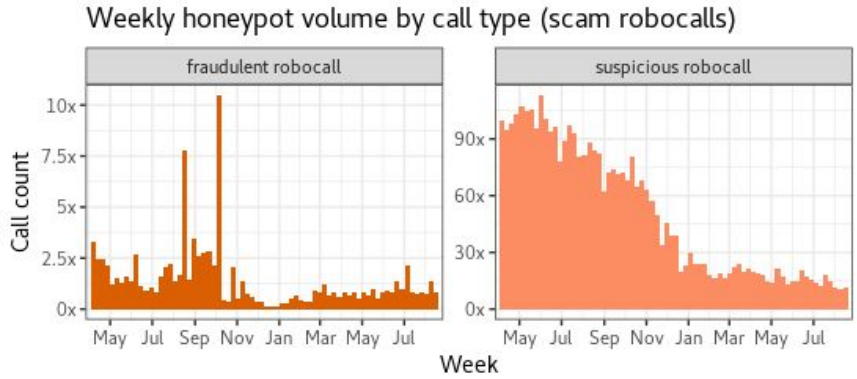
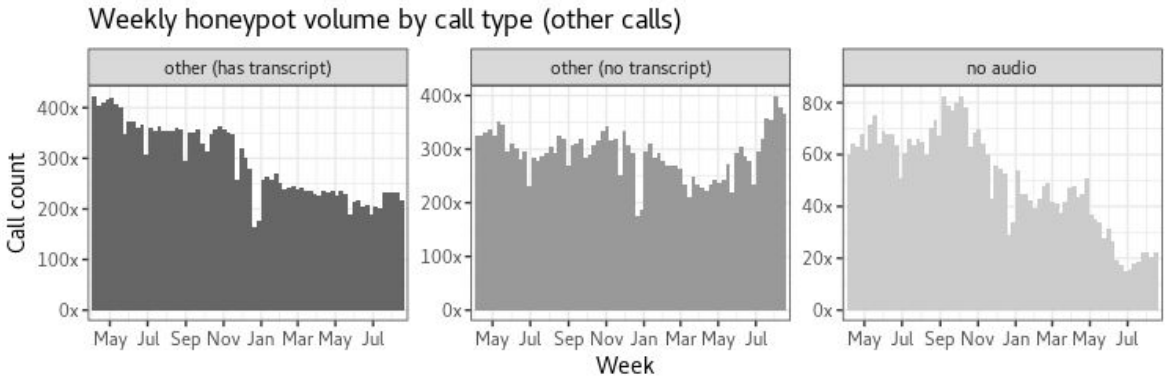
Where Have All The Robocalls Gone? Countering Evolving Telecom Fraud

Ashley Lynn, Kate Kutchko, Jonathan Hurley, Chris Oatway
September 17, 2026

verizon

Suspicious robocalls to our honeypot decreased May 2025 – August 2026





Based on honeypot data, robocalls have dropped dramatically throughout 2025 - 2026 as a direct result of policy changes, successful enforcement, industry best practices e.g. KYC

Fraudulent robocalls show different behaviors than “suspicious” robocalls: **primarily opportunistic**

Spikes in fraudulent robocall volumes in summer 2025 correspond to PBX hacking events of school systems

Other types of honeypot calls (bottom) have also decreased, but not nearly to the same extent as suspicious robocalls

Increased law enforcement and robust industry-wide practices (Know Your Customer, Blocking) have had a dramatic impact on robocalling

