Graphika

ATLAS

GRAPHIKA HIGHLIGHTS REPORT

Scams & Fraud: Social Engineering at Scale

Selected Insights From Graphika's ATLAS Intelligence Reporting on Online Scams

04.2025

Scams & Fraud

Selected Insights From Graphika’s ATLAS Intelligence Reporting on Online Scams

Overview

This report contains selected insights from Graphika’s ATLAS intelligence reporting on Scams & Fraud between March and April 2025. Graphika subscribers can access a full set of insights, as well as accompanying data and signals. Please visit the Graphika website for more information. Below is a summary of our findings:

- Online scammers continue to exploit trusted institutions and social media platforms to deceive users, with recent activity focusing on impersonating banks, aid organizations, and government agencies. These accounts leverage familiar branding, urgent messaging, and false promises to extract money or sensitive information — often targeting financially vulnerable individuals and exploiting real-world events like tax season or job insecurity.

- Scammers impersonating bank employees continue to target Chase customers who use the bank’s money transfer app, Zelle. Social media users report increasingly sophisticated tactics — including spoofed caller IDs, official-sounding terminology, and detailed scripts — to mimic internal fraud response procedures and trick victims into irreversible transfers.

- Other fraud campaigns have hijacked trusted platforms like Facebook and TikTok to pose as financial aid intermediaries, especially promoting fake grants or donations. These efforts rely on stock imagery, deceptive language, and private communications to establish false legitimacy and lure users into sharing sensitive information.

- Scammers are also exploiting economic pressures and seasonal trends, such as tax refund concerns and job insecurity, to promote fraudulent fund recovery and fake employment opportunities. These accounts often masquerade as cybersecurity professionals or corporate recruiters and redirect victims to encrypted messaging apps, such as WhatsApp or Telegram, to continue the deception beyond public scrutiny.

- These social engineering campaigns will almost certainly continue to evolve, with scammers adapting their tactics to new technologies, trusted brands, and socio-economic vulnerabilities. This trend presents ongoing risks for individuals and institutions alike—particularly as fraudsters exploit the reach and trust of social platforms to scale their operations.

Insights

Social Media Users Report Persistence of Bank Impersonation Zelle Scam

Published on April 4, 2025

Key Finding: Cybersecurity and fraud-focused users on Reddit, Facebook, and X are reporting incidents of scammers impersonating bank employees and tricking victims into sending money via Zelle to fake accounts under the guise of fraud recovery.

Why It Matters: This long-running scam has proved resilient despite efforts from the Consumer Financial Protection Bureau (CFPB) and some major banks to protect customers from Zelle-related fraud.

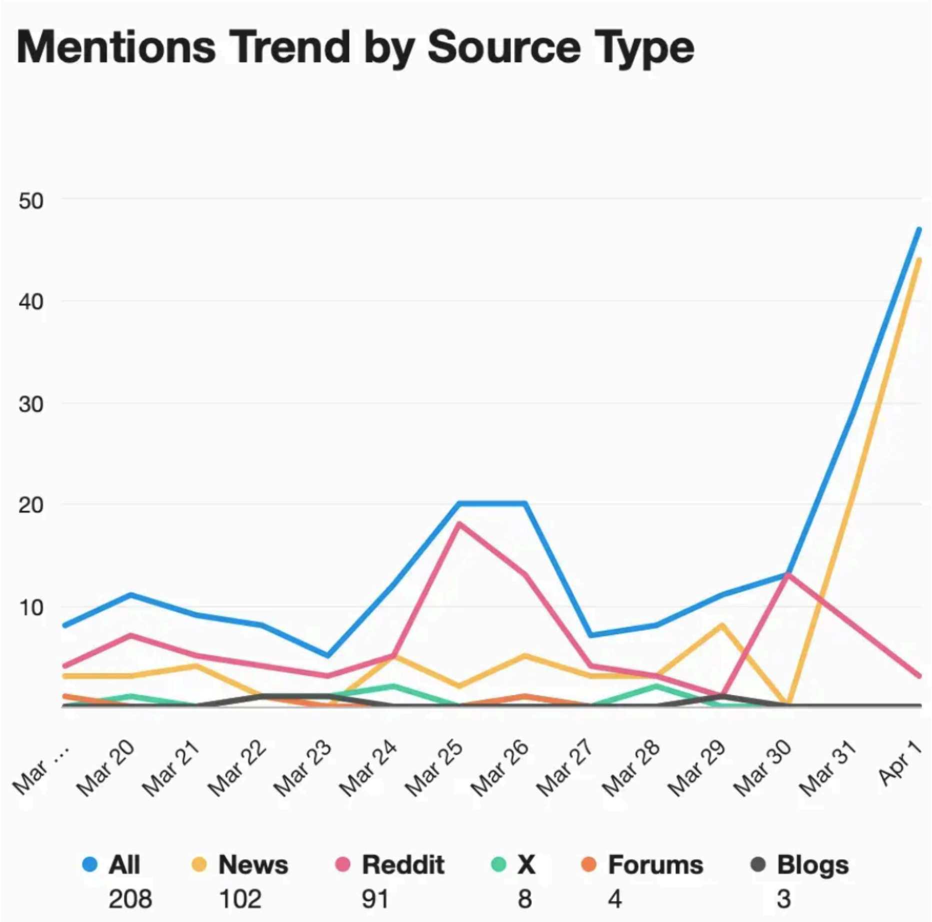
Online Activity:

