

Bitdefender Labs Warns of Global Fake Toll Text Scams

B bitdefender.com/en-us/blog/labs/operation-road-trap

Alecsandru Cătălin DAJ

Operation Road Trap: Fake toll and parking texts are spreading worldwide

[Alina BÎZGĂ](#) [Adina Lenuta Maria COLF \(MATEESCU\)](#) [Vlad CONSTANTINESCU](#)

April 29, 2026



A new mass smishing campaign uncovered by Bitdefender Labs shows that scammers are sending tens of thousands of fraudulent text messages to mobile users across 12 countries, impersonating transport authorities, toll operators, and parking services.

Key takeaways

- Since December 2025, Bitdefender Labs researchers have been tracking smishing campaigns targeting drivers on a global scale. The scam campaigns are still active as of April 2026
- **Over 79,000 fraudulent messages** have already been detected in 40 distinct SMS scam campaigns
- The scams impersonate **DMVs, toll operators, and parking authorities** from all over the world
- Victims are redirected to **fake payment sites or, in some cases, malware downloads**

- Its infrastructure is characterized by rapid domain generation, sender-ID spoofing, and multiple evasion techniques targeting mobile operating systems

Since **December 2025 through April 2026**, Bitdefender Labs has been monitoring ongoing smishing campaigns targeting drivers worldwide.

So far, according to Labs' researcher Alecsandru Catalin Daj, fraudsters used:

- **79,000+ scam text messages (over 29,200 unique variants)**
- **Our anti-phishing systems detected over 31,900 different URLs spreading through these unsolicited text messages**
- Activity across **a dozen countries**, including the US, Canada, Australia, New Zealand, France, Spain, Colombia, Brazil, India, the UK, Ireland, and Luxembourg
- Messages delivered in multiple languages, including **English, Spanish, Portuguese, French, and Hindi**



All messages share a common goal: to persuade recipients to pay a fake fine, hand over sensitive information or install spyware.

While the activity is widespread and highly coordinated, **Bitdefender Labs has not attributed these scams to a specific threat actor or group.**

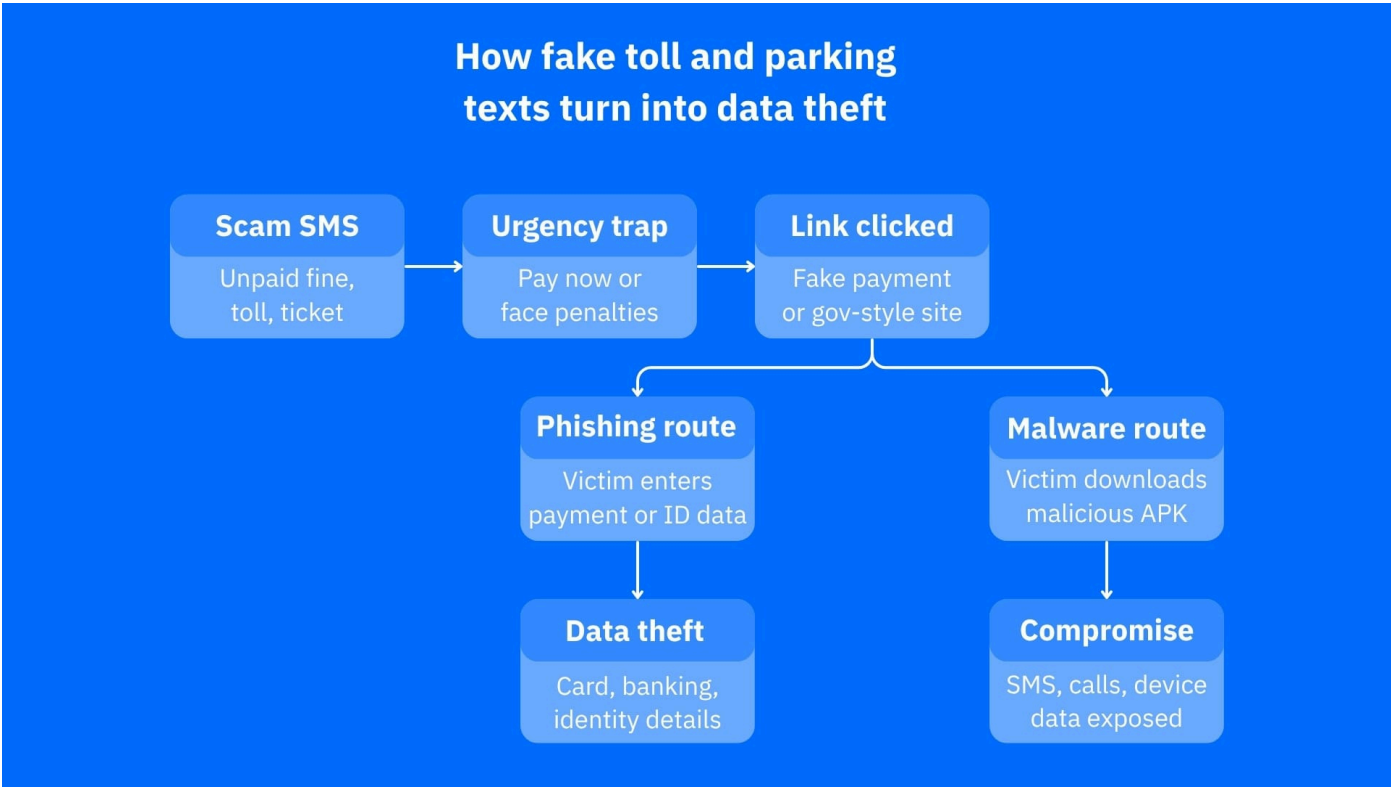
At this stage, there's no confirmed link tying these campaigns together, beyond a shared theme of **messages about unpaid tolls, parking violations, or traffic fines.**