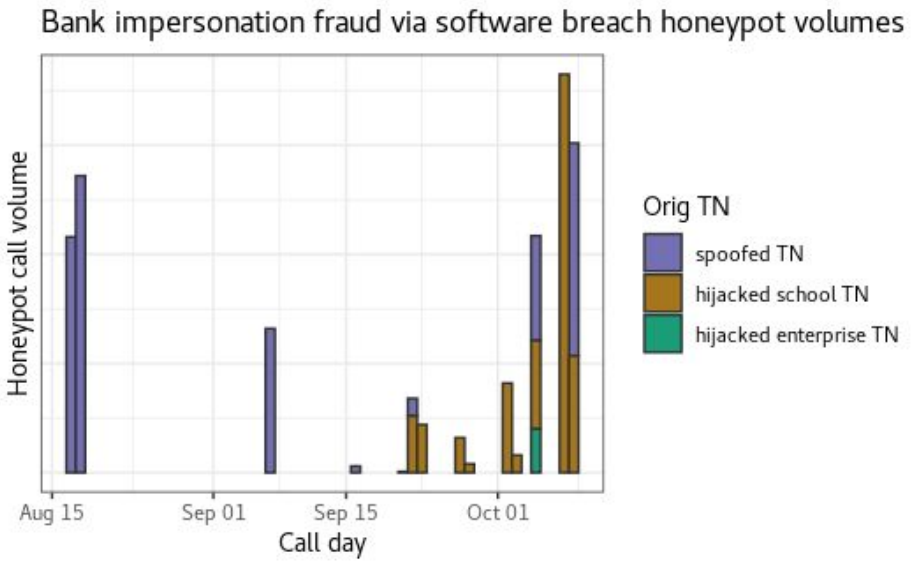
How are robocallers getting around these restrictions?

We see the following in our honeypot:

- **Hacking legitimate enterprises**
- **Exploiting network vulnerabilities**
- **Laundering legitimacy**

Hacking legitimate enterprises: School system calling software breaches

- Bank impersonation via hijacking legitimate communication channels (e.g., school system calling software)
- Both school TNs and (spoofed) bank TNs were seen in the honeypot, as a result of school system calling software compromise
- In one attempt the scammers attempted to place over 1M calls

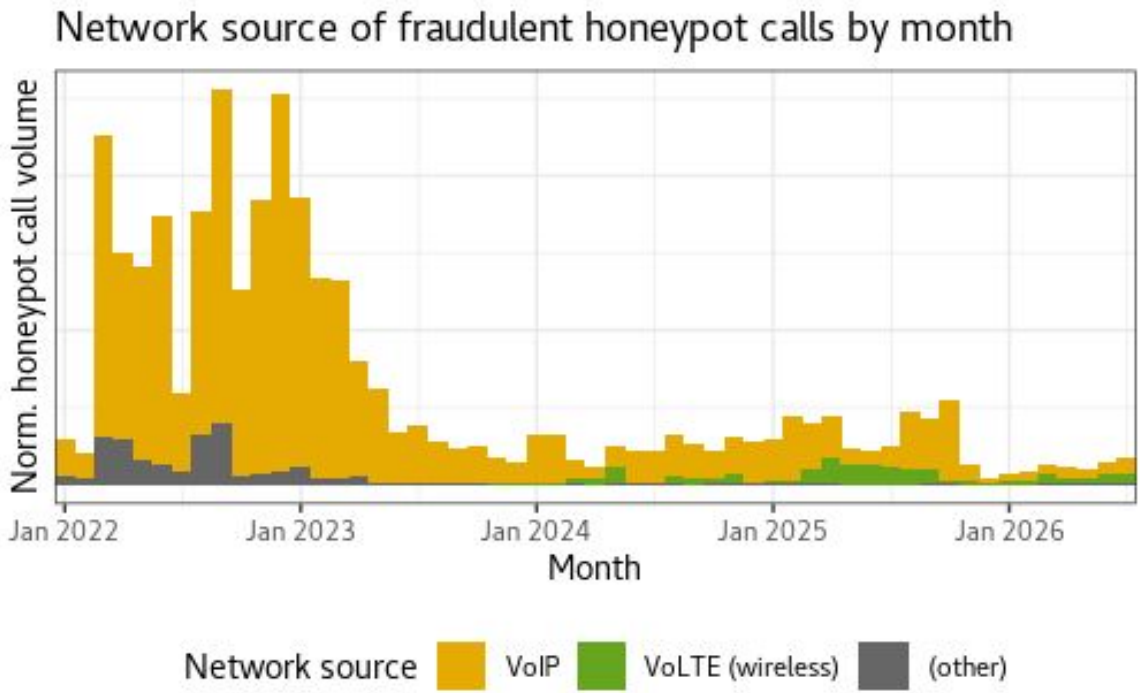


"Bank of America. A purchase was declined for 296.35 at apple.com. Press 1 if you recognize this purchase. If you do not recognize this purchase call us at ..."

