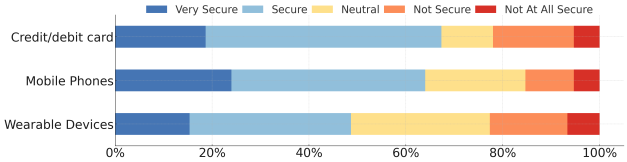

Figure 3. Users' Perception on Security of Contactless Payment Devices.

5. Results

5.1. General Knowledge and Preferences

Our exploration of user understanding and acceptance of contactless technology revealed varying levels of familiarity. About half of users claimed comprehensive knowledge, while 40% had only a general understanding. Interestingly, most respondents accurately defined contactless technology as a payment method that doesn't require card insertion or PIN entry, commonly involving a card or phone tap. They recognized technologies like RFID and NFC in enabling these transactions, with some identifying digital wallets like Apple Pay and Google Pay. While some users correctly mentioned transaction limits (e.g., £100 in the UK), others were unsure or oversimplified their responses. Adoption of contactless payments is widespread, with 99.3% having used it in the past six months. Usage frequency varied: 40% used it once or twice daily, 30.7% weekly, and 24.7% multiple times per day. Credit or debit cards were the preferred payment method (97.3%), followed by mobile phones (66.7%) and wearables (11.3%). Users valued the speed and convenience but had concerns about security, technical issues, and payment caps. Despite this, 85% considered contactless features important for businesses. Additionally, 42.7% showed interest in emerging technologies like contactless cash withdrawals, exemplified by Barclays' feature allowing ATM withdrawals via card tap [4].

5.2. Perception on Contactless Payment Security

5.2.1. General Security Concern. We first asked participants what they thought about the overall security of making contactless payments. Only a small group of the people (around 18%) said they were concerned or very concerned about this. In contrast, nearly half of the users (around 49%) said they weren't concerned or were only somewhat concerned. Interestingly, the biggest group (around 33%) among the five categories did not feel strongly either way. This means they were unsure about how secure it is to make payments in this way.

5.2.2. Payment Devices Security Perception. Our analysis of the security perceptions surrounding contactless payment devices such as credit/debit cards, mobile phones, and wearable technologies are shown in Fig. 3.

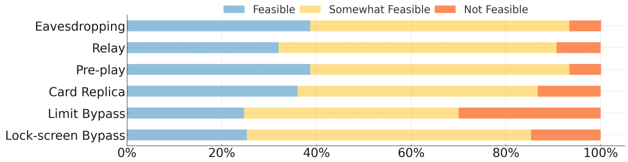

Figure 4. Users' Perceived Feasibility of Each Contactless Attack.

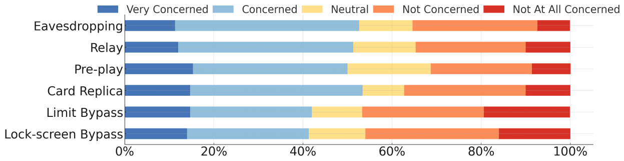

Figure 5. Users' Concerns Level on Different Contactless Attacks.

While credit/debit cards and mobile phones are generally viewed as secure by a majority of participants, wearable devices lag behind in perceived security. For credit and debit cards, a majority of participants (67.4%) view them as either "very secure" (18.7%) or "secure" (48.7%). A small percentage of participants (5.3%) feel these cards are "not at all secure". Approximately 16.7% of respondents perceive them as "not secure" while the rest (10.7%) maintained a neutral stance on their security. When it comes to mobile phones, a slightly lower percentage of participants (64%) view them as secure with 24% saying they are "very secure" and 40% considering them "secure". The view that mobile phones are "not at all secure" is held by an identical 5.3% of the respondents as with credit/debit cards. However, fewer respondents (10%) see mobile phones as "not secure" compared to credit/debit cards. A significant 20.7% remain neutral about mobile phone security, which is nearly double the neutral response for credit /debit cards. Wearable devices are perceived as less secure overall, with 48.6% of respondents viewing them as either "very secure" (15.3%) or "secure" (33.3%). This represents a decrease compared to the perception of security for credit /debit cards and mobile phones. A slightly higher percentage (6.7%) consider these devices as "not at all secure", and 16% perceive them as "not secure". Interestingly, wearable devices have the highest percentage of neutral responses (28.7%) among the three technologies discussed.

5.2.3. Users Perceived Feasibility of Attacks. The feasibility of each attack from the user's perspective is depicted in Fig. 4. Our analysis indicates that Eavesdropping and Pre-play attacks are regarded as the most feasible attacks from the users' perspective. For both these types, 54.7% of participants consider them "somewhat feasible", and 38.7% view them as "feasible". Only 6.7% of participants consider these attacks as "not feasible". This similarity in the results could be attributed to the similarity of the threat models in both attack scenarios; the attacker uses an NFC reader to approach the victim and steals data for fraudulent purposes. On the other hand, Limit Bypass and Lock-screen Bypass attacks are perceived as less feasible than other attack types. For Limit Bypass attacks, 45.3% of respondents regard it as "somewhat feasible", 24.7% deem it "feasible", while a considerably larger group, 30%, considers it "not feasible" (highest "not feasible" compared to all attack categories). Similarly, for Lock-screen Bypass, 60% regard it as "somewhat feasible". 25.3% view it as "feasible", and 14.7% consider it "not feasible".

