

VISA

How Consumers are Embracing Security Measures in the Era of Digital Payments

Insights from Visa's Stay Secure Study 2025



Table of Contents



Executive Summary	3
Key Findings	4
Falling for Scams: Once Bitten, Twice Shy	5
Spotlight: Friends, Family Seen as More Susceptible to Scams	6
On the Lookout for Bad Actors and Fraudsters	7
Taking Precautions to Secure Payments	8
Digital Payments Increasingly Gain Traction	9
Building Trust in Digital Payments	10
Spotlight: Consumers Take Comfort in Digital Payments	11
Conclusion	12
Methodology	13

Executive Summary



Online scams are prevalent around the world, prompting consumers to be on alert for phishing attempts and other schemes that put their financial stability at risk amid growing adoption of digital payments.

To better understand consumer awareness and behaviors around fraud, **Wakefield Research, commissioned by Visa, conducted a survey of 5,800 adults across the CEMEA region (17 markets in Africa, Eastern Europe and the Middle East).**

The research reveals that **97% consumers** in these markets have taken **cautionary measures around digital payments**, such as ignoring requests via email and other means asking them to transfer money on someone else's behalf and setting up text messages to notify them of transactions.

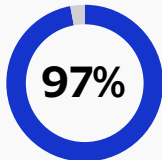
97% also consider themselves knowledgeable when it comes to recognizing fraud and scams, versus 92%* in 2023. This increase indicates that consumers across the CEMEA region are becoming increasingly savvy when it comes to recognizing fraudulent activity. This growing awareness offers hope as online scams grow in sophistication and frequency. It is also crucial given the growing adoption of digital payments across the region - 74% of consumers anticipate using digital payments more in the coming 12 months.

When it comes to falling victim to fraud, the research shows that consumers are most likely to respond to potential scam emails that warn of a security risk, such as a stolen password or data breach (39%) or a notice that their credit card has been blocked (35%). They are also vulnerable to the allure of a financial opportunity, such as a good deal (33%). When this question was asked in 2023, 44%* were likely to click on a financial opportunity, indicating that industry efforts to educate consumers about scams could be yielding dividends. Those likely to act on messages commonly used by scammers, including clicking on a link or responding to the sender has also decreased since 2023, from 90% to 86%.

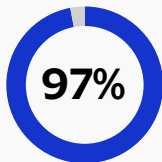
Across all markets, consumers have embraced digital payments, and the research shows there is high trust, with 76% confirming they mostly or completely trust digital payments.

This report outlines the survey's key findings across seven key themes.

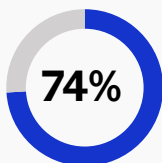
Key Findings



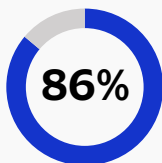
have taken **precautions** to **secure payments**



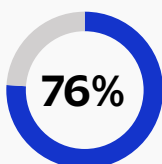
consider themselves **knowledgeable** when it comes to recognizing **fraud and scams**



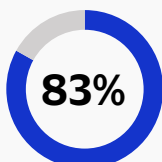
anticipate using **digital payments** more in the coming **12 months**



are likely to act on **messages commonly** used by scammers, including **clicking on a link or responding to the sender**



mostly or completely **trust digital payments**

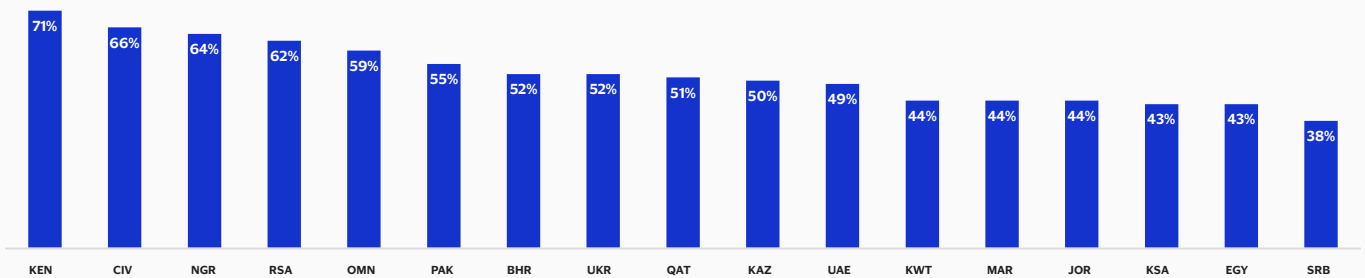


feel more secure making online payments when they're required to enter a texted code or click on a link from the vendor to confirm their identities

