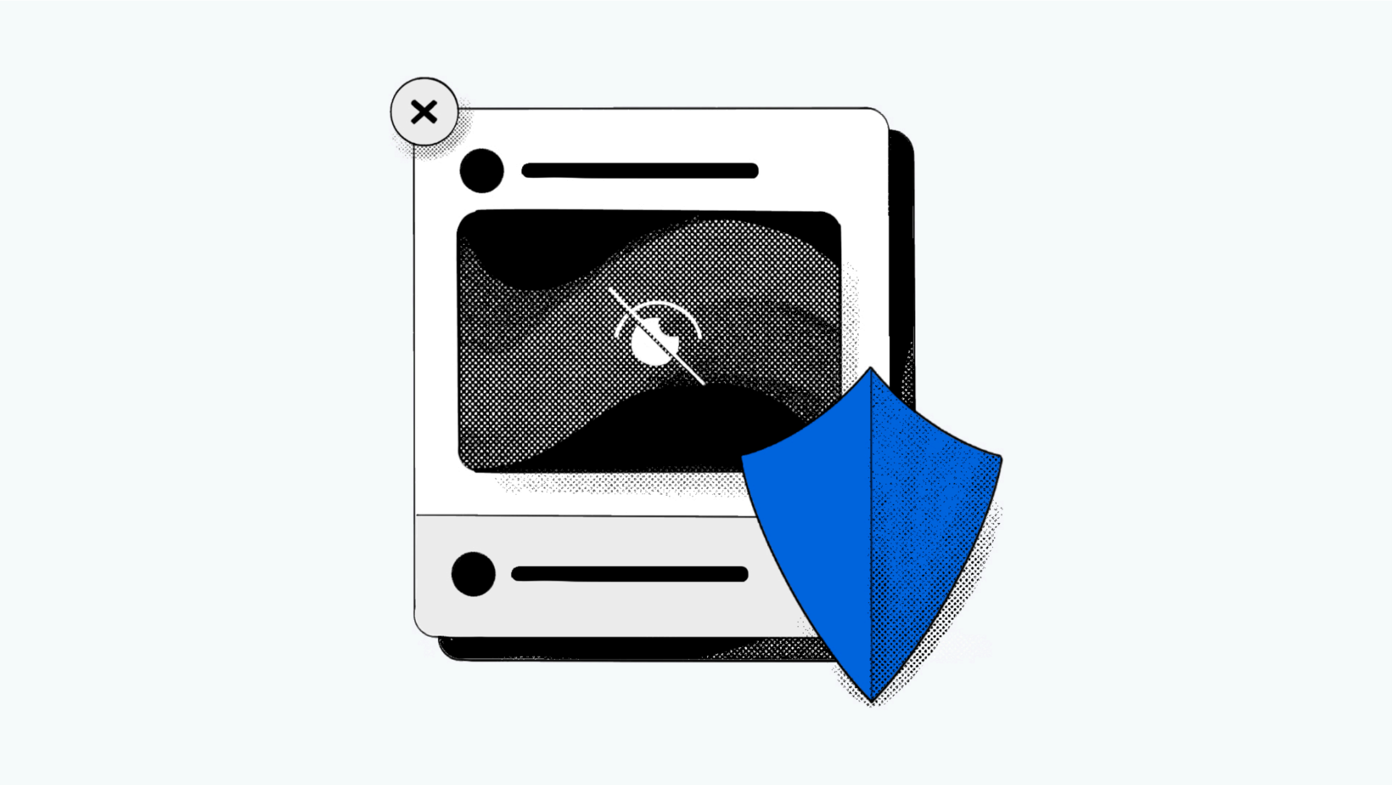
Back to Newsroom

Meta

Combating Financial Sextortion Scams From Nigeria

July 24, 2024



Takeaways

- Financial sextortion is a borderless crime, fueled in recent years by the increased activity of Yahoo Boys, loosely organized cybercriminals operating largely out of Nigeria that specialize in different types of scams.
- We've removed around 63,000 Instagram accounts in Nigeria attempting to target people with financial sextortion scams, including a coordinated network of around 2,500 accounts.
- We've also removed a set of Facebook accounts, Pages and Groups run by Yahoo Boys – banned under our Dangerous Organizations and Individuals policy – that were attempting to organize, recruit and train new scammers.

Financial sextortion is a horrific crime that can have devastating consequences. Our teams have deep experience in fighting this crime and work closely with experts to recognize the tactics scammers use, understand how they evolve and develop effective ways to help stop them. Like many crimes, financial sextortion crosses borders, and over recent years there's been a growing trend of scammers — largely driven by cybercriminals known as Yahoo Boys — targeting people across the internet, both with these and other types of scams. We've banned Yahoo Boys under Meta's Dangerous Organizations and Individuals policy — one of our strictest policies — which means we remove Yahoo Boys' accounts engaged in this criminal activity whenever we become aware of them.

Following our recent Q1 2024 Adversarial Threat Report, today we are announcing the strategic network disruption of two sets of accounts in Nigeria that were affiliated with Yahoo Boys and were attempting to engage in financial sextortion scams.

First, we removed around 63,000 Instagram accounts in Nigeria that attempted to directly engage in financial sextortion scams. These included a smaller coordinated network of around 2,500 accounts that we were able to link to a group of around 20 individuals. They targeted primarily adult men in the US and used fake accounts to mask their identities.

We found the coordinated network of around 2,500 accounts through a combination of new technical signals we've developed to help identify sextorters and in-depth investigations by our expert teams. The majority of these accounts had already been detected and disabled by our enforcement systems, and this investigation allowed us to remove the remaining accounts and understand more about the techniques being used to improve our automated detection.

While our investigation showed that the majority of these scammers' attempts were unsuccessful and mostly targeted adults, we did see some also attempt to target minors, and we've reported those accounts to the National Center for Missing and Exploited Children (NCMEC). Since these criminals don't limit themselves to any one platform, we also share relevant information with other tech companies through the Tech Coalition's Lantern program, so they can take action too.

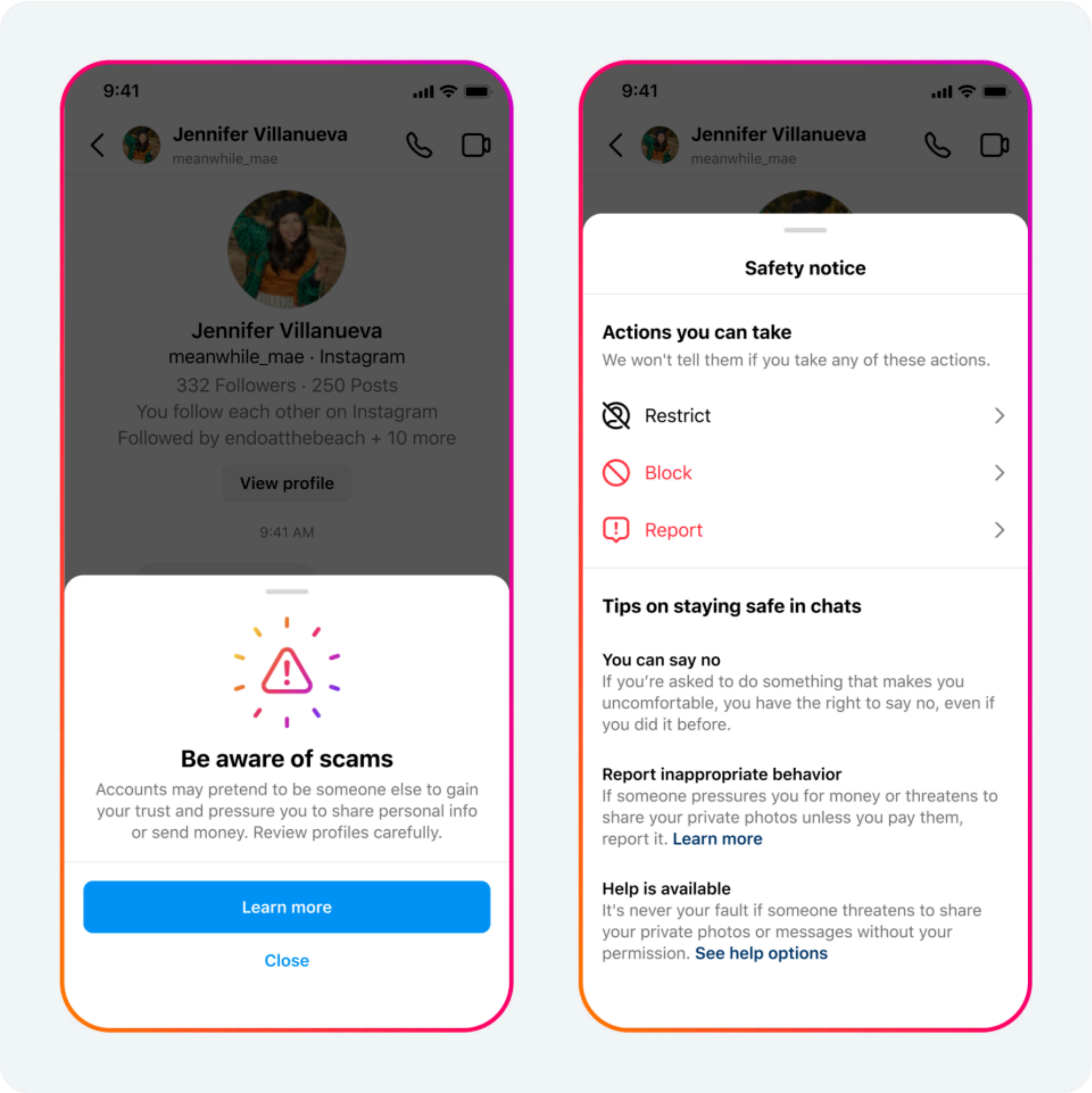
Applying lessons learned from taking down terrorist groups and coordinated inauthentic behavior, we used our identification of this coordinated network to help us identify more accounts in Nigeria that were attempting to engage in similar sextortion scams, bringing the total to around 63,000 accounts removed.

Second, we removed around 7,200 assets, including 1,300 Facebook accounts, 200 Facebook Pages and 5,700 Facebook Groups, also based in Nigeria, that were providing tips for conducting scams. Their efforts included offering to sell scripts and guides to use when scamming people, and sharing links to collections of photos to use when populating fake accounts.

Since this disruption, our systems have been identifying and automatically blocking attempts from these groups to come back, and we continue to strengthen those systems to make them as effective as possible. We've also used the new tactics we observed to further improve our ability to detect accounts, Groups and Pages engaging in this activity.

While these investigations and disruptions are critical, they're just one part of our approach. We continue to support law enforcement in investigating and prosecuting these crimes, including by responding to valid legal requests for information and by alerting them when we become aware of someone at risk of imminent harm, in accordance with our terms of service and applicable law. We also fund and support NCMEC and the International Justice Mission to run Project Boost, a program that trains law enforcement agencies around the world in processing and acting on NCMEC reports. We've conducted several training sessions so far, including in Nigeria and the Cote d'Ivoire, with our most recent session taking place just last month.

We also want to help people recognize and avoid these scams, while making it as difficult as possible for the criminals behind them to succeed. It's why we default teens under 16 (under 18 in certain countries) into stricter message settings so they can't be messaged by anyone — even other teens — they're not connected to, and show Safety Notices encouraging them to be cautious.



Jennifer Villanueva
meanwhile_mae · Instagram
332 Followers · 250 Posts
You follow each other on Instagram
Followed by endoatthebeach + 10 more

Be aware of scams

Accounts may pretend to be someone else to gain your trust and pressure you to share personal info or send money. Review profiles carefully.

Safety notice

Actions you can take

We won't tell them if you take any of these actions.