What connects them are similarities in tactics, messaging, and delivery methods, rather than a clearly identified single source.

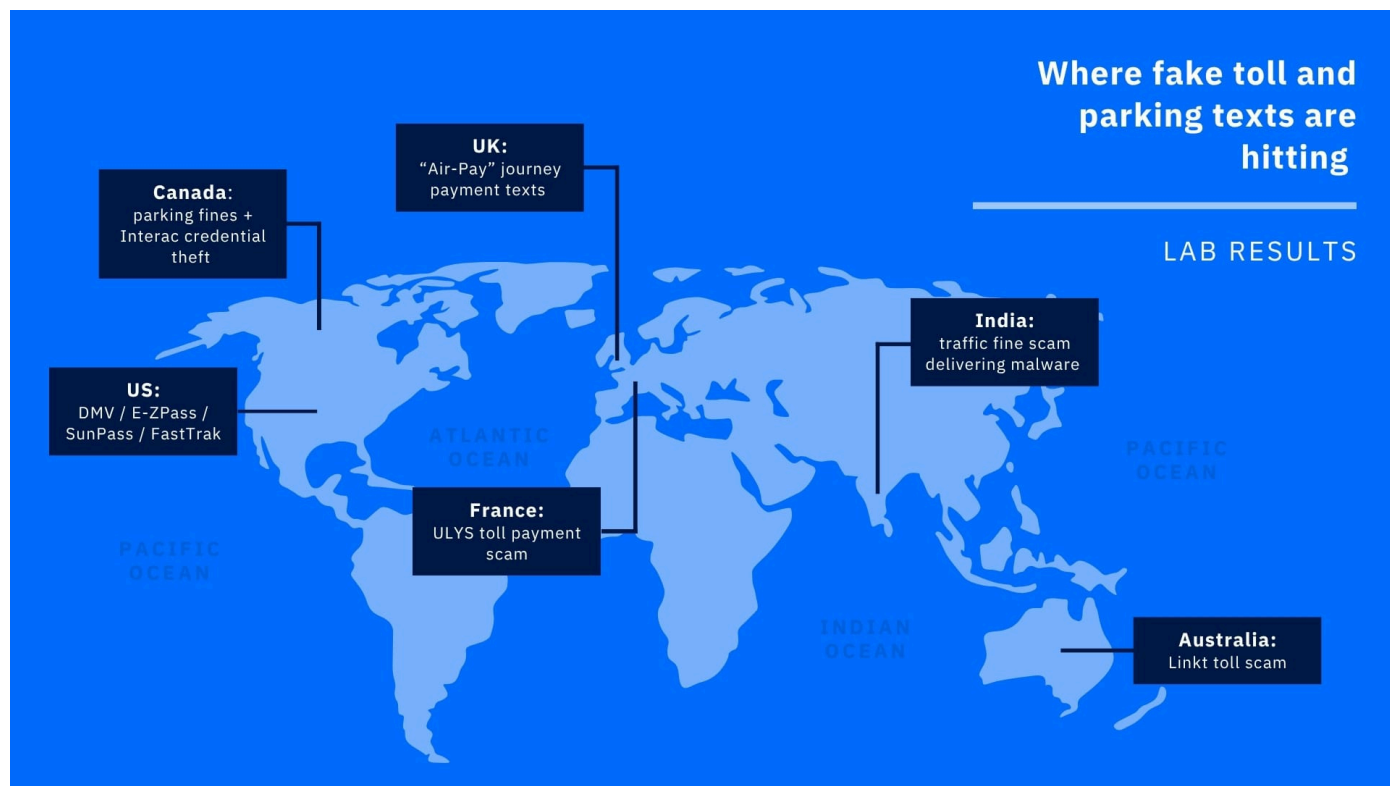
How the scams work

These scam messages are designed to create a sense of urgency and pressure drivers into acting quickly. A typical message claims that the recipient has an unpaid toll, traffic fine, or parking ticket and sets a short deadline, usually between 24 and 72 hours, to resolve the issue. To increase the sense of risk, the message often threatens consequences such as additional fees, license suspension, legal action, or even arrest warrants. It then prompts the recipient to click a link to “resolve” the matter.

That link leads to a fraudulent website designed to closely resemble an official government or toll payment portal. Once there, victims may be asked to enter sensitive information, including card details, personal data, and in some cases, banking credentials. In certain regions, the attack goes a step further by delivering malware instead of a payment page.



Variants by Country



The United States

The largest smishing campaign we've tracked targets drivers in the United States.

The messages rotate between well-known and trusted entities including:

- US state DMVs (California, Florida, North Carolina, Washington DC, and others)
- Toll systems like E-ZPass, SunPass, and FastTrak

Here we've identified:

- 17 distinct scam campaigns and over 25,000 phishing URLs were linked to this fraudulent activity
- Most targeted regions include California and Texas
- Use of spoofed sender names, making messages appear legitimate
- Delivery via short codes (like 7726), which can appear more trustworthy

Example message:

"California Administrative Penalty Notice: You have an unpaid traffic ticket... An arrest warrant will be issued... Your vehicle registration will be suspended starting March 18... Pay: [https://ca\[.\]gov-okqs.bond/portal](https://ca[.]gov-okqs.bond/portal) — (Reply 'Y' and reopen to click the link)"

