VISA

Fraudulese:

The language of fraud

2022 Fraud Report

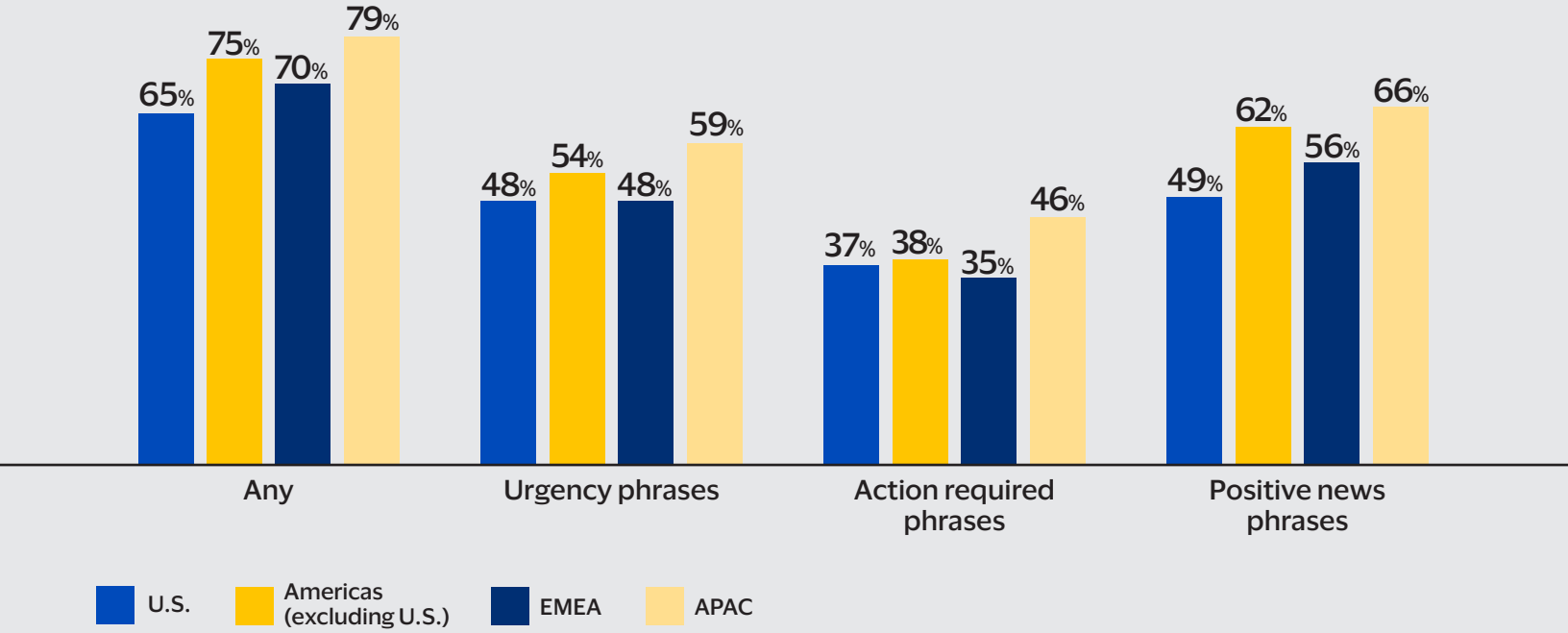
Overview of global report

A turn of phrase can turn a simple click into a breach of personal information. Today's online and text scams have reached a level of sophistication that ensnares even savvy consumers around the world who believe they are experts at spotting them. **While nearly half (48%) of those surveyed globally are confident they can recognize a scam, nearly 3 in 4 (73%) typically respond to terms or phrases scammers commonly use in emails or text messages.**

At Visa, we are committed to protecting people from online payment fraud. Conducted in partnership with Wakefield Research, Visa's report highlights the propensity for consumers to fall for fraudulent text and email messages. **Surveying 6,000 adults in 18 countries** highlights the various phrases and terms con artists use to trick consumers of all ages.