- On March 29, one Reddit user shared a detailed account of being coached through a fake Chase fraud case — complete with "cancel codes," jazz hold music, and instructions to Zelle $1,998.88 to an account with "VOID 2000" in the memo. The scammer even closed the call with cybersecurity tips after successfully extracting the money, the user said.

- Other social media users' posts reveal that the scam exploits Zelle's instant, irreversible transactions and the trusted branding of major banks – especially Chase – often spoofing caller IDs to display real branch names and phone numbers.

- Victims are directed to fake Zelle branches and told to send money to accounts labeled with initials like "JPMC," further mimicking internal Chase procedures.

- Users on X and Facebook shared firsthand accounts of the scam. One Facebook user reported growing cybersecurity threats, emphasizing Chase and Zelle, suggesting the scam remains widespread and effective, even after legal scrutiny and growing public awareness.



This visualization shows heightened activity for "Zelle," "bank," and "scam" from March 24 – 27, reflecting Chase's Zelle restriction update and continued scam activity. Source: Meltwater.

Facebook and TikTok Accounts Posing as Financial Aid Facilitators to Ensnare Vulnerable Users

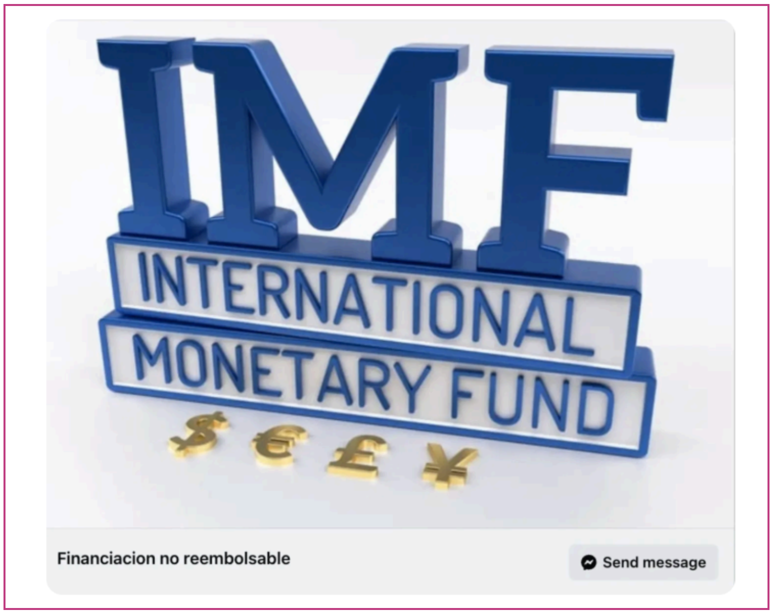
Published on April 3, 2025

Key Finding: Facebook and TikTok accounts are claiming to offer users non-refundable financial aid, such as grants, presenting themselves as intermediaries in requests for assistance from financial institutions. They encourage private communication, likely hoping to lure users into social engineering scams.