Canada: Parking fine scam escalating to banking theft

In Canada, particularly in **British Columbia**, the scam evolves into a more complex attack.

It starts as a **parking citation message**, but doesn't stop there.

We've observed:

- Messages impersonating **local parking or city collection services**
- Most targeted regions include British Colombia, Alberta and Ontario
- A second stage targeting **Interac e-Transfer credentials**

This means victims may first attempt to pay a fine, then unknowingly provide **online banking details**, leading to a much broader financial compromise.

Example message:

"Parking Notice: Past due violation on file. Handle the matter before we initiate collection proceedings, please visit the link below. [https://myparking-help\[.\]com](https://myparking-help[.]com)

United Kingdom: 'Air-Pay' road payment texts

One of the most recent identified waves of scam messages is targeting users in the **United Kingdom**, using a simple but effective lure related to road or journey payments.

Researchers spotted:

- A **single active campaign** using this theme
- Use of **minimal text and direct links** to prompt quick action

Example message:

"Pay for your journey by card, click <https://im.air-pay.uk/...>"

Unlike other regions that rely on threats or penalties, this campaign uses a **low-friction approach**:

- No mention of fines or legal consequences
- No urgency or escalation language
- A simple request to "pay for your journey"

Ireland: eFlow toll scam

In Ireland, scammers are impersonating **eFlow**, the electronic toll system used on the M50 motorway.

Researchers identified:

- Most targeted regions include Leinster and Connacht
- Use of **short code 7726**, also seen in campaigns targeting the United States

The messages claim a toll is unpaid and direct users to a payment link.