These figures suggest a higher degree of uncertainty about the likelihood of these attacks relative to Eavesdropping and Pre-play attacks. Regarding Relay and Card Replica attacks, the "somewhat feasible" and "feasible" responses lie between the most feasible groups (Eavesdropping and Pre-play) and the least feasible ones (Limit Bypass and Lock-screen Bypass). This suggests a moderate level of perceived feasibility among participants. For Card Replica attacks, 50.7% perceive it as somewhat feasible, 36% as feasible, and 13.3% regard it as not feasible. Meanwhile, for relay attacks, 58.7% consider them somewhat feasible, 32% as feasible, and 9.3% as not feasible.

5.2.4. Users Concern Regarding Attacks. The results of users' concern level about each attack are shown in Fig. 5. We consider the "very concerned" and "concerned" categories as "high concern", and the "not concerned" and "not at all concerned" as "low concern". The survey results reveal that users exhibit varying degrees of concern regarding different types of attacks. For some types of attacks, such as Eavesdropping, Relay, and Pre-play attacks, there is a relatively uniform level of concern. Approximately half of the users express high levels of concern about these three types of attacks, while around a third consider these attacks to be of lesser concern. Interestingly, users seem to exhibit a higher degree of uncertainty regarding the Pre-play attack. Approximately one-fifth of the respondents remain neutral about this type of attack, indicating a potential lack of understanding or familiarity with it. The Card Replica attack showed the most definitive reactions, with the lowest percentage of users remaining neutral among all types of attacks. The level of concern for this type of attack was the highest among all, with about 55% of respondents indicating high concern. Meanwhile, about 37% of respondents expressed low concern for the Card Replica attack. Finally, the concern levels for both the Limit Bypass and Lock-screen Bypass attacks were similar to each other but notably lower when compared with other categories of attacks. Only about 40% of the respondents expressed high concern for these two types of attacks, and almost half of the users (46%) had low concern. This significant deviation suggests a greater degree of uncertainty or possible underestimation of these attacks among users.

Comparing the concern levels with the perceived feasibility of attacks generally reflects a pattern in the data; the perceived feasibility of an attack closely ties to the level of concern participants feel about it, with an exception. The Eavesdropping and Pre-play attacks, which participants thought were the most feasible, also triggered a high level of concern. This alignment suggests that participants are more concerned about attacks they believe are most feasible. Similarly, the Limit Bypass and Lock-screen Bypass attacks which were viewed as the least feasible attacks, attracted less concern among users. However, the Card Replica and Relay attacks present an interesting deviation from this trend. Although participants considered them less feasible than the Eavesdropping and Pre-play attacks, they still expressed substantial concern levels, similar to these attacks. This discrepancy is most pronounced for the Card Replica attack, which provoked the highest level of concern overall. This can suggest that despite the lower perceived feasibility, the potential consequences of these types of attacks are a significant source of worry for participants.

5.2.5. General Security Concern (Revisited). After providing the attack descriptions along with example scenarios and asking participants about the level of possibility and their concern about each attack, we again asked participants how they would evaluate the overall security of contactless payment. We noted an increase in the proportion of users in the "very concerned" category, with the figure rising from 3.30% to 14%. Similarly, the "concerned" category saw an increase from 14.69% to 27.30%. This suggests that awareness of the threats inherent in contactless payment systems significantly increased the perceived level of concern among the users. Simultaneously, the "neutral" category saw a considerable decrease from 32.67% to 12.70%, suggesting that the information provided helped users form more definitive opinions regarding the security of contactless payment systems. Interestingly, the "not concerned" category remained relatively stable, shifting from 30.67% to 30%, indicating that for a segment of users, their concern level was not significantly influenced by the presented information. Finally, the proportion of users who were "not at all concerned" showed a slight decrease from 18.68% to 16.00%. This implies that even among those initially unconcerned, education had some impact in heightening their sense of concern.

5.2.6. Demographic Results. Different demographics showed varying levels of concern about contactless payment security after learning about potential attacks. Below, we present average concern levels by age group, education, and gender, measured on a scale from 1 (Not At All Concerned) to 5 (Very Concerned). These averages were calculated by converting qualitative responses into numerical scores, and then averaging them within each group before and after exposure to attack information.

Gender. Fig.6 provides an analysis of the impact of familiarity with attacks on concern levels across different gender groups. Initially, females exhibited a higher average concern level compared to males. After becoming familiar with the risks, both groups showed an increase in concern levels, with females continuing to show the highest level of concern. The most significant increase in concern was observed among males, indicating that familiarity with the risks had a more substantial impact on raising their awareness and concern levels. This difference in impact might be attributed to varying levels of initial awareness and perceptions of risk associated with contactless payment systems. Familiarity likely addressed specific knowledge gaps and misconceptions more prevalent among male participants, leading to a more pronounced shift in their concern levels.

Age. Fig. 7 shows that older individuals are usually more concerned about the security risks associated with contactless payment systems. The general trend indicates that familiarity positively impacts almost all age categories, significantly increasing concern levels after becoming familiar with the risks. However, as seen in some groups, such as the 25–34 age group, familiarity had a limited impact on changing their perceptions about these security risks. This suggests that while familiarity is generally effective in raising awareness, certain age groups may already have formed strong opinions or possess a level of skepticism that is not easily influenced.