Why It Matters: By posing as legitimate aid facilitators, these likely scammers exploit vulnerable individuals seeking financial support and can manipulate victims into providing personal or financial information that may lead to financial loss or identity theft.

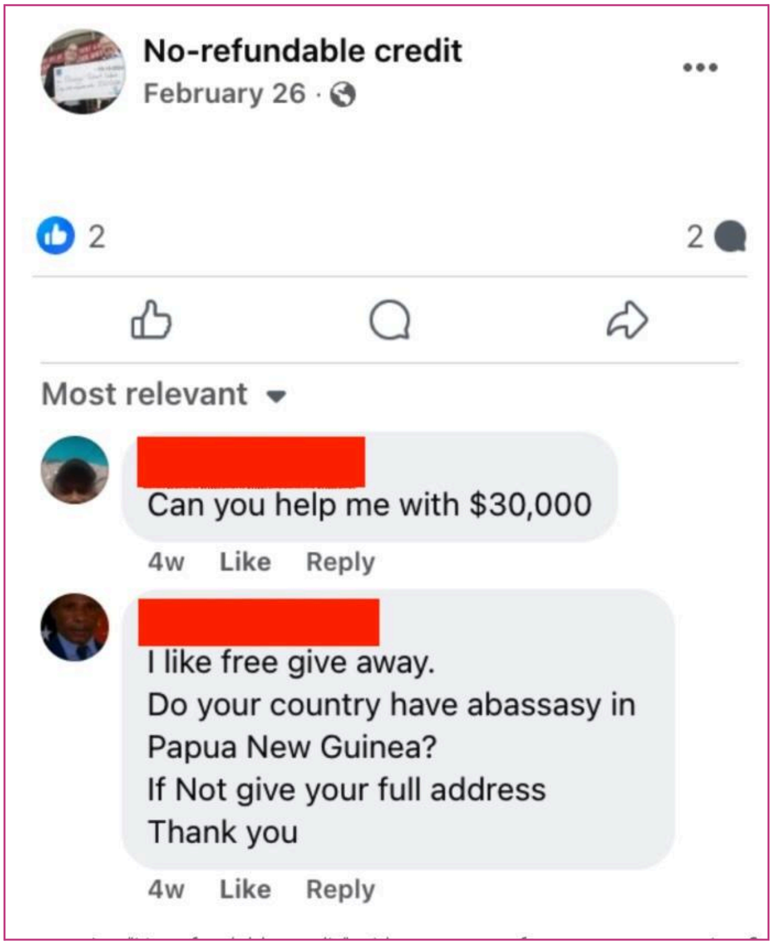
Online Activity:

- Facebook and TikTok accounts are claiming to facilitate access to non-refundable aid from such institutions as the International Monetary Fund (IMF) in promotional posts and account details. The accounts use misleading language to suggest that individuals and businesses can receive grants, donations, or other aid that doesn't require repayment.
- Unlike legitimate financial aid bodies, the accounts request direct contact outside official channels. They provide call-to-action buttons and website links, and also encourage victims to respond via direct message, email, or phone, with contact details in their bios or posts.
- Other signs of illegitimacy include all the accounts being created within the past year, their use of stock images, and their inconsistent details, such as phone number area codes inconsistent with the page administrator's stated location.
- Posts on these accounts claim to facilitate applications by handling administrative procedures. They foster a sense of credibility through terminology – such as "0% Non-Refundable International Financing Facility (NRIF)" – and imagery associated with financial institutions, increasing the likelihood that users will share personal or financial information.



Financiacion no reembolsable

An image included in a likely inauthentic financial assistance offer posted on Facebook. The post requests direct contact through a call-to-action button.



No-refundable credit
February 26 ·

2 2

[redacted]
Can you help me with $30,000
4w Like Reply

[redacted]
I like free give away.
Do your country have abassasy in
Papua New Guinea?
If Not give your full address
Thank you
4w Like Reply

A Facebook page promoting "No-refundable credit," with comments from users requesting financial assistance. Redactions added by Graphika.