Hello this is an important message from Kenosha Unified School District 1. To listen to the message press 1 or simply stay on the line... Wells Fargo. Did you attempt to purchase of 237.49 at Best Buy? Reply yes or if was not you call us immediately at ..."

Simboxes are a new network exploit as fraudsters leave VoIP

- Regulatory changes (traceback, Know Your Customer, STIR/SHAKEN, RMD) have pushed fraudulent robocalls away from VoIP and towards wireless
- Spike in wireless corresponds to simboxes and other forms of wireless abuse – a previously unexploited threat vector



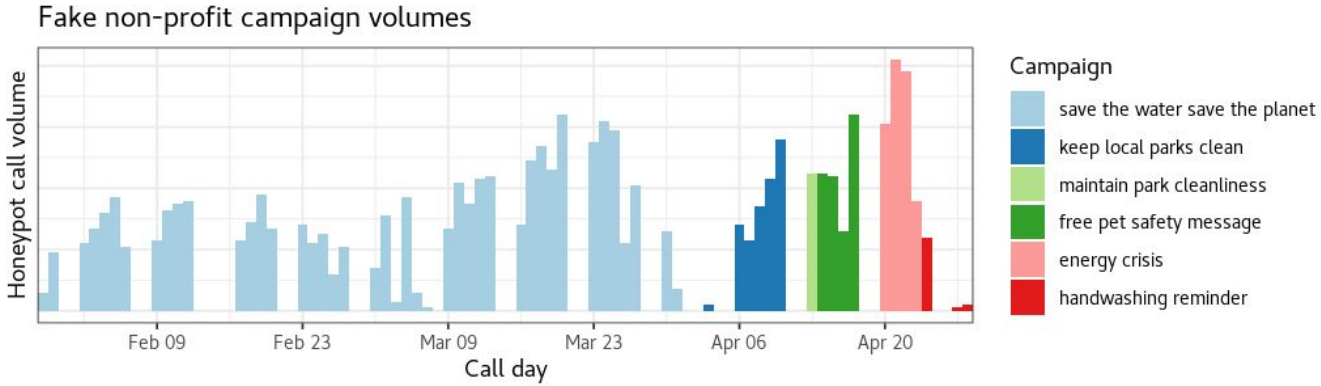
Laundering legitimacy: fake non-profit (and similar) calls

“We are reaching out to you as part of the **Save the Water Save the Planet** helpline. It would mean a lot to me keep track of your impact and engage in our community challenges. You can change your notification preferences or opt out at any time by following the instructions. Every drop can be saved to protect our future. Goodbye...”

“I'm reaching out to inform you of our important initiative to **maintain the cleanliness and safety of our local parks** and communities for all. If you're not interested you can opt out. Would you like to learn more about how you can get involved? For any query call XXX-XXX-XXXX...”

“Hello. This is PetSmart with a **free pet safety message**. Never leave pets in a parked car. Temperatures can become deadly in minutes. Maintain fresh water and shade all year round. Always keep pets on a leash in public and clean up after them. A responsible pet owner protects their pet and their community. Press 1 now or say stop to stop receiving future calls. Press 2 to repeat...”

“hello this is Jonas calling from safeguard. you can reach us at XXX-XXX-XXXX. We're contacting you regarding handwashing. Reminder, **wash your hands with soap and water** for at least 20 seconds about the time it takes to sing Happy Birthday twice.”



Laundering legitimacy: Expired domain “takeovers”

Fraudsters buy old websites from domain name registrars to evade scam detection based on DNS registration age, and to provide a front to evade Know Your Customer programs.

We see multimodal robocalling and text activity in our honeypot utilizing these fronts.

