How and why overconfidence can make you more vulnerable to scams?

A comprehensive guide to protect yourself from online scams

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. Scams are evolving in sophistication with criminals using new approaches to trick unsuspecting consumers. Whether in the workplace or on the go, we're peppered by phone, text and email with offers for "free gifts" and traps to "act now" to supply personal information before a vital service gets cut off. And this barrage of persuasive and manipulative language is working.

Unfortunately, according to **Visa Stay Secure CEMEA Study 2023***, even the most tech-savvy users are prone to being tricked: **while more than half (56%) consider themselves to be knowledgeable about fraud, 9 out of 10** would act on messages commonly used by scammers. It appears that false confidence makes people even more vulnerable, making them prone to act without thinking and neglecting to first check for red flags.

From a spoofed service notification from a shipping company to an email announcing that you've won products from your favorite store, or even job postings that make it seem like you've been hired by a top-tier company, scams hit almost every touchpoint in our digital lives. Scammers do not shy away from using the most manipulative schemes, such as pretending to be representatives from the law enforcement or government, which, according to the Visa Stay Secure Study, prompts a high response rate from the victims.

* Stay Secure CEMEA Study 2023 was conducted by Wakefield Research

Consumer education is Visa's top priority

At Visa, we're staying one step ahead of these increasingly sophisticated bad actors by taking a 360-degree approach to security to meet consumers' needs related to safety, trust, reliability, and convenience. We believe that consumer education is key in the fight against fraud, and we continue to help consumers to become aware of the risk and identify key threats in order to enable them to spot fraudulent activity and protect their sensitive information.

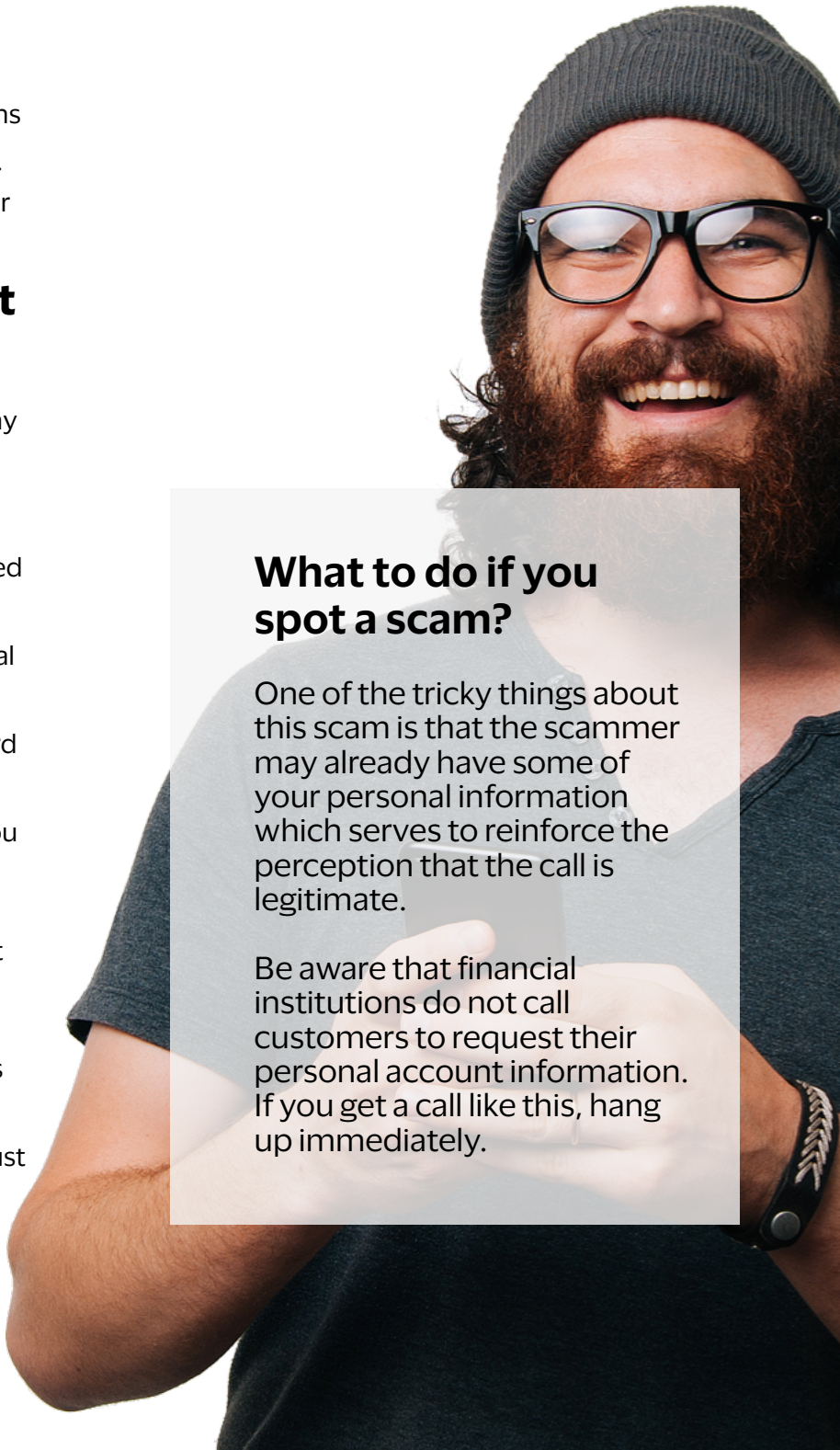
To help educate consumers on what to look out for, we've put together some common forms of scams with tips on how to spot the warning signs early and stay one step ahead.

