STAY SECURE

Visa's Study – Uncovering How and Why Consumers Fall For The Language of Fraud.

Table of Contents

Foreword

Security is Visa's Top Priority

In today's digital-first world, eCommerce platforms and online marketplaces have become destinations of choice for consumers. The abundance of options, speed and convenience, as well as secure and seamless payment methods, have delivered next-level experiences at our fingertips.

However, digital acceleration also opened the door to bad actors. There is an urgent requirement to raise awareness of increasingly sophisticated fraudsters who are using new approaches and persuasive tactics to trick unsuspecting consumers.

At Visa, we strive to protect people from payment fraud and strengthen their ability to spot scams and transact with the highest level of trust, safety and confidence.

In partnership with Wakefield Research, Visa conducted a survey among 5,800 adults in 17 countries across Central and Eastern Europe, the Middle East and Africa (CEMEA) to assess consumer knowledge about the language of fraud. It examines their ability to spot a scam and understand the likelihood of consumers falling for fraudulent text and email messages.

Summary

Costly Confidence:
How Online Scams and Judgement Collide

The Visa Stay Secure Study found a disconnect between consumers' confidence in recognizing fraud and their online behavior, reflecting a tendency to put themselves at risk.

While over half of the respondents (56%) consider themselves very or extremely knowledgeable when it comes to recognizing fraud and scams, 90% would click on links or return messages that routinely act as vehicles for these types of malicious behaviors.

To overcome the discrepancy, the Visa Stay Secure Study explores the most common phrases to understand what lures victims and why. The Study data identifies persistent blind spots and finds that consumers are highly responsive to unsolicited texts, emails or messages offering free gifts, creating a sense of urgency, or requiring action.

The Visa Stay Secure Study also reveals that over half of respondents (52%) have been a victim of a scam at least once. Even more alarming is that 15% of this group have been tricked multiple times.

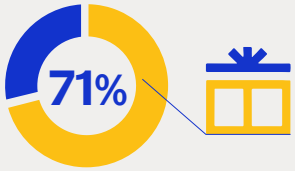
The Visa Stay Secure Study
Key Findings

56%

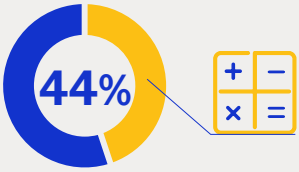
Consider themselves **very or extremely knowledgeable** when it comes to recognizing fraud and scams

90%

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



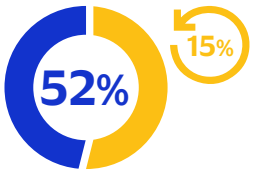
Would **take action** if the message had positive phrases: “free gift”, “you’ve been selected”, “claim your prize”, or “you are a winner”



Would **click** on a link or **reply** to a message that offered a **financial opportunity**

1 in 2

52% are concerned their friends or family may fall for a scam email **offering a free gift**



Over half were previously a **victim of a scam**, including **15%** who have been scammed **multiple times**

Section 1:
What Makes Us Click

In Online Scams, the Majority Are Prone to Taking the Bait

Most Enticing Messages Promise Financial Opportunities

The objective of any scam is to appear legitimate at first glance – especially when online messaging is viewed so quickly that a glance is all a recipient gives it. Scammers attempt different approaches to crafting messages that appear genuine, most notably with the content. They're looking to entice or compel recipients to take immediate action, like clicking on a link, opening an attachment, or responding to a sender. Unfortunately, several different types of these messages can and have been quite effective.

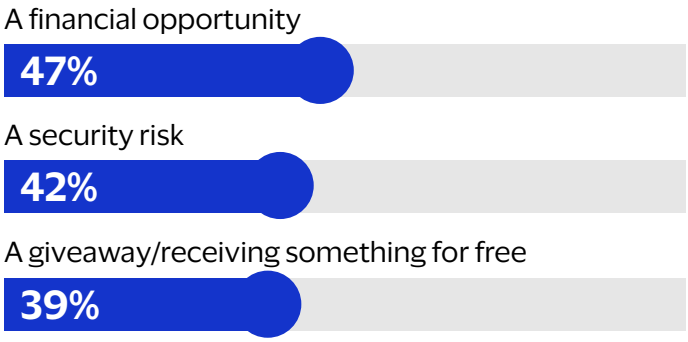
Offers of easy money, a free gift or even threat of a data breach are designed to pique the interest of the recipient. The problem is most consumers might take the bait. **The vast majority (90%) in these 17 markets are likely to act on messages commonly used by scammers, including clicking on a link or responding to the sender.**

The most common message that would spur action is a financial opportunity, with 44% of respondents saying they'd click on that link or reply to the sender.

