Report | August 2025

SCAM HOOKS:

How Even Smart People Take the Bait

Understanding the traps behind modern fraud

CTM360®

Executive Summary

Online scams are on the rise, inflicting both financial and emotional damage on individuals and businesses around the globe. In 2024, scammers took advantage of various tricks to deceive their victims, leading to losses of over **$1.03 trillion** globally. This staggering figure underscores just how urgent and widespread the scam threat has become. **(Source: Global Anti-Scam Alliance)**

This report highlights some of the **key traps** scammers use, among many others that go unnoticed. By familiarizing themselves with these tactics, individuals and businesses can better spot scams early and avoid them before any damage is done.

The main traps include:

- **Psychological Traps**: Scammers exploit emotions like fear, urgency, and greed to manipulate victims into taking quick actions.
- **Technical & Design Traps**: These involve deceptive websites, fake payment screens, and malicious apps designed to steal personal information.
- **Social Engineering Traps**: Scammers build trust through impersonation and fake customer service, often through social media or direct communication.
- **Content & Media-Based Traps**: These traps use fake content, such as fraudulent giveaways, job offers, and media stories, to lure victims into revealing sensitive information.

Advances in AI and deepfake technology are making scams harder to detect and more widespread. Vulnerable groups, like the elderly and those in financial distress, are particularly targeted by these tactics.

This report goes beyond identifying traps; it equips readers with the awareness needed to resist manipulation in an era of growing digital deception. While awareness is the first step in recognizing a threat, vigilance is what helps prevent falling for it.

INDUSTRY	COUNTRY	REGION	DATE
All	All	Global	24-08-2025

Overview

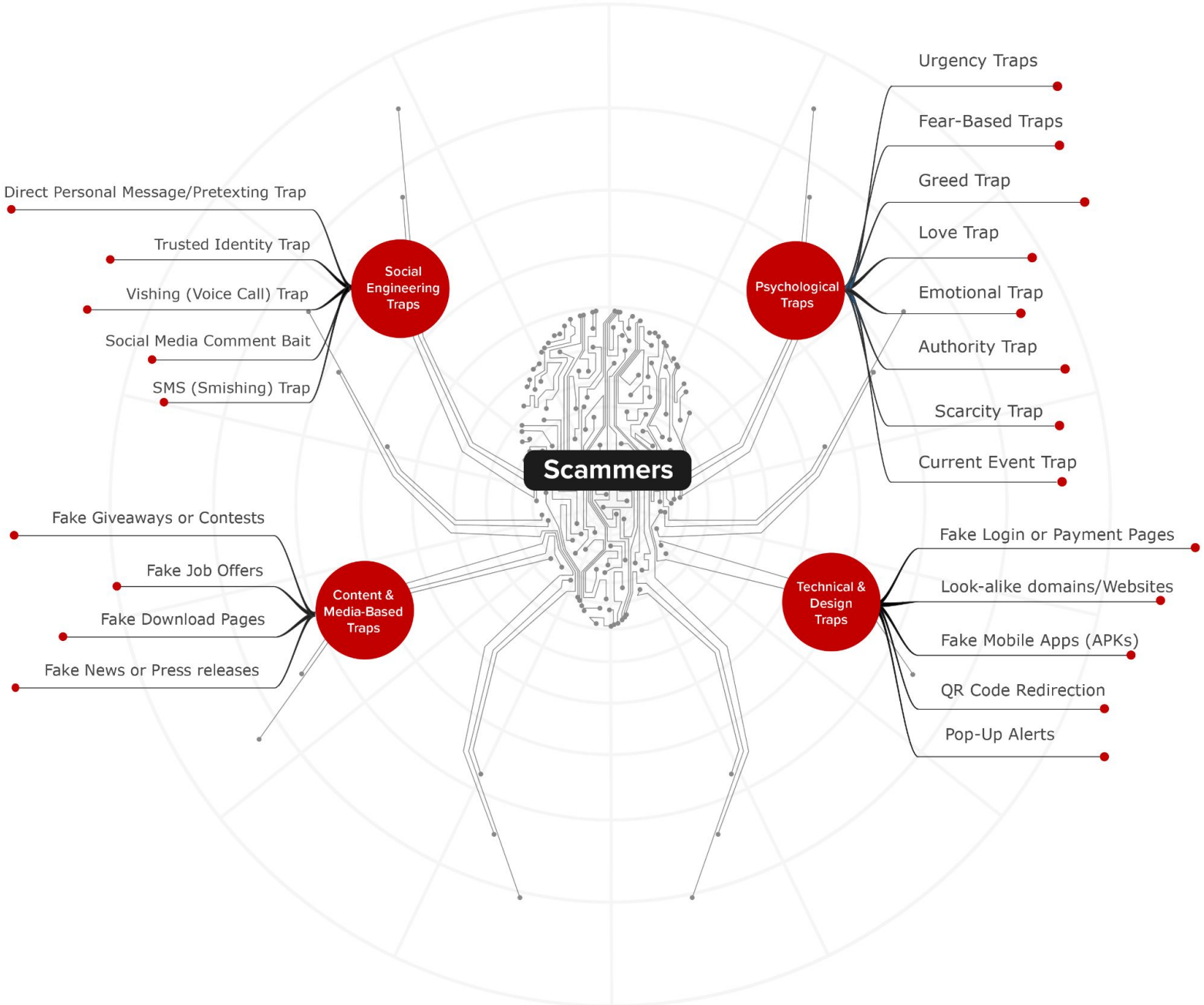
The internet has transformed the way we communicate, shop, and access services. However, this convenience comes with a significant downside; the rise of online scams. These tactics have evolved far beyond simple phishing emails or fake job postings. Modern scammers exploit human emotions, target vulnerabilities, and increasingly use advanced tools such as artificial intelligence and deepfakes to deceive their victims.

