

Form Security Report 2026

How scammers abuse online forms,
which brands they impersonate, and
how forms.app finds and removes them.

Data period
April - October, 2026

Inside the report



Key findings

Page 03

The numbers that matter, across two pages

01

The landscape

Page 05

Our commitment, and how many flagged forms turned out to be harmful

02

Most targeted brands

Page 07

The most impersonated brands, banks, payment firms and agencies

03

Common “Forms” of fraud

Page 14

Lure types and the data they steal

04

The phisher's playbook

Page 17

Nine tactics, shown on real fraud forms

05

The “who” behind the fraud

Page 28

Where creators sign up from and how they operate

06

How forms.app fights back

Page 31

Four layers of detection, enforcement and partnerships

07

Staying safe

Page 35

Advice for people, organisations and brands



Methodology & glossary

Page 37

How the data was collected, classified and checked



What scammers target most

THE MOST TARGETED INDUSTRY

Finance

26% of forms that impersonate an organisation pose as a bank, payment app, crypto or investment firm. Games and betting follow with 24%.

THE MOST IMPERSONATED BRAND

SASSA

SASSA (South Africa's social security agency) was impersonated the most, with 618 forms. Attackers try to collect national IDs under the pretext of changing phone numbers or claiming grants.

THE MOST COMMON PHISHING FORM

Fake logins

23% of phishing and fraud forms copy a sign-in screen to steal a password. Identity and KYC harvesting comes second, at 17%.

THE MOST REQUESTED INFORMATION

National ID numbers

Requested by 5,028 confirmed phishing forms, narrowly ahead of passwords (5,002). A password can be changed. An ID number can't.

By the numbers

FRAUD FORMS REMOVED

22,286

phishing and scam forms confirmed and banned in six months, out of 34,492 flagged.

BIGGEST SHARE OF FRAUD FORMS

Indonesia

13.5% of fraud forms came from accounts in Indonesia, ahead of the United States (12.6%) and Nigeria (8.7%), out of 168 countries.

ESTIMATED VPN USE

39%

of phishing accounts were flagged as using a VPN at sign-up, or signed up from a country that doesn't match their device clock. Legitimate accounts: 2%.

AUTOMATIC BANS

63%

of bans were fully automatic, rising from 25% in May to 77% in October. Each ban feeds new rules, similarity checks and model training.

01

SECTION 01

The landscape

Six months of flagged forms: how many were harmful, and how we confirm them.

Our commitment to safer forms

At forms.app, security is always a priority. For the form owner and for the people who fill it out. Over the years, we have dealt with many phishing and fraud forms and built a strong multi-layered system to detect and remove them.

In 2026, we decided to remove form response and team member limits, from any plan including the free plan. Before the change went into effect in June, we knew we had to update our security measures, making them air-tight. And we did.

This report covers every form flagged from April to October, 2026.

34,492 flagged forms

65%

9%

27%

22,286

confirmed fraud

2,977

suspicious / unclear

9,229

legitimate



Careful checks

All flagged forms are inspected so legitimate users are not affected.



Self-improving

Each attempt helps our security system adapt and get better.



Confirmed only

Sections 02 - 05 count confirmed phishing / fraud forms only.



02

SECTION 02

Most targeted brands

Phishing forms affect 14 sectors, such as banking, gaming and government, and target 1,351 brands.

The 20 most impersonated brands

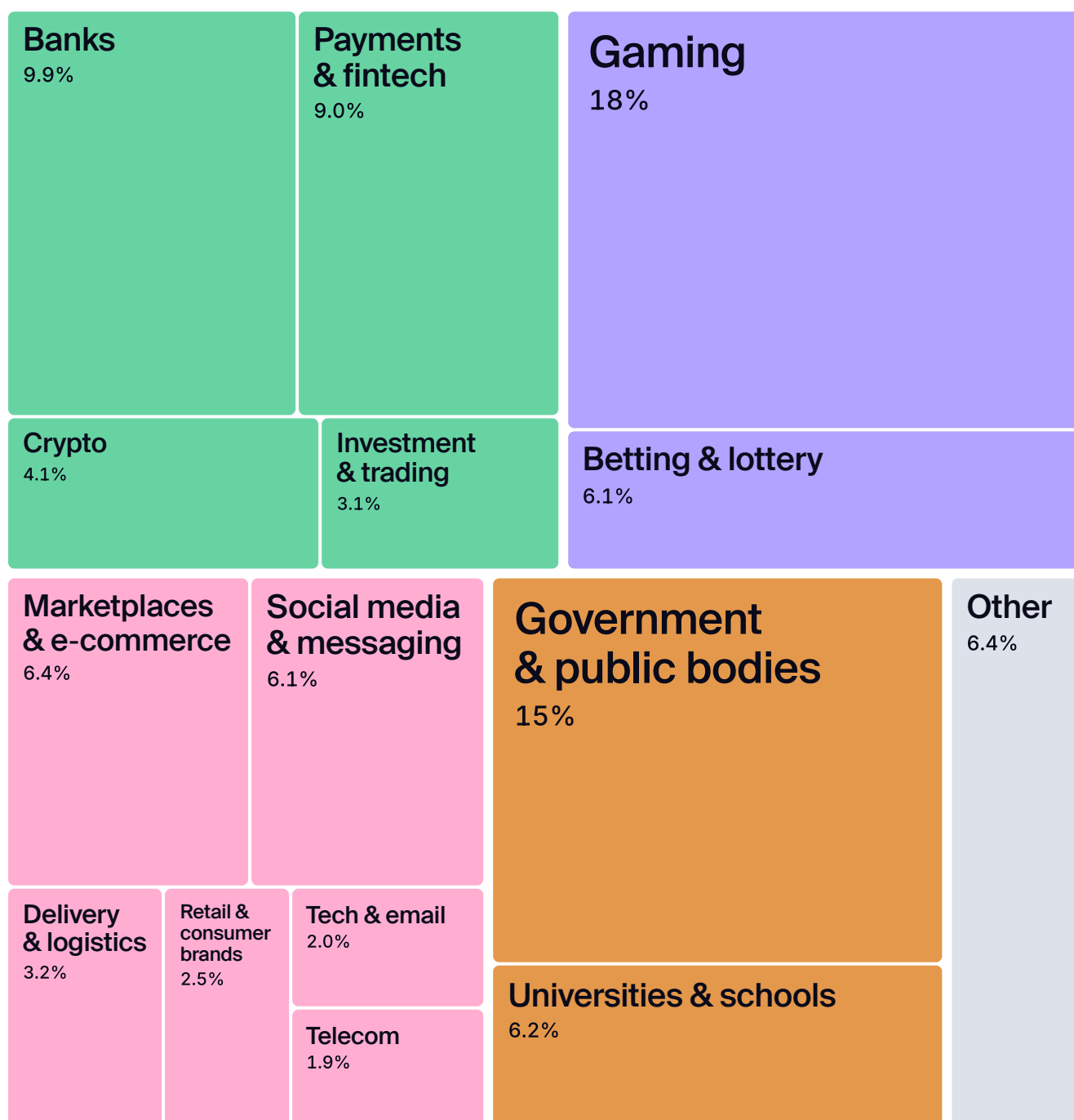
Three brands account for 28% of all branded phishing forms. The top 20 alone span 12 different sectors.



Finance and gaming are the top targets

One in every four forms targets a financial institution.