Falling for Scams:

Once Bitten, Twice Shy

Reliance on digital payments is on the rise around the world as the adoption of these payments continues to rapidly grow. As we look ahead, the future of payments is increasingly digital, with 74% of consumers anticipating that they will use digital payments more in the coming 12 months. Unfortunately, digital payment scams are also prevalent and often successful. More than half of consumers across **17 markets (52%) have previously fallen for a scam, compared with 52%* in 2023.** In fact, an unfortunate 16% have been victims on multiple occasions.



Q: Have you ever been the victim of a scam? - % Yes Shown

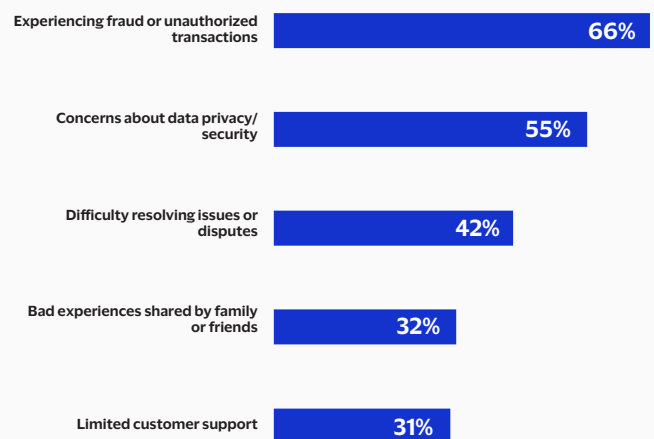
Consumers in Sub-Saharan Africa (66%) are the most likely to admit being a victim, **with the largest number in Kenya (71%).** This suggests that **Kenyans have more experience** than some of their neighbors with schemes such as smishing, which involves fraudulent text messages targeting data extraction, in what appears to be an especially active market for fraudsters.

Across countries, the impact of these scams is significant for consumer confidence and loyalty, with a majority (66%) believing that experiencing fraud or an unauthorized transaction would reduce their trust in digital payments. Yet, it is noteworthy that among those who have been a past victim of a scam,

75% mostly or completely trust **digital payments**

76% nearly equal to the level of trust of those who have never fallen for fraud (76%).

Q: Which of the following would reduce your trust in digital payments?





Spotlight:

Friends, Family Seen as More Susceptible to Scams



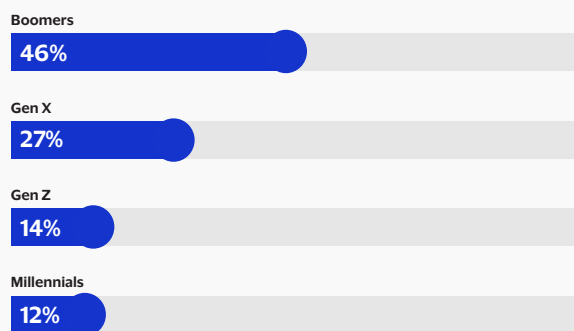
While consumers have some degree of confidence in their own ability to spot fraud, they worry more about those closest to them.

Almost all (95%) believe their friends or family would fall for a potential scam, especially if it's a text message asking them to verify account information (57%). When the same question was asked in 2023, 96%* said they believed their friends or family would fall for a potential scam.

Consumers in Ukraine (67%) are the most concerned their friends or family would respond to a sham text message requesting account verification, while in Kuwait only 48% think their loved ones would react.

Across the regions, 86% believe that Gen X (44-59 years old) digital payment users are most likely to get scammed online – with even Gen X consumers themselves choosing their own generation as the most susceptible (84%).

Q: Who is most likely to fall victim to online scams?