Scammers Entice US Taxpayers With Fund Recovery Services on Facebook, TikTok

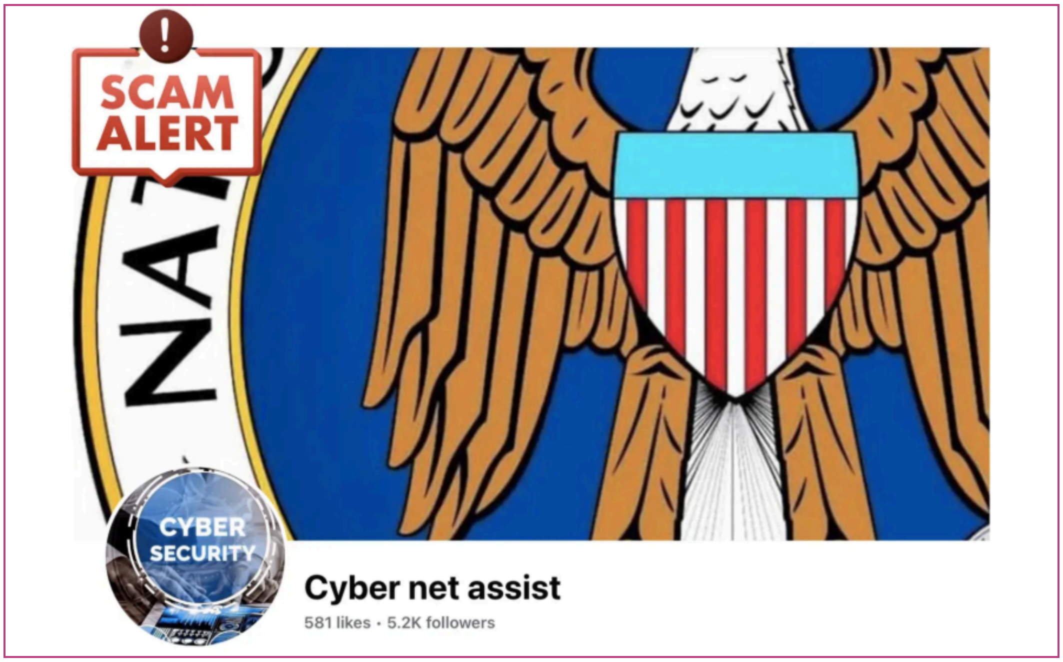
Published on March 24, 2025

Key Finding: Scammers are exploiting the U.S. tax season by infiltrating discussions on Facebook, TikTok, and other social media platforms about Internal Revenue Service (IRS) scams, posing as past victims who have allegedly recovered stolen funds, or as recovery specialists offering assistance. Their messages use persuasive language, likely to lure individuals into fraudulent recovery schemes.

Why It Matters: This well-known tactic highlights the growing threat of scammers capitalizing on means of real-time online interaction, in this case exploiting vulnerable individuals' trust so they fall prey to more scams, leading to significant financial loss and continued victimization.

Online Activity:

