In the fight against fraud, overconfidence is our kryptonite

Nine out of ten consumers are at significant risk of falling prey to a scam – even the most experienced ones.

Bylined by Charles Lobo, Senior Vice President, Regional Risk Officer for Central and Eastern Europe, Middle East and Africa at Visa

A few weekends ago, while at breakfast with my family, I answered a distraught call from an old friend. "I don't understand how this happened to me," he exclaimed.

He had received an email about a parcel in transit the night before. He had been expecting a delivery in the coming days, so the email seemed timely. It included a tracking number and a link, which he clicked on without giving it much thought, and was only mildly confused when the page mentioned an outstanding import duty of AED7.50.

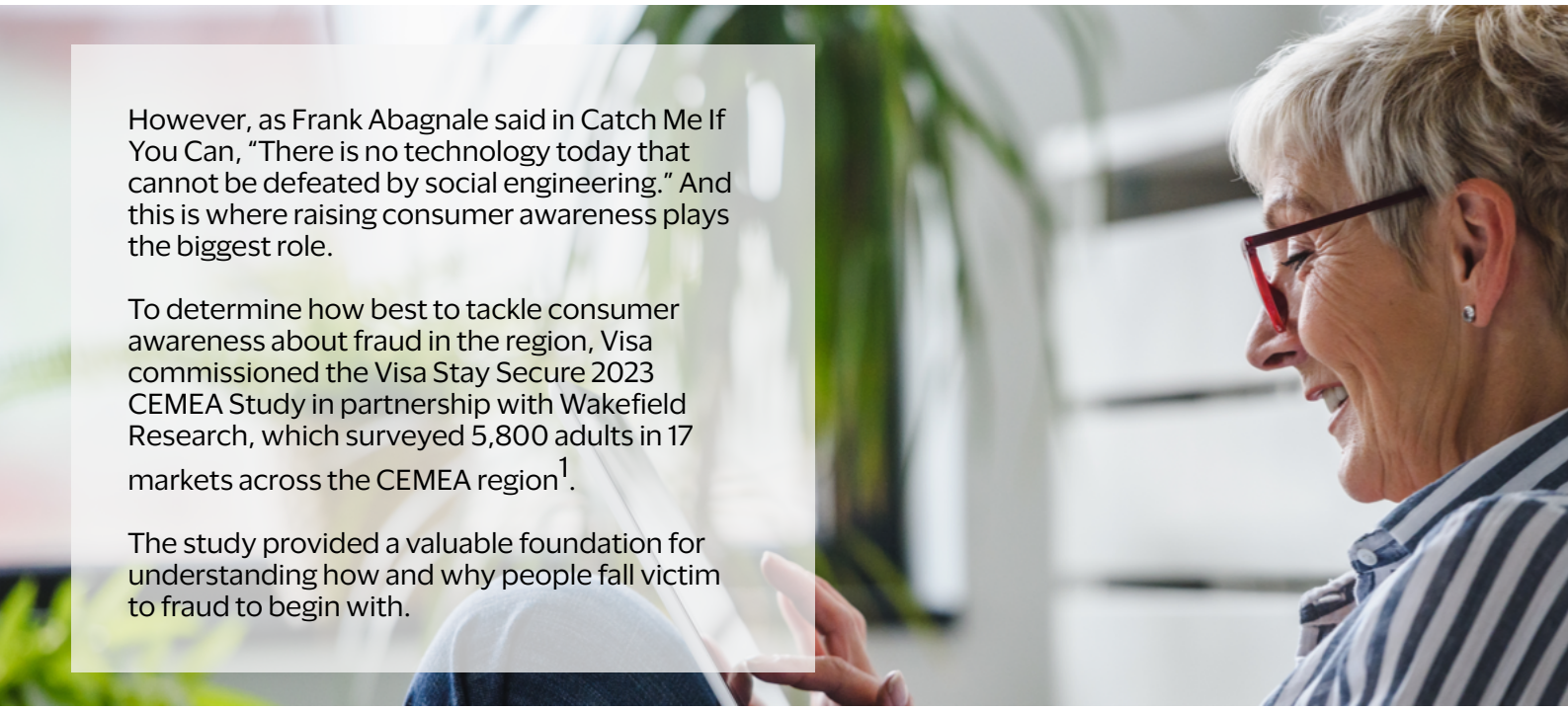
With such a relatively small amount, he plugged in his card credential details and went to bed.

The next day, he woke up to a text message from his bank that significant amount had been debited from his bank account.

"I don't understand how this happened to me" is a valid question for my friend, an experienced consultant, to ask. Being tech savvy is a prerequisite in his industry – how was it even possible for him to have fallen victim to such a simple scam?

Unfortunately, my friend is no exception.

Scams are becoming increasingly prevalent with the rapid pace of digitization. At Visa, we continue to innovate and are putting the best technology in place to protect the digital ecosystem and educate consumers to be more vigilant. Last year alone **Visa prevented USD 27.1 billion worth of attempted fraudulent payments across 122 million transactions**, stopping fraudsters in their tracks.



However, as Frank Abagnale said in Catch Me If You Can, "There is no technology today that cannot be defeated by social engineering." And this is where raising consumer awareness plays the biggest role.