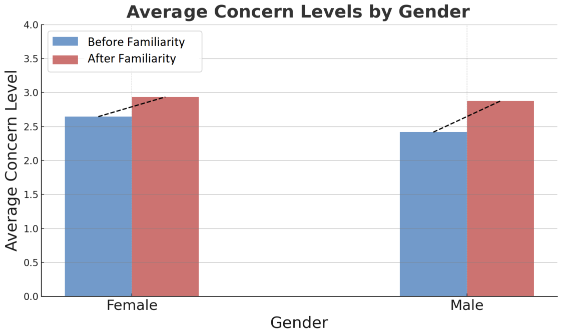

Figure 6. Average Concern Levels Based on Gender.

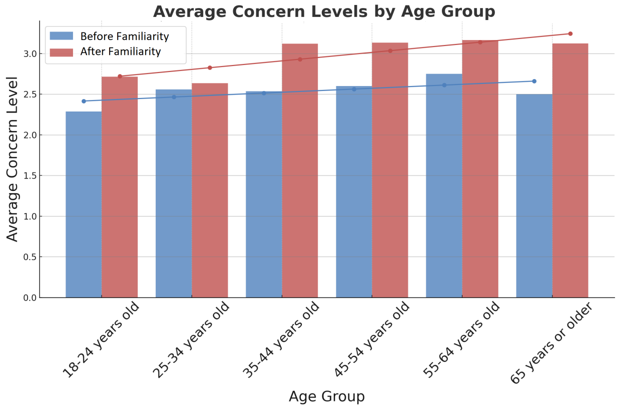

Figure 7. Average Concern Levels Based on Age.

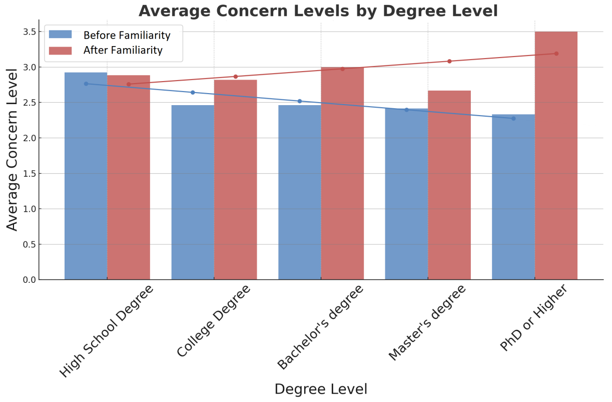

Figure 8. Average Concern Levels Based on Educational Degree.

Educational Degree. Fig. 8 presents the analysis of the impact of familiarity with the risks of contactless payment systems and associated attacks, based on educational degree levels. As can be seen, prior to becoming familiar, individuals with a high school degree exhibited the highest average concern levels. The trend indicates

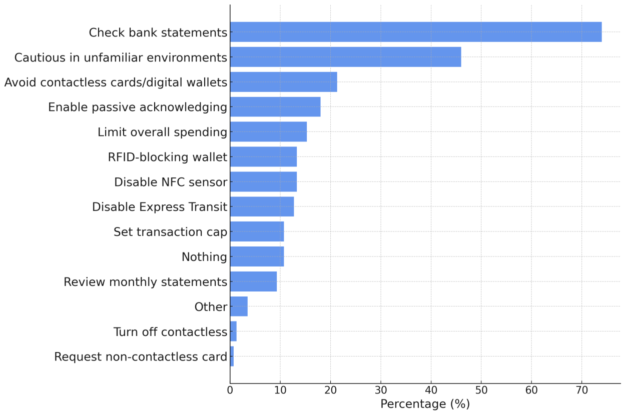

Figure 9. Protective Actions Taken by Users.

that as the degree level increased, the initial concern levels dropped, suggesting that individuals with higher education levels were initially less concerned about the security of contactless payment systems. However, after becoming familiar with the risks, there was a noticeable increase in concern levels across all education levels, with individuals holding a PhD or higher showing the most significant increase, reaching the highest concern level post-familiarity. The trend demonstrates that as participants become more familiar with the risks of contactless payment attacks, the higher the education degree, the greater the impact. This suggests that individuals with higher educational backgrounds may initially underestimate the risks due to a lack of specific knowledge, but once informed, they recognize the potential threats more acutely.

5.3. Protective Actions

Results of the specific twelve protective actions that users take to protect their contactless payment security are depicted in Fig. 9. The most adopted security measure, as reported by 74% of participants, was regularly checking bank receipts and accounts. The second most taken protective action was being cautious when utilizing contactless payments in unfamiliar or untrusted environments, with 46% of respondents. Approximately one in five (20%) participants choose not to carry cards or add cards with large amounts of funds to their digital wallets. This practice potentially mitigates attacks aimed at digitally pickpocketing from stolen cards. Close behind, 18% of participants have activated passive notifications such as SMS or calls for each transaction, while around 15.3% limit the total amount they can spend before their PIN is required. A few people (13%) adopt security measures such as RFID blocking wallets, disabling “express transit” mode on their digital wallets when not in use, or turning off the NFC sensor on their phones, all aimed at preventing unauthorized NFC access to their payment devices. Around 10% of respondents limit the maximum transaction amount and prefer reviewing monthly paper statements. The least common measures, as reported by about only 1% of participants involved disabling the contactless feature completely or requesting a card devoid of the contactless feature. Notably, about 10% of users do not implement any specific protective measures against contactless payment attacks.