Scams are now a complex threat for both individuals and organizations around the world. Scammers tap into fear, greed, urgency, and trust to push victims into quick decisions. **These manipulative tactics are known as Scam hooks**: designed to grab attention, trigger emotions, and push people into quick unsafe actions. Unlike traditional fraud, which relied on generic spam, today's hooks are carefully crafted, convincing, and often backed by **real data stolen from breaches or leaks**.

As scams become more advanced, awareness and prevention needed more than ever. **Scammers use AI and stolen data to make their attacks harder to spot and more convincing. This report explores the key traps scammers set and provides steps to detect and avoid them before they cause harm.**

Mapping the Different Traps Used by Scammers

As online fraud becomes more sophisticated and harder to spot, it is essential for individuals and organizations to understand how scammers think and operate. **The mapping below lays out the traps fraudsters set to draw victims into their schemes**.



***Note** that many of these traps overlap because scammers often combine several techniques to improve their success rate. The next section explains each trap in detail.*

Online Fraud Traps – How Users Are Lured into Fraud

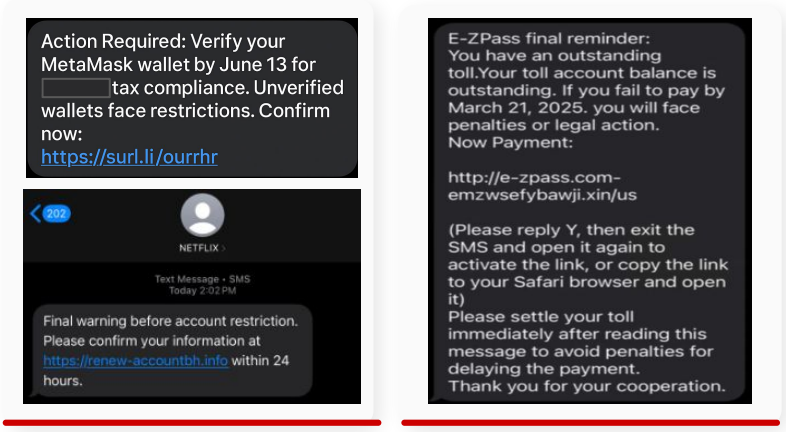
Scammers constantly innovate, refining their methods to deceive and manipulate users. Their online schemes are meant to exploit emotional triggers, technical gaps, and social engineering flaws, drawing people into theft, fraud or data compromise.

While they may use many different tactics, some of the key traps include:

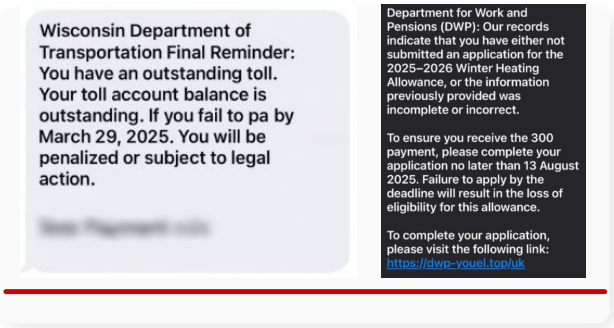
A. Psychological Traps:

These tactics prey on the emotions and cognitive biases of users, forcing them to act impulsively or irrationally.

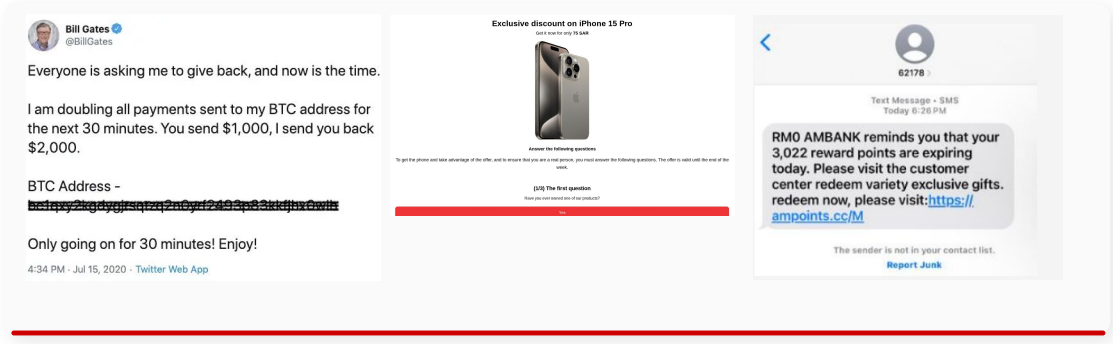
- **Urgency Traps**: Your account will be locked in 1 hour!
  - Scammers create a sense of urgency to rush victims into making quick decisions without verifying the authenticity of the message.



- **Fear-Based Traps**: You are under investigation. Pay now to avoid arrest.
  - These scams exploit the victims fear of authority or consequences, pushing them to act quickly without thinking.



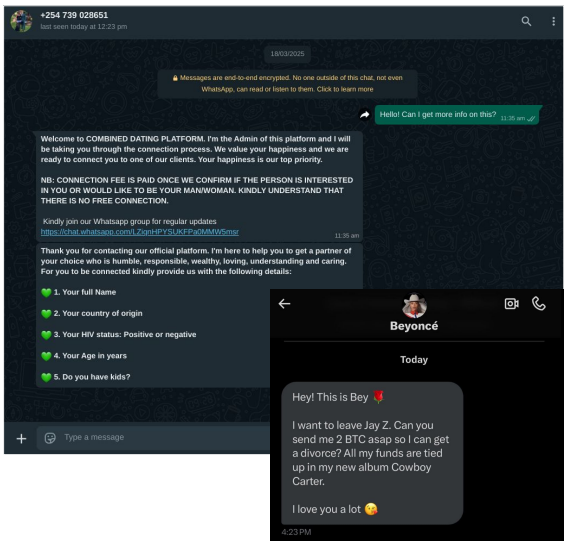
- **Greed Trap**: You've won a cash prize! Claim within 5 minutes.
  - Scammers lure victims by false promises of rewards or easy wealth, leading to hasty actions.