To determine how best to tackle consumer awareness about fraud in the region, Visa commissioned the Visa Stay Secure 2023 CEMEA Study in partnership with Wakefield Research, which surveyed 5,800 adults in 17 markets across the CEMEA region[1].

The study provided a valuable foundation for understanding how and why people fall victim to fraud to begin with.

The honeypot

Like in my friend's case, o**ver half of the respondents (56%) claim to be extremely knowledgeable at recognizing a scam**. However, the reality is that nine out of ten (90%) consumers typically respond to common terms or phrases scammers utilize in emails and text messages.

Of even more concern is the fact that those who describe themselves as being "very" or "extremely" knowledgeable at recognizing scams, are more likely to be fooled and act on at least one type of common scam message than those who are less confident in their scam-deducing abilities.

It appears that there is a strong correlation between overconfidence and being too quick to click. Or, as the common adage goes: "Pride comes before a fall."

Indeed, it could be attributed to optimism bias, the belief that we are much less likely to experience adverse events than positive ones. So, when a friend calls us at breakfast to admit they fell victim to a scam, we think, "Well, that could never happen to me." But the truth is that it could happen to any single one of us.

Visa's study revealed a pattern of the language and scenarios that scammers tap into to nudge their victims to respond in a way that benefits their purposes. Namely: **urgency**, **positive news**, and **action required**.

Scammers orchestrate a sense of urgency to trigger impulsive action in their target. According to the Visa Stay Secure 2023 CEMEA study, **being offered a financially advantageous opportunity will prompt 44% of people to click on a link.** Other examples include being notified of a security risk - such as a stolen password, a data breach - or receiving a notice from an authority such as the government entity or law enforcement.

In such scenarios, individuals must make an effort to avoid reacting instantly or impulsively. Whatever the apparent urgency at first glance – stop and take a moment to verify the credibility of the email or message. Is the email address or the phone number it was sent from valid? Does it include the company name and logo? Is the information personalized? And make sure to check for grammatical errors and spelling mistakes.

Trojan horses such as "**free gift/gift card**," "**you have been selected**," or "**you are a winner**" should set off alarm bells. Sadly, unexpected 'good' news is not always what it may seem at first glance. And yet, we are so keen to believe in sudden windfalls and good fortune, especially when it comes to money: the Visa Stay Secure 2023 CEMEA study found that nearly 71% of respondents would take action if the message had positive news phrases!

[1]Visa Stay Secure 2023 CEMEA study online research was conducted across 17 CEMEA markets.

The final theme in the scammer playbook is to present the target with an easily resolvable problem. For example, my friend's outstanding import duty seemed like a quick fix and it was a nominal amount, he didn't dwell too much on its legitimacy. Other examples include false notices about a frozen account, problems with an order, or expiring subscriptions – all of which will prompt 60% of consumers into action.

Exploiting the cracks

Overall, cybercriminals seek to extract confidential information from consumers, threatening their security. These are all cases of social engineering, where a malicious actor attempts to deceive a user in order to access personal information, financial data, or even corporate confidential infomation.

Social engineering comes in various forms, many of which have made the headlines in recent years. Terminologies such as phishing, pretexting, baiting, and tailgating are now familiar to us, and yet we are still falling for the associated scam. Despite how shrewd, tech-savvy or worldly we might tout ourselves to be our most significant security risk remains – regrettably – only us!

Sometimes, we willingly offer it up by broadcasting every intimate detail of our lives, pets' names, and our whereabouts on social media. For scammers, this is a treasure trove they can plunder to access our personal preferences, mine to ascertain the answers to common security questions, and devise bespoke scams specifically tailored to you.

Our study found that over one in two people (52%) in the CEMEA region has been a victim of a scam at least once, while 15% have experienced being conned multiple times.

These incidents are not the sole concern of each individual consumer. All it takes is for one person to put an entire organization or network at risk. That's why we see so many headlines about cybersecurity breaches that immobilize operations or put data security to ransom – they get to the finish line by finding the weakest link, which is usually a human folly.

Security, a shared responsibility

At Visa, we're staying one step ahead of an increasingly sophisticated band of bad actors by taking a 360-degree approach to security. It's working: **our uncompromising commitment to security has kept fraud at historic lows**. We heavily invest in cutting-edge cybersecurity, including artificial intelligence and data analytics, to detect, deter and disrupt fraud preemptively.

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 lines of defense against criminal intent.**

Visa's study is part of a larger effort to ensure that individuals and organizations know the risks and can adequately safeguard themselves from attacks. Understanding the language of scams is essential in our digital-first world.

Collaborating to enforce robust legislation, prioritizing security in technological innovation, and integrating scam awareness into public safety programs are but some of the milestones on the horizon.

As technology progresses, people must preserve the human quality of questioning. Social media and artificial intelligence can impair the foundations of trust and security. Equipping the weakest link – the consumer – with the tools they need to combat increasingly sophisticated fraudulent tactics is the only way forward for a robust and exciting digital future.

Bylined by Charles Lobo, Regional Risk Officer CEMEA, Visa