Example message:

“eflow: You have an unpaid toll on the motorway. Please pay to avoid penalties at: eflow[.]ie-paytoll.info”

Australia: Toll scam impersonating Linkt

In Australia, scammers are impersonating **Linkt**, a legitimate toll operator used across **New South Wales, Victoria, and Queensland**.

What makes this campaign particularly persuasive is how the messages are delivered.

We’ve observed over **2,200+ shortened URLs** used to hide malicious links

The sender name is spoofed as “Linkt,” which can cause the message to appear in **existing, legitimate message threads** on some devices.

Example message:

“Linkt: Your toll remains unpaid. Last reminder — outstanding toll fees may escalate to recovery action and result in rego restrictions. Pay now: <https://cutt.ly/...>”

“Last reminder - outstanding toll fees could escalate to recovery action and result in rego restrictions. Pay now to avoid impact. [https://paylinkt\[.\]vip/au](https://paylinkt[.]vip/au)”

New Zealand: Police and justice system fine scam

In New Zealand, scammers are impersonating **NZ Police and the Ministry of Justice**, targeting users with messages about overdue traffic fines.

What stands out:

- Scammers’ use of **government-themed domains** to look legitimate
- Most-targeted regions include: Auckland, Wellington Region and Canterbury
- Inclusion of **mobile-specific instructions** to increase interaction

The messages claim a traffic fine is overdue and warn of escalating consequences if not paid.

Example message:

“NZ Police: Your traffic fine is overdue over 10 days. Avoid late fees or court referral. Settle the payment now: [https://polices-govt\[.\]link/nz](https://polices-govt[.]link/nz)
(Please reply ‘Y’ then reopen the message to access the link)”

France: ULYS toll payment scam

In France, scammers are impersonating **ULYS**, sending messages in French that closely resemble legitimate toll notifications.

Researchers identified:

- **Most-targeted regions:** Île-de-France, Rhône-Alpes and Provence-Alpes-Côte d'Azur
- **400+ flagged malicious URLs**
- Messages written entirely in **French**, tailored to local users

The messages claim that a small toll amount remains unpaid and must be settled quickly.

Example message:

“ULYS PEAGE : Bonjour <User> Un solde de 6,80 EUR reste impayé suite à un passage au péage avec votre véhicule [redacted]. Merci de régulariser la situation...”

Luxembourg: Government portal parking fine scam

In Luxembourg, scammers are impersonating **Guichet.lu**, the official government services portal, using formal messages related to parking violations.

What stands out:

- One of the smallest smishing campaigns we’ve tracked
- Includes a case reference number, making it feel official
- Mentions specific dates and violations

The messages claim a parking infraction has been recorded and must be resolved to avoid additional penalties.

Example message:

“Guichet – Grand-Duché de Luxembourg. Référence dossier : 2026-458721. Motif : Infraction de stationnement relevée le 21/03/2026. Régularisez via [https://lu-retrofacturation\[.\]com](https://lu-retrofacturation[.]com) afin d’éviter une majoration.”

Colombia: Toll and traffic fine texts at scale

The second-largest wave of scam messages has been targeting users in Colombia, particularly in **Bogotá, Antioquia, and Valle del Cauca**.

The messages impersonate **toll operators and traffic authorities**, using multiple sender numbers to distribute the scam at scale.

We've identified:

- **11,000+ scam messages** linked to this fraudulent activity
- **Multiple rotating short codes** (including 893181–893183 and 893175)
- Use of **repeated domain patterns**, mainly through bibtly.cc and bitcutt.cc

All links ultimately redirect users to phishing pages designed to collect payment details.

Example message:

Sr(a) INFRACTOR! Iniciamos proceso juridico por sanciones viales. Salda HOY con DCTO del 50% en nuestro portal. Consulta: .b2026.biltly[.]cc/ Aplican TyC

Spain: DGT traffic fine scam

In Spain, scammers are impersonating the **DGT (Dirección General de Tráfico)**, the official traffic authority.

Researchers identified:

- The most-targeted regions include Madrid, Catalonia and Andalusia
- Use of **spoofed sender names**, including “DGT” and “miMultas”

The messages are written in Spanish and warn users about an unpaid traffic fine.