While all of these communications may not be illegitimate, overconfidence in recognizing scams can leave the recipient of the message more vulnerable than they may think, even among those who have fallen victim before.

In fact, for those who previously have been defrauded by scams, financial opportunities are the top draw (47%). Similarly, this carries over to the messages alerting to a security risk, which they tend to trust (42%). They are also more likely to act on a message with a giveaway or receiving something for free (39%).

Communications Most Likely to Act on Those Who Have Been Victims of a Scam

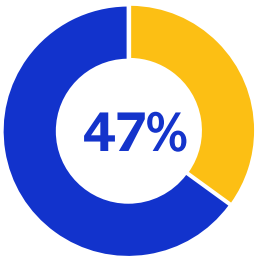


Age, Confidence Level, and Crypto Use May be Linked to Vulnerability

Gen Zers across all 17 markets are less likely to act on a notice from the government (31%, compared to 36% overall). But these same respondents are more likely to act on a giveaway (39%, compared to 35% overall). Meanwhile, older respondents (Gen X and Boomers) in these markets are more likely than their younger counterparts to act on a notice about their taxes (30% and 34%, respectively.) This compares to 25% overall who are more likely to act on such notices.

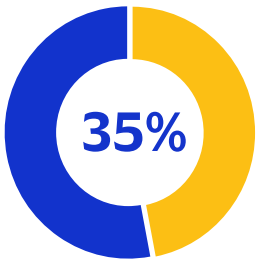
This likelihood of responding to official-looking messages is true even among those who are possibly among the most tech-savvy. In what is perhaps a reflection of confidence, those who use cryptocurrency for purchases are more likely to act on a giveaway (47%) than those who don't (35%).

Most Likely to Act on a Giveaway Among Those Who Use and Don't Use Cryptocurrency



Those who use cryptocurrency

VS



Those who don't use cryptocurrency

Section 2:
Stirring Suspicions

Consumers are Most Suspicious of Requests Involving passwords, in Addition to Notices involving Orders, Product Offers, or Feedback

Some seemingly innocuous messages promising no rewards or opportunities can leave consumers even more vulnerable than overtly enticing ones. For example, 34% of surveyed ranked requests to reset their password as the communication they are most suspicious of. Nearly 7 in 10 (69%) ranked such requests among the top 3 most suspicious. Among the types of communications seen as less suspicious were updates regarding a delivery or shipping(42%) and ;marketing communications regarding a sale or new product offering (41%).

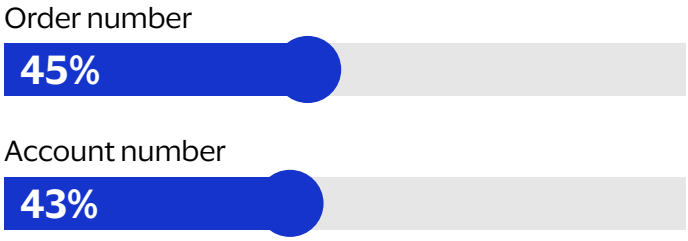
Nearly 7 in 10 suspicious of requests involving password

or an invitation to provide feedback on their recent experience (37%).

When suspicious, many take steps to verify offers, links, or requests for information, with more than half look for a valid email address (57%) or a company name/logo attached to the message (52%) to confirm legitimacy, even though these can often be spoofed.

