Visa study: Overconfidence exposes consumers to fraud risk

Over-confidence is leaving consumers in Central and Eastern Europe, the Middle East, and Africa (CEMEA) at risk of becoming victims of fraud, according to Visa's latest Stay Secure study.

Source: https://www.pexels.com/search/cybercrime/Pexels

Research across 17 countries revealed a disconnect between consumers' confidence in recognising fraud and their online behavior, highlighting the importance of staying alert and mindful of fraud attempts.

Despite more than half of consumers (56%) claiming to be savvy enough to sidestep online and phone scams, 90% are likely to disregard the warning signs that suggest online criminal activity.

With October designated as Cybersecurity Awareness Month, the study forms part of Visa's Stay Secure campaign, focused on raising consumer awareness, strengthening education, and building confidence to combat social-engineering threats.

The campaign aims to pave the way for a secure and seamless digital-payments experience. Through this initiative, Visa provides educational content, including videos, infographics, and tips designed to equip consumers with the knowledge and skills to recognise and prevent fraud.

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%). The study also found that most adults in Kenya (74%), Nigeria (72%), and South Africa (64%) report having been the victim of a scam or fraud. However, those in Tunisia (43%) and Morocco (33%) are the least likely to report this.

“In today’s digital-first world, scams are evolving in sophistication, with criminals using new approaches to trick unsuspecting consumers. Whether it’s a parcel held up at customs, a streaming subscription claiming to have expired, or a free voucher for a favourite brand, scammers are adopting persuasive tactics to deceive.

“Understanding the language of fraud is increasingly essential, and our Visa Stay Secure educational platform provides the knowledge and skills to help stay ahead of fraudulent activity online,” explains Irene Auma, head of risk for sub-Saharan Africa at Visa.

Key findings of the study

- **The knowledge gap.** Considering themselves knowledgeable might make people even more vulnerable, as false confidence can propel someone to click on a fake link or respond to a scam offer. Those who consider themselves more knowledgeable are more likely to respond to a requested action from scammers compared to those who say they are less knowledgeable, including positive news (74% to 67%) or urgent action (65% to 55%).

- **Concern for the vulnerability of others.** While respondents feel confident in their own vigilance, over half (52%) are concerned that their friends or families will fall for a scam email offering a free gift card or product from an online shopping site. Over a third (36%) of respondents are concerned about children or minors, as well as retired people falling prey to online scams.

#CybersecurityMonth: One question can keep you safe from phishing scams

10 Oct 2023

- **People's suspicion triggers.** In addition to notices involving orders, product offers, or feedback, people are most suspicious of password requests. Less suspicious types of communications are updates regarding delivery or shipping (just 42% listed as a top three source of suspicion), marketing communications regarding a sale or new product offering (41%), or an invitation to provide feedback on a recent experience (37%) - all of which can be used by scammers.Overlooking telltale signs.

Only 57% reported looking to ensure communications are sent from a valid email address, while 52% will check if the company name or logo was attached to the message. Fewer than half of correspondents look for an order number (45%) or an account number (43%). Only 33% look to ensure words are spelt correctly.

Decoding the language of fraud

Scammers try different approaches to craft messages that appear genuine and compel recipients to take immediate action. The Visa Stay Secure study identified prevalent patterns in the language most associated with scams – and how vulnerable respondents in the surveyed countries are.

- **Orchestrating urgency:** Cybercriminals often feign urgency to spur people into action, such as in the case of clicking a link or responding to a sender. Up to 40% of respondents will fall for messages about a security risk, such as a stolen password or a data breach, while a notice from a government entity or law enforcement can trick 36%.

- **Sharing positive news:** 71% of respondents would take action if a message had a positive hook, like “free gift”,

"you've been selected" or "you're a winner". Gen Zers are more likely to act on a giveaway (39%) than a notice from the government (31%), while 44% of respondents would click on a link or reply to a message that offered a financial opportunity.

- **Action required:** 60% would respond to action-required phrases, though respondents are most suspicious of requests to reset their password.

#CybersecurityMonth: SA enterprises can benefit from AI cyber protection

Steven Kenny 17 Oct 2023

Detect, learn, prevent scams

Consumers can better protect themselves by taking a few extra moments before clicking, including understanding the language scammers use.Here are some simple but effective best practices:

- Keep personal account information to yourself.
- Don't click on links before verifying that they'll take you where they say they will.
- Regularly check purchase alerts, which provide near real-time notification by text message or email of purchases made with your account.
- Call the number on corporate websites or the back of your credit- and debit cards if you are unsure if a communication is valid.

Visit Visa's Stay Secure web page for more insights from the 2023 study and learn about the language of fraud.

Securing the payments and commerce ecosystem

While cybercrime persists in an increasingly digital world, Visa is tirelessly working behind the scenes to stay one step ahead. Worldwide, it has invested over $10bn over the past five years in technology in a bid to reduce fraud and enhance network security.

This has included $500m on Artificial Intelligence (AI) and data infrastructure, enabling it to power 100 different capabilities that use AI to protect its clients and customers. More than 1,000 dedicated specialists protect Visa's network from malware, zero-day attacks and insider threats 24 x 7x 365. In fact, over the last year alone, Visa proactively prevented $27.1bn in potential fraud.