Example message:

“[DGT]: Último recordatorio antes del aumento de su multa pendiente de pago. Consulte su expediente en el siguiente enlace: [https://seguridad-ahora\[.\]im/dgt.php](https://seguridad-ahora[.]im/dgt.php)”

“Ultimo recordatorio antes del aumento de su multa pendiente de pago. Consulta tú expediente: [https://mimultas-es\[.\]wasmer](https://mimultas-es[.]wasmer) STOP/INFO: [https://mcsms\[.\]io/aua1bG](https://mcsms[.]io/aua1bG)”

Brazil: Traffic fine and tax obligation scam

In Brazil, scammers are combining **traffic-related themes with tax-related pressure**, targeting users with messages about obligations tied to their **CPF (Brazilian tax ID)**.

Researchers identified:

- Messages written in **Portuguese**, tailored to local users
- Most messages were concentrated in **São Paulo, Rio de Janeiro and Minas Gerais**
- Use of **short code 70101** for delivery

The messages warn users about an alleged open obligation and urge them to act quickly to avoid restrictions.

Example message:

“🚨 Comunicado importante: Obrigação tributária em aberto. Tome as devidas providências, evitando restrições em seu CPF. Confira: [https://confira\[.\]online/app3](https://confira[.]online/app3)”

India: Traffic fine scam delivering malware

In India, the campaign takes a more direct approach by delivering **malware disguised as traffic fine notices**.

The messages impersonate:

- The **Ministry of Road Transport and Highways (MoRTH)**
- Mobile carrier **Airtel**

We’ve identified:

- **828 URLs** delivering malware
- Most-targeted regions include Karnataka, Maharashtra and Telangana
- Multiple variations using realistic “e-challan” (traffic fine) references

Unlike other regions, the goal here is not just to collect payment details but to **install malicious APK on the victim’s device**.

Example message:

*RTO Notice: Your vehicle has an Over Speeding challan [redacted] issued on 22-03-2026.
Check & Download now: [malicious link]*

How these scams trick people into clicking

Even though the messages come from different countries and impersonate different agencies, they share a very similar pattern designed to pressure you into acting fast.

The “escalation” tactic

Most messages follow the same script:

- Recipients are told they have an **unpaid toll, fine, or citation**
- They’re given a **short deadline** (often 24–72 hours)
- A **penalty fee** is added (commonly around 35%)
- The message warns of consequences, including license suspension, vehicle registration issues, and even legal action or arrest

- Users are pushed to **click a link to resolve the issue immediately**

Tricks designed specifically for mobile users

Bitdefender researchers also observed several techniques meant to bypass phone protections and make messages look more convincing:

“Reply Y” before clicking

Some messages ask you to reply first. On iOS devices, this activates links that would otherwise be blocked, making the scam easier to access.

Messages that look identical to legitimate ones

Multiple scam campaigns substitute Cyrillic lookalike characters (e, s, m, i, τ) for their Latin equivalents, to bypass keyword-based SMS spam filters.

Websites that mimic government pages

Links often include words like “gov” or “official,” even though they lead to fake domains.

Sender ID spoofing

Messages may appear to come from trusted brands or authorities and can even show up in existing message threads. Examples include “Linkt” in Australia and “miMultas” in Spain, which cause messages to appear in the victim’s existing legitimate brand thread on some devices.

Hidden or shortened links

URL shorteners disguise the final destination, making malicious links look harmless.

Constantly changing domains

The scamsites are frequently replaced, helping campaign stay active even after some links are blocked.

Hidden Malware Layer

While many of these scams aim to steal payment details, some cases go further.

We’ve spotted hybrid attacks especially targeting drivers in India. Here, the text messages include **direct “Download” calls to action**, pushing users to install apps like *Rtochallan.apk* hosted on platforms such as GitHub.

According to **researcher Adina Mateescu**, the app typically loads a **fake payment interface inside a WebView** (a built-in browser component), designed to mimic a government portal and collect personal data.

The screenshot shows a mobile application interface titled "eChallan System Enforcement Solution" with the subtitle "Ministry of Road Transport & Highways". It features the Indian national emblem at the top left. The form contains four input fields: "Full Name" (placeholder: "Name as per RC"), "Mobile Number" (placeholder: "10 Digit Mobile Number"), "Mother Name" (placeholder: "Mother's Name"), and "Date of Birth" (a date picker). A blue "PROCEED" button is at the bottom of the form. Below the form is a copyright notice: "Copyright © 2025. All Rights Reserved." At the bottom of the screen is a banner image showing a person in a uniform using a handheld device to scan a document labeled "E-CHALLAN". The entire interface is displayed within a mobile app container with a status bar at the top and an Android navigation bar at the bottom.

