How scammers hack your brain and how to protect yourself

ASU researchers provide insight into the psychology of scams for Cybersecurity Awareness Month

By Monique Clement, ASU News
October 5, 2026

Story highlights

Researchers say scams target emotion, not intelligence.

AI, current events and personal information available online help scammers create more convincing messages at a larger scale.

The best defense is to slow down, talk to others and verify information through other channels.

“Your package is being held for delivery,” began a text message sent to Susan Phillips.

She had recently ordered several things online, so the message seemed plausible. It linked to an official-looking page for a delivery company that said Phillips owed $5. New fees are everywhere these days, she thought, so she paid it and went on with her day.

Later, when none of her packages arrived from that carrier, she realized it was a scam. And Phillips (not her real name) is embarrassed about it.

You may be thinking “I would never fall for that.” But scams are designed to hack your brain into believing the seemingly unbelievable.

Arizona State University cybersecurity and psychology researchers explain why even smart people fall for scams and what you can do to protect yourself.

Why you get so many scam texts, calls and emails

Your voicemail is full, you get more texts and DMs from scammers than your friends, and your inbox is a minefield of suspicious links and attachments.

Artificial intelligence is in part to blame.

Scammers used to have to manually craft messages or sit on calls. They were often clumsy with obvious errors that tipped off most savvy internet users. But now, in the age of AI?

Get cyber smart

Test your knowledge and learn more about cybersecurity at research.asu.edu/cybersecurity.

“The whole thing can be basically automated,” says Jaron Mink, an assistant professor in the School of Computing and Augmented Intelligence, part of the Ira A. Fulton Schools of Engineering at ASU. Mink leads the Happy Lab, which studies how human factors shape security and AI.

“The scale is much bigger, and people can make things that look a lot more convincing for a lot less.”

Still, there are ways you can thwart even the most convincing scams if you know what to look for.

Common scam tactics

Xusheng Xiao is an associate professor in the School of Computing and Augmented Intelligence. He studies the psychological techniques and patterns scammers use to trick people.

By analyzing more than 100,000 reports from the Better Business Bureau Scam Tracker, Xiao’s research teamXusheng Xiao’s work is supported in part by the National Science Foundation. identified nine common psychological techniques scammers use:

Authority and impersonation: Pretending to represent a government agency, employer, bank or other trusted organization takes advantage of people’s tendency to trust credible authorities.

Phantom riches: Dangling an attractive reward, unexpected prize or high earnings for little effort can keep you from thinking rationally about the risks.

Fear and intimidation: Using threats or frightening consequences, such as arrest or fines, triggers fear and pushes you to act quickly.

Liking: Appearing friendly, complimentary, helpful or personally interested lowers your guard.

Urgency and scarcity: Presenting time-sensitive or limited opportunities encourages you to act before you have time to think.

Pretext and trust: Creating a plausible story with your personal information and relevant details increases credibility.

Reciprocity: Offering something first — like a job opportunity, money or another benefit — makes you feel obligated to give something back or cooperate.

Consistency: Building on people's tendency to follow through on previous choices or commitments, scammers start with small requests that make larger commitments, such as sending money, feel like a natural next step.

Social proof: Claiming that others have taken the same action makes a scammer's request seem normal, credible or safe.

Xiao says the tactics are often combined for greater effectiveness. For example, a message will impersonate an authority, demand urgent action and create fear by threatening consequences, like the examples below.

Scammers pair these patterns with regional news, upcoming events and personal details to tailor their messages.

"It's plausible, it's trustable and it's very convincing," he says.

> **Scams are about finding the vulnerabilities in humans. They're not only about hacking your computer. They're also about hacking your brain. When your brain is hacked, that's very difficult to fix.**
>
> —
>
> **Xusheng Xiao**
> Associate professor, School of Computing and Augmented Intelligence

Back-to-school and holiday shopping seasons bring fake storefront, fraudulent charge and delivery problem scams. Students receive fake internship offers that collect application fees. Residents of border states are targeted with customs- or immigration-related scams.

"Scams are about finding the vulnerabilities in humans," Xiao says. "They're not only about hacking your computer. They're also about hacking your brain. When your brain is hacked, that's very difficult to fix."

Why smart people fall for scams

Scams use the power of stories to hack our brains.

Movies, TV shows, video games, books, the news and more draw us in and make us feel things. Scam narratives do the same.

“It’s about emotion and not intelligence,” says Thomas Talhelm, the Robert B. Cialdini Endowed Professor of Social Influence in the The College of Liberal Arts and Sciences at ASU.

Talhelm studies how moods affect the ways people think. He also studies persuasive techniques used to influence people in business negotiations, marketing and other scenarios.

Emotion plays a key role. Fear can rush you into acting to get out of a scary situation, like a scammer’s threat of arrest or danger to a loved one. But Talhelm says positive emotions can also affect decision-making in surprising ways.

“Feeling happy often makes people worse at spotting particular details,” he says.

If you’re excited — to win money, get tickets to a sold-out concert or find love — you might not be thinking clearly, Talhelm says. The consequences can be devastating.

Helping fraud investigators catch scams early

Xusheng Xiao is using AI and the knowledge of psychological techniques to help identify bank-related scams in real time. Read more.

Samuel Ellis (name changed for privacy) was lonely when he saw an ad for a dating site. He signed up and connected with “Sofia.” She made him feel cared for and happy. After talking for several months, Sofia planned to fly to see Ellis. He was ready to welcome her into his life. The day finally came, and so did the excuses for why she wasn’t there. The reality of the situation began to sink in.

What did Ellis miss? Stolen or AI-generated photos, an identity and elaborate story constructed to earn his trust, and a dating site that suspiciously charged money to send and receive messages.

“I think the most important part of his story is that this wasn’t simply about losing money,” says Ellis’s son-in-law. “Someone, or some system, recognized the vulnerability of an older man who was lonely and hopeful about finding companionship. They used that hope to keep him emotionally invested and to keep him paying.

“That’s the part that stays with me. He had to come to terms with the fact that someone he had developed feelings for, and a future he had begun imagining with her, may never have existed at all.”

How to avoid scams: Slow down before you act

Talhelm says the good news is that it doesn’t take much to take back control.

“You don't need to be an expert to prevent a lot of these psychological tricks that are being used against you,” he says. “It's not about controlling your emotions. It's to just slow down and don't make a decision right away,”

That’s advice Talhelm wishes he had taken when he got scammed.

Talhelm is an avid runner. After he missed a spot in a half-marathon he had been running for several years, a stranger messaged him. He offered Talhelm his race bib in exchange for the $50 registration fee.

“I was pretty skeptical of this, but then I logged into the race system and the bib had been assigned to me. It was in the system,” Talhelm says.

He believed he was on the official website, so it felt safe to proceed quickly. But once Talhelm sent the person $50, the bib disappeared from his account.

If he could go back, he would have contacted the race organizer to ask if the stranger was in the system and whether buying the bib was allowed. When Talhelm checked after being scammed, the organizer said all bib exchanges should go through him.

“If I just slowed down and thought ‘I don't need to solve this now, I don't need to make a decision now,’ then that wouldn’t have happened,” Talhelm says.

Once you pause, try these strategies recommended by Talhelm and other experts.

Tip 1: Verify through official channels

Don’t follow provided links. Find another way to verify the claim.

Log in to your banking app or navigate to your bank website separately. Hang up on a suspicious call and dial your loved one or the official number of the organization the caller claims to represent.

Why this research matters

Research is the invisible hand that powers America’s progress. It unlocks discoveries and creates opportunity. It develops new technologies and new ways of doing things.

Learn more about ASU discoveries that are contributing to changing the world and making America the world’s leading economic power at

Note that government agencies will never call, email, text or message you on social media to ask for money or personal information.

You can also search online for the scenario or reference the Better Business Bureau Scam Tracker.

Tip 2: Talk to someone you trust

People who aren't involved in the scam attempt are more likely to see the situation clearly. Another person can slow you down and help you see whether something is suspicious or truly urgent.

Mink also says people can consider creating secret phrases with loved ones to help verify you're actually talking to them.

Tip 3: Shift your mindset

Talhelm recommends changing your thought process from "Can I believe this?" to "Must I believe this?" The concept, from social psychologist Jonathan Haidt, plays a role in decision-making.

If you're asking whether you can believe something, you usually want it to be true and it won't take much to convince you. If you think you have to believe something, you're more likely to look for reasons not to.

"See if you can get yourself in a 'Must I believe this?' mindset," Talhelm says. "If you're in that mindset, you'd be much more likely to call the company, call their official line and look for disconfirming evidence."

Device and account security still matter

Human behavior is a key factor in scams, but cybersecurity is also about protecting computers, networks and data from attacks.

The internet wasn't originally built with security in mind, says Jedidiah Crandall, an associate professor in the School of Computing and Augmented Intelligence — so it's a constant race for cybersecurity professionals to address vulnerabilities before they're exploited.

Crandall studies network security, particularly for the most at-risk users living under restrictive governments or those who work with sensitive information. But all users should be aware of the limitations of tech security.

Verified apps are usually secure, but it's impossible to be 100% sure. Something that's harmless now might be exploited later. Crandall says The Citizen Lab is a trusted source of the latest research on app security and privacy issues.

Apps also often sell your data, which can give scammers information they can use to make a scam seem real.

researchmatters.asu.edu.

Even virtual private networks, which are designed to encrypt your online activity, may not be as private as they seem, ASU researchers found.

Computer networks and security infrastructure can also get confused. For example, email servers can be fooled into showing a legitimate email address, like your boss's, when in fact the message was from a scammer.

Because of factors like these, scams can be very sophisticated and difficult to detect. Slowing down, verifying the claims and talking with others can help.

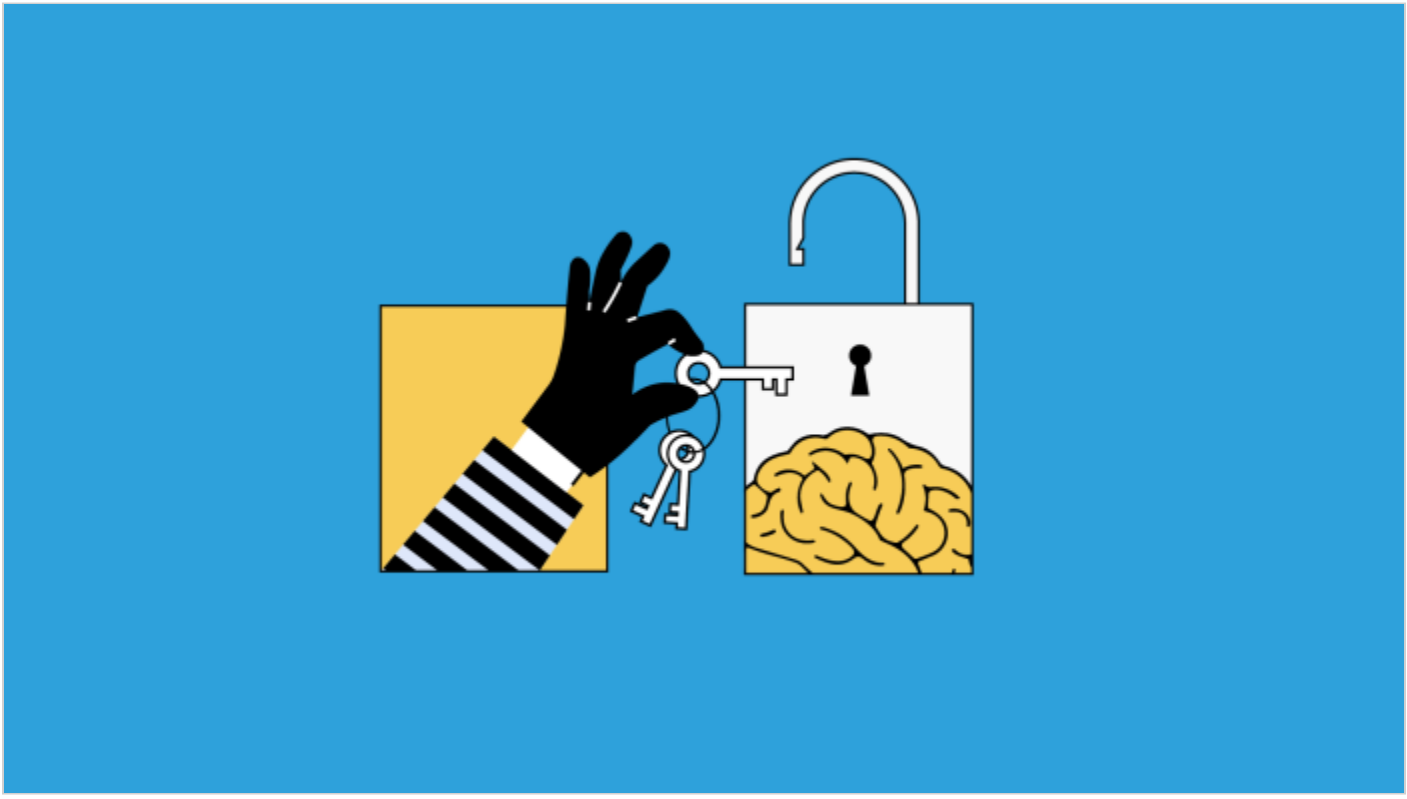
Security practices like unique passwords, multifactor authentication and installing updates are also important to protect your devices and accounts.