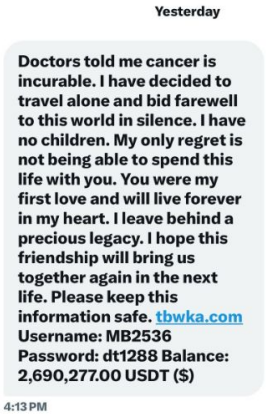
Online Fraud Traps – How Users Are Lured into Fraud

A. Psychological Traps:

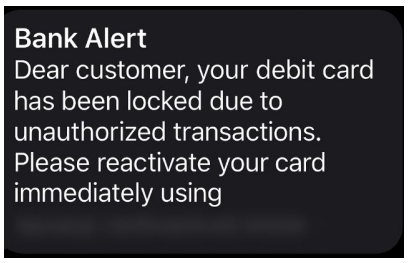
- **Love Traps**: I love you, but I need your help urgently.
  - Exploiting emotions, these scams create a false sense of intimacy, using trust to manipulate victims into action.

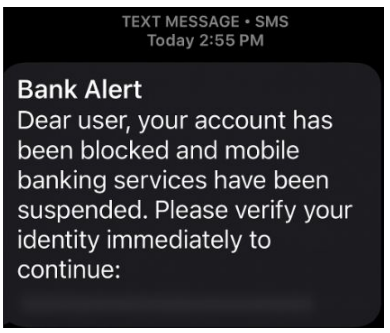


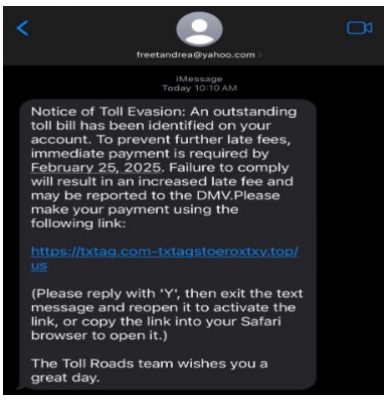
- **Emotional Traps**: My mother is in the hospital. Please help.
  - Scammers prey on emotions, exploiting sympathy to prompt donations or payments under false pretenses.



- **Authority Traps**: This is your bank/police/CEO speaking.
  - Fraudsters impersonate authoritative figures to create a sense of legitimacy, compelling users to comply with their demands.



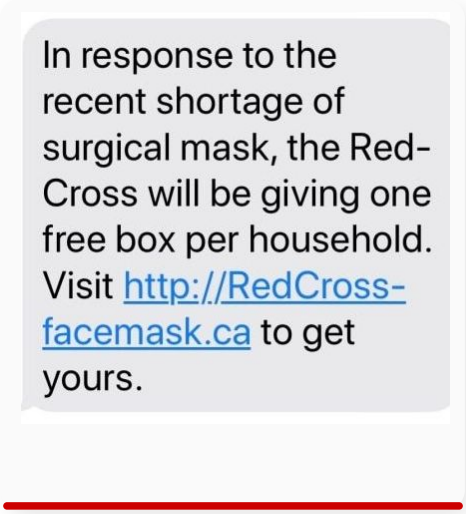


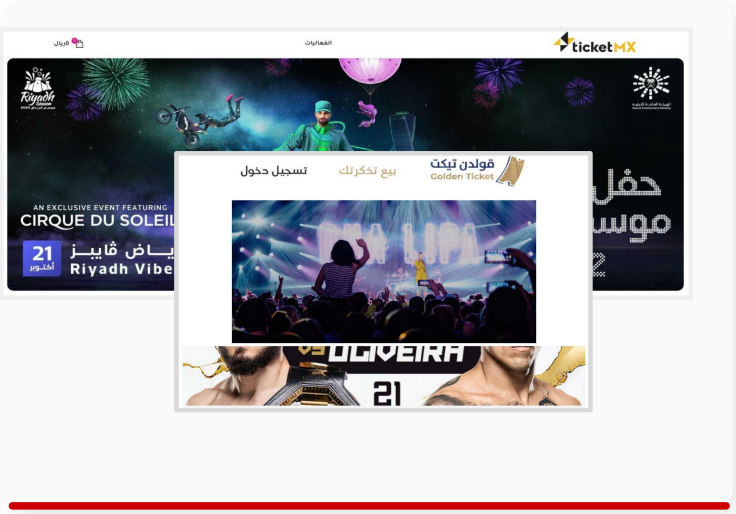


Online Fraud Traps – How Users Are Lured into Fraud

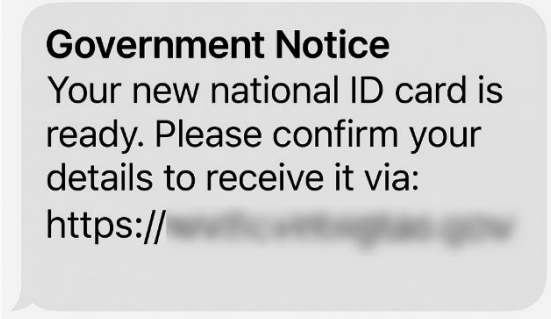
A. Psychological Traps:

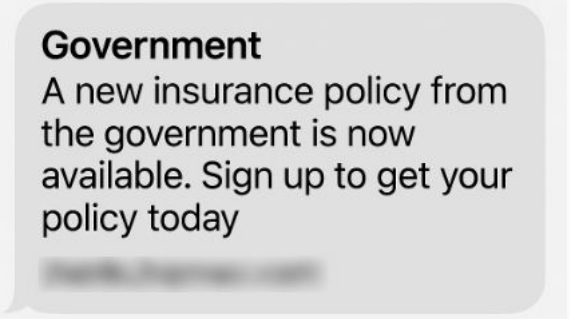
- **Scarcity Trap:** Only 2 spots left, book now!
  - Scammers create a false sense of limited availability such as exclusive deals or "last chance" offers to pressure victims into making quick decisions. The fear of missing out can override caution, leading individuals to act without verifying the legitimacy of the offer.