The results reveal that despite the availability of various protective measures against the discussed attacks, users primarily rely on straightforward methods for protection. These include routinely checking their bank receipts and accounts, and being cautious when utilizing contactless payments in untrusted environments. While these measures are beneficial, they may not be adequate against all threats. More advanced measures are used less frequently, suggesting a need for increased awareness and education on a wider range of protective measures.

6. Discussion

6.1. Users’ Perception vs. Technical Feasibility

Comparing the technical feasibility of various contactless payment attack categories in Table 2 with user perception in Section 5.2 reveals interesting insights about the users’ understanding and awareness of potential threats. We can categorize the attack types into three categories: accurate estimation, overestimation, and underestimation of vulnerabilities.

Accurate Estimation: accurate estimation of vulnerabilities presents three key categories: Eavesdropping, Relay, and Pre-play attacks. In the case of Eavesdropping, users perceive this attack as highly likely and express high concern, which aligns well with the technical feasibility. This accurate estimation of vulnerabilities might result from increased awareness about data privacy and security issues, fueled by frequent news about data breaches, leading to a realistic understanding of the vulnerabilities. Regarding Relay attacks, even though users were not sure about the feasibility of this attack, they still showed high levels of concern, which matches our technical feasibility evaluation. While users recognize the vulnerabilities, they may lack full comprehension of the execution methods. Their limited awareness of these techniques, combined with the real-time nature and proximity requirement of these attacks, may contribute to the misconception that these attacks are less feasible than they truly are. Lastly, Pre-play attacks are perceived by users as highly probable, eliciting considerable concern. Their perception aligns with its technical feasibility, suggesting that users’ understanding of these attacks is relatively accurate. Their comprehension of Pre-play attacks could be attributed to the intuitive nature of these attacks; the concept of an attacker intercepting and replaying transaction information might be easy to grasp, leading to an accurate estimation of its feasibility.

Overestimation: Users have expressed substantial concern about Card Replica attacks more than any other category. However, this attack requires extensive time and specialized tools and is limited in its scope. Additionally, the success of these attacks primarily relies on the use of mag-stripe mode, which has its limitations. The selling of card data becomes necessary for the attack to be fully effective, particularly as mag-stripe is now restricted in many regions [15]. This additional step increases the complexity of the attack, making it even less likely to happen frequently. It suggests that users may be overestimating this attack, likely fueled by concern over the potentially severe consequences of such attacks.

Underestimation: users tend to underestimate Limit Bypass and Lock-screen Bypass attacks. In the case of the Limit Bypass attack, users have shown low concern levels compared to other attacks, and they have recognized this attack as the least feasible attack among all, regardless of the technical feasibility of these attacks and the high negative impacts that they have. This underestimation could stem from a lack of awareness of potential loopholes in transaction limits and EMV messages, and the fact that attackers can alter certain transaction data that are not authenticated by the bank. Similarly, for Lock-screen Bypass attacks, users regard these attacks as less likely and express less concern, indicating an underestimation of this attack, although it affects several digital wallets and several card brands. Users may underestimate the vulnerabilities of this attack due to faith in the security measures of their mobile devices, as also shown in Fig. 3 on the security of payment devices, particularly the lock-screen feature. The lack of familiarity with the "express transit" mode, used in some of these attacks, might also contribute to this underestimation, as about 85% of users reported never using this technology when asked in our survey. Notably, underestimation could expose users to threats they are not fully aware of and is different from overestimation.

6.2. Recommendations

While users have found contactless payments fast and convenient, they have raised serious security concerns regarding contactless payment systems. To address these concerns, first, the security of payment systems needs to be enhanced, and second, users need to be educated about potential vulnerabilities and what they can do to protect themselves during these improvements. However, while user education is important, it is equally vital to recognize that end-users may not always possess the technical understanding or motivation to manage security risks. A user-centred approach should prioritize minimizing the need for active intervention from users and instead focus on embedding robust protections at the system level.

Regarding enhanced security, payment providers like Visa [57] and Mastercard [34], and standardization bodies such as EMVCo [16] should refine their protocols and introduce extra security checks to mitigate these threats. Furthermore, payment providers like Apple Pay [3], Google Pay [22], and Samsung Pay [44] should integrate additional protective features and ensure the security of edge devices, specifically NFC-enabled mobile phones. These phones are often the target of numerous attacks, however, while some users perceive them to be secure, they generally were more neutral regarding the security of mobile phones compared to credit/debit cards (as shown in Fig. 3).

Regarding education, end users must remain alert. They should strive to understand the vulnerabilities associated with contactless payments and actively take protective actions, as provided in Fig. 9, such as setting up and monitoring passive acknowledgement of payments, applying possible limits, regularly checking bank statements, and being careful when using contactless payments in unfamiliar or untrusted environments. Banks should also play their part in educating users about the variety of attacks that exist and the protective actions they can take on their online and mobile banking systems. Our results demonstrate how education on contactless payment attacks can effectively increase users' level of concern about these vulnerabilities in payment systems. Furthermore, as discussed in Section 5.2.6, familiarity with attacks varied across different demographic groups. This suggests that user education should be tailored to each group, focusing on their specific needs and characteristics.