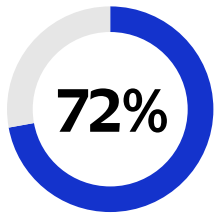


Meanwhile, nearly 9 in 10 Gen Z consumers (89%) admit they are likely to act on suspicious communication, significantly higher than Millennials (85%), Gen X (85%), and Boomers (80%). Gen Z would most likely be fooled by a message about a security risk, such as a stolen password or data breach (40%).

* Data from published 2023 Visa Report, Stay Secure Visa's Study - Uncovering How and Why Consumers Fall for the Language of Fraud, 2024

On the Lookout for Bad Actors and Fraudsters

Consumers are very much on guard for suspicious communications via email or text message that could be traps set by scammers set on stealing some of their hard-earned cash.



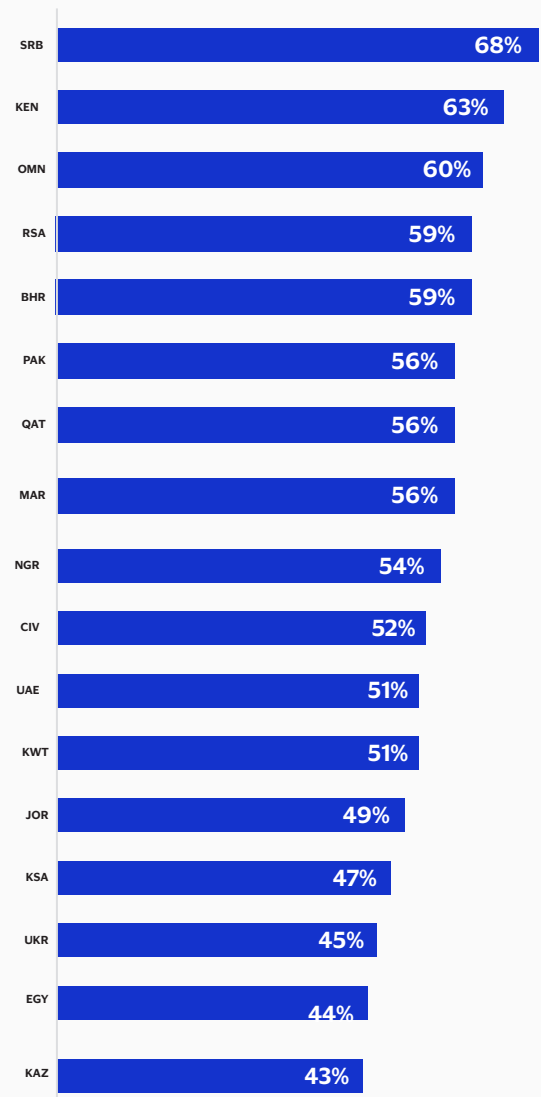
The biggest red flag that a message is coming from a fraudster is a request to reset a password or account information because of a potential data breach, with 72% ranking that communication among the top three most suspicious communications they receive.

The good news: awareness that this type of message is a scam is improving. When this question was asked in 2023, 69%* ranked it among their top three. These messages raise an even higher alarm for consumers in Sub-Saharan Africa (SSA) and the Commonwealth of Independent States and South and Eastern Europe (CISSEE), 78% of whom ranked these requests among the three most-suspicious messages they might receive.

Notices regarding problems with an order, subscription, or account (55%) also raise alarms, with CISSEE consumers (61%) once again more wary compared to other regions. Ukraine (67%) stands above all others in skepticism about these notices. Notifications that the consumer has received a reward, coupon or gift card also raise eyebrows (55%), with that caution rising to over two thirds for consumers in CISSEE (67%), in particular those from Serbia (72%) and Ukraine (69%).

And for a majority (53%), news of cyber fraud such as data breaches and email scams have led them to reduce their use of digital payments. Consumers in Serbia are especially discouraged (68%) by news of cyber fraud.