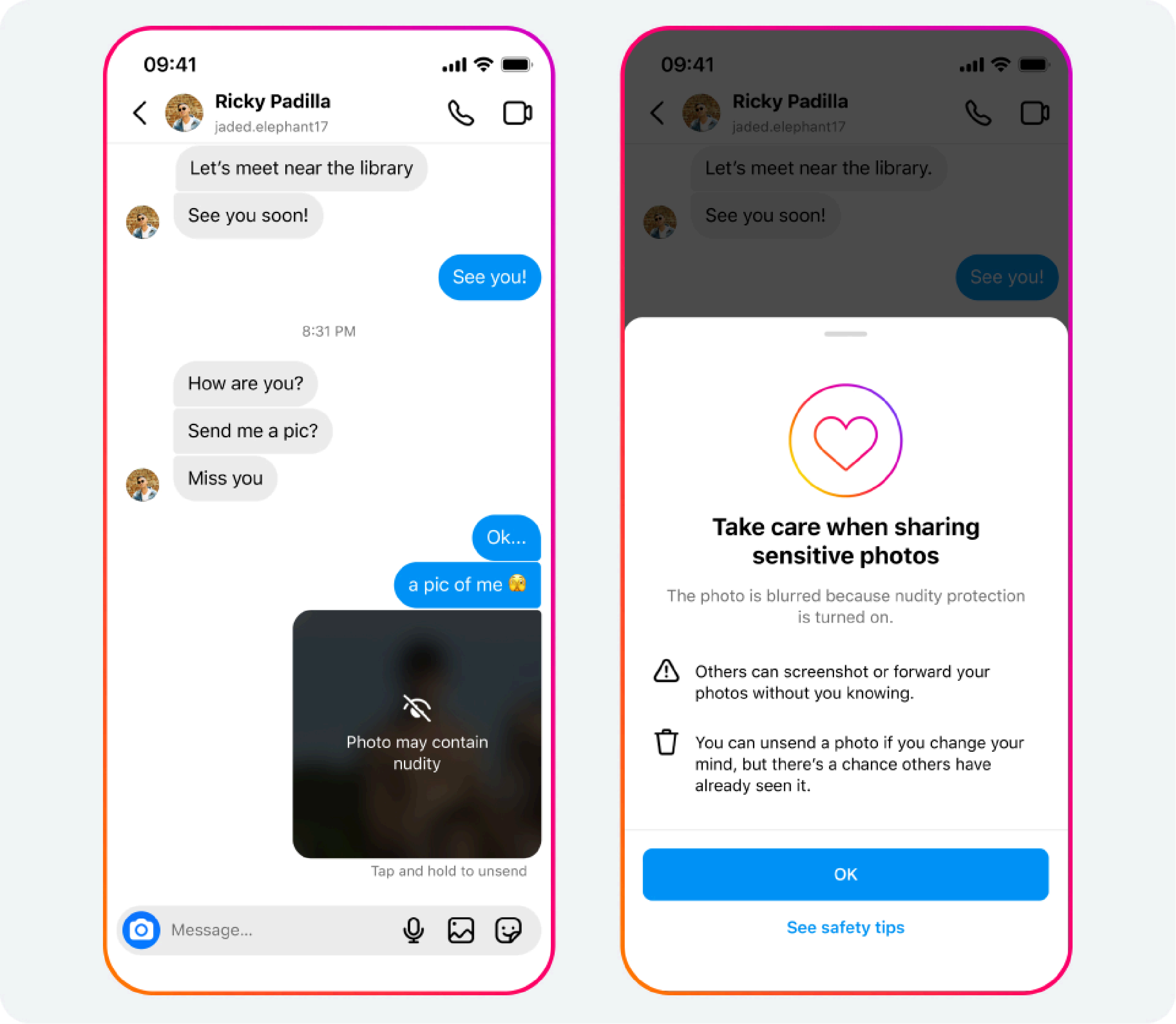
Tips on staying safe in chats

You can say no
If you're asked to do something that makes you uncomfortable, you have the right to say no, even if you did it before.

Report inappropriate behavior
If someone pressures you for money or threatens to share your private photos unless you pay them, report it. Learn more

Help is available
It's never your fault if someone threatens to share your private photos or messages without your permission. See help options

We also recently announced that we've developed new signals to identify accounts that are *potentially* engaging in sextortion, and are taking steps to help prevent these accounts from finding and interacting with teens. Finally, we've started testing our on-device nudity protection feature in Instagram DMs, which will blur images detected as containing nudity, encourage people to be cautious when sending sensitive images and direct people to safety tips and resources, including NCMEC's Take It Down platform.



09:41

Ricky Padilla
jaded.elephant17

Let's meet near the library

See you soon!

See you!

8:31 PM

How are you?

Send me a pic?

Miss you

Ok...

a pic of me 😳

Photo may contain nudity

Tap and hold to unsend

Message...

09:41

Ricky Padilla
jaded.elephant17

Let's meet near the library.

See you soon!

See you!

Take care when sharing sensitive photos

The photo is blurred because nudity protection is turned on.

Others can screenshot or forward your photos without you knowing.

You can unsend a photo if you change your mind, but there's a chance others have already seen it.

This is an adversarial space where criminals evolve to evade our ever-improving defenses. We will continue to focus on understanding how they operate so we can stay one step ahead, and will continue our vital cooperation with child safety experts, law enforcement and the tech industry to help disrupt these criminals across all the platforms they use.

Categories:
Facebook, Instagram, Meta, Public Policy, Safety and Expression

Tags: Safety, Well-Being

RELATED NEWS

Meta

New Tools to Help Protect Against Sextortion and Intimate Image Abuse

We're testing new features to help protect young people from sextortion and intimate image abuse.

April 11, 2024

Topics

Company News

Technology and Innovation

Data and Privacy

Safety and Expression

Combating Misinformation

Economic Opportunity

Election Integrity

Strengthening Communities

Diversity and Inclusion

Featured News

Meta

Meta AI Is Now Multilingual, More Creative and Smarter

July 23, 2024

Meta

Open Source AI Is the Path Forward

July 23, 2024

Our community

Our actions

Support

Community Standards

Data Policy

Terms

Cookie policy

United States

(English) ▼