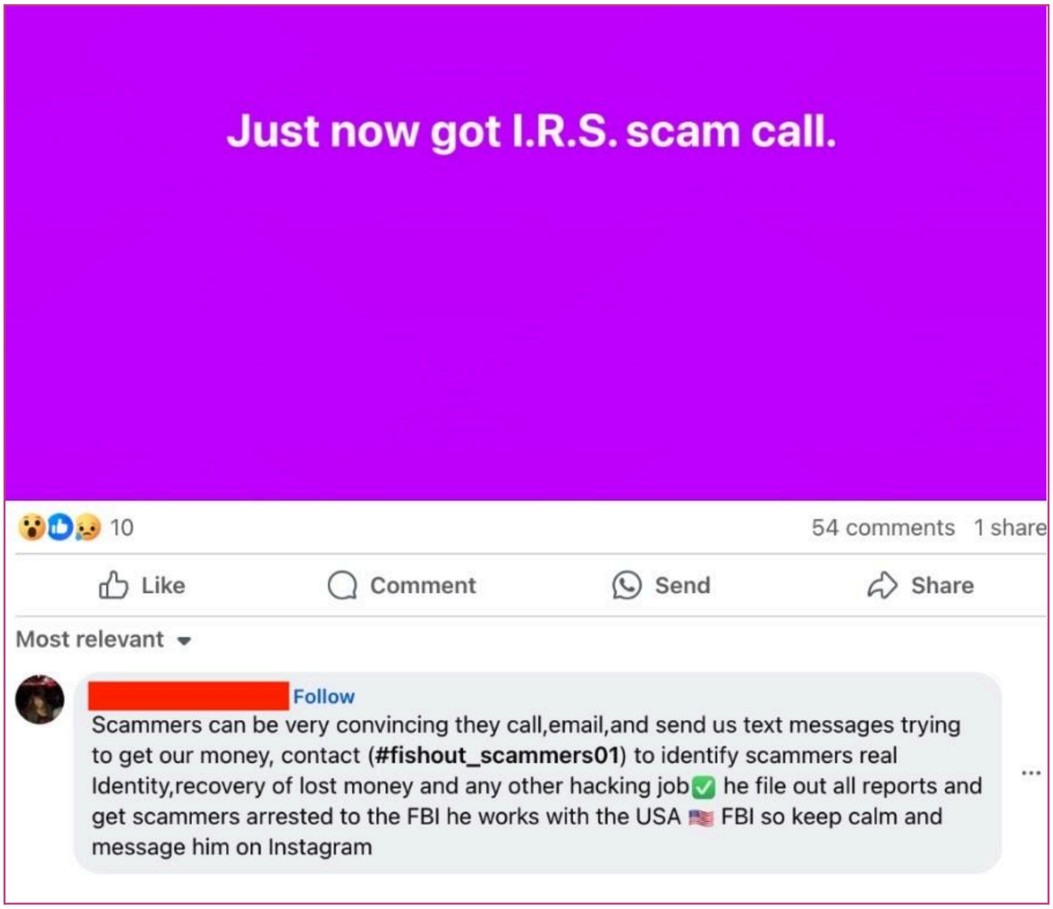
- Primarily on Facebook and TikTok, scammers have been targeting individuals who have previously reported receiving fake IRS messages, commenting on their public posts discussing IRS-related fraud.
- The scammers pose as either recovery specialists offering scam victims assistance, or as past victims who claim they successfully recovered their stolen funds. Using emotive and sometimes urgent language, such as "My money were [sic] taken by some impersonators. I was so depressed and felt like the whole world is against me," they urge the social media users to contact them via direct message or follow links or hashtags to other accounts on Facebook, Instagram, or Telegram.
- The scam operators often impersonate cybersecurity professionals, law enforcement officials, or so-called ethical hackers, adopting authoritative names and branding on their social media accounts. They use imagery related to cybersecurity, hacking, and financial recovery to enhance credibility.



Cyber net assist

581 likes • 5.2K followers

A reply to a Facebook user's post about a U.S. tax scam contained a hashtag leading to an account of a purported professional cybersecurity service.



Just now got I.R.S. scam call.

[redacted] Follow

Scammers can be very convincing they call,email,and send us text messages trying to get our money, contact (**#fishout_scammers01**) to identify scammers real Identity,recovery of lost money and any other hacking job✅ he file out all reports and get scammers arrested to the FBI he works with the USA 🇺🇸 FBI so keep calm and message him on Instagram

Facebook post from a user claiming to have received fake messages from the Internal Revenue Service, and a reply encouraging the user to seek help via a hashtag leading to an Instagram account. Redactions added by Graphika.

Fraudsters Pose As TikTok Recruiters in UK Social Engineering Using WhatsApp

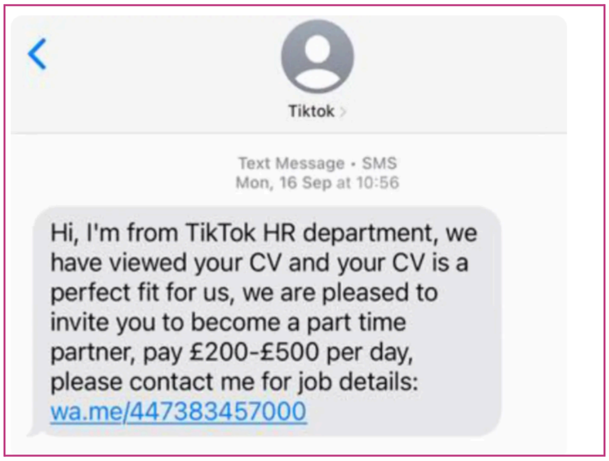
Published on March 17, 2025

Key Finding: Fraudsters are impersonating TikTok human resources (HR) staff in SMS phishing messages offering U.K. recipients lucrative jobs and directing them to private WhatsApp conversations. Based on media reports and past similar activity, we assess the scammers are very likely using these social engineering techniques to elicit sensitive personal and financial information.