6.3. Limitations

This study has limitations that should be taken into account when interpreting the findings. First, while we made a concerted effort to ensure that the attack descriptions were clear to participants, some individuals may have still found them difficult to fully understand. This could be due to the inherent technical complexity of certain attacks or the overlapping nature of some attack characteristics. Second, we focused on attacks documented in academic literature, excluding media-reported incidents due to lack of technical detail. This may limit the alignment between our scenarios and users' real-world awareness. Third, our analysis was primarily descriptive in nature. Given the relatively modest sample size of 150 participants, we did not apply statistical methods, which limits the generalisability of our conclusions. Future research with larger, more diverse samples could provide more statistically robust insights. Finally, all study participants were located within the UK. Since consumer payment behaviours, threat perceptions, and levels of cybersecurity awareness can vary between countries and cultural contexts, our findings may not be directly transferable to populations in other regions.

7. Conclusion

Our exploration of contactless payment attacks and their technical feasibility has revealed important insights into users' perceptions and understanding. Despite the ubiquity of contactless payment technology and its adoption in everyday life, users' perceptions of potential threats do not necessarily align with their technical feasibility. Users overestimate the vulnerabilities of Card Replica attacks due to fear of significant consequences, yet they underestimate Limit Bypass and Lock-screen Bypass attacks, likely due to unawareness of these methods and overconfidence in mobile device security. However, users accurately assess vulnerabilities associated with Eavesdropping, Relay, and Pre-play attacks, indicating a better awareness in these areas. Our research also unveiled that to protect against these attacks, users often adopt basic measures such as reviewing their bank statements and being cautious in unfamiliar environments. Although these methods are effective, they are not sufficient to fully mitigate the potential vulnerabilities. These findings highlight the urgent need to improve the security of payment systems and to enhance targeted education and awareness efforts, as different demographic groups reacted differently to the risks and attacks associated with contactless payments.

References

[1] Lukas Aldag, Karen Renaud, Benjamin Berens, Reyhan Duezguen, Mattia Mossano, and Melanie Volkamer. Reporting on insights gained into uk citizens' perceptions of contactless card risks. *Karlsruher Institute for technology (KIT). doi*, 10, 2020.

[2] Apple. Applepay express transit mode. Available at https://www.apple.com/uk/apple-pay/transport/. Accessed 11 January 2023.

[3] Apple. Apple pay: Here to pay. https://www.apple.com/uk/apple-pay/, 2023. Accessed: 15 May 2023.

[4] Barclays. Contactless cash. Available at https://www.barclays.co.uk/ways-to-bank/contactless-cash/. Accessed 11 January 2023.

[5] David Basin, Ralf Sasse, and Jorge Toro-Pozo. Card brand mixup attack: Bypassing the PIN in non-visa cards by using them for visa transactions. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 179–194. USENIX Association, August 2021.

[6] David Basin, Ralf Sasse, and Jorge Toro-Pozo. The emv standard: Break, fix, verify. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 1766–1781. IEEE, 2021.

[7] David Basin, Patrick Schaller, and Jorge Toro-Pozo. Inducing authentication failures to bypass credit card pins. *32rd USENIX Security Symposium (USENIX Security*, 2023.

[8] Thomas Bocek, Christian Killer, Christos Tsiaras, and Burkhard Stiller. An nfc relay attack with off-the-shelf hardware and software. In Rémi Badonnel, Robert Koch, Aiko Pras, Martin Drašar, and Burkhard Stiller, editors, *Management and Security in the Age of Hyperconnectivity*, pages 71–83, Cham, 2016. Springer International Publishing.

[9] Tom Chothia, Flavio Garcia, Joeri Ruiter, Jordi Breekel, and Matthew Thompson. Relay cost bounding for contactless emv payments. *International Conference on Financial Cryptography and Data Security*, 2015.

[10] Harshal Dev, Raj Gupta, and Dhruv Kumar. From cash to cashless: Upi's impact on spending behavior among indian users. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, pages 1–10, 2024.

[11] Martin Emms, Budi Arief, Troy Defty, Joseph Hannon, Feng Hao, et al. The dangers of verify pin on contactless cards. *School of Computing Science Technical Report Series*, 2012.

[12] Martin Emms, Budi Arief, Leo Freitas, Joseph Hannon, and Aad van Moorsel. Harvesting high value foreign currency transactions from emv contactless credit cards without the pin. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 716–726, 2014.

[13] Martin Emms, Budi Arief, Nicholas Little, and Aad van Moorsel. Risks of offline verify pin on contactless cards. In *Financial Cryptography and Data Security: 17th International Conference, FC 2013, Okinawa, Japan, April 1-5, 2013, Revised Selected Papers 17*, pages 313–321. Springer, 2013.

[14] Martin Emms et al. Practical attack on contactless payment cards. *HCI 2011: Health Wealth and Happiness*, 2011.

[15] EMVCo. EMV Contactless Specifications for Payment Systems Book C-3 (Version 2.6). Online, February 2016.

[16] EMVCo. EMVCo - Enabling Seamless and Secure Payments Worldwide, 2023. [Accessed 26 May 2023].

[17] Peter Fillmore. Crash and pay: Owning and cloning payment devices. *BlackHat*, 2015.