These apps are not isolated threats. They belong to a broader **malware family of Android trojans** designed to steal financial and personal data while maintaining ongoing access to the device.

Once installed, the malware immediately establishes persistence by running a **foreground service** (often with a generic name like *MyService*), ensuring it continues operating even after the app is closed or the device is rebooted.

From that point, it begins:

Device profiling

Collecting information such as device ID, Android version, IP address, carrier, and battery status

SIM and phone data enumeration

Gathering phone number, SIM details, and network provider information

SMS harvesting and monitoring

Accessing messages and filtering them for financial keywords related to banking, payments, and transactions

This activity happens **independently of user interaction**, meaning data collection starts even if the victim never completes the phishing form.

How data is stolen and commands are executed

This malware family uses a dual infrastructure for communication and control.

Telegram

Telegram is used as a primary channel for data exfiltration and operator communication. The malware loads embedded bot tokens and chat IDs from its internal resources (such as `res/raw/Loda` or `assets/index.html`) and uses the Telegram Bot API to send messages directly to attacker-controlled channels. Through this mechanism, stolen data is transmitted in real time, allowing operators to receive detailed reports that include device information, intercepted SMS messages, and summaries of victim activity.

Firebase — remote command and control

At the same time, the malware connects to Firebase Realtime Database, which functions as a live command-and-control panel. Through this channel, attackers can remotely interact with the infected device, forwarding incoming SMS messages to their own numbers, sending messages from the victim's phone, and enabling or disabling call forwarding. They can also push commands and update the malware's behavior in real time. This setup turns the infected phone into a remotely managed device.

Why this is especially dangerous

What sets this malware family apart is how it combines multiple capabilities into a single attack chain:

- **WebView-based phishing** to collect personal and identity data
- **SMS interception** to capture banking alerts and one-time passwords
- **Call and message control** to manipulate communications
- **Cloud-based command systems** for real-time attacker control

In short, it operates as a **hybrid phishing + SMS interception + call forwarding threat**, specifically designed to target **financial data, mobile banking activity, and user identity information**.

Technical indicators (malware samples)

Bitdefender Labs researcher **Adina Mateescu** also identified multiple Android malware samples associated with this campaign, including both **droppers** (initial installers) and the **payload apps** they deploy.

Observed MD5 hashes:

- Dropper: 014cda697a053d39f0504f626cb4aa4b
Dropped APK: bcc411c84a3ba169e1f989929115834f
- Dropper: a2b03b138ec0a6263b73e17372063345
Dropped APK: 71bd06e73ad26ccf19cbc59c02630f14
- Dropper: 25604ed81bc7b603897e390c3c7920e0
Dropped APK: 116b2280004a9d313a30acb767b1a85e
- Dropper: 3711004997a5efc09e3eefab8b2fa91f
Dropped APK: fdd449fc92ea92b8a5b5478b56c56ecd
- Dropper: 3c45b541cb7f29bb60a83564850e775a
Dropped APK: ce83808d52dcff0c6f96ee5874fd841

Most of the dropped applications use package names designed to look legitimate, such as “**com.uptodown**,” while others mimic popular apps like “**com.baidu.searchbox.lite**”.

Fake toll text red flags

- ✓ You weren't expecting the message
- ✓ The message demands urgent payment
- ✓ It threatens license suspension, legal action, or arrest
- ✓ The link looks unusual or shortened
- ✓ You're asked to reply "Y" before opening the link
- ✓ It mentions a "35% late fee"
- ✓ It asks for card, banking, or personal details
- ✓ The sender appears official, but the domain doesn't match

If you receive a message about a toll or parking fine, take a moment to think about the following:

- Did you expect this message?
- Is there pressure to act immediately?
- Does the link look unusual or unfamiliar?
- Are you being asked to reply before accessing the link?
- **Does the message mention a “35% late fee”?**

This exact phrase has been identified across multiple scam campaigns and serves as a serious red flag.

Legitimate authorities **rarely request payments through unsolicited text messages with embedded links.**

These scams aren’t new, but they’re getting worse

Scam texts about unpaid tolls or fines have been circulating for years, but their scale is growing rapidly. Authorities across the US have issued multiple warnings, highlighting the extent of the problem. The FCC has received complaints about messages impersonating toll services such as E-ZPass, FasTrak, and I-PASS, while the FBI recorded 59,271 toll scam complaints in 2024 alone. At the same time, the Federal Trade Commission reports that consumers lost \$470 million to text-based scams in 2024, a fivefold increase compared to 2020. According to the FTC, these types of messages, including toll-related scams, are now among the most common forms of fraud.

What to do if you receive one

- Do not click the link
- Do not reply to the message
- Verify the information directly on the official website
- Delete and report the message

If you’re unsure, you can safely check suspicious links or messages using tools like [Bitdefender Link Checker](#) or [Bitdefender Scamio](#), which can help you assess whether something is a scam without putting your data at risk.

Why mobile protection matters more than ever

Because these attacks are designed specifically for smartphones, having protection directly on your device is essential.

A mobile security solution can help reduce the risk by blocking malicious links before they load, detecting scam patterns in messages and websites, and flagging suspicious activity even when links are shortened or disguised. But with campaigns like these constantly evolving, protection isn’t just about reacting to threats — it’s also about recognizing them early.

[Bitdefender Mobile Security](#) includes [Scam Radar](#), a feature built into its Scam Protection layer that focuses on early warning. Instead of waiting for a threat to reach your device, Scam Radar monitors emerging scam campaigns and alerts you when they start spreading, including those targeting your region.

It also provides real examples of scam messages, highlights which brands or authorities are being impersonated, and offers clear guidance on what to watch out for. This kind of context is especially useful for scams involving tolls or parking fines, where familiarity and urgency are key tactics.

Knowing that a scam is already circulating (and what it looks like) makes it much easier to recognize and avoid before you click.

tags

[Scam Research](#)

Author

[Alecsandru Cătălin DAJ](#)

Working as Team Lead in the Mobile Security & Forensics Unit, I am always ready to deal with the latest threats in the Android Ecosystem. I like to play the saxophone in my spare time and go fishing.

[View all posts](#)

[Alina BÎZGĂ](#)

[View all posts](#)

[Adina Lenuta Maria COLF \(MATEESCU\)](#)

As part of Bitdefender's android research team, it became natural for her to develop a passion for analyzing malware and developing continuous automated threat elimination tools.

[View all posts](#)

[Vlad CONSTANTINESCU](#)

Vlad's love for technology and writing created rich soil for his interest in cybersecurity to sprout into a full-on passion. Before becoming a Security Analyst, he covered tech and security topics.

[View all posts](#)

Right now Top posts



[Scam Research](#)

[Active Subscription Scam Campaigns Flooding the Internet](#)

April 30, 2025

8 min read

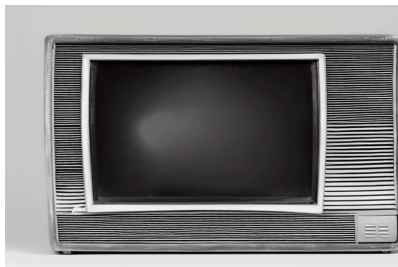


[Anti-Malware Research](#)

[Infected Minecraft Mods Lead to Multi-Stage, Multi-Platform Infostealer Malware](#)

June 08, 2023

5 min read

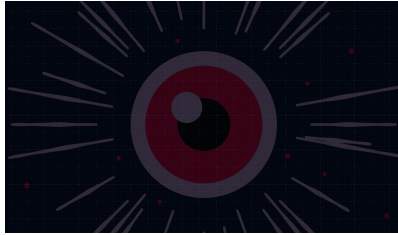


[IoT Research Whitepapers](#)

[Vulnerabilities identified in Amazon Fire TV Stick, Insignia FireOS TV Series](#)

May 02, 2023

2 min read



[Anti-Malware Research Whitepapers](#)

[EyeSpy - Iranian Spyware Delivered in VPN Installers](#)

January 11, 2023

2 min read

FOLLOW US ON SOCIAL MEDIA
