# New cybersecurity challenges are on the horizon; will the world be ready?

## ASU cybersecurity experts are creating solutions to protect us for the future

By Mikala Kass, ASU News
October 19, 2026

***Editor's note:*** *This is part two of our series for Cybersecurity Awareness Month. Read part one for ASU experts' insights into how scammers trick us and how you can protect yourself.*

### Story highlights

ASU cybersecurity experts anticipate new cybersecurity challenges and are working on solutions to prepare for them.

Understanding how vulnerabilities in robots could impact security will help us keep them working safely.

Capturing the biological patterns associated with human speech can help verify if a voice is real or cloned.

Creating a way for sub-systems in a network to prove their trustworthiness will prevent a small breach from causing a major breakdown.

A hacked robot assistant gathers intel to steal the identity of a senior in a care facility. A caller with a deepfake of a loved one's voice begs a family member to pay a ransom to a "kidnapper." A compromised car sensor prevents it from braking safely.

Cybersecurity is a shifting landscape, and new technologies, for all their promise, can also threaten new nightmare scenarios.

That is why experts across Arizona State University are going beyond addressing today's challenges to create proactive approaches that prevent these cybersecurity nightmares from becoming reality.

These cybersecurity researchers are creating solutions that can be employed before emerging challenges have the chance to gain a foothold in our lives or impact our national security.

## Keeping bots and bugs in check

AI is ushering in a new era for robotics. Thanks to advances in large language models, or LLMs, like ChatGPT and Claude, robots can read human language and behavior more clearly than before.

More helpful robots can be useful in more places, like warehouses, hospitals, senior care facilities and homes. But Tiffany Bao, an associate professor in the School of Computing and Augmented Intelligence, sees the inherent risk in technology that interacts with our physical space.

### Eager to test your cybersecurity knowledge?

Check out our dedicated cybersecurity page with quizzes, resources, news and more

"Naturally that comes with security concerns. If robots in the future will be deployed in these places, they're going to be exposed to actual human beings," says Bao, who is also the assistant director of research at the Center for Cybersecurity and Trusted Foundations. "In specific scenarios where those humans are senior people, patients or kids, they're more vulnerable."

A hacker could exploit a robot to make it stop working, alter its behavior or even do something malicious to the humans around it. For some robots, like those used for military, communications or manufacturing tasks, a hacker-induced failure on the job could have costly national security repercussions.

Bao worked with a program called DARPA FIRE, which looked into vulnerabilities in military drones and unmanned and manned aviation vehicles and how those vulnerabilities could impact their tasks in the real world.

> **A sophisticated attacker can chain vulnerabilities together — they behave in a way where one plus one is greater than two.**
>
> —

**Tiffany Bao**
Assistant director of research in the Center for Cybersecurity and Trusted Foundations

AI has introduced another challenge by making it easier to discover numerous bugs in a system. These weak points could be used to hack robots as well as accounts, software providers or critical infrastructure.

Bad actors can combine multiple vulnerabilities in a system to create what's called a "cascade effect" of damage bigger than the sum of its parts. Bao worked on another DARPA project called HARDEN to study how these attacks happen.

"A sophisticated attacker can chain vulnerabilities together — they behave in a way where one plus one is greater than two," Bao says. "We want to understand the comprehensive effect of all the vulnerabilities, because the specific combination of them turns out to be very important."


## Related

ASU-based startup Artiphishell helps cyber defenders sort and prioritize software bug patches


A small bug may seem minor — especially when buried in a mountain of other discovered bugs — until we realize it's a link in a larger chain that can do more damage. Being able to prioritize patches is a key tool to reducing that risk.

Bao's research advances efforts to create AI tools for cyber defense, including smart systems that self-audit, patch and test.

## Reclaiming the human voice

We use digital communications in all kinds of contexts — and while text-based scams have been around awhile, it was a safe assumption that if you heard someone's voice or watched them speak through a video call, it was authentic.