Another effective hook used by scammers are account and order numbers, which don't require the graphics expertise of, say, a phishing email. **Though fraudulent account and order numbers might expose a scam, fewer than half look for an order number (45%) or an account number (43%).**

What People Look for in a Message to Confirm It's Legitimate



Spotlight: The Lure of Something for Nothing

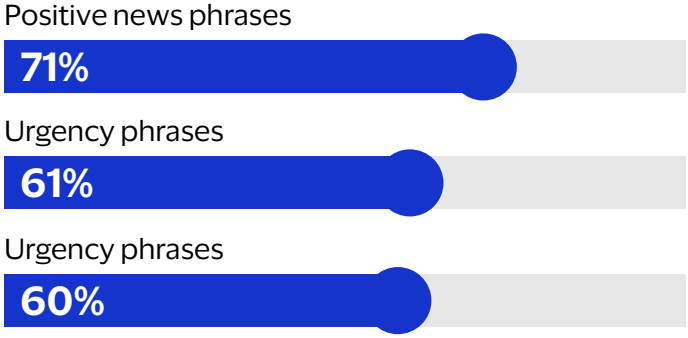
In the digital world, the "If it's too good to be true" dictum is one worth heeding, no matter how convincing a message seems. Phrases that convey urgency, **like "Urgent", "Open now", or "48 hours only", would prompt 60% of respondents into action.**

Reacting to several different phrases meant to spur action, most respondents (71%) said they would act on positive news phrases like "free gift", "you've been selected", "claim your prize", or "you are a winner."

In this case, as in others, over-confidence can cause problems.

Those who consider themselves more knowledgeable are more likely to respond to a requested action for each of these compared to those who say they are less knowledgeable, including for phrases indicating positive news (74% to 67%) or phrases conveying urgency (65% to 55%).

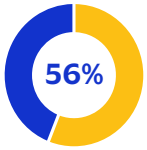
Phrases That Typically Prompt a Response to a Specific Action



Section 3:
Costly Confidence

The Majority of Respondents are Confident in Their Own Knowledge and Ability to Identify Scams, which put them at Greater Risk

Over half respondents in these 17 markets (56%) consider themselves very or extremely knowledgeable when it comes to recognizing fraud and scams.



Over half of consumers consider themselves very or extremely knowledgeable

But considering themselves knowledgeable may make people even more vulnerable, as false confidence can propel someone to click on a fake link or respond to a scam offer. **Of the 56% who consider themselves very or extremely knowledgeable about online scams, 92% of them say they would act on at least one type of message or offer, compared to 88% of who admitted to being somewhat knowledgeable or less. Specifically, those who claim to be most knowledgeable are more likely to act on messages about a security risk (42% vs 37% of somewhat or less knowledgeable), a notice from the government or police (39% compared to 33%), and a giveaway or opportunity to get something for free (37% compared to 33%).**

Particularly for younger generations raised in a digital world, these feelings of confidence and mastery can play into scammers' hands. When it comes to online payments, those who use crypto currency consider themselves more aware of scams, at 64%, than respondents overall.

This includes nearly 3 in 10 (29%) who consider themselves "extremely knowledgeable", compared to 21% overall.

Interestingly, those who use crypto for payments are more likely to have been a victim of a scam (66%) and even multiple scams (31%). This may also indicate their heightened awareness of when they've been the target of a scam.

According to the Study, confidence in the ability to spot a scam, and the vulnerability it may bring, is highest in countries like Qatar (69%), Kenya (65%), South Africa (65%), Saudi Arabia (64%), and Nigeria (63%).

Despite high confidence among respondents across all 17 markets, over half of them (52%) say they've been the victim of an online scam, including 15% who say they've been tricked multiple times (another 5% aren't sure).

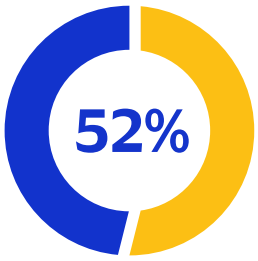
Over half of respondents say they've been the victim of an online scam

Section 4:

