

What are tomorrow's quantum threats?

In recognition of World Quantum Readiness Day, an ASU expert discusses quantum computing, AI and the future of cybersecurity

By Kelly deVos, ASU News
September 11, 2026

Most people trust that the passwords, bank accounts, medical records and private messages they use every day are protected by encryption. But as quantum computing advances, some of today's most widely used security tools could eventually become breakable.

That means information stolen now could potentially be saved and unlocked years later, when quantum computers are powerful enough to crack protections that current computers cannot.

[World Quantum Readiness Day](#), observed this year on Sept. 17, is meant to raise awareness of that risk and encourage governments, companies and researchers to prepare for a more secure future using post-quantum cryptography, or PQC.

[Michel Kinsy](#) is an associate professor in the [School of Computing and Augmented Intelligence](#), part of the [Ira A. Fulton Schools of Engineering](#) at Arizona State University. In his role as director of ASU's [Secure, Trusted, and Assured Microelectronics, or STAM, Center](#), he leads research in hardware security, secure microelectronics design and post-quantum cryptography systems.

In this Q&A, Kinsy explains what quantum readiness means and why advances in quantum technologies and artificial intelligence may affect the way society protects information in the years ahead.

Question: Many people think of quantum computing as something far in the future, but cybersecurity experts are already urging organizations to prepare now. Why is this a problem that can't wait until large-scale quantum computers arrive?

Answer: Moving to quantum-safe cryptography is not something organizations can accomplish overnight. It is a multiyear effort, even once new standards exist. Before anything else, organizations must identify all the places where encryption is built into their software, hardware, devices and supply chains, then test and deploy replacements without disrupting existing operations. History shows that these transitions take time.

For example, it took much of a decade for [organizations to move away from SHA-1](#), an older security algorithm that was once widely used but was eventually found to be vulnerable to attack. That is part of why this feels urgent now, even though large-scale quantum computers are not available yet. Attackers do not need one today to benefit from one later. Through what is called

“harvest now, decrypt later,” they can capture encrypted data now and simply hold onto it until a quantum computer capable of breaking it comes along. If that data needs to stay sensitive for the next 10 to 15 years, the time to prepare is now, not once the technology actually arrives.

Q: You said organizations must identify the parts of their systems that rely on encryption to protect data. What is encryption?

A: At its core, encryption is a mathematical process for turning readable information into unreadable information. The original message, file or transaction is called plaintext. An encryption algorithm uses a key to transform that plaintext into ciphertext, which looks like random data to anyone who does not have the right key. The intended recipient uses a corresponding key to turn it back into readable information. That process is what helps keep sensitive information protected as it moves across digital systems.

Q: When we hear that quantum computers could “break encryption,” what does that actually mean, and what should the public understand without assuming everything will suddenly become insecure overnight?

A: Quantum computers pose a real threat to the public-key cryptography we rely on today, including [RSA](#) and [elliptic-curve cryptography](#), two common methods used to protect digital information. These systems are secure because they depend on mathematical problems that are extremely difficult for conventional computers to solve. A large, stable quantum computer could run algorithms like [Peter Shor’s algorithm](#) to solve those problems efficiently and recover private keys from public information.

That said, this is not something quantum computers can do today. Breaking modern RSA or elliptic-curve cryptography would require a large-scale, error-corrected quantum computer that is beyond the capabilities of currently available systems. It is also important to understand that quantum computing does not suddenly make all classical encryption useless. [Symmetric encryption](#), another major form of encryption that protects most of our stored and transmitted data, is much less affected and