But that assumption no longer holds. Advances in AI have made voice cloning and deepfake videos easier and cheaper than ever, putting our entire framework of digital trust at risk.

"Anyone can create this content in real time on their own computer. You don't need any sort of specialized hardware, and it's completely inexpensive," says Visar Berisha, the associate dean of research and commercialization in the Ira A. Fulton Schools of Engineering. "The internet wasn't set up with this problem in mind. I think this really opens the floodgates to a new set of problems that we've never had to deal with before."

## Why this research matters

Berisha studies how humans produce speech and develops AI models to analyze speech for early signs of cognitive decline or other health issues. But he found another use for his work when he realized the internet was missing built-in tools to validate that what we see and hear is genuine.

His lab has created a “proof of personhood” device that captures the biological signals associated with someone speaking and checks it against the audio the microphone captures. It works by using millimeter wave radar, which sends low-energy radiofrequency waves toward a person to detect small movements the body makes while talking.

“You can get a pattern of the lungs expanding and contracting, a pattern of the heart beating, a pattern of the vocal folds vibrating, a pattern of the lips, jaw and the tongue moving," Berisha says. "And all of these have to be very closely tied to what the microphone is picking up, because it is this process that is producing the sound.”

If a bad actor were to use technology to make their voice sound like someone else, the device would detect that the person’s biological patterns don’t match the sound patterns picked up by the microphone and flag the audio as suspicious.

Berisha recently spun out his technology to create a startup called OriginStory.

“In the future, we hope that this is embedded within all of the existing devices that we use — laptops, phones, headphones, microphones — because it will create this layer of trust infrastructure that’s currently missing in digital communications,” he says.

## Forming a circuit of trust

Separate technology systems, each with its own purpose and security protocols, are increasingly connected. That means a cybersecurity vulnerability in one element — whether from a hack, a spoofed signal or a piece of corrupt hardware — threatens the whole network. Michel Kinsy, an associate professor in the School of Computing and Augmented Intelligence, calls this idea “system-of-systems cybersecurity.”

“A car is a good example — it is really a system of systems made up of sensors, control units, infotainment, communication modules and cloud services built by different suppliers and expected to work together safely,” says Kinsy, who directs the Secure, Trusted, and Assured Microelectronics Center.

## Related

Read more about Kinsy’s work to protect data in a future with decrypting quantum computers

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 researchmatters.asu.edu.

The same applies to tools necessary for national defense, like a modern radar system. If a single subsystem is compromised, it can corrupt the output of the whole radar system. That's why Kinsy's center works on ways to continuously verify trustworthiness within these complex systems.

> **The end goal is computing platforms that can defend themselves and keep operating safely and reliably, even in contested or hostile environments.**
>
> —
>
> **Michel Kinsy**
> Director of the Secure, Trusted, and Assured Microelectronics Center

Picture a water treatment controller that authenticates every command before acting on it, a car that can tell the difference between a jammed sensor and a genuine stop command, or a smart home device that will not hand over your usage patterns without your consent. Each of these systems would be capable of verifying its own integrity and isolating itself the moment something looks wrong, rather than quietly handing an attacker a foothold.

“Instead of waiting for an attack to succeed and cleaning up afterward, these systems continuously check their own trustworthiness, watch for suspicious behavior and respond in real time. The end goal is computing platforms that can defend themselves and keep operating safely and reliably, even in contested or hostile environments,” Kinsy says.

He aims to move these ideas out of the lab and into systems that run our critical infrastructure, vehicles and everyday devices.

“Some of my former students are already taking this work into the commercial world themselves," Kinsy says, "launching startups built on what they developed at the center, and I am very proud of that."

---

In the face of scary headlines, it's helpful to know there are experts working hard to keep us safe from challenges we may face ahead. But it's also important for you to take steps to protect yourself against today's threats.

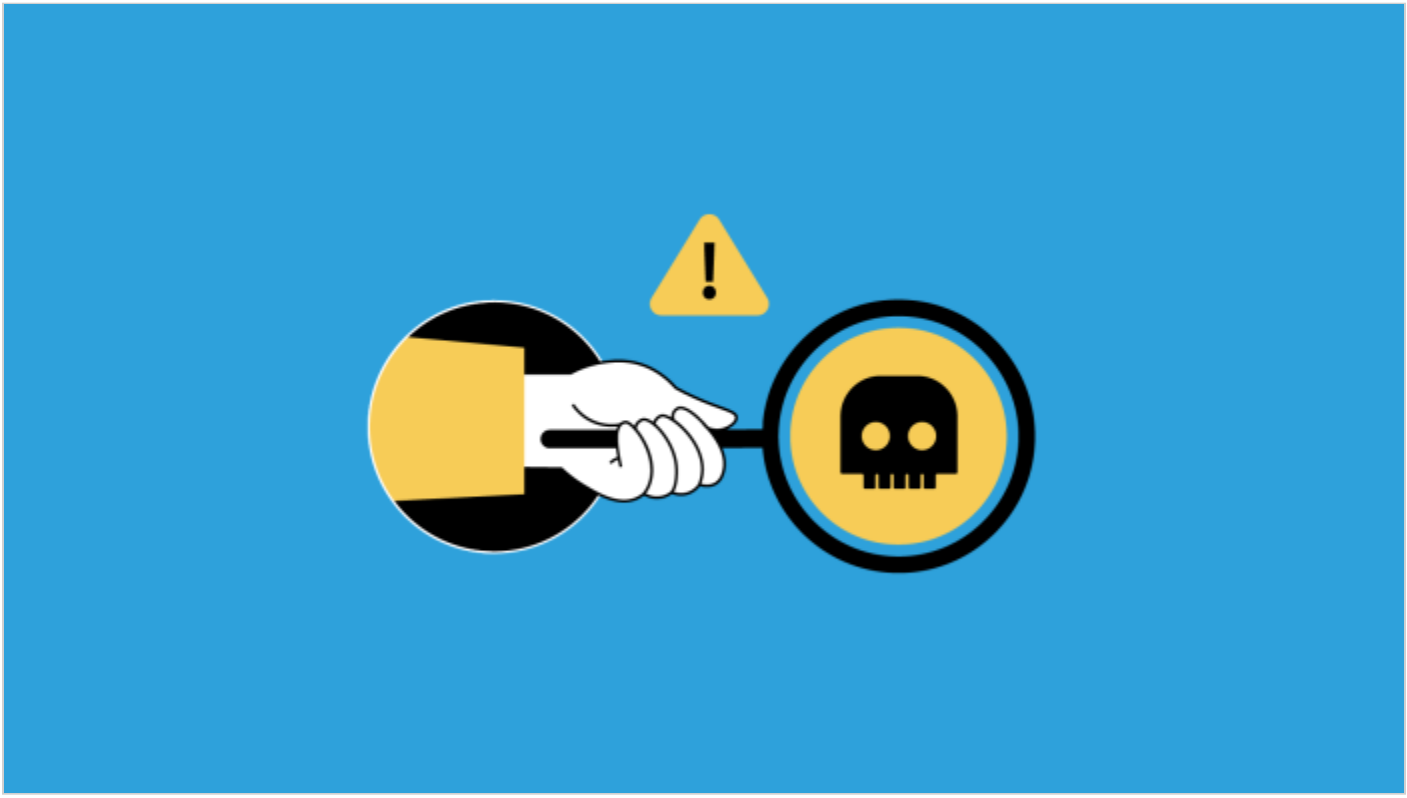
Read ASU experts' tips on personal cybersecurity, scams to watch out for, and what to do if you think you've been hacked or scammed.

*The Center for Cybersecurity and Trusted Foundations is a unit of the Advanced Capabilities for National Security Institute.*

---

*This story originally appeared on ASU News.*

## Main image



ASU cybersecurity experts are looking ahead at emerging challenges and creating solutions that can be employed before those problems gain a foothold. Illustration by Andy Keena/ASU Knowledge Enterprise