- **Current Event Traps:** National ID ready. confirm details to get your card.
  - Scammers often time their messages around news stories, seasonal events, or key times of the year like holidays, or major public announcements. These scams feel relevant because they align with what people are already expecting, making it easier to catch victims off guard.





Online Fraud Traps – How Users Are Lured into Fraud

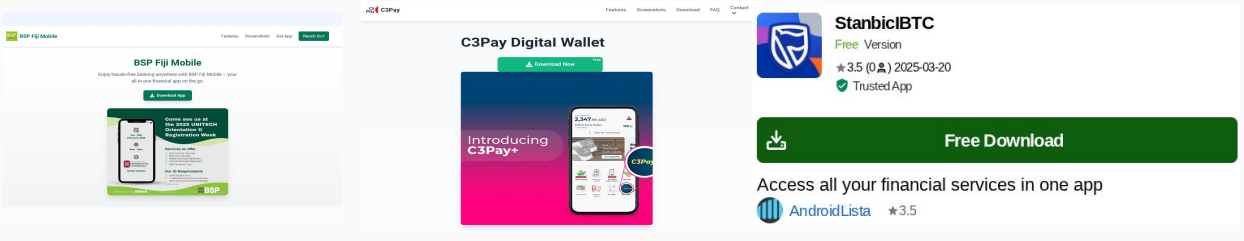
B. Technical & Design Traps

These traps are designed to look legitimate, often using deceptive interfaces or techniques to harvest sensitive information from unsuspecting users.

- **Fake Login or Payment Pages:** Scammers build exact copies of real sign-in or checkout screens to capture your credentials. These pages match the original site's design, logos, and layout so you do not notice anything is wrong. **For example,** you might enter your bank username and password on a page that looks genuine, only to have those details sent directly to the scammer.

- **Look-Alike Domains and Websites:** A single typo or extra character can send you to a fraudulent site. URLs such as "micr0soft.com" instead of "microsoft.com" mimic the real address so closely that most people do not spot the difference before entering sensitive information. **For example**, clicking a link to "paypa1.com" could prompt you to enter your credit-card number on a counterfeit checkout page.

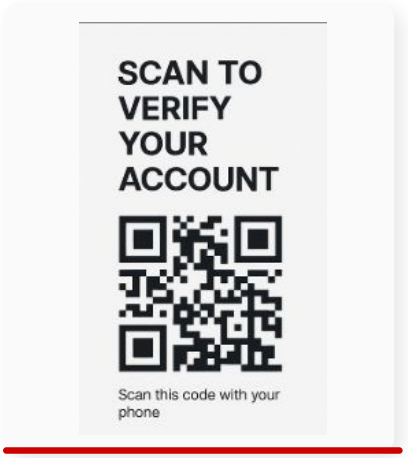
- **Fake Mobile Apps:** Apps distributed outside official stores may request unnecessary permissions and harvest personal data. They often masquerade as popular tools or games but install malware that steals contacts, messages, or device identifiers. **For example**, a "WhatsApp Plus" APK might promise extra features yet upload your entire address book to a remote server.



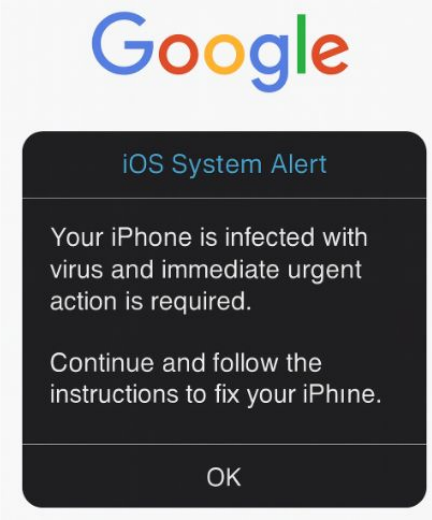
Online Fraud Traps – How Users Are Lured into Fraud

B. Technical & Design Traps

- **QR Code Redirects:** Malicious QR codes, often pasted over genuine ones, send you to phishing sites or trigger unwanted downloads. Scanning feels quick and safe, so users rarely verify the destination URL. **For example**, a cafe's "free-wifi-here" code could open a fake login page that steals your credentials.



- **Pop-Up Alerts:** Scammers use fake system or browser alerts to warn of infections, trick users into downloading a so-called 'fix' that secretly installs malware. The alarming message is designed to override your caution. **For example**, a full-screen alert might proclaim "Critical Infection Detected" and then deliver malware when you click to "remove" it.

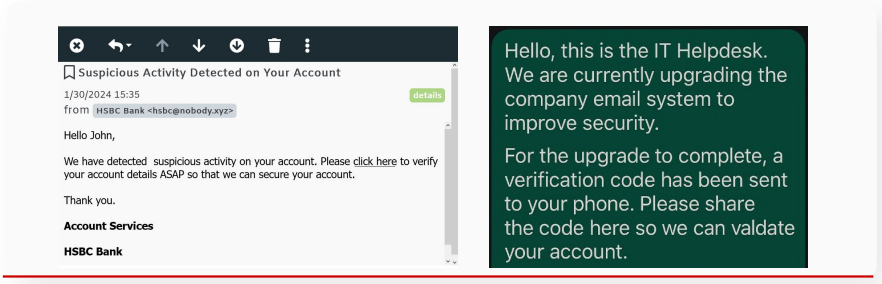


Online Fraud Traps – How Users Are Lured into Fraud

C. Social Engineering Traps

These scams manipulate social interactions or online behaviors, creating a false sense of trust or urgency to push the victim into compromising actions.