Phone call scams

Scammers may pose as financial institutions or payment companies to trick consumers into providing a 3-digit verification number typically placed on the back of their card, or other sensitive information.

Warning signs to look out for

- A phone call from a payment company or financial institution, typically from someone who works in the "Risk" or "Security and Fraud Department."
- You are told your card has been flagged for suspicious transactions or you're requested to reset your password or account information due to a potential breach.
- You've received a notice that your card account has been blocked or frozen.
- One of the common traps is asking you for a KYC (Know Your Customer) verification update.
- Fraudsters may also ask for proof that you have the card in your possession.
- You may even be asked to provide personal account information such as your full card number, three-digit number on the back of your payment card, a one-time passcode that was just sent to you, or your PIN.



What to do if you spot a scam?

One of the tricky things about this scam is that the scammer may already have some of your personal information which serves to reinforce the perception that the call is legitimate.

Be aware that financial institutions do not call customers to request their personal account information. If you get a call like this, hang up immediately.

Text message scams

With more companies using text messages to communicate with their customers, it can sometimes be difficult to distinguish between a legitimate message and a fraudulent one.

Warning signs to look out for

- A link or email address instead of a phone number to call.
- Inconsistencies in language, such as errors in grammar and spelling.
- A sense of urgency to complete an action, such as 'click now to secure your account.'
- Look out for phrases like 'send (...) here' or 'click (...) below', or undated timeframes such as "in 24 hours".
- The text you receive may not contain the name of the organization or any other information.
- The text requests that you log in to your bank account to verify a transaction, enter your PIN, or provide your three-digit security code.

Email scams

Typically, you receive an email from a trusted organization (such as your bank), asking you to click on a link. Once you click on the link, you're taken to a site that looks identical to the real thing. But in this case, it's a phishing site that can capture your log-in information and then use it to drain your account.

Warning signs to look out for

- Spelling and grammar errors in the subject line or body of the email.
- A hard deadline. Sometimes scammers will include a deadline and threaten account suspension to add urgency, the intention being to override your normal sense of caution.
- The email address doesn't match that of the organization (i.e., irs.net or amazon.mil).
- The email does not address you by name.
- No contact information. If something feels suspicious, contact your financial institution directly using the phone number on the back of your card.
- Suspicious requests. Visa, like other financial institutions, does not contact cardholders to request their personal account information.
- Suspicious hyperlinks. Avoid clicking on hyperlinks if possible. A single click can cause your computer to become infected with malware.

Website scams

Scammers are getting better at designing websites that look legitimate. You may click on a link that comes up via a web search or from an email that appears legitimate but instead directs you to a fake site run by a scammer.

Warning signs to look out for

- There's something slightly 'off' about the web address or the actual page. Look for misspelled words, substitutions or updated logos.
- An unusual pop-up on the site requesting that you enter your account information.
- HTML links that don't match their destination.
- The website URL contains misspellings and does not match the original URL of the real company.

What to do if you spot a scam?

Many modern browsers offer options for anti-phishing protection that can warn you if you're visiting an unsafe website.

However, one of the best tools to protect yourself is by using your common sense and by avoiding clicking on links that come up via a search or are sent to you in an email, especially one with an offer that seems too good to be true – instead, enter the URL of the related website into your browser yourself to avoid putting yourself at risk.