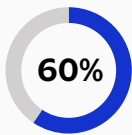
Q: How much has news about cyber fraud (e.g., data breaches, email scams, phishing, etc.) impacted your use of digital payments?
- % Reduce Use Shown



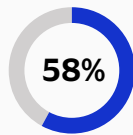
Taking Precautions to Secure Payments

Amid so much risk, it's best to take precautions. **Nearly all consumers (97%) have acted cautiously, refraining from sharing their card or account credentials (58%) and not responding to emails asking them to transfer money on someone else's behalf (60%).** Many have proactively adopted measures to secure payments, such as setting up text message alerts (48%) to notify them of account transactions.

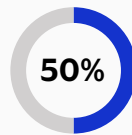
Q: What measures have you taken to secure your payments?



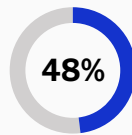
Avoid responding to emails/calls requesting money transfers on someone else's behalf



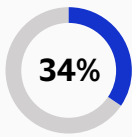
Refrain from sharing my card or account credentials with others



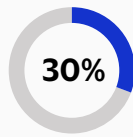
Regularly monitor my bank and credit card statements for suspicious activity



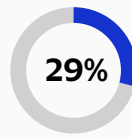
Set up text message alerts to notify me of account transactions



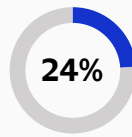
Customize notifications on my accounts by transaction amount, type, or category



Set custom spending limits or budgets



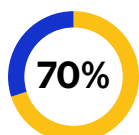
Use virtual credit card numbers for online transactions



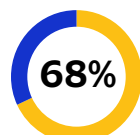
Resort to cash payments instead of digital transactions

Amid an onslaught of scam attempts, consumers in the SSA region are more proactive when it comes to safeguarding their savings: 71% refrain from responding to requests via email and other means asking them to transfer money on someone else's behalf and 67% refrain from sharing their card or other account credentials.

Once again, Kenya is an outlier:



monitor their **bank and credit card** statements for suspicious activity

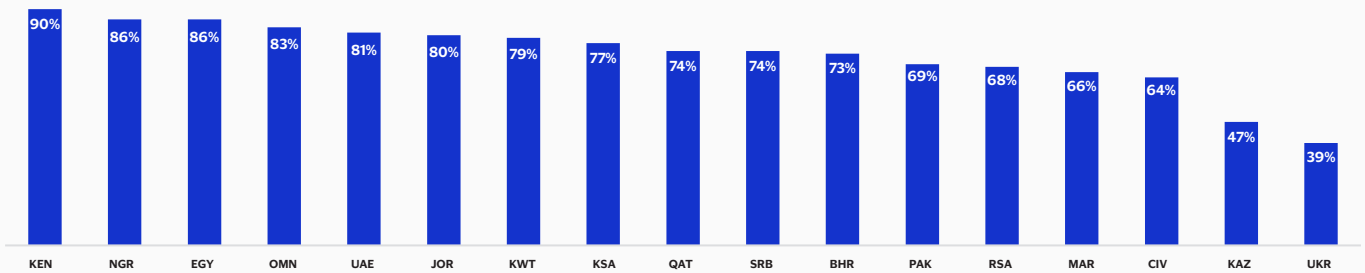


and set up text message alerts to notify them of transactions in their account(s).

Across the markets, nearly a quarter of consumers have resorted to cash payments in an effort to safeguard their transactions.

Digital Payments Increasingly Gain Traction

Consumers have embraced digital payments in all 17 markets, **where three-out-of-four anticipate using digital payments more in the coming 12 months.** They use a variety of methods, the most common of which is bank transfers via a mobile banking application or platform (62%), which has made their lives easier.

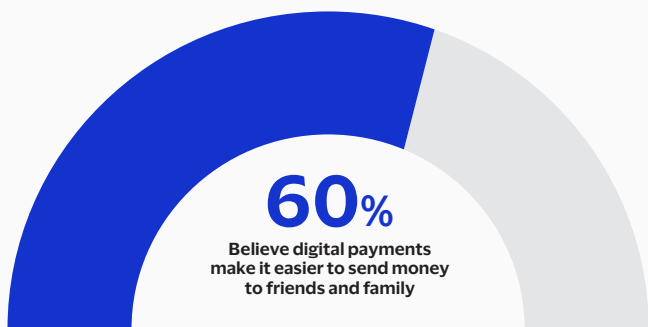


Q: Looking ahead, do you expect that you will use digital payments more, less, or exactly the same in the next 12 months? - % More Shown

There's a clear preference among the types of digital payments that consumers are gravitating towards. The vast majority (85%) report using e-commerce payment methods such as credit or debit card payments online (54%) and mobile payments through smartphone apps or QR code (49%). UAE (67%) and Ukraine (67%) are the top two markets that use credit or debit cards to make payments online, while mobile payments via smartphone app are most likely to be used by consumers in the Kingdom of Saudi Arabia (66%), Bahrain (66%), and Kazakhstan (66%).