Why It Matters: This activity demonstrates how scammers exploit trusted brands and a desire for well-paid work opportunities. It also follows a pattern of scammers directing targets to end-to-end encrypted messaging services, where it's easier to avoid detection by network providers or law enforcers.

Online Activity:

- The scammers primarily use SMS to pose as TikTok HR in messages sent from U.K. phone numbers. They offer enticing, inauthentic opportunities for easy income, such as, "We are pleased to invite you to become our part-time partner, with a salary of £300-800 per day."
- The messages end with the sender inviting the recipient to a private chat on WhatsApp via a wa.me "click-to-chat" link. On WhatsApp they very likely attempt to trick targets into sharing sensitive personal and financial details.
- Reports of the scam have surfaced on social media platforms, such as X and Facebook, with users sharing screenshots of fraudulent messages and warning others about the scam's deceptive tactics.
- Recent news articles on the scam note that the messages sometimes describe the inauthentic work as watching and "liking" TikTok videos. These reports highlight the scam's growing impact on U.K. users.



Text Message • SMS
Mon, 16 Sep at 10:56

Hi, I'm from TikTok HR department, we have viewed your CV and your CV is a perfect fit for us, we are pleased to invite you to become a part time partner, pay £200-£500 per day, please contact me for job details: wa.me/447383457000

Phishing scam message purportedly from TikTok's human resources department, offering a part-time job for substantial compensation and providing a WhatsApp chat link.

Scammers Target US Drivers with Fake Toll Charges Via SMS, Email, and iMessage

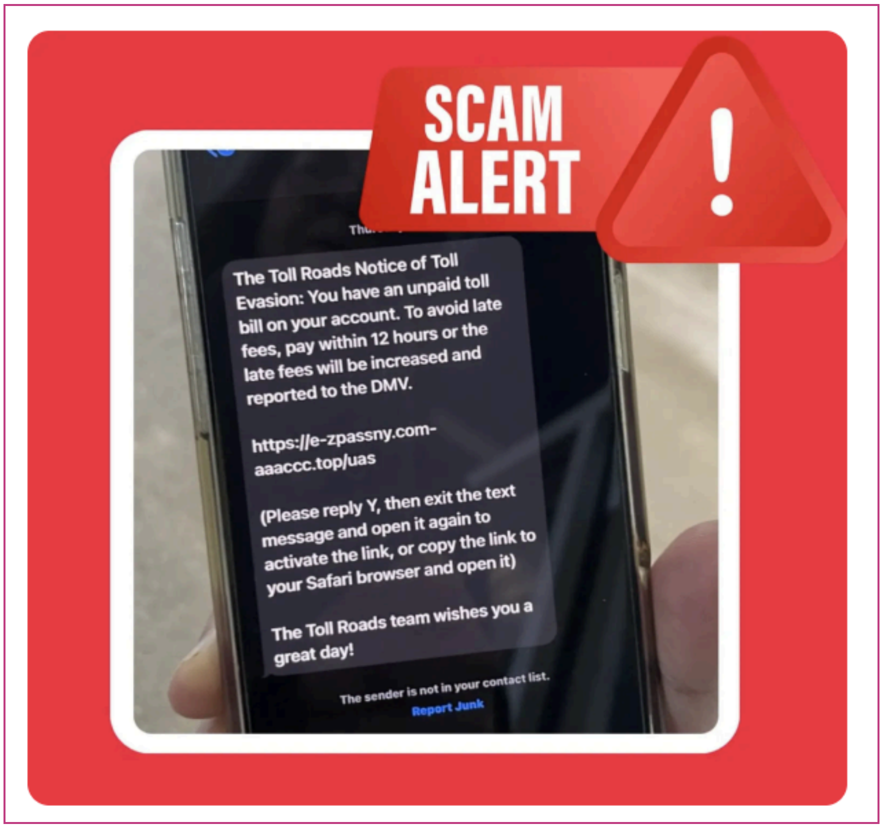
Published on Mar 10, 2025

Key Finding: Scammers are impersonating U.S. state agencies and electronic toll systems to issue fake toll charges and steal sensitive information from U.S. drivers. The scammers distribute the fake charge notices via SMS, iMessage, and email, warning of purported traffic fines and directing recipients to a fraudulent website that mimics official road agencies.