Call it Fraudulese

Scam phrases consumers admit they typically respond to:



Confidence is deceiving

Consumers who describe themselves as very or extremely knowledgeable in recognizing scams are more likely than others to respond to or act on at least one type of message commonly used by scammers (72%, compared to 64% of those who say they are somewhat knowledgeable or less). They are particularly **more likely to respond to messages about a financial opportunity** (34%, compared to 23% of those who describe themselves as less knowledgeable).

The devil is in the details

More than **4 in 5 (81%) respondents check the wrong details** to determine the authenticity of a communication, focusing on features scammers can easily fake, including the company's name or logo (46%). This includes an order number (45%), an account number (38%), and personalization of the first line of a salutation (27%).

Only 60% of people globally reported looking to ensure a communication is sent from a valid email address domain. Fewer than half look to ensure words are spelled properly (47%) and check order numbers for companies they've placed orders with (45%). Those in the United States are most likely to look for this type of information (70%), compared to 64% in EMEA, 69% in APAC and 59% in Canada and Latin America.

Gullible by geography

Those in the Americas, excluding the U.S., are most likely to act on messages commonly used by scammers (77%, compared to 68% globally). **In particular, nearly 2 in 5 are likely to respond to messages about a financial opportunity (39%, compared to 28% globally).** Those in EMEA (Europe, Middle East and Africa) (61%) are least likely to act on any type of message commonly used by scammers, as nearly 2 in 5 (39%) say they would never click on a link or respond to the sender for the types of communications scammers commonly send, compared to 32% globally.

Top Fradulese traps

Consumers fall for a variety of phrases and messages from scammers

Win online gift card (48%)

Exclusive deal (30%)

Act now (25%)

Click here (21%)

Limited time offer (25%)

Urgent (22%)

Action needed (21%)

Free/giveaway (32%)

Circle of concern

While consumers feel confident in their own vigilance, the vast majority **(90%) are concerned that friends or family members may fall for a potential scam in emails** (61%) or text messages (59%.) asking people to verify their account information. Half (50%) are worried about an overdrawn banking account email and 48% are worried about a winning a gift card or product email from an online shopping site.

The crypto contradiction

The vast majority of crypto users (93%) admit they're likely to act on the types of communications they receive that are commonly used by scammers, compared to 66% of non-crypto users. **More than half of crypto users say they're likely to act on communications about financial opportunities, such as a good deal or a way to earn money (54%) and on communications about a giveaway or opportunity to receive a free item from a company (52%).**

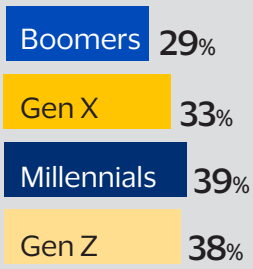
Yet, crypto users may also be more cautious about reviewing this wealth of communications for signs of potential fraud. While they're equally as likely to look for a valid email address for the sender, proper spelling, and a company name/logo and contact information, crypto users are more likely than others to look for their order number (51%, compared to 44%) or account information (49%, compared to 37%), as well as a personalized salutation line (39%, compared to 26%) to confirm the validity of digital communications.

Note: The Visa Security — Global Survey was conducted by Wakefield Research (www.wakefieldresearch.com) among 6,000 Nationally Representative Adults in 18 Markets: US, Canada, Brazil, UK, France, Germany, Netherlands, UAE, Spain, Italy, Ireland, Australia, China, Hong Kong, India, Japan, Singapore, Taiwan, between September 7th and September 14th, 2022, using an email invitation and an online survey.

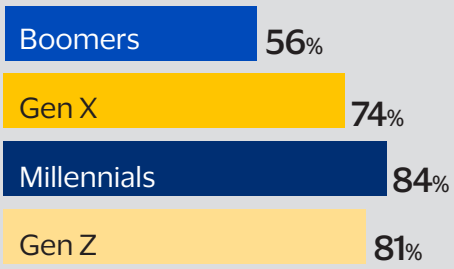
Age and awareness

While 87% of global consumers assume older adults are more likely to fall victim to online scams than college students, the data suggests quite the opposite.

Those most likely to report being a victim of a scam:



Those most likely to fall victim to at least one fradulese phrase:



Those most likely to act on a fradulese phrase: