

The pattern behind every scam

By analyzing more than 100,000 real-world fraud reports, ASU researcher discovered that modern scams follow a surprisingly predictable playbook

By Kelly deVos, ASU News
August 7, 2026

Your phone buzzes.

A package couldn't be delivered. Your bank account has suspicious activity. The IRS says you owe money. Your power company threatens to disconnect your electricity unless you pay immediately.

They seem like different scams because that's exactly what they're designed to do.

To Arizona State University researcher [Xusheng Xiao](#), however, they're variations on the same theme.

Xiao is an associate professor of computer science and engineering in the [School of Computing and Augmented Intelligence](#), part of the [Ira A. Fulton Schools of Engineering](#) at ASU, where he leads the cybersecurity-focused Reliable, Intelligent, Secure, and Efficient Software and System lab.

"Scammers are much more systematic than most people realize," he says. "They don't create a brand-new scam every time. They reuse the same psychological strategies and simply adapt them to different situations."

From phishing and romance fraud to fake jobs and cryptocurrency schemes, cybersecurity researchers tend to treat scams as isolated incidents, each with its own tactics and victims. Xiao suspected there was a deeper structure hiding beneath the endless stream of new headlines.

And instead of asking what scammers were saying, he asked why it kept working.

Inside the scammer's playbook

The answer emerged from one of the largest analyses of scam reports ever conducted.

Working with collaborators from the University of Notre Dame and cybersecurity startup [Charm Security](#), Xiao analyzed more than 102,000 reports submitted to the Better Business Bureau's

Scam Tracker.

Rather than sorting scams by surface-level categories, his team searched for recurring psychological patterns, trying to find the emotional levers scammers pull to persuade people to ignore their instincts and act before they think.

What they found surprised even them.

Modern scammers aren't endlessly inventing new fraud schemes. They're recycling the same psychological playbook.

"The psychology is only one piece of the puzzle," Xiao says. "What scammers really reuse is the entire playbook. They tend to recycle the story, the sequence of interactions and the psychological triggers that make people believe it."

The team's analysis uncovered 18 recurring scam scenarios organized into categories, driven by familiar human vulnerabilities: authority, fear, urgency, promises of wealth, trust and social obligation.

Fake government officials, investment opportunities, online shopping deals and employment offers may appear unrelated, but underneath they rely on the same small collection of psychological techniques.

Scams at scale

Those techniques are rarely used alone.

Xiao's team found that more than 75% of scam reports employed multiple psychological tactics simultaneously. Even more striking, every additional tactic corresponded with roughly a 26% increase in the victim's expected financial loss. Fear alone might not convince someone to send money. Fear combined with authority, urgency and credibility often does.

The research also revealed that scammers themselves are far more organized than many people realize.

By tracking shared domains, email addresses, phone numbers and IP addresses across reports, researchers identified coordinated scam campaigns operating across multiple fraud categories. One campaign alone connected more than 3,800 reported incidents spanning every scam scenario in the study. Rather than building new operations from scratch, scammers repeatedly repurpose the same infrastructure while swapping stories to fit different audiences.

For Xiao, these patterns represent something larger than fraud statistics.

Before the money moves

Understanding those behavioral patterns opened the door to the project's next challenge.

To move the research beyond the lab, Xiao's partnership with Charm Security gave his team access to real-world fraud investigations, allowing them to test whether their research could work outside an academic setting.

Avichai Ben, co-founder and chief technical officer of Charm Security, says research like this is an essential component of protecting the public from fraud.

“Metadata can identify suspicious activity, but human-centric fraud cannot be understood through signals alone,” Ben says. “To distinguish a false positive from a customer under active manipulation, you need to understand the story, tactics and vulnerabilities unfolding in the conversation.”

The team wondered if artificial intelligence, or AI, could recognize a scam as a bank customer described what had happened.

Their answer is the Early Anti-scam Recognition System, or EARS, which analyzes conversations between bank representatives and customers as they unfold, identifying the scam’s underlying playbook before a case becomes another fraud statistic.

When tested on more than 1,100 customer-service conversations modeled after real fraud investigations, the system correctly identified high-level scam tactics approximately 84% of the time. In more than 90% of conversations, the correct scam scenario appeared among its top three predictions.

The human factor

For Xiao, the partnership reflects the kind of impact he’s pursued throughout his career: turning fundamental research into practical tools.

His work has spanned software engineering, cyber threat detection, mobile security and blockchain systems, all united by the common goal of using automated analysis to recognize when complex systems behave in unexpected ways.

“For me, it’s never just about finding a bug or detecting an attack,” Xiao says. “It’s about understanding the behavior behind it.”

Today, that idea extends beyond software to the people who use it. As scammers increasingly rely on psychology instead of technical exploits, Xiao believes the next generation of cybersecurity will need to understand both.

For him, uncovering the pattern behind every scam isn’t simply about classifying fraud. It’s about giving people a better chance to recognize it — and stop it — before they become the next victim.

This story originally appeared on [ASU News](#).

Main image



Xusheng Xiao is an associate professor of computer science and engineering in the School of Computing and Augmented Intelligence, part of the Ira A. Fulton Schools of Engineering at Arizona State University. He is studying ways to protect the public from financial scammers who share and recycle the same scripts and techniques. Photo by Erika Gronek/ASU