Why It Matters: This activity shows how scammers impersonate trusted entities and directly contact users to trick them into making fraudulent payments or revealing sensitive personal information. Scammers have used fake warnings of unpaid traffic charges as a long-standing "hook" to lure in targets.

Online Activity:

- On March 6, we observed a surge in online discussions about fraudulent messages impersonating toll agencies. The scam involves informing recipients of alleged unpaid tolls and directing them to fake websites that prompt users to input their personal and financial information.
- The scammers use SMS, iMessage, and iCloud email addresses and send messages from U.S., U.K., and Philippine phone numbers. The messages reference a real agency and often warn of penalties like late fees or license suspension – likely to lend credibility to the operation and create a sense of urgency.
- Each message includes a link to various fraudulent websites that mimic an official road agency but with slight domain name changes, design inconsistencies, and mismatched branding.
- Cases have been reported on social media in Ohio, Illinois, New York, and Florida. Social media users on X, Facebook, Instagram, TikTok, and Reddit have shared screenshots of their personal experiences encountering the scam.



The Toll Roads Notice of Toll Evasion: You have an unpaid toll bill on your account. To avoid late fees, pay within 12 hours or the late fees will be increased and reported to the DMV.

https://e-zpassny.com-aaaccc.top/uas

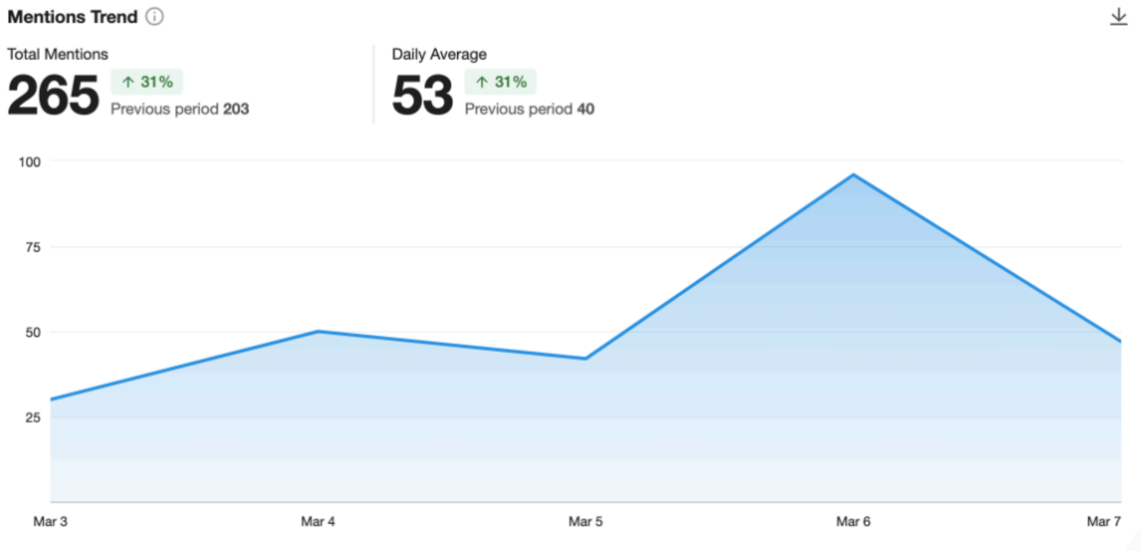
(Please reply Y, then exit the text message and open it again to activate the link, or copy the link to your Safari browser and open it)

The Toll Roads team wishes you a great day!

The sender is not in your contact list.