Share of phishing and fraud forms, by sector



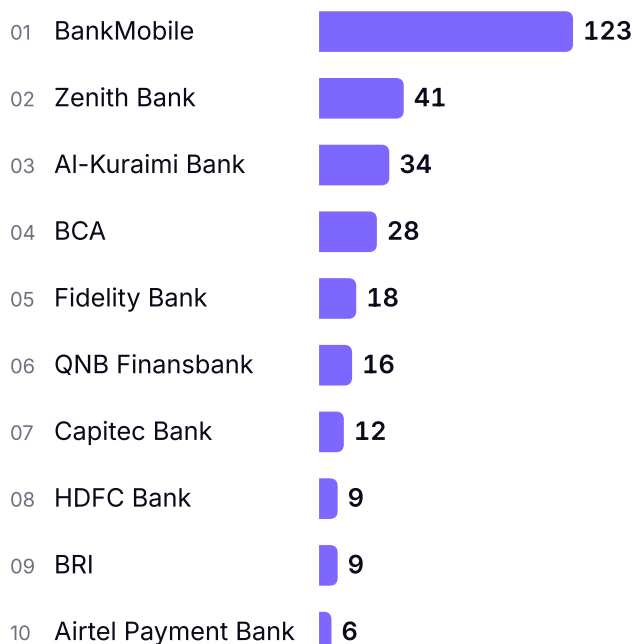
■ Finance **26%**
■ Games & betting **24%**
■ Consumer services **22%**
■ Public sector **21%**
■ Other **6%** (fake employers, insurers, health providers, charities, media)

Banks, payment firms and crypto

Bank phishing reaches from US student banking to Nigeria, Yemen and Indonesia. In payments, PayPal leads, followed by Europe's new Wero wallet.

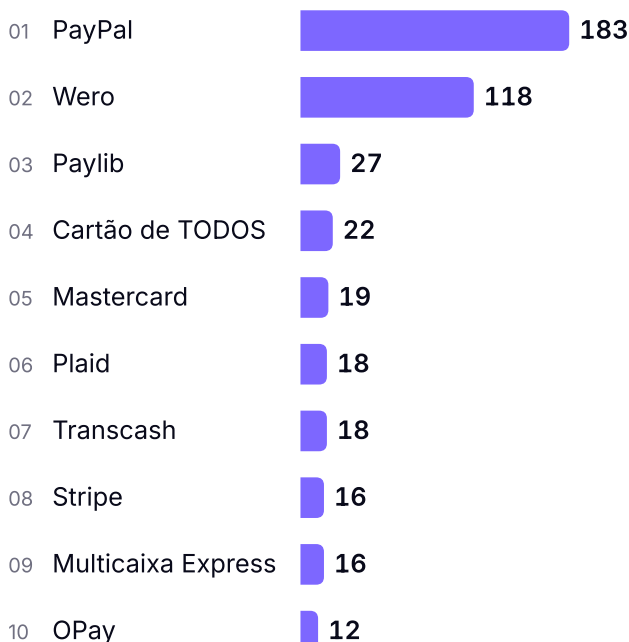
Most impersonated banks

Confirmed phishing forms



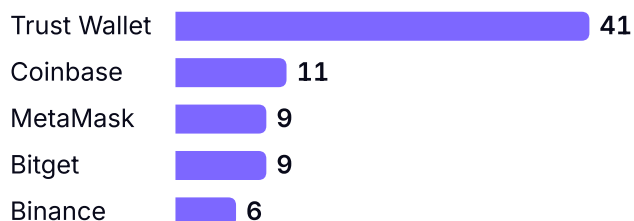
Most impersonated payment & fintech brands

Confirmed phishing forms



Most impersonated crypto brands

Confirmed phishing forms



Few forms, total loss

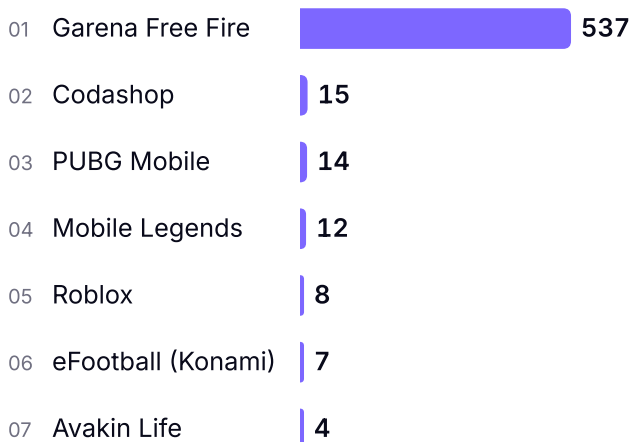
Fake Trust Wallet support forms ask for the 12-word recovery phrase. Whoever holds it controls the wallet, and transfers can't be reversed.

Games and social platforms

The lure is almost always something free: diamonds, skins or coins. What the attacker wants is always the victim's login.

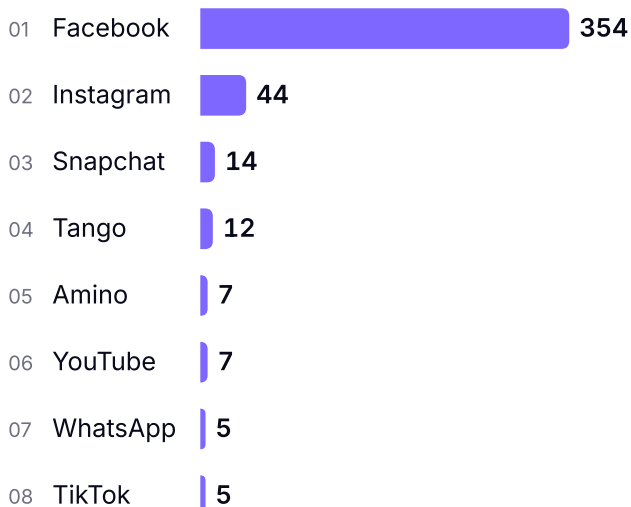
Most impersonated games & gaming services

Confirmed phishing forms



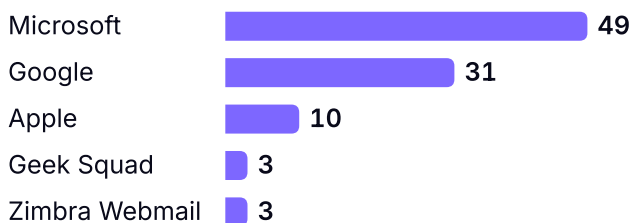
Most impersonated social & messaging platforms

Confirmed phishing forms



Most impersonated tech & email providers

Confirmed phishing forms



One login, many accounts

Many games let players sign in with Facebook or Google. A fake giveaway that asks for those logins gets far more than a game account: email, contacts and every other service linked to them.



Government agencies and public bodies

People trust official-looking forms. Scammers exploit that with fake grant applications, tax notices and visa forms.

Most impersonated government & public bodies

Confirmed phishing forms

01	SASSA	618
02	Tanzania Revenue Authority	17
03	Minha Casa Minha Vida	12
04	Corporate Affairs Commission (Nigeria)	11
05	U.S. Dept. of Health & Human Services	8
06	IRS	7
07	Central Bank of Nigeria	6
08	SBA	6
09	Aadhaar	4
10	Nationale	4

SASSA SRD UPDATE

1. ID NUMBER
T

2. OLD NUMBER
T

3. NEW NUMBER
T

4. YOU WERE RECEIVING THE MONEY IN SHOPS OR ACCOUNT
T

A fake SRD grant update form

Fake SASSA grant updates

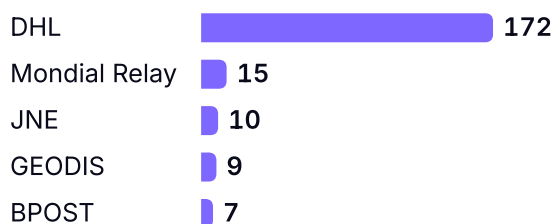
Fake SASSA forms pose as Social Relief of Distress (SRD) grant services: a number change, a balance check or a new application. They collect ID numbers and phone numbers.

Delivery, marketplaces, telecom and universities

Smaller sectors by volume, but each has a recognisable playbook.

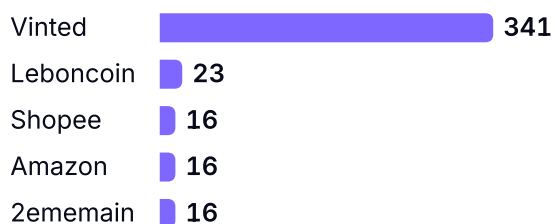
Delivery & logistics

Card details to "release" a parcel



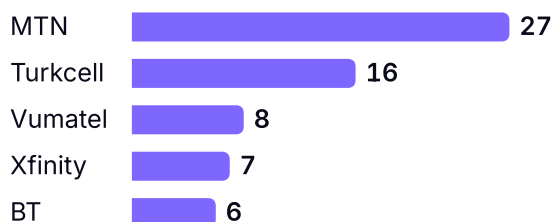
Marketplaces & e-commerce

Fake buyer payments and seller logins



Telecom

Data bundles, rewards and account checks



Universities & colleges

Student email passwords and aid "refunds"



DHL phishing is 74% card theft, typically a small fee to redeliver a parcel. 70% of the accounts behind it signed up from Italy.

University phishing asks for student email passwords, often with a financial-aid pretext. One campaign, also posing as BankMobile, targets Miami Dade and Broward College.

03

SECTION 03

Common "Forms" of fraud

The lures phishers use and the data they're after.

The most common phishing forms

The fake login leads: **23%** of phishing and fraud forms exist to steal a password.

Fake logins copy a sign-in screen and ask for an email and password. They're cheap to make and easy to scale.

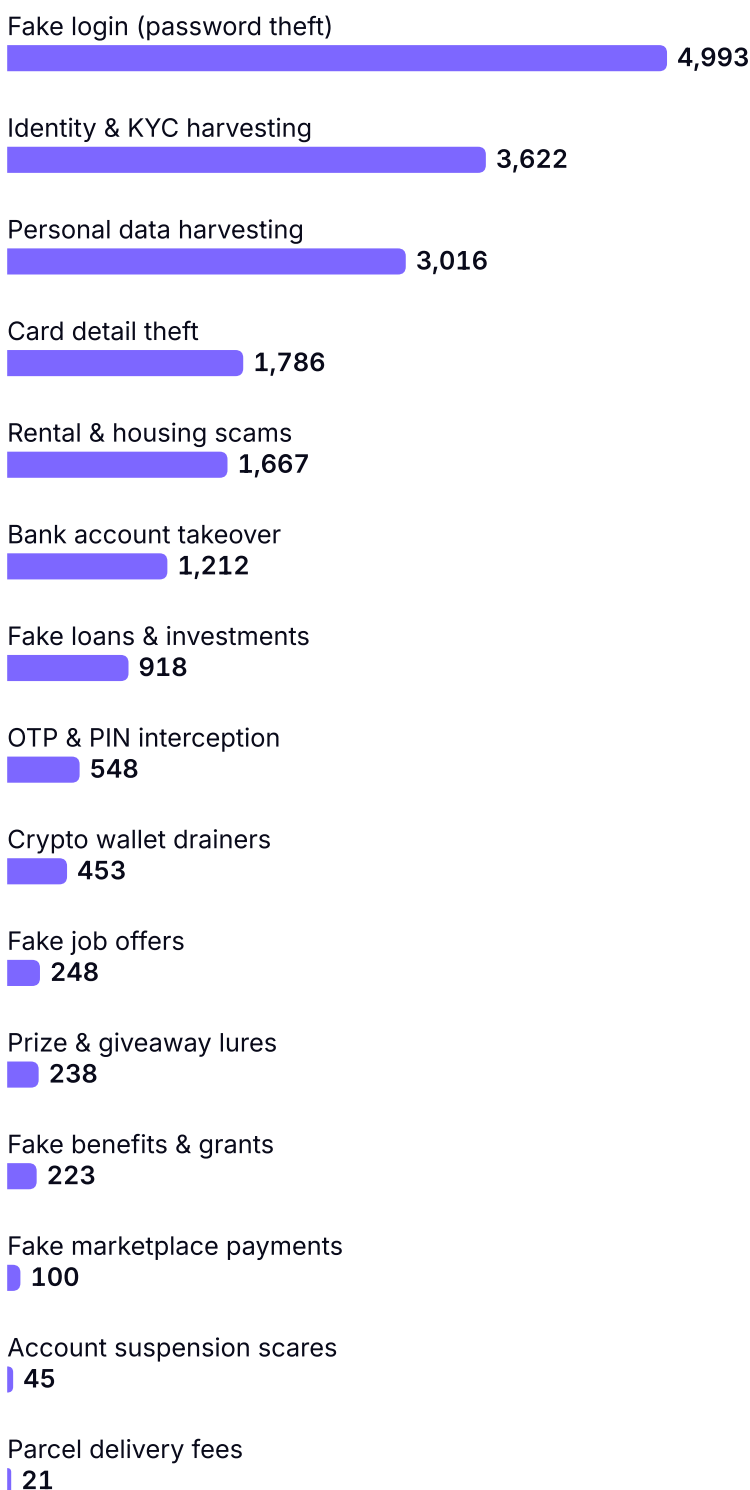
Identity harvesting collects ID numbers and documents under a pretext such as a grant, loan or job. The data is used later for fraud.

Rental scams advertise a home that doesn't exist, then ask for an application fee or deposit before any viewing. 81% of the accounts behind them signed up in the US.

Card theft asks for card number, expiry and CVV to "verify", "refund" or "unlock" something.

Phishing and fraud forms by type

Main lure or data target of each form



Based on 21,901 confirmed forms classified by type.

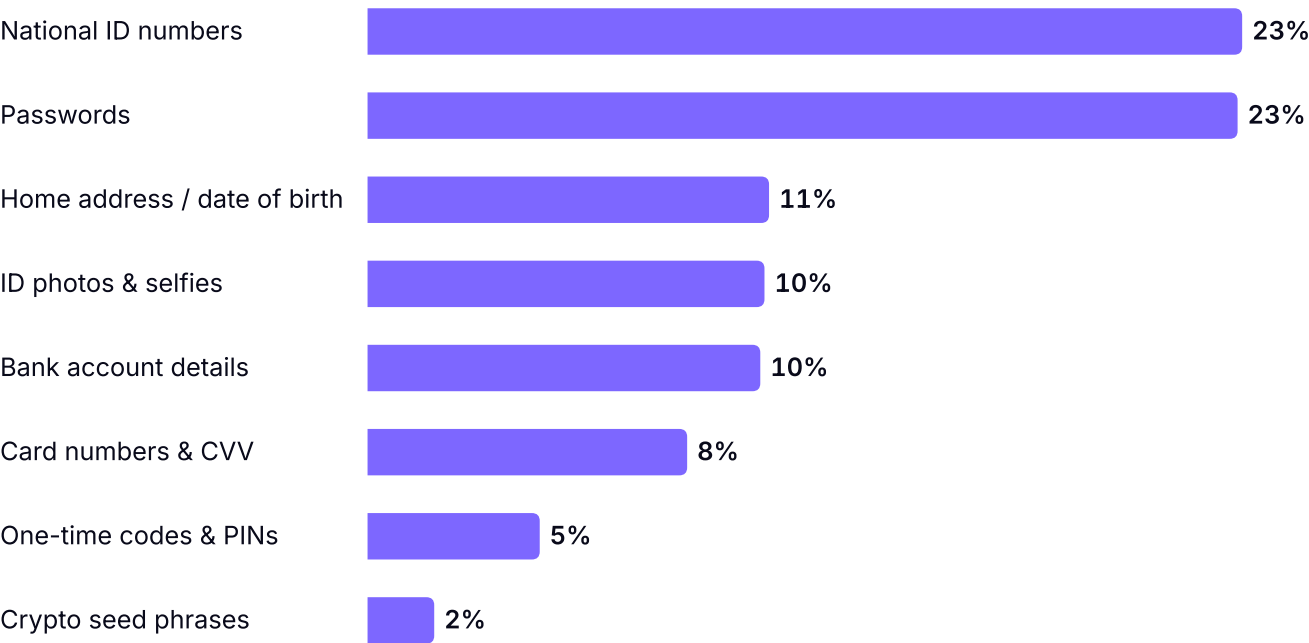


What phishing forms ask for

National ID numbers and passwords are requested almost equally. A password can be changed. An ID number can't, so once it's stolen, it stays stolen.

Share of confirmed phishing forms requesting each type of data

A form can request several



Dangerous combinations

A password plus a one-time code lets an attacker log in on the spot, even with two-factor authentication on. An ID number plus a selfie passes many online identity checks.

REQUESTED TOGETHER	FORMS
ID number + ID photo or selfie	1,543
Password + card or bank details	643
Password + one-time code	263
Card details + one-time code	75



04

SECTION 04

The phisher's playbook

How do scammers avoid detection and trick people at the same time? Let's look at real examples.

Tactics used by phishers and scammers

How do scammers avoid detection and trick people at the same time? Let's explore with real examples.

Phishers and scammers write for two audiences at once: the person filling in the form and the system checking it. The form has to win over one and slip past the other.

Looking official

Phishers pay extra attention to how their forms look. These forms usually copy the brand colours, the logos, and other official elements.

Only one part of the scam

However, the form plays only a part. In most cases, the attackers usually create official-looking forms and then contact the victim through other channels.

SECTION 07 · PAGE 35

Staying safe

Eight tips for anyone filling in a form.

01 Using images and claims to build trust



02 Using a timer to build pressure



03 Disguising the word "password"



04 Putting questions inside images



05 Hiding requests inside input fields



06 Telling the fee is refundable



07 Asking for one-time codes or PINs



08 Offering rewards for wallet secrets



09 Stealing an identity with innocent questions



Using official images and reviews to build trust

Familiar colours, promotional images, ratings and reassuring language make a form feel connected to a service you already know.



1

Official brand elements and colours

The French heading tells the visitor to sign into Vinted to accept a payment. The scammers use official imagery to make it feel familiar.

2

Social proof to make it look real

Scammers can add social proof elements like ratings or reviews. It makes the form look more authentic, especially if the rating is from a trusted source like Trustpilot.



A countdown to rush a decision

The timer field is a useful element in forms and quizzes. However, it can also be used to create a sense of urgency by scammers. A countdown can make a respondent feel that the form is legitimate and time-sensitive.



23 : 58 : 56
Heures Minutes Secondes

Le paiement instantané réinventé pour vous.



Veuillez suivre les instructions pour confirmer votre identité et finaliser la validation de votre compte. Nous vous remercions de votre coopération.

A deadline beside familiar branding

Same "password", in other words

Asterisks, abbreviations and unusual spelling changes are the dead giveaways. These tricks are used to avoid automated detection. While our system can detect them, a human respondent may not notice the subtle difference.

FEDERAL SECURED SERVER

1. USERNAME

T

2. PASS***

T

An official-sounding login

4. BANKMOBILE EMAIL/ ECSI USER



5. BANKMOBILE / ECSI PASSW**D

T

A student banking pretext

Using images to ask questions

In the screenshot, the highlighted text says “Şifrenizi Girin” (“Enter your password”). This is a picture added above a question, while the question itself is left empty.

Başlıksız form

f

1. Kullanıcı Adınız

T

Şifrenizi Girin

2.

T

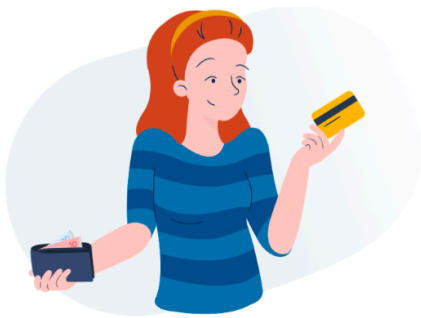
Gönder

The image carries the password request

forms.app counters this trick with OCR (optical character recognition): our checks read the text inside images too.

Using placeholders to ask questions

The heading promises “Legal and encrypted information”, while the placeholders ask for “CARD NUMMER” (card number) and “Vervaldatum” (expiry date). The reassuring label conceals the payment details being requested.



Informations légales et cryptées *

T ICARD NUMMER

Card number

Informations légales et cryptées *

12-27

T Vervaldatum

Expiry date

Rental scam forms ask for "refundable" fees

Rental scam forms mostly target people in the US. They ask for an application fee and call it "refundable", and they often list Zelle, Chime and Cash App; these are payment apps that rarely appear in any other kind of fraud form. Yet the form has no payment field. It is just one part of the scam, used to gather the applicant's personal information.

21. How soon do you want to get the entrance key?

T

22. How much do you have at hand now to secure the property? *

T

23. REFUNDABLE APPLICATION FEE \$75 (NOTE CASH AND CHECK IS NOT ACCEPTABLE FOR APPLICATION FEE *)

☐ Cash App

☐ Zelle

☐ Chime

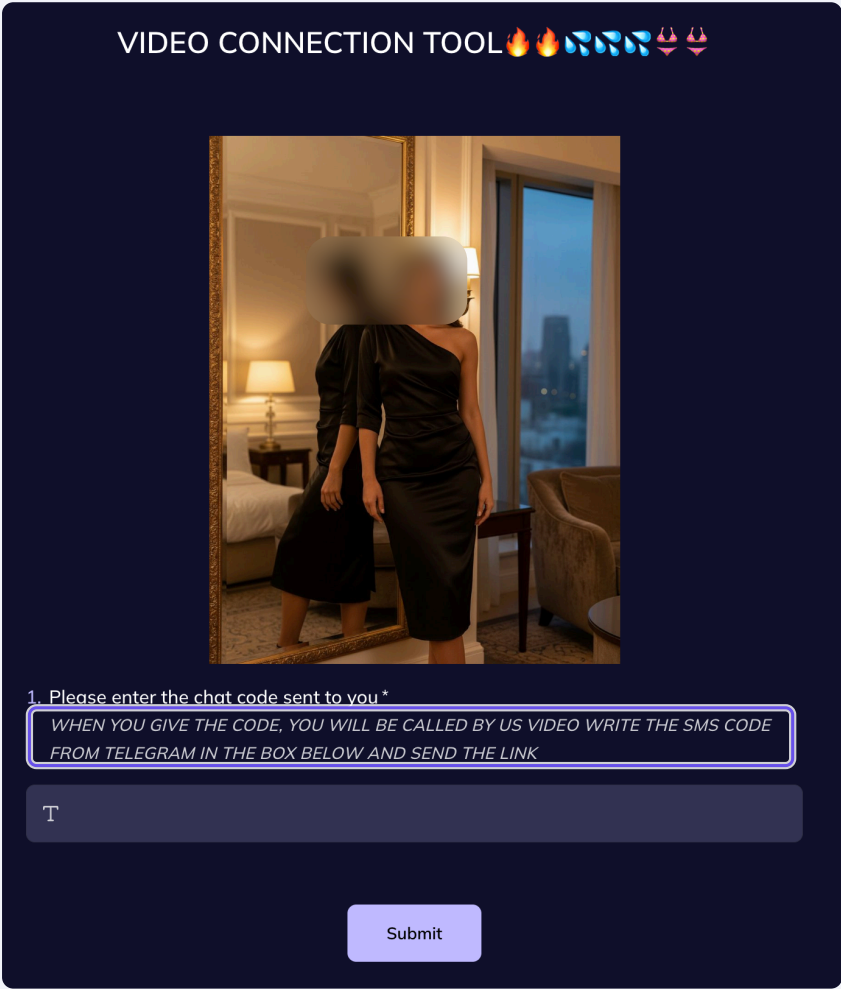
☐ Apple Pay

☐ PayPal

A promise of a refund

Offering rewards or promising security to get PIN codes

A form may call a login code a "chat code", or claim that sharing a payment PIN will protect your account. The secret still grants access.



VIDEO CONNECTION TOOL 🔥🔥🔥🔥🔥🔥🔥🔥

1. Please enter the chat code sent to you *

WHEN YOU GIVE THE CODE, YOU WILL BE CALLED BY US VIDEO WRITE THE SMS CODE FROM TELEGRAM IN THE BOX BELOW AND SEND THE LINK

T

Submit

A code to start a chat

1

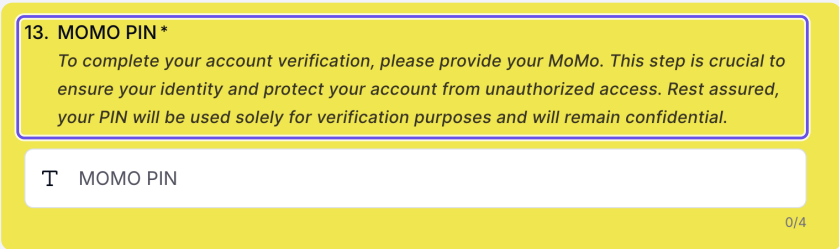
The message tells you what it unlocks

The first example explicitly requests a Telegram SMS code. Calling it a "chat code" does not change its purpose.

2

"For verification" is the pretext

The second example asks for a payment PIN and promises confidentiality. That explanation does not make disclosure safe.



13. MOMO PIN *

To complete your account verification, please provide your MoMo. This step is crucial to ensure your identity and protect your account from unauthorized access. Rest assured, your PIN will be used solely for verification purposes and will remain confidential.

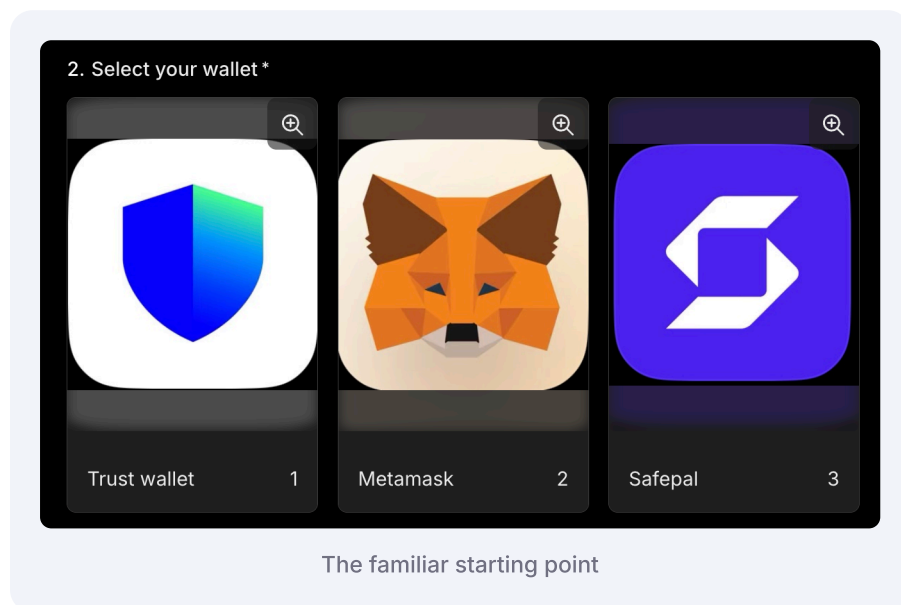
T MOMO PIN

0/4

A PIN to verify an account

Offering a reward for a wallet secret

An airdrop promises free crypto. After familiar wallet choices, the form asks for recovery words as the price of claiming the reward.



1

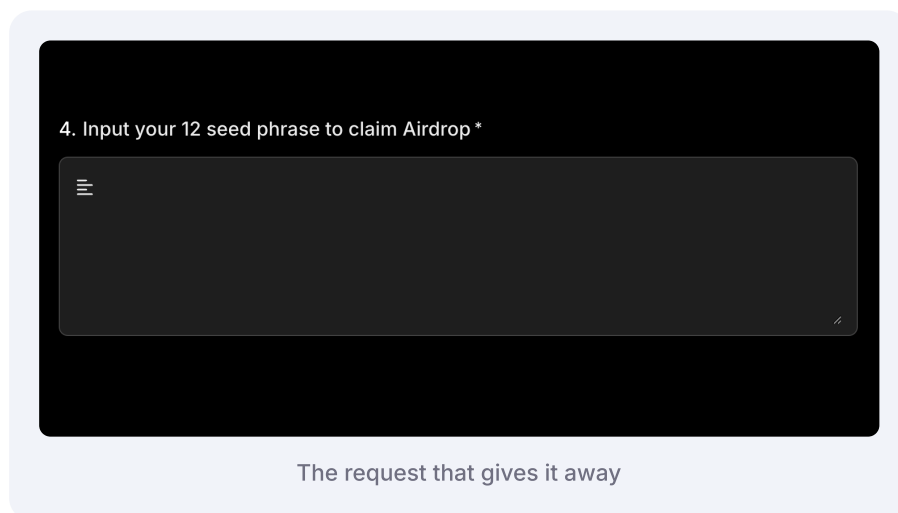
Recognisable wallets lower suspicion

A menu of wallet brands makes the process look like a normal connection step. These logos do not authorise the form.

2

Recovery words are the real prize

The form asks for a 12-word seed phrase. Someone who obtains it can gain control of the wallet and its funds.



Questions themselves can look innocent

Each question can look harmless, and the form looks like an ordinary application. Forms like this tend to be long, and together the answers are everything an identity thief needs. On top of that, these forms usually are part of a larger scam, and the answers are used to make the next step more convincing.

Online registration form for the green card lottery

Name and surname

Pay attention to the fact that your name and surname are indicated in Latin exactly the same way as it is recorded in the passport.

An official-sounding application



Upload a photo

• JPEG (.jpg) format • Size should not exceed 240 kilobytes (240 kB) • Must be square in size (height equal to width) • 600x600 pixels

A portrait completes the profile

05

SECTION 05

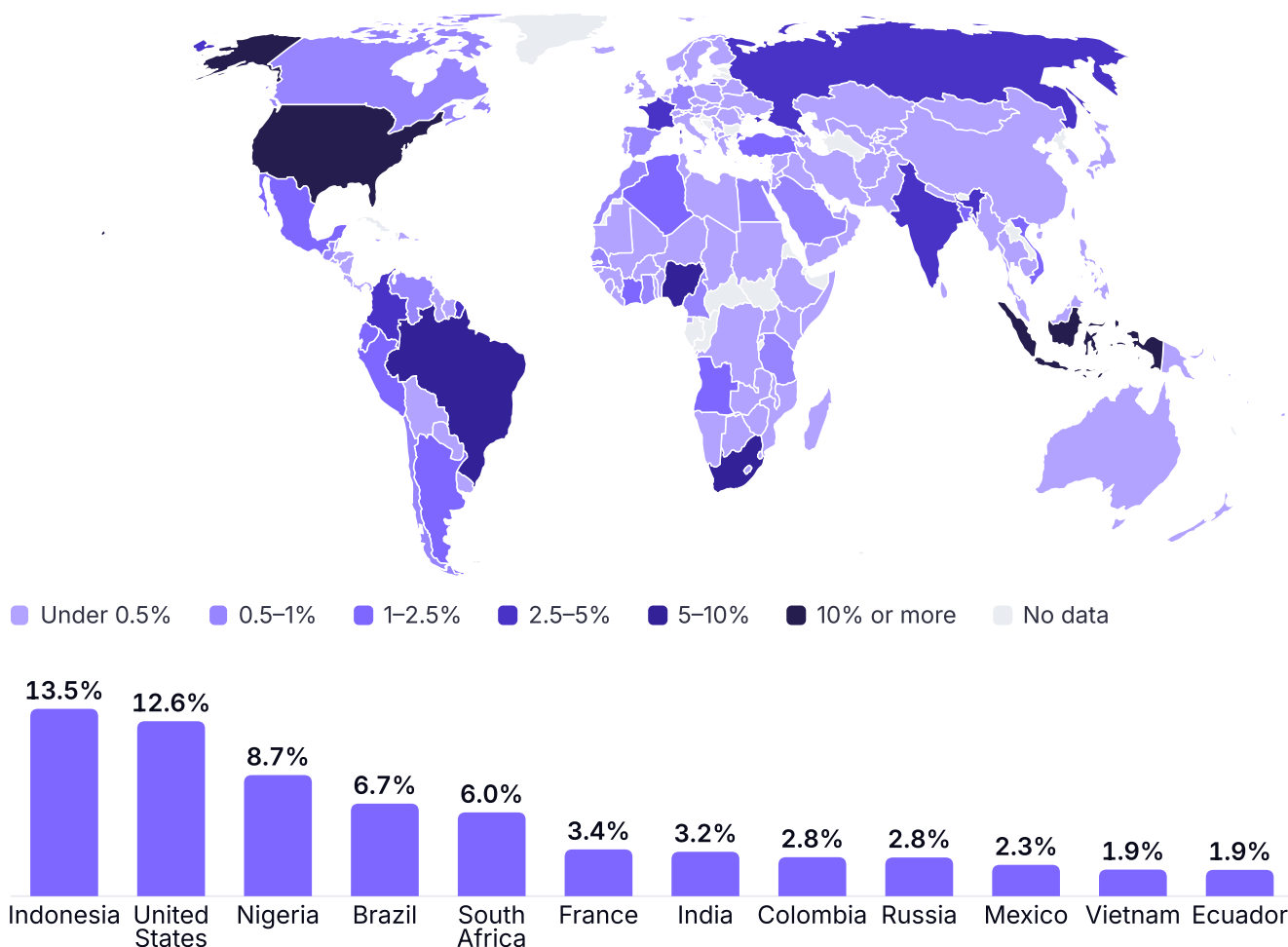
The “who” behind the fraud

What account data tells us about who creates phishing forms, and how.

Where phishing accounts come from

Phishing accounts operate from **168 countries**. If the country and timezone of the account don't match, we count time zone as the more reliable indicator of location.

Where confirmed phishing accounts operate from



21%

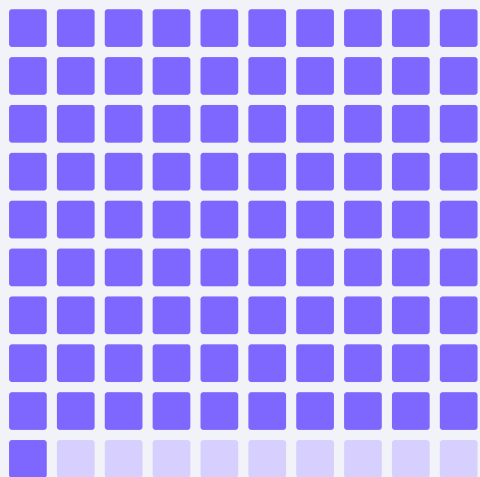
of phishing accounts signed up from a country that doesn't match their device clock, a sign of VPN use. For legitimate accounts: 2%.

31%

of phishing accounts were flagged as using a VPN at sign-up. For most accounts, we couldn't tell if VPN was enabled. So the true share is likely higher.

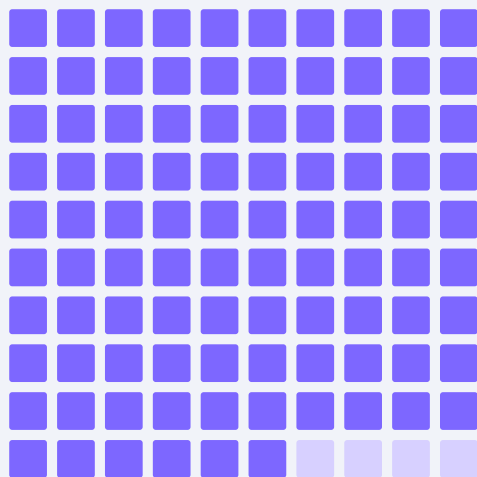
Disposable accounts, free email

The typical phishing operator signs up with a free webmail address, publishes a single form and moves on.



91%

of confirmed phishing accounts used a free webmail address. 84% used Gmail.



96%

of phishing accounts published exactly one form. 20,876 accounts created 21,901 forms.

Why burner accounts matter

When one account is banned, the operator opens another. That's why we focus on fast, automatic detection of each form, instead of relying on account history.

Sign-up protections

Every new account has to verify its email address before sign-up is complete. We block disposable email addresses, and banned users can't sign up again from the same device.

06

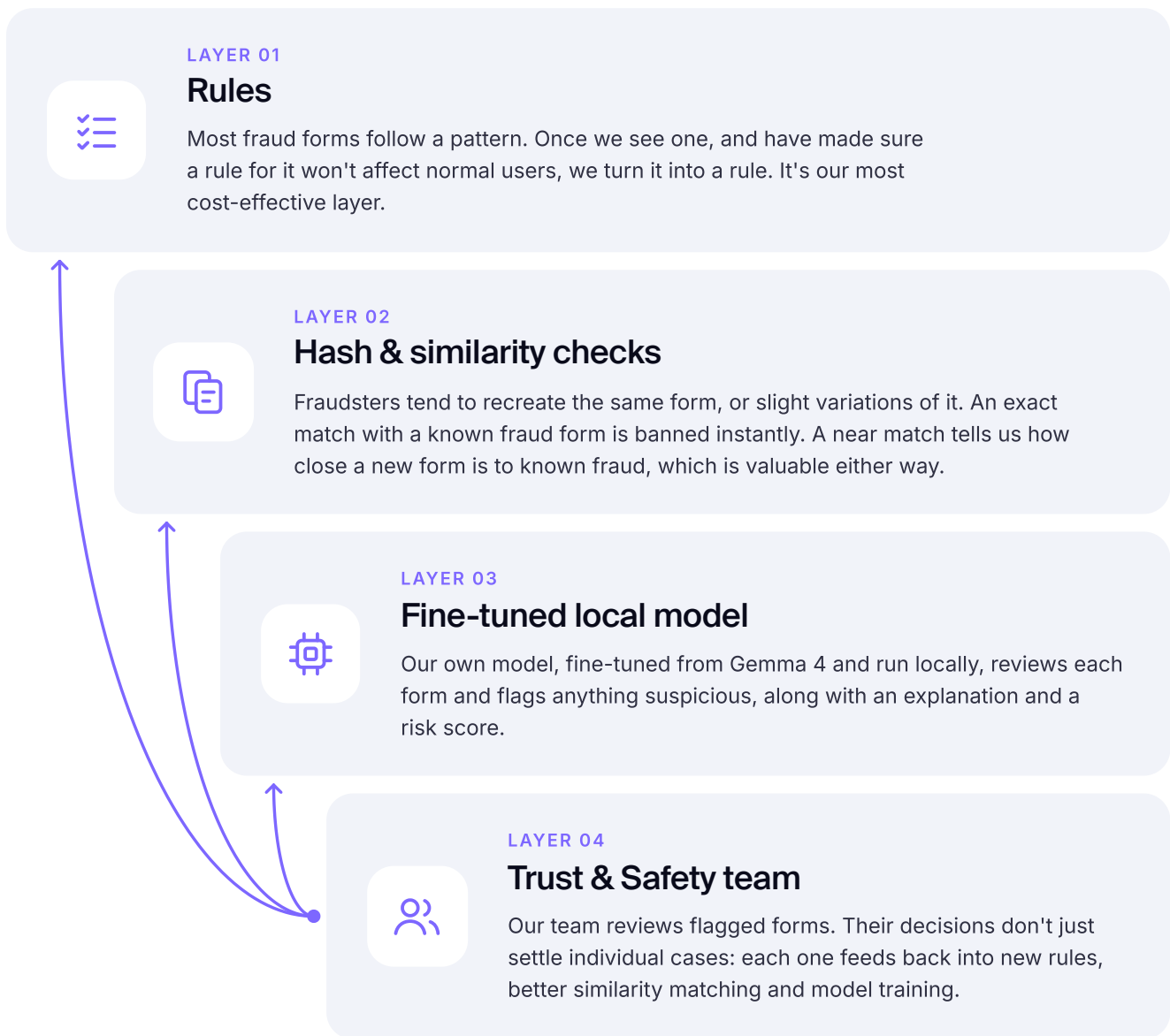
SECTION 06

How forms.app fights back

Combining automated detection, human review and outside reports.

Four layers of detection

Each layer catches what the one before it can't. It goes from fast and cheap to slower and more expensive, but also more accurate.



Fast where it can be, careful where it must be

A wrongful ban hurts a real business, so ambiguous cases go to people. Clear-cut fraud is removed automatically, without waiting for a victim to report it.

What each layer costs

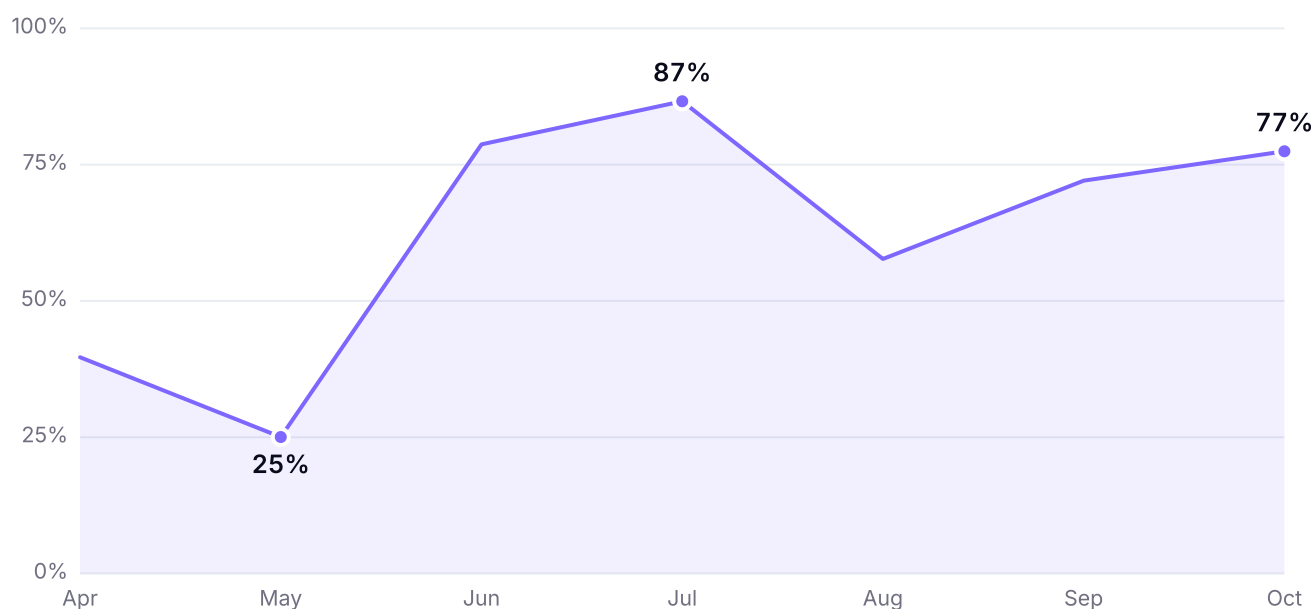
Rules are almost free to run. Similarity checks are cost-effective, and our local model costs five times as much as a similarity check. Manual bans cost the most, because each one takes our own team's time.

Self-improving mechanism

63%

of bans were fully automatic (14,094 forms).

Automatic bans by month



Every ban makes the next one faster

Each form we ban teaches the system something. A recurring pattern becomes a new rule, the form's fingerprint joins our similarity checks, and the case is added to the data our model learns from. The next copy of that form is caught automatically.