Other People's Money

People Worry About Vulnerability of Others More than Themselves

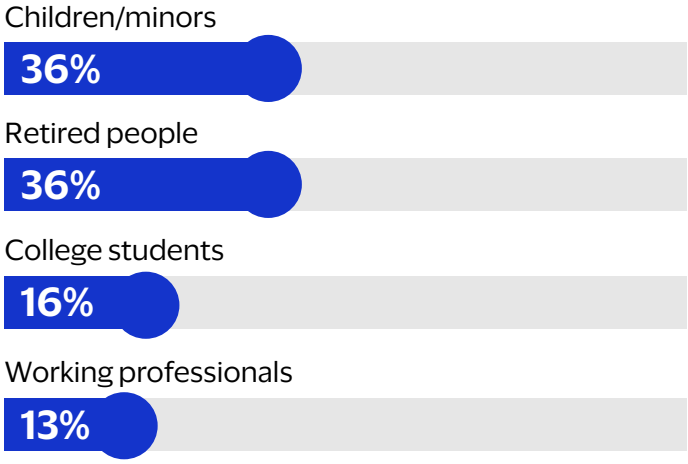
People are more worried about other people falling for scams than they are about themselves. **Despite their own proclivity to act on financial opportunities, more than half of respondents (52%) say they're concerned that their friends or family may fall for a scam email offering a free card or product from an online shipping site.** In a similar vein, 51% are concerned about friends or family falling for an investment scam including those involving cryptocurrency. And those who use crypto are more concerned for their family and friends (58%) than those who do not use it (50%).



More than half are concerned their friends or family may fall for a scam email offering a free gift card or product from an online shopping site

When it comes to falling prey to online scams, respondents are most concerned about children or minors (36%) and retired people (36%) falling prey to online scams. Just 13% think working professionals are the most likely to fall victim to scams, reflecting how over-confidence can make adults even more vulnerable.

Who is Believed To Be Most Likely to Fall Victim to Online Scams



Spotlight: Looking Out for Loved Ones

According to the Visa Stay Secure Study, respondents are particularly worried about their partners being conned. **More than half of respondents in a relationship or married (58%) are very or extremely concerned about their partner falling for a scam.**

Those who have previously fallen victim to a scam are much more concerned, 68% to 47%, which seems to indicate a recognition of how people may not realize how vulnerable they are.

Kenyans in a relationship are very or extremely concerned about their partner falling for a scam (83%), followed by Nigeria (77%), Pakistan (76%), Kuwait (70%), and the UAE (70%). Consumers in these countries may overlook how vulnerable they are, even as they are concerned for others.

Conclusion

STAY SECURE

Stopping Fraud in Its Tracks

Digital consumers surveyed across 17 markets in the CEMEA region increasingly rely on mobile apps, online shopping sites, e-mail and text updates, and offers. In fact, an overwhelming 96% shop online, while 45% use their credit cards to make an online purchase. While enabling seamless and secure consumer experiences, new platforms also open the door to emails, text updates, and other potentially fraudulent offers.

The Visa Stay Secure Study highlights the propensity for consumers to fall for fraudulent messages and provides a valuable foundation to understand why and how this happens.

The Study reveals that consumers' confidence in detecting scams appears to far outweigh their actual knowledge and ability to spot scams. More than half (56%) claim to be tech-savvy enough to sidestep online and phone scams. The reality is that nine out of ten (90%) are likely to disregard the warning signs that suggest criminal activity. Equally alarming is the finding that over half of all respondents (52%) admitted to being the victim of a scam at least once, while 15% have been conned multiple times.

The engine of fraud is primarily driven by persuasive language and increasingly sophisticated notifications. There is a need for digital consumers to be more vigilant of phrases such as "act now," "urgent," or "request for password verification." Advancements in payment security will continue to help drive down fraud. However, technology can only do so much. Consumer awareness and education are the critical first line of defense against criminal intent. As digital-first habits evolve, people must preserve the human quality of questioning and being curious.

The Visa Stay Secure Study is part of our continued efforts to ensure that individuals and organizations know the risks and can adequately safeguard themselves from attacks.

Methodology

The Visa Stay Secure Survey was conducted by Wakefield Research (www.wakefieldresearch.com) among 5,800 adults ages 18+ in 17 markets: UAE, KSA, Qatar, Kuwait, Oman, Bahrain, Egypt, Pakistan, Tunisia, Morocco, Nigeria, Kenya, S. Africa, Côte d'Ivoire, Kazakhstan, Serbia, and Ukraine, between March 31st and April 10th, 2023, 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.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 4.0 percentage points in Egypt, 4.4 percentage points in Pakistan and Nigeria, and 5.7 percentage points in the remaining markets from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

About Wakefield Research

Wakefield Research is a leading, independent provider of quantitative, qualitative, and hybrid market research and market intelligence. Wakefield Research supports the world's most prominent brands and agencies, including 50 of the Fortune 100, in 90 countries.

VISA

STAY SECURE