[18] Lishoy Francis, Gerhard Hancke, Keith Mayes, and Konstantinos Markantonakis. Practical relay attack on contactless transactions by using nfc mobile phones. *IACR Cryptology ePrint Archive*, 2011:618, 01 2011.

[19] Leigh-Anne Galloway. It only takes a minute to clone a credit card, thanks to a 50-year-old problem. *Tech Report*, 2020.

[20] Leigh-Anne Galloway and Yunusov. First contact: New vulnerabilities in contactless payments. *Black Hat Europe*, 2019, 2019.

[21] Aznida Wati Abdul Ghani, Abdul Hafaz Ngah, and Azizul Yadi Yaakop. Why should i continue using it? factors influencing continuance intention to use e-wallet: The sor framework. In *International Conference on Information Systems and Intelligent Applications: ICISIA 2022*, pages 1–16. Springer, 2022.

[22] Google. Google pay: Seamlessly pay online, pay in stores or send money. https://pay.google.com/about, 2023. Accessed: 15 May 2023.

[23] United Kingdom Government. 2021 budget plan. Available at https://www.gov.uk/government/publications/budget-2021-documents. Accessed 01 June 2021.

[24] Jian Yuan Haoqi Shan. Man in the nfc. *DEF CON 25*, 2017.

[25] Thomas S. Heydt-Benjamin, Daniel V. Bailey, Kevin Fu, Ari Juels, and Tom O'Hare. Vulnerabilities in first-generation rfid-enabled credit cards. In Sven Dietrich and Rachna Dhamija, editors, *Financial Cryptography and Data Security*, pages 2–14, Berlin, Heidelberg, 2007. Springer Berlin Heidelberg.

[26] Serena Hillman, Carman Neustaedter, Erick Oduor, and Carolyn Pang. Mobile payment systems in north america: user challenges & successes. In *CHI'14 Extended Abstracts on Human Factors in Computing Systems*, pages 1909–1914. 2014.

[27] Muhamad Fitri Ismail, Mohd Akmal Rohiat, Azlan Salim, and Dewi Eka Murniati. Customer experience towards contactless payment service practices in the pandemic covid-19 era. a case study: Fast food restaurants. *Journal of Technology and Humanities*, 3(1):1–6, 2022.

[28] iZettle. izettle card reader. Available at https://www.izettle.com/, 2023. Accessed 11 January 2023.

[29] Ricardo J. Rodriguez Jose Vila. Relay attacks in emv contactless cards with android ots devices. *HITBSecConf*, 2015.

[30] Crystal T Lee and Ling-Yen Pan. Smile to pay: predicting continuous usage intention toward contactless payment services in the post-covid-19 era. *International Journal of Bank Marketing*, 41(2):312–332, 2023.

[31] Eddie Lee. Nfc hacking: The easy way. In *Defcon hacking conference*, volume 20, pages 63–74, 2012.

[32] Makayla Lewis and Mark Perry. Follow the money: Managing personal finance digitally. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pages 1–14, 2019.

[33] Scott Mainwaring, Wendy March, and Bill Maurer. From meiwaku to tokushita! lessons for digital money design from japan. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 21–24, 2008.

[34] Mastercard. Experience the world with mastercard. https://www.mastercard.co.uk/en-gb.html, 2023. Accessed: 15 May 2023.

[35] Mahshid Mehr Nezhad and Feng Hao. Opay: an orientation-based contactless payment solution against passive attacks. In *Annual Computer Security Applications Conference*, pages 375–384, 2021.

[36] Julien MILLAU. Pro credit card reader nfc. https://play.google.com/store/apps/details?id=com.github.devnied.emvnfccard.pro&hl=en&gl=US. Google Play Store.

[37] Uma Thevi Munikrishnan, Abdullah Al Mamun, Nicole Kok Sue Xin, Ham Siu Chian, and Farzana Naznen. Modelling the intention and adoption of cashless payment methods among the young adults in malaysia. *Journal of Science and Technology Policy Management*, 2022.

[38] Kristin Paget. Credit card fraud: The contactless generation. *ShmooCon*, 2012.

[39] Gary Pritchard, John Vines, and Patrick Olivier. Your money's no good here: The elimination of cash payment on london buses. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pages 907–916, 2015.

[40] Prolific. Prolific, quickly find research participants you can trust. https://www.prolific.co, 2023. Accessed: 15 May 2023.

[41] Andreea-Ina Radu, Tom Chothia, Christopher J.P. Newton, Ioana Boureanu, and Liqun Chen. Practical emv relay protection. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1737–1756, 2022.

[42] Sazzadur Rahaman, Gang Wang, and Danfeng Yao. Security certification in payment card industry: Testbeds, measurements, and recommendations. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 481–498, 2019.

[43] Michael Roland and Josef Langer. Cloning credit cards: A combined pre-play and downgrade attack on EMV contactless. In *7th USENIX Workshop on Offensive Technologies (WOOT 13)*, Washington, D.C., August 2013. USENIX Association.

[44] Samsung. Samsung pay: A better wallet, already in your hand. https://www.samsung.com/uk/samsung-pay/, 2023. Accessed 15 May 2023.

[45] Aleksandr Shevelev. NFC reader. https://play.google.com/store/apps/details?id=info.iso8583.nfcreader&hl=en&gl=US&pli=1. Google Play Store.