Report Junk

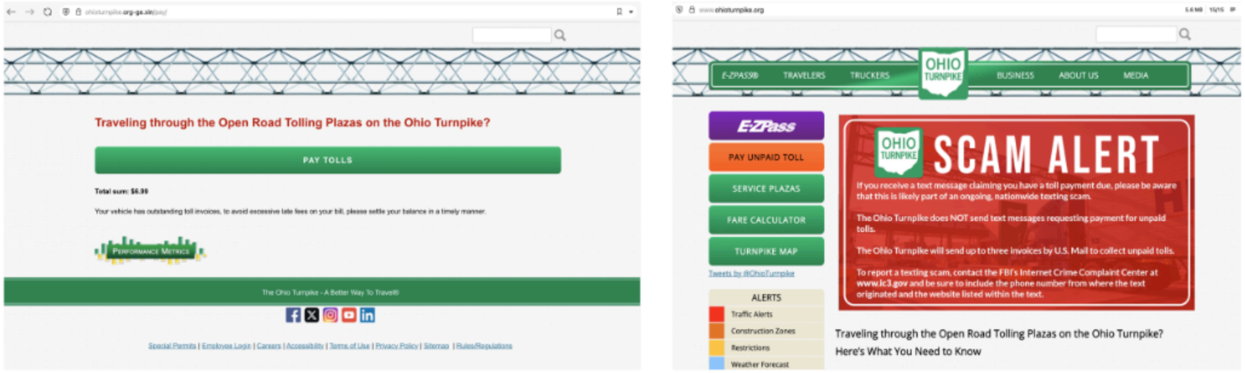
A police department in Virginia shared this image warning about scams using a fraudulent unpaid toll notice that urges immediate payment through a suspicious link.


Mentions Trend

Total Mentions
265 ↑ 31%
Previous period 203

Daily Average
53 ↑ 31%
Previous period 40

Social media discussion around an "unpaid toll" related to scams, fraud, or phishing in the U.S. surged on March 6. Source: Meltwater.



Traveling through the Open Road Tolling Plazas on the Ohio Turnpike?

Total sum: $6.99

Your vehicle has outstanding toll invoices, to avoid excessive late fees on your bill, please settle your balance in a timely manner.

The Ohio Turnpike - A Better Way To Travel®

SCAM ALERT

If you receive a text message claiming you have a toll payment due, please be aware that this is likely part of an ongoing, nationwide texting scam.

The Ohio Turnpike does NOT send text messages requesting payment for unpaid tolls.

The Ohio Turnpike will send up to three invoices by U.S. Mail to collect unpaid tolls.

To report a texting scam, contact the FBI's Internet Crime Complaint Center at www.ic3.gov and be sure to include the phone number from where the text originated and the website listed within the text.

Traveling through the Open Road Tolling Plazas on the Ohio Turnpike?
Here's What You Need to Know

Fake Website

Original Website

This image compares a fraudulent toll payment website (left) that mimics the Ohio Turnpike's official site. The legitimate website (right) warns about ongoing scams and clarifies that toll payments are not requested via text messages.

Estimative Language Legend

Assessments of Likelihood

Graphika uses the following vocabulary to indicate the likelihood of a hypothesis proving correct. If we are unable to assess likelihood due to limited or non-existent information, we may use terms such as "suggest."

Almost No Chance	**Very Unlikely**	**Unlikely**	**Real Chance**	**Likely**	**Very Likely**	**Almost Certain(ly)**
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%

Confidence Levels: Indicators of Sourcing and Corroboration

Graphika uses confidence levels to indicate the quality of information, sources, and corroboration underpinning our assessments.

Low Confidence	**Medium Confidence**	**High Confidence**
Assessment based on information from a non-trusted source and/or information we have not been able to independently corroborate.	Assessment based on information that we are unable to sufficiently corroborate and/or information open to multiple interpretations.	Assessment based on information from multiple trusted sources that we are able to fully corroborate.

Graphika

About Us

Graphika *is the most trusted provider of actionable open-source intelligence to help organizations stay ahead of emerging online events and make decisions on how to navigate them. Led by prominent innovators and technologists in the field of online discourse analysis, Graphika supports global enterprises and public sector customers across trust & safety, cyber threat intelligence, and strategic communications spanning industries including intelligence, technology, media and entertainment, and global banking. Graphika continually integrates new and emerging technologies into our proprietary intelligence platform and analytic services, empowering our customers with high-precision intelligence and confidence to operate in a complex and continuously evolving information environment.*

For more information or to request a demo, visit our website.

© Graphika All Rights Reserved 2025