Hi Michael, we await your confirmation: ***txt[.]johnarias[.]com****/vx8xkGEYB Confirm today! Reply STOP to end*

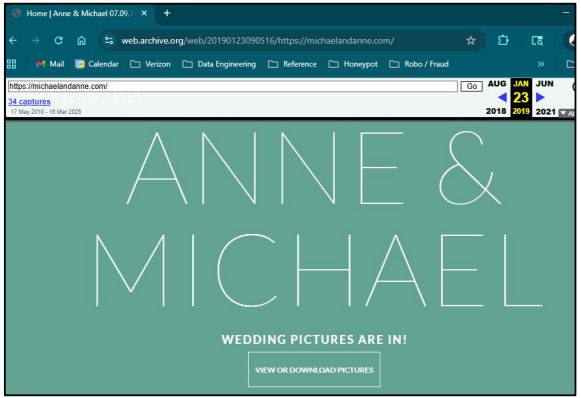
Hi Samiuela, 2 hours left to verify this is your details update. Review it here: ***txt[.]michaelandanne[.]com****/M58ZLD Stop to END*

Hey Linda Your Name Could Be On The List, Find Out Here: ***txt[.]francaismonde[.]com****/qegYydlg Reply STOP to end*

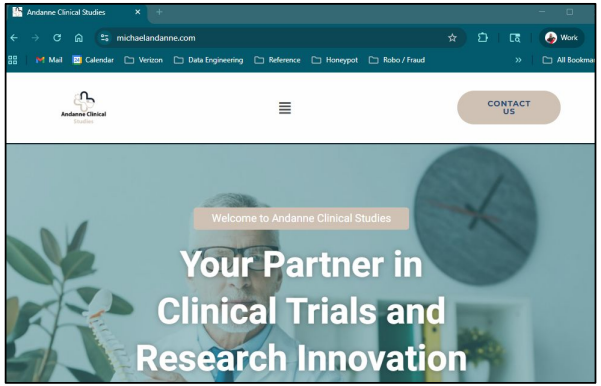
You're subscribed! ***txt[.]suzannemorales[.]com****/1dwlO96 Msg freq. varies. Msg&Data rates may apply. txt HELP for help, STOP to unsubscribe*

Brad, confirm your agreement to proceed here: ***txt[.]andreakrafft[.]com****/kmAHfUlaB STOP to End*

michaelandanne.com circa 2019



michaelandanne.com circa 2025



3-Way Handshake Malicious Mobile Messaging

Malicious Campaign Operators use messaging that imitates Application to Person (A2P) as an initial probe/filter mechanism prior to engaging via a different communications channel, often voice calls, initiated from a different source than the mobile messaging sender address

Initial contact	• Imitates legit A2P communications • Often includes A2P opt-out boilerplate or "correct" brand URLs • Prompts victim to respond to mobile message
Victim Response	• Victim responds "appropriately" to initial contact prompt
Callback Prep	• MCO sends follow up to victims who respond • Prepares victim to receive contact via voice channel

3-Way Handshake Malicious Mobile Messaging

- **Content changes frequently**
- **Length of message and low rate of messages when compared to Spam Reporting System (SRS) messaging suggests RCS fallback**

Real World examples (victim replies msg omitted):

```
FreeMsg US Bank Fraud : Did you try a charge of ¤287.32 ¡ Walmart Supercenter?
(     Portland,     OR     97060     )     Reply     YES     or     NO.     To     opt     out
of fraud txt reply STOP
```

```
FreeMsg US Bank Fraud Ctr Thank you for responding
to this activity. One of our representatives will contact you shortly. Opt Out reply STOP
```

```
FreeMsgg:
USAA SECURITY ALERT

We Declined ¤540.25 with your card at
WALGREENS near Houston, TX on
05/26 was this you?

Reply YES or NO. If yes, you recognize
and authorize this transaction if "NO" will be marked as
Unauthorized.

MSG & DATA RATES APPLY.
CASE ID-L027M
```

```
FreeMsgg: Thank you for confirming this activity. All access has been blocked. An account specialist
will contact you shortly. Msg & data rates may apply
```

What do we expect to see for future telecom fraud?

- Targeted scams including live calling and multi-modal approaches
- Spreading out operations to stay under volumetric thresholds
- Less “spam” activity; more “scam” activity
- Less activity on highly-regulated protocols (i.e. fewer voice robocalls)
- Exploiting any gaps in anti-spam protocols

Fraud
How do we respond when it seems benign?

Opportunism
Can we address it with policy or enforcement?

Collaboration
What are our best opportunities?

Let’s chat
What are your questions?

verizon