[46] Wesam Shishah and Soha Alhelaly. User experience of utilising contactless payment technology in saudi arabia during the covid-19 pandemic. *Journal of Decision Systems*, 30(2-3):282–299, 2021.

[47] Smasung. Set up your samsung pay transit card. Available at https://www.samsung.com/au/support/mobile-devices/samsung-pay-transit-card-setup/. Accessed 11 January 2023.

[48] Square. Square card reader. Available at https://squareup.com/gb/en. Accessed 11 January 2023.

[49] Sumup. Sumup card reader. Available at https://www.sumup.com/en-gb/. Accessed 11 January 2023.

[50] Aleksei Stennikov Timur Yunusov, Artem Ivachev. New vulnerabilities in public transport schemes for apple pay, samsung pay, gpay. *White Paper*, 2021.

[51] UK Finance. Annual fraud report 2024, 2024. Accessed 10 March 2025.

[52] UK Finance. Payment markets summary 2023, 2024. Accessed 14 March 2024.

[53] Jordi van den Breekel. Relaying emv contactless transactions using off-the-shelf android devices. *BlackHat Asia, Singapore*, 2015.

[54] Aditya Vashistha, Richard Anderson, and Shrirang Mare. Examining the use and non-use of mobile payment systems for merchant payments in india. In *Proceedings of the 2nd ACM SIGCAS Conference on Computing and Sustainable Societies*, pages 1–12, 2019.

[55] Vidushi Vatsa and Bhawna Agarwal. Factors impacting adoption and continuous use of contactless digital payments in the new normal. *International Journal of Electronic Finance*, 11(4):317–344, 2022.

[56] John Vines, Paul Dunphy, Mark Blythe, Stephen Lindsay, Andrew Monk, and Patrick Olivier. The joy of cheques: trust, paper and eighty somethings. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work*, pages 147–156, 2012.

[57] Visa. Visa, a trusted leader in digital payments. https://www.visa.co.uk/, 2023. Accessed: 15 May 2023.

[58] Timur Yunusov. Hand in your pocket without you noticing: Current state of mobile wallet security. *Black Hat Europe*, 2021.

[59] Qingyu Zhang, Salman Khan, Mei Cao, and Safeer Ullah Khan. Factors determining consumer acceptance of nfc mobile payment: An extended mobile technology acceptance model. *Sustainability*, 15(4):3664, 2023.

[60] Yongping Zhong and Hee-Cheol Moon. Investigating customer behavior of using contactless payment in china: A comparative study of facial recognition payment and mobile qr-code payment. *Sustainability*, 14(12):7150, 2022.

8. Appendix

8.1. User Study Survey Template

8.1.1. Introduction and Consent. Welcome, and thank you for participating in our research study. Our aim is to explore user perspectives on contactless payment, understanding its usage, perceived security risks, and protective measures. Before proceeding, please be aware of the following:

- This study is entirely voluntary. You may withdraw at any point by closing your browser.
- We collect minimal personal data, such as demographic information and Prolific IDs to manage participation and compensation and to ensure response quality.
- Your data will be securely stored, accessible only to our investigators for scientific analysis. The findings might be shared at conferences or in publications.
- The study has received approval from the University of [anonymous] research ethics committee.

Section 2 of this survey may make you think about potential fraud risks associated with contactless payment. If this causes you to worry, you can take the protective actions provided at the end of the survey to enhance the security of your contactless payments. For any questions or concerns, please contact [anonymous].

8.1.2. General Knowledge and Preferences. [This section includes general questions about your contactless payment.]

1.1. How well do you know contactless payment? [I've Never heard of it, I've Heard of it but don't know what this is, I know what this is, but don't know how it works, I know generally how it works, I know very well how it works.]

1.2. In your own words, explain how contactless payment works. [long-answer text box]

1.3. Have you used contactless payment in the past six months? [Yes, No, I don't remember]

1.4. How often do you use contactless payment? [Several times a day, One or two times a day, One or two times a week, One or two times a month, Never]

1.5. Which of the following contactless payment devices do you use? (Select all that apply) [Contactless credit or debit card, Mobile contactless payment (e.g. Apple Pay, Google Pay), Wearable contactless payment (e.g. Smartwatch, Smart jewellery, accessories, etc.), other]

1.6. What do you like about contactless technology? (Select all that apply)

[It is fast, It is convenient, It is secure, other]

1.7. What do you dislike about contactless technology? (Select all that apply)

[Technical issues (e.g. connectivity problems, device compatibility), Lack of familiarity with the technology, Concerns about security or fraud, Its maximum payment cap, other]

1.8. How often have you used the "Express Transit" mode in a contactless transaction to buy tickets on Transport For London (TFL)? (when you do not need to wake or unlock your device or authenticate with Face ID, Touch ID, or your passcode)?

[Never, Almost Never, Occasionally, Frequently, Always]

1.9. If you have used the "Express Transit" mode, please share your experience with it and any opinions and concerns you may have.