Why some cases still need a person

Some forms can't be judged on their content alone. A form asking for bank details may be a real loan application or a phishing page. A rental listing may be genuine or a deposit scam. Or a form may ask nothing suspicious but be part of a complex scheme.

Partnering with threat intelligence

forms.app receives phishing reports from various external sources via our report form or via direct integrations. Since June, reported forms have been banned automatically, a median of **13 minutes** after our partners identified them.

30

threat reports received

13 min

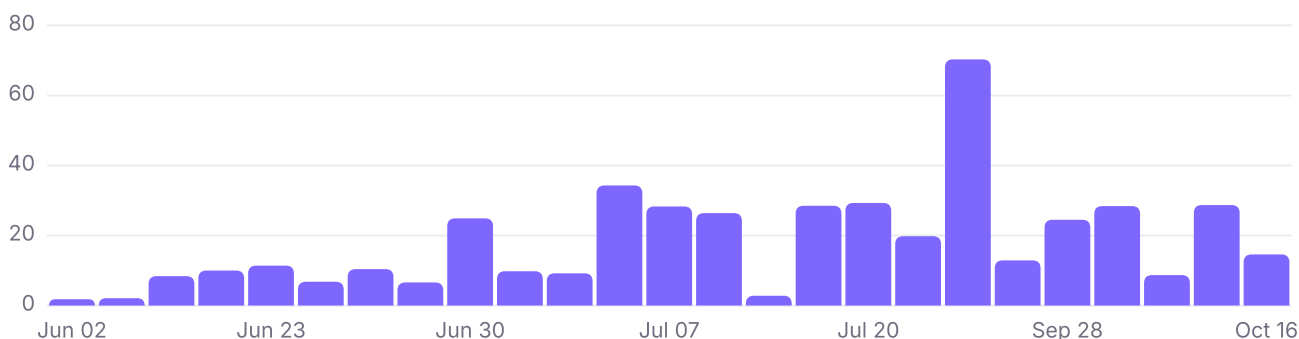
median from detection to ban

100%

of reported forms banned

Minutes from report to ban

Each column is one live report, in date order since the integration went live



A focus on Wero

27 of the 30 reports involved Wero, mostly French-language forms posing as Wero activation or "secure payment" pages. The rest targeted the French bank CIC and the US lender LightStream.

Before and after

Direct integrations and AI triage made the process faster and more efficient. Since it went live, the slowest report was banned in just over an hour.

07

SECTION 07

Staying safe

Practical advice drawn from the patterns in this report.

How to spot a phishing form

Check every URL.

Not just the form's address, but also the link or message that brought you there, and any page the form sends you to next. The form is often only one part of the scam.

When in doubt, ask.

Get in touch through the organisation's official website, app or phone number, not through the links or numbers the form gives you.

Never share one-time codes or PINs.

A code sent to you is for you only. Anyone asking for it is trying to get into your account.

Weird quirks are a red flag.

Labels like "PASS****" or questions written inside images are tricks to slip under the radar of automated checks. Genuine forms don't hide what they ask.

01

02

If an offer is too good to be true, it probably is.

Free diamonds, prizes, cheap rentals and easy loans are bait. The catch is in what the form asks for.

03

04

Never share a password on a custom form.

Logins happen on the service's own website or app, never in a survey, giveaway or form.

05

06

Never share your seed phrase.

No support agent will ever ask for it. Anyone who has it can take everything in your wallet.

07

08

Report it, even if you're not 100% sure.

Use our report form at online.forms.app/forms/report-abuse-n or email support@forms.app, and our Trust & Safety team will take a look.

METHODOLOGY

How we built this report

34,492

forms flagged

22,286

confirmed & banned

Data sources

Every form that entered forms.app's abuse review between April 1 and October 19, 2026, whether it was flagged by our automated detection, matched by our rules, or reported by a threat-intelligence partner. For each form we used its moderation notes, account details and final decision. Each save triggers a review, so passing the first review, then changing the form is not a solution for phishers and fraudsters. The period starts on April 1 to include the security update we made before removing response and team member limits in June (see section 01).

Of the 34,492 forms flagged, 22,286 were banned, 9,229 were legitimate, and 2,977 were not banned but didn't get whitelisted either (Technically, they are legitimate, however left out of whitelist due to various reasons).

What counts as fraud

We count a form as fraud if it shows clear signs of phishing (forms that impersonate a brand to collect logins, payment or personal details) and scams (forms that take money or data under a false pretext). 7% of bans came from automated rules, a further 56% from automated AI detection, 37% from human review and 0.1% from partner reports.

Fraud forms made up 4% of the 557,700 forms created on forms.app in this period.

Brands

In total, fraud forms targeted 1,351 brands. A brand needs at least three fraud forms to appear in this report's rankings. Spelling variants of the same brand were merged by hand.

Limitations

This report shows the fraud we caught, not all fraud on forms.app. Our rules look for known patterns, and partners tend to report the brands they protect. However, abuse reports are few and falling, which suggests our new automated detection catches most fraud before anyone reports it.



Terms used in this report

Phishing form

A form designed to trick people into handing over credentials, financial details or personal data, typically by impersonating a trusted organisation or using a false pretext.

Scam form

A form that takes money or personal data under a false pretext, such as a rental deposit, a loan or a job offer, without necessarily impersonating anyone.

Flagged form

A form our detection systems marked as possibly harmful, for review or an automatic ban.

Confirmed phishing

A flagged form that forms.app banned, including instant bans by keyword rules or after a Netcraft report.

Impersonation

A form presenting itself as, or as affiliated with, a real brand, agency or institution it doesn't represent.

Lure

The promise or threat that gets someone to fill in a form: a prize, free game currency, a refund or an account warning.

Credential harvesting

Collecting usernames and passwords to take over accounts.

OTP

One-time password: a short code sent by SMS, email or app as a second login factor.

KYC

"Know your customer": identity checks using ID numbers, documents and selfies.

Seed phrase

The 12 or 24 words that give full control over a crypto wallet.

Placeholder

The hint text inside an empty input field. Fraud forms use it to ask for data without a visible question.

VPN

Virtual private network: a service that hides where a user really is by routing their traffic through another country.

Hash & similarity check

Comparing a new form with known fraud forms. An exact copy has the same hash, a fingerprint of its content; a near copy scores as similar.

Auto-ban

A form removed automatically by forms.app's systems, without manual review.

Harm level

What a victim could lose: *critical* means credentials or financial data plus one-time codes, seed phrases or ID documents; *high* means passwords, card or bank details; *moderate* means ID numbers, address or date of birth.

Who we are

forms.app is an online form-building platform with unlimited responses, unlimited team members, powerful features. We started forms.app with simplicity, accessibility and mobile-first principles in mind. But we also know that with great power comes great responsibility. We take the safety of our users seriously, and we work hard to keep forms.app a safe place for everyone.

Today, individuals and organisations around the world use it to create forms, surveys, quizzes and online stores. Our Trust & Safety team works to keep the platform safe for the people who build forms and the people who fill them in.

2018 Founded	4M+ Users	170+ Countries
------------------------	---------------------	--------------------------

//

Most people never think about who is behind a form, and they shouldn't have to. Our job is to make every form on forms.app one they can trust.



Tolga Kızılkaya
Co-Founder & CPO, forms.app



Form Security Report 2026

How scammers abuse online forms, which brands they impersonate, and how forms.app finds and removes them.

Data period: April - October, 2026 · © 2026 forms.app