Growth in digital payments comes with many benefits. **Consumers across the markets view these types of payments as quicker and simpler than other methods (70%) and appreciate that they allow them to make payments anytime, anywhere (68%).**

Q: How have digital payments impacted your daily life?



Importantly, **60% believe digital payments make it easier to send money** to friends and family, especially for consumers in

Kenya

75%

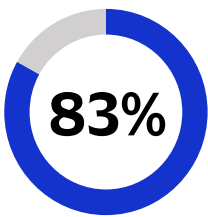
and Nigeria

74%

Remittances from abroad are a major source of income in both countries, and a lifeline to needy families, reinforcing the need for secure payments.

Building Trust in Digital Payments

As digital payments grow in use and popularity, there are steps that retailers, banks and payments processors can take to promote even greater trust. This includes requiring shoppers to enter a code they receive via text message or to click on a link to confirm a purchase or attach a security badge, symbol, or other icon to digital transactions.



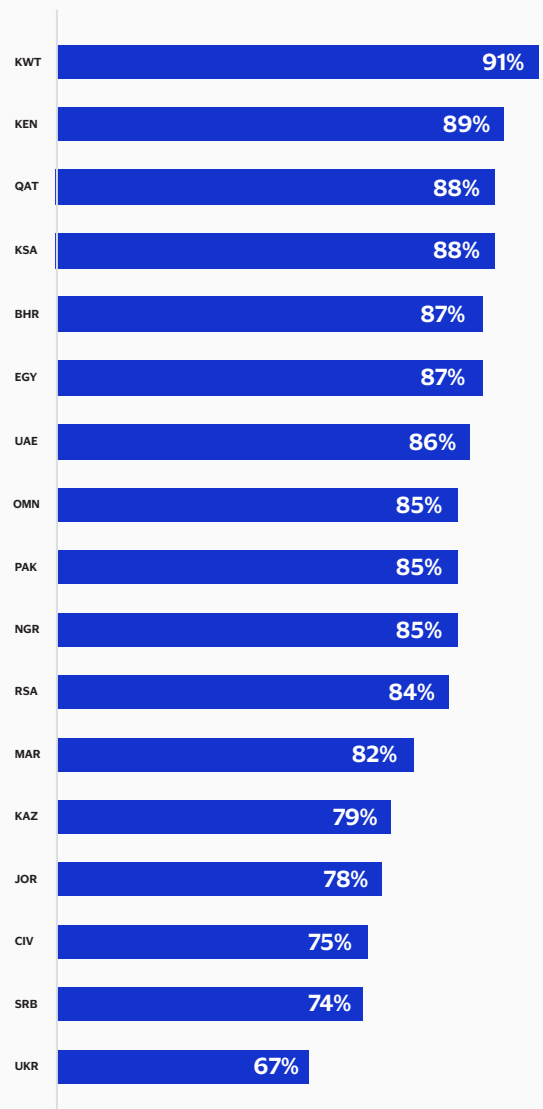
Across the markets, consumers who use digital payments feel markedly more secure (83%) making online payments when they're required to enter a texted code or click on a link from the vendor to confirm their identities.

Consumers are also reassured when they see security badges, symbols, or icons from trusted companies while shopping online (48%).

Government efforts to introduce digital payments for disbursements or citizen programs may also instill confidence by partnering with well-known brands. When it comes to payment programs run by governments in the UAE, Ukraine, or Nigeria - such as instant payments and local cards - consumers are more likely to trust those payment methods or schemes when they partner with a well-known brand (83%), like Visa.