[Long-answer text paragraph]

1.10. How important is it to you that businesses (shops, cafes, etc.) offer contactless payment options?

[Not important, Somewhat important, Very important]

1.11. Have you ever used a contactless method to withdraw cash from an ATM?

[Yes, No]

1.12. Would you be interested in using a contactless card or digital wallet to withdraw cash from an ATM in the future?

[Yes, I am interested, No, I prefer the traditional card and PIN method to withdraw cash, I am unsure/neutral]

8.1.3. Perception on Contactless Payment Security. Description: Contactless technology allows users to make payments by simply tapping their contactless-enabled devices, like cards, smartphones, or wearable, close to a contactless reader. It uses Near Field Communication (NFC) technology, which enables the transfer of data over short distances through the air. NFC has a range of a few centimeters, ensuring that payment information is only transmitted to the intended recipient. During a contactless payment, the payment device sends transaction data to the nearby terminal using NFC. The terminal then forwards the information to the bank for authorization. The bank reviews and approves or rejects the payment, notifying the terminal of the decision. This section focuses on attacks targeting contactless payment methods. Please read each attack description carefully before answering the related questions.

2.1. How concerned are you about the general security and privacy of your contactless payments?

[Very Concerned, Concerned, Neutral, Not Concerned, Not At All Concerned]

2.2. How secure do you think each contactless payment method is?

[Table with a list of payment devices in the rows Contactless credit/debit card, Mobile Devices (e.g., Apple Pay, Google Pay), Wearable Devices (e.g., Smartwatch) and familiarity level in the columns (Very Secure, Secure, Neutral, Not Secure, Not At All Secure)

2.3 to 2.14: asks users to what extent they think each of the following six attacks is feasible (Feasible, Somewhat Feasible, Not Feasible) and how concerned they are about each attack in particular (Very Concerned, Concerned, Neutral, Not Concerned, Not At All Concerned)

A) Eavesdropping Attack: Attackers utilize different techniques to gain unauthorized access to sensitive information from contactless payment cards. This includes extracting crucial data such as the Primary Account Number and expiry date, which subsequently compromises the overall security and confidentiality of the cardholders' personal and financial data.

[Example included from Table 3.]

B) Relay Attack: Although the typical NFC range is limited to a few centimeters, it is possible to extend this range significantly. Attackers can intercept and relay payment information between a payment card and a distant terminal, utilizing two devices. The initial device captures payment data and transmits it to the second device, which then relays it to the payment terminal, allowing attackers to make unauthorized transactions in real-time without users' knowledge.

[Example included from Table 3.]

C) Pre-play Attack: Attackers record payment information during a legitimate transaction, preserving it for future fraudulent activities. By compromising the payment terminal, they intercept and store the payment data without the user's awareness, enabling them to conduct fraudulent transactions at a later time. This attack is difficult to detect during a legitimate transaction, as the payment terminal appears to function normally.

[Example included from Table 3.]

D) Counterfeit Card Replica Attack: Attackers intercept and extract all the magnetic stripe data from a physical payment card, like a credit or debit card, either through the NFC interface or by swiping the card, and subsequently store the information for later use in creating a replicate by writing it onto a blank magnetic stripe card that can be used later for fraudulent activities.

[Example included from Table 3.]

E) Contactless Payment Limit Bypass Attack: Attackers exploit the contactless transaction limit to steal money by surpassing the set limit. In the UK, where the current limit is £100 for a single contactless payment without a PIN, attackers initiate a payment to the victim's payment device. Using specialized equipment, typically smartphones, they manipulate the payment information during the transaction and authorize high-value contactless transactions without requiring a PIN.

[Example included from Table 3.]

F) Lock-screen Bypass Attack: Attackers exploit the "transit mode" feature in lock-screen payment devices (e.g., smartphones), which is designed for convenient fare payment on public transport without requiring unlocking the phone. By bypassing the lock-screen, they carry out unauthorized transactions without the victim's knowledge. This can occur through close proximity, specialized equipment, or terminal compromise.

[Example included from Table 3.]

2.15. How concerned are you about the general security and privacy of your contactless payments?

[Very Concerned, Concerned, Neutral, Not Concerned, Not At All Concerned]

8.1.4. Protective Actions.

[Description: This section covers protective actions for contactless payments.]

3.1. How do you monitor your payment activities and account(s)?

[Online banking on PC or laptop, Mobile banking app, keeping and checking purchase receipts, Someone else does it for me (parent, partner, lawyer, etc.), Other]

3.2. What measures do you take for your contactless payment security and privacy?

- I use RFID-blocking wallets or card sleeves,
- I am cautious when using contactless payment in unfamiliar or untrusted environments,
- I disable the "express transit" feature on my smartphone/smartwatch if not using it,
- I switch off the NFC sensor on my mobile phone,
- I limit the maximum I can spend (spread over multiple payments) before I need to enter my PIN in online or mobile banking,
- I limit the maximum transaction amount for contactless payment to a single tap in online or mobile banking,
- I do not carry cards or add cards to my digital wallets with lots of funds,
- I'd ask the bank if they can issue a card without a contactless feature,
- I switch off contactless transactions entirely through settings in online or mobile banking,
- I enable passive acknowledging of transactions (such as SMS notifications, bank calls, etc.),
- I check my bank receipts and bank accounts regularly,
- I ask to receive a monthly paper statement and review it in detail,
- Nothing,
- Other: ———-

3.3. What are other actions that you think are effective in protecting your contactless payment security and privacy?

[Long-answer text paragraph]

8.1.5. Demographic Data, Feedback, and Compensation.

Questions about age, gender, the highest level of education, and users' feedback is asked, and a code for compensation is provided to be claimed on Prolific [40].