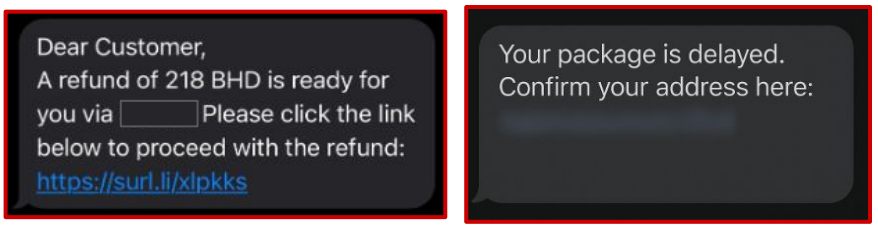
- **Direct Personal Message/Pretexting Trap:** Scammers reach out directly through messaging platforms such as WhatsApp, SMS, LinkedIn, or Telegram, pretending to be someone you know or trust; a colleague, supplier, executive. They use a believable story or context to make the interaction seem legitimate and gradually build trust. Once you are comfortable, they will ask you to take an action, such as sharing login codes, transferring money, clicking a malicious link, or downloading a harmful file. **For example:** You get a **WhatsApp message** from someone claiming to be your **company's IT support.** They say they are upgrading the email system and need you to share the **verification code** sent to your phone. In reality, they are using it to gain access to your account.



- **Trusted Identity Trap:** One of the most powerful tricks scammers use is impersonation. The danger is not just urgency or fear, it is that the message appears to come from someone you already trust. When that trust is exploited, people are far more likely to act without thinking. This happens across social media and messaging platforms every day: **For example:** a cloned Facebook profile of a colleague **asking for help**, an Instagram DM from a "**friend**" sharing a **giveaway link**, a Discord "moderator" **sending a fake update**, or fake Telegram admins in crypto groups pushing "**airdrop**" links that drain crypto wallets.

  By disguising themselves as trusted contacts, scammers bypass skepticism and make their requests feel normal and safe; **exploiting the most powerful factor in human relationships: trust.**

- **SMS (Smishing) Trap:** Fraudsters send deceptive text messages that appear to come from legitimate sources, such as banks, delivery companies, or government agencies. The goal is to get recipients to click on a link, call a fake number, or share personal details. **For example:** You receive a **message** saying, "Your package is delayed. Confirm your address here: [link]." The **link directs you to a fake website** designed to steal your data.

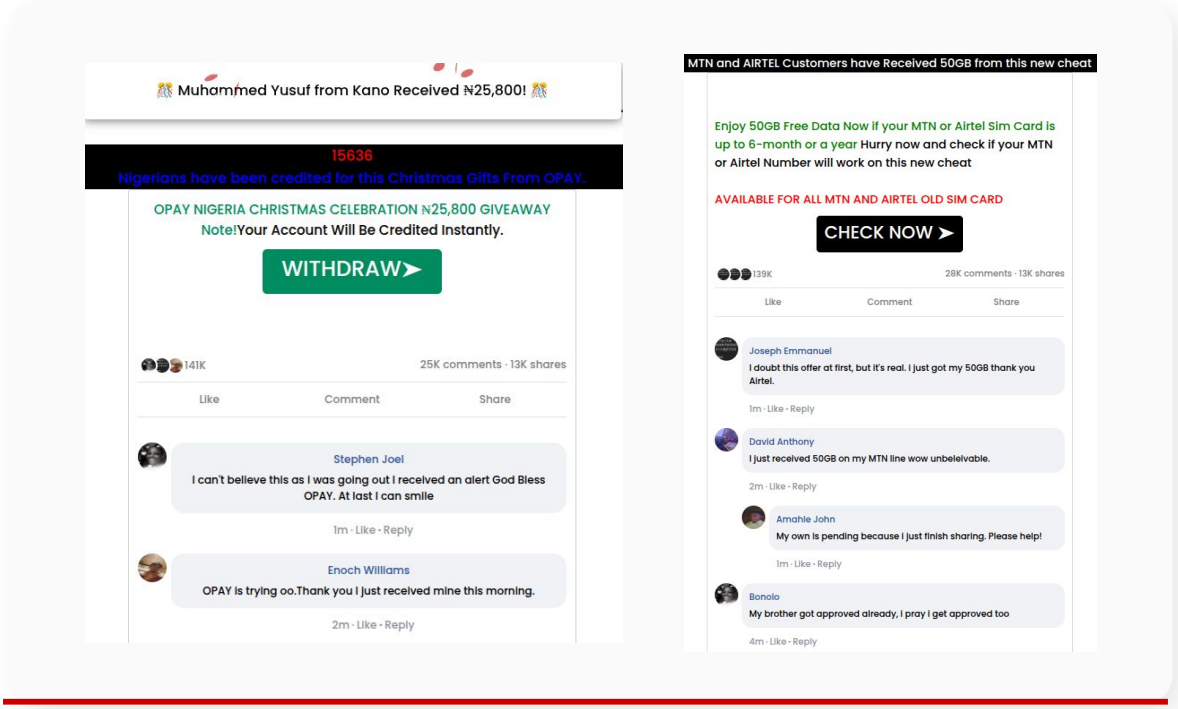


Online Fraud Traps – How Users Are Lured into Fraud

C. Social Engineering Traps

- **Vishing (Voice Call) Trap:** Scammers use phone calls to impersonate trusted individuals or organizations, such as bank representatives, government agencies, or company executives. They create a sense of urgency or authority to pressure you into revealing sensitive information or taking harmful actions. **For example:** You receive a call from someone claiming to be from **your bank's fraud department**, saying your account has been **compromised** and asking you to **confirm your card details** to "secure" it. In reality, the caller is a scammer stealing your information.

- **Social Media Comment Bait**: Scammers post attention grabbing offers, giveaways, or urgent messages on social media to encourage public comments. Once you respond, they send private messages with fraudulent links or payment requests. **For example:** A post promises a **free gift** for everyone who comments "YES." After you reply, **you get a direct message with a link** to "claim" your prize, which leads to a phishing page.

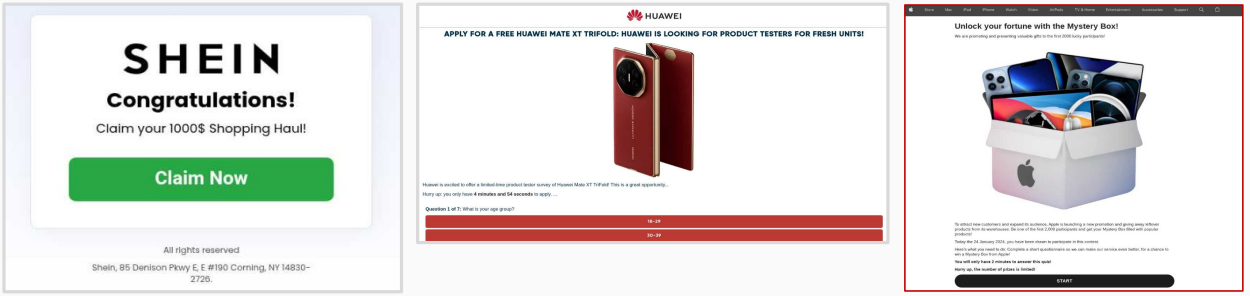


Online Fraud Traps – How Users Are Lured into Fraud

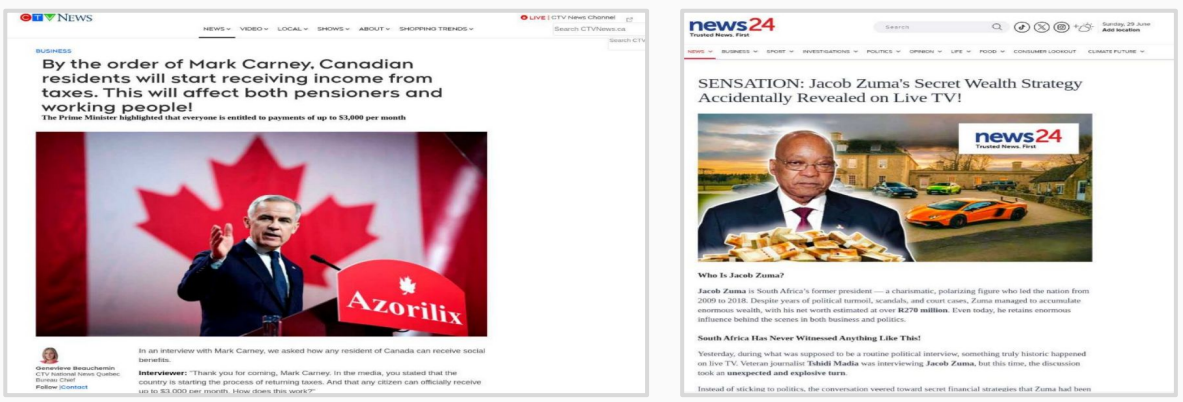
D. Content & Media-Based Traps

These scams utilize media, fake content, and false promises to engage users, leading them into fraudulent actions.

- **Fake Giveaways or Contests:** Scammers use enticing offers of prizes, free products, or exclusive rewards to draw in potential victims. Individuals are typically asked to click on a link, share a post, or make a small payment for “shipping” or “processing” fees to claim the prize, which in reality does not exist. This method can lead to both financial loss and the exposure of personal information. **For example:** A **post claims you have won** a new smartphone and **requests a small shipping fee** to deliver it. Once payment is made, no product arrives, and your payment details are compromised.



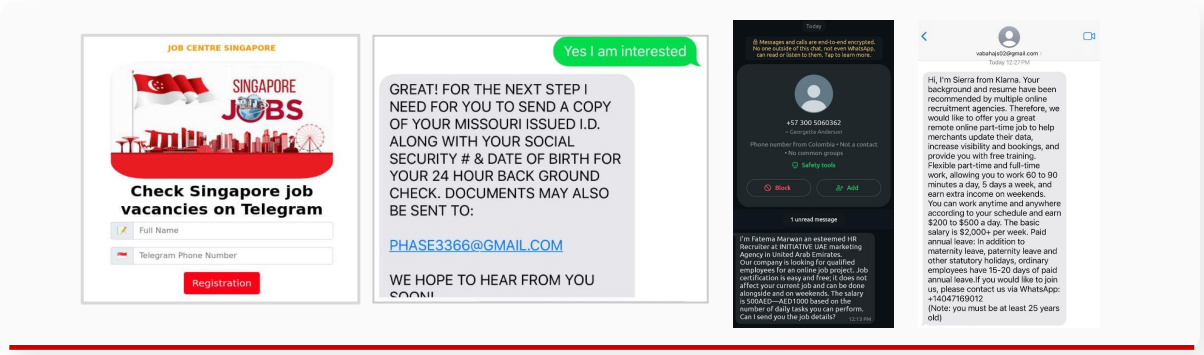
- **Fake News or Press Releases:** Scammers create fake news articles or press releases promoting products, platforms, or services that do not exist. By using the name, logo, or style of trusted media outlets, they make the content look real and convince people to invest, register, or make purchases. They may also use deepfake videos of well known people and run fake ads to make their claims seem more believable. As previously highlighted in our **BaitTrap report**, such tactics are becoming increasingly common in blending scams into trusted online spaces. **For example:** A **news style online article** promotes a “government-backed” **investment program** and uses the branding of a **reputable newspaper**. The program is fake and intended to trick readers.



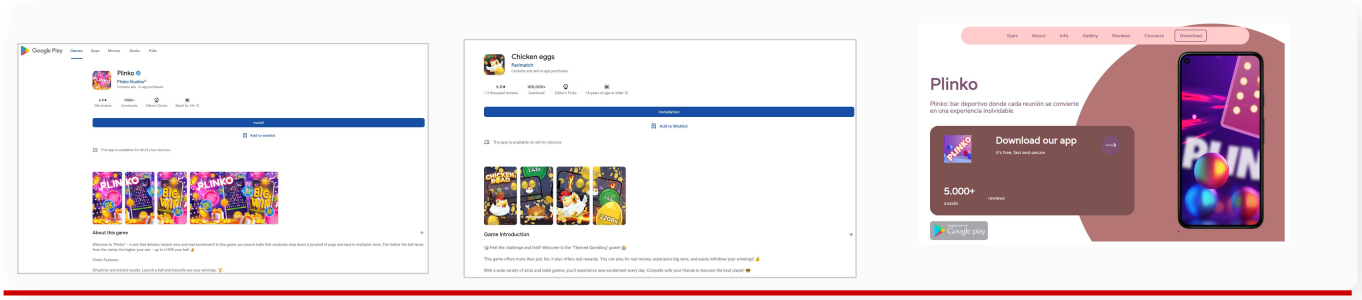
Online Fraud Traps – How Users Are Lured into Fraud

D. Content & Media-Based Traps

- **Fake Job Offers:** Scammers issue fraudulent job offers that appear genuine but are intended to exploit job seekers. These schemes may request upfront fees for “processing,” “training,” or “background checks,” or distribute documents embedded with malware. **For example:** An email offering a high-paying remote job. The contract appears official but asks for **a payment to cover a background check**. Once payment is made, the employer disappears, or the attachments provided install malware on the victim’s device.



- **Fake Download Pages:** Scammers create fake websites that look like legitimate download portals for software, games, or tools. Instead of the real application, these downloads install malware that can steal information. They also run fake mobile game ads promising rewards, which lead to imitation app store pages that install malicious software. As previously observed in our **PlayPraetor report,** this trend also includes fraudulent Google Play Store download pages crafted to mislead users. **For example:** You click on an **ad for a money making game** and are taken to a fake app store page. After installing the game, your device is infected with malware that captures your saved passwords.



Online fraud is a serious and growing issue that directly affects individuals and businesses every day. Scammers are constantly refining their tactics to exploit vulnerabilities, using both psychological manipulation and advanced technology to deceive victims. **With generative AI, they can now mass produce convincing, tailored lures for multiple organizations in minutes; turning what once took hours into industrial scale targeting**. These scams result in more than just financial loss, they can compromise personal information, destroy reputations, and cause lasting damage.

The reality is simple: fraud is not a distant threat. It is happening now, and it can happen to anyone. The consequences are real, and without awareness, it is only a matter of time before you become a target.

Notable Statistics you should know

Attackers now use **AI chatbots** to generate typo-free and convincing phishing emails, **mimicking** legitimate messages almost perfectly

(Source: Axios**)**

AI-driven scams now use **publicly available personal data** to craft emails that impersonate friends or family, deceiving even cautious users

(Source: Identity Theft**)**

Attackers often impersonate brands like **Microsoft, Google, and Amazon**, with Cloudflare reporting that **51.7%** of phishing emails mimic these companies.

(Source: Keepnet Labs**)**

In 2024, scammers stole over **$1 trillion** globally, a significant rise in online fraud.

(Source: Global Anti-Scam Alliance**)**

In 2024, the average loss per scam victim in the U.S. was **$3,520.**

(Source: MSN**)**

28% of individuals have encountered **AI-driven** voice cloning scams, with **46%** unaware that such technology was being used to manipulate them into transferring funds.

(Source: The Guardian**)**

In 2024, consumers reported losing over **$12.5 billion** to fraud, a **25%** increase from the previous year.

(Source: Federal trade Commission**)**

Losses to government imposter scams rose by **$171 million** from 2023, totaling **$789 million** in 2024.

(Source: Federal trade Commission**)**

In 2024, **online shopping scams** ranked among the top fraud categories, resulting in significant financial losses.

(Source: Federal trade Commission**)**

In 2024, victims lost **$672 million** to romance scams.

(Source: CBS News**)**

In 2024, global cybercrime losses reached over **$16 billion**, marking a **33%** increase from the previous year.

(Source: Reuters**)**

In 2024, **gift cards** were the most commonly used payment method in various scams, including romance and tech support scams.

(Source: Federal trade Commission**)**

How to Spot Online Scams

Detecting online scams is essential to protecting yourself and your personal information. Scammers are constantly refining their tactics to deceive and manipulate, but there are several key indicators and methods you can use to identify fraudulent activities before it's too late. **Below are practical steps and tips to help you spot online scams quickly and effectively:**

1. **Verify Who You are Dealing With**

- **Look closely at who is contacting you:** Scammers often hide behind email addresses, phone numbers, or usernames that look almost identical to the real thing. A single extra letter, misplaced symbol, or unusual domain can be the only clue. **For example**, **paypal.com** versus **paypa1.com**.
- **Check where a link really leads:** Before you click, hover your mouse over the link or button to see the full web address. If it does not match the official site you know and trust, or it lacks "**https://**" and the padlock icon, do not click.
- **Double-check using trusted contact information:** If you have any doubts, go to the organization's official website and use their published phone number or email. **Never use the contact details provided in a suspicious message**.
- **Search for independent confirmation:** If an email, text, or post makes a claim, whether it is about a product, payment, or opportunity; search online for reviews, news, or scam reports. A quick search with words like '**scam**' or '**fraud**' often reveals if others have reported it.

2. Assess the Message and Its Content

- **Treat sudden, urgent demands with caution:** Messages telling you to "**act now**," "**confirm immediately**," or risk losing access are designed to pressure you into acting without thinking. If it is important, it will still be valid after you verify.
- **Question anything that sounds too good to be true:** Offers of guaranteed profits, large cash rewards, or free gifts for little effort are a **classic hook**. If it feels unreal, it is probably a scam.
- **Pay attention to how the message is written:** Poor grammar, awkward phrasing, or formatting that feels unusual can be a sign it is **not** genuine.
- **Never give away sensitive details in response to an unsolicited request:** No legitimate company will ask for passwords, ID numbers, OTP or bank details **by email, text, or phone calls.**
- **Verify unexpected attachments before opening:** Even harmless-looking files (**e.g.** "**invoice.pdf**") can contain malware. Always confirm their legitimacy before opening.

How to Spot Online Scams

3. Check the Action and Payment Requests

- **Only share information on secure, trusted websites:** Look for "**https://**" and a padlock icon before entering personal or payment information. Avoid sites with poor design, broken links, or low-quality images.
- **Be cautious if they want unusual payment methods: Gift cards**, **cryptocurrency**, and **wire transfers** are favorites for scammers because they are hard to reverse. If someone insists on these, treat it as a **red flag**.
- **Listen to your instincts:** If something feels wrong, it probably is. Stop, verify, and act only when you are sure it is legitimate. Scammers count on you making quick, emotional decisions.

Awareness and **vigilance** are your strongest defenses in an ever-changing digital world.

Conclusion

We stand at a defining moment in the digital age. As technology changes, so do the tactics of those who wish to take advantage. Scammers have grown more skilled, **exploiting people through scam hooks rather than just technology.** They no longer just steal money; they attack the trust we place in the digital world. **Scammers bait us with scam hooks that mimic daily online interactions, making them harder to spot**.

It only takes one well-timed message or realistic video to cause serious harm. As seen in the **FraudonTok report,** scammers are increasingly targeting TikTok Shop users and affiliates through deceptive techniques. Threat actors are using fake Meta advertisements, AI-generated videos, and lookalike domains to lure victims into phishing sites or trick them into downloading trojanized applications. The **BaitTrap report** unveils another campaign, where thousands of malicious websites were found mimicking legitimate news sources. Similarly, the **Info-Stealer report** revealed that threat actors are often bypassing traditional exploits altogether, simply logging in using stolen credentials from data breaches.

These examples highlight just how crucial it is to maintain strong credential hygiene and vigilance, not just technical defenses. **The threat has shifted from machines to minds, and the frontline is now every user's judgment.**

AI has made scamming easier than ever. Attackers no longer need to carefully craft targeted attacks as they once did; **AI enables them to shift tactics daily, adapting to current trends with speed and precision**. This makes scams harder to detect, as chances are **the fake will look even more genuine to the user.** In the days ahead, scams will grow at an exponential rate, blurring the line between what is real and what is fraudulent. To keep up, **our security mechanisms must evolve to detect and mitigate these threats,** because **doing the same things as before will no longer work**. **Change is not optional; it is necessary.** The choices we make today will define tomorrow's digital world. **With scams targeting nearly every internet user each day**, we can either let criminals exploit what makes us human, or we can protect the trust and the shared space that connects us all.

A wave of scams is coming, and awareness will allow us to safely surf the wave rather than sink beneath it.

References

- *https://www.europol.europa.eu/media-press/newsroom/news/crypto-investment-fraud-ring-dismantled-in-spain-after-defrauding-5-000-victims-worldwide*
- *https://www.globenewswire.com/news-release/2025/06/25/3105287/0/en/AI-Generated-Scams-Claim-62-More-Victims-Year-Over-Year-Despite-Declining-Consumer-Concern-New-Sift-Report-Reveals.html*
- *https://www.infosecurity-magazine.com/news/reported-impersonation-scams-surge/*
- *https://www.thebureauinvestigates.com/stories/2025-06-27/quishing-new-qr-code-scam-sweeps-uk-car-parks*
- *https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai*
- *https://www.msn.com/en-us/money/personalfinance/scam-losses-worldwide-this-year-have-reached-1-trillion-how-to-protect-yourself/ar-AA1tFwHV*
- *https://www.theguardian.com/money/2024/sep/18/warning-social-media-videos-exploited-scammers-clone-voices*
- *https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024?utm_*
- *https://www.cbsnews.com/news/online-scams-2024-statistics-fbi/?utm*
- *https://www.reuters.com/world/us/fbi-says-cybercrime-costs-rose-least-16-billion-2024-2025-04-23/?*
- *https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams*
- *https://www.cyber.gov.au/learn-basics/explore-basics/recognise-and-report-scams*
- *https://antifraudcentre-centreantifraude.ca/protect-protegez-eng.htm*
- *https://keepnetlabs.com/blog/top-phishing-statistics-and-trends-you-must-know*
- *https://identitytheft.org/attacks/phishing/statistics/*
- *https://www.axios.com/2025/05/27/chatgpt-phishing-emails-scam-fraud?*

CTM360®

Making you a Harder Target in Cyberspace

External | Consolidated | Turn-key | Fully Managed