Learn more about these security practices and others at research.asu.edu/cybersecurity.

This story originally appeared on ASU News.

[1] Xusheng Xiao's work is supported in part by the National Science Foundation.

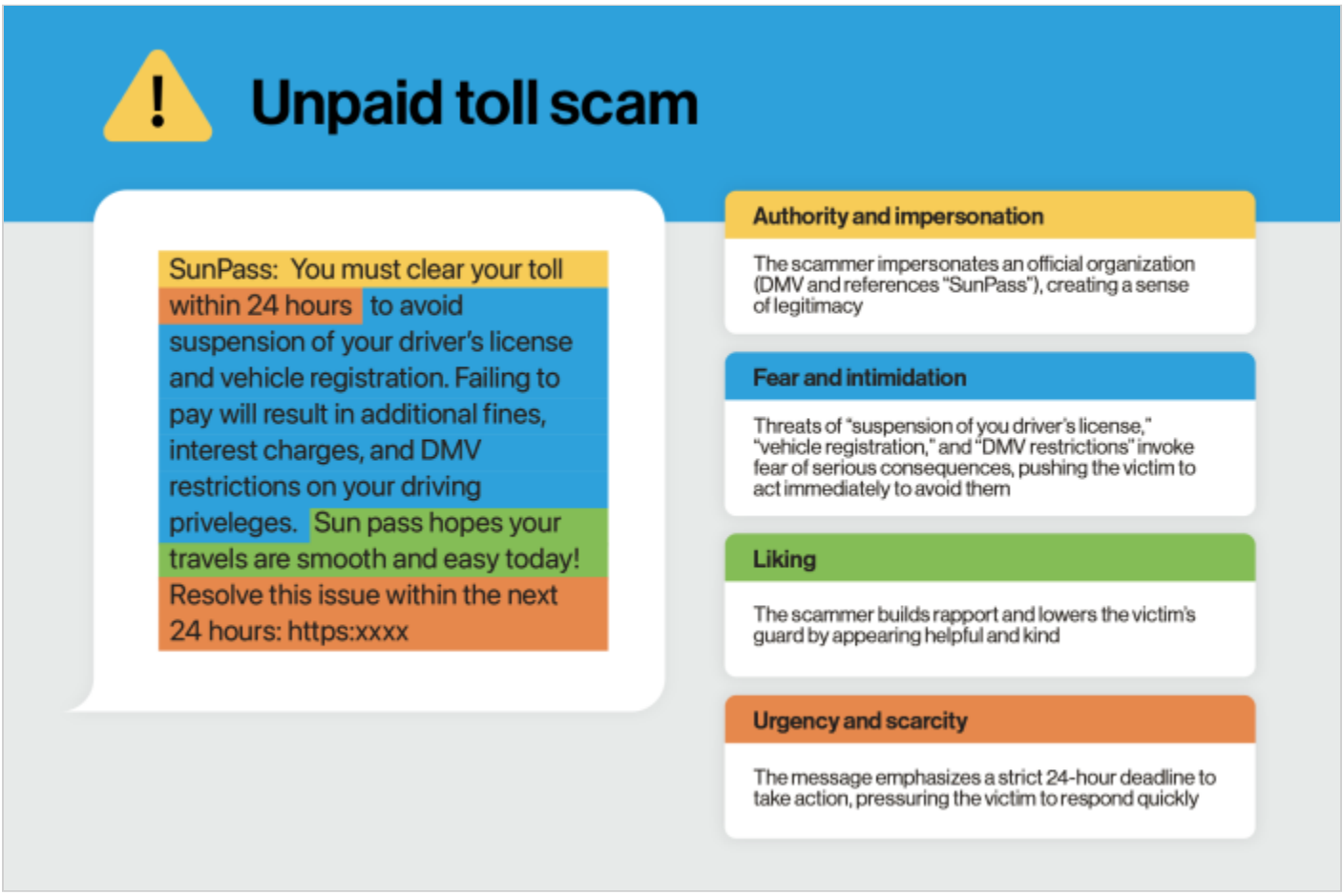
Main image



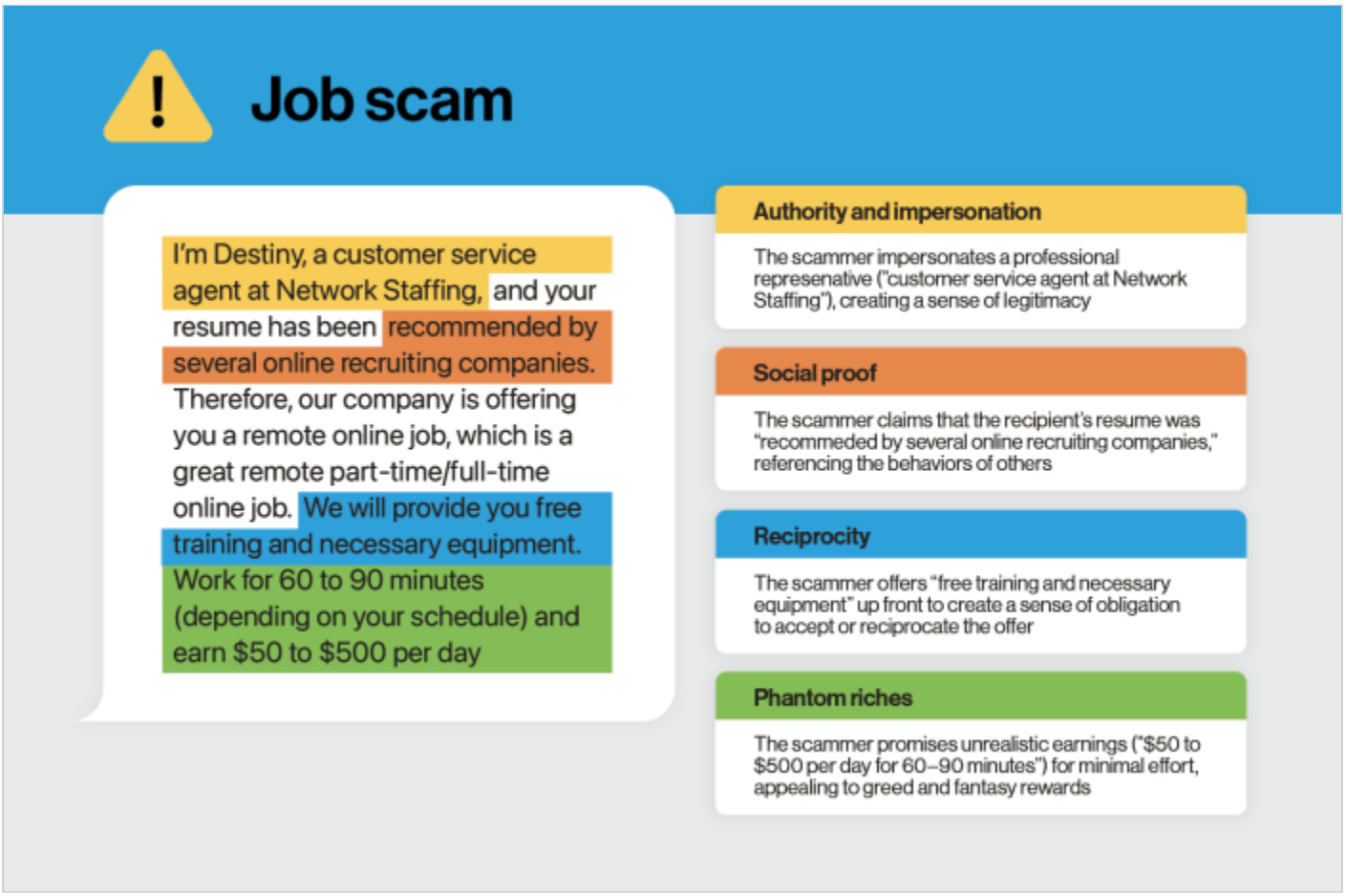
Cybersecurity often focuses on protecting devices and data, but many scams succeed by targeting people's emotions and decision-making. For Cybersecurity Awareness Month, Arizona State University cybersecurity and psychology researchers explain how psychological tactics are used

for scams and ways you can protect yourself. Graphic by Andy Keena/ASU

Text image(s)



Xusheng Xiao's research team analyzed more than 100,000 reports in the Better Business Bureau Scam Tracker and collected the psychological tactics scammers use. View full size. Graphic by Xusheng Xiao/ASU and Andy Keena/ASU



The psychological tactics Xiao's team found are often used together in effective patterns that make recipients more likely to comply. View full size. Graphic by Xusheng Xiao/ASU and Andy Keena/ASU