This confidence in payment programs is influenced by both consumers' knowledge of scams and their recognition of trusted brands. Among consumers who consider themselves very knowledgeable in recognizing fraud and scams, 51% are much more likely to trust government-run payment programs if they partnered with a well-known brand.

Q: When making online payments, how much more secure do you feel when you're required to enter a texted code or click on a link from the vendor to confirm your identity?





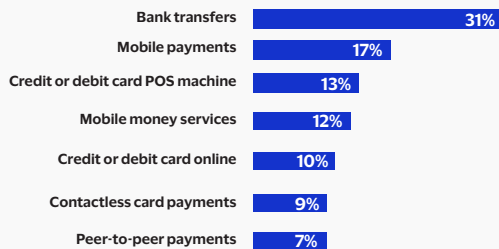
Spotlight:

Consumers Take Comfort in Digital Payments

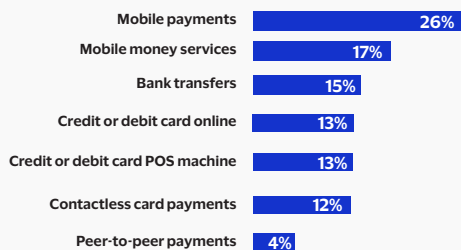


Mobile payments are seen as one of the two safest and most secure digital payment methods, with trust in mobile payments running especially high in **Cote d'Ivoire**, where **74% view this as their safest digital payment option**. **Mobile payments (55%) are also seen as the easiest digital payment method**.

Q: Which digital payment methods are the safest and most secure? - % Ranked 1st Shown



Q: Which digital payment methods are the easiest to use? - % Ranked 1st Shown



Across markets, **49% view mobile payments as the second-safest digital payment option**, and although a third of adults use peer-to-peer payments (33%), they are least likely to rank this option as the safest and most secure digital payment option.

The most-frequently used methods of payment are not necessarily the easiest to use. **Though 62% of respondents use bank transfers**, as in payments made via mobile banking apps or platforms, **only 15% consider bank transfers as the easiest payment option**. The same applies for credit and debit card payments made online, **which are used by 54% of respondents even though only 13% chose that option as their easiest digital payment method**.

Conclusion



Consumers across 17 countries in Africa, the Middle East and Eastern Europe have embraced digital payments to make their lives easier and anticipate using these payments even more in the future. This deepening comfort with digital payments, however, is being shadowed by a proliferation of scams as fraudsters target a growing pool of money. Additionally, the rise in fraud is fueled by the sophistication of new threats, such as AI-driven attacks, including deep fakes and social engineering. Fortunately, consumers are increasingly savvy when it comes to identifying and disregarding phishing attempts.

Even though most consider themselves knowledgeable of the many ways that fraudsters try to steal their money, more than half of consumers (52%) across the 17 markets have previously fallen for a scam. This includes 16% who have fallen victim on multiple occasions. The prevalence and prowess of scams has prompted consumers to take measures to protect themselves when transacting online.

The vast majority of adults (76%) mostly or completely trust digital payments for making transactions, so there is a significant opportunity to deepen that trust and bridge the gap for those who remain skeptical. Trust is hard earned and easily lost, which is why consumers need to be equipped with knowledge and tools to avoid falling prey to a scam.

Even though most consider themselves knowledgeable of the many ways that fraudsters try to steal their money, more than half of consumers (52%) across the 17 markets have previously fallen for a scam. This includes 16% who have fallen victim on multiple occasions. The prevalence and prowess of scams has prompted consumers to take measures to protect themselves when transacting online.



Methodology Statement

* The 2024 Visa Stay Secure III Survey was conducted by Wakefield Research among 5,800 adults ages 18+ in 17 markets: Ukraine, Kazakhstan, Serbia, South Africa, Kenya, Nigeria, Côte d'Ivoire, Egypt, Morocco, Pakistan, Jordan, UAE, Qatar, Kuwait, KSA, Bahrain and Oman, between December 4th and December 15th, 2024, using an email invitation and an online survey. Quotas were set for 300 respondents per market, except in Egypt (600), Pakistan (500), and Nigeria (500). Data has been weighted.

The 2023 survey was conducted among the same audience in 17 countries but included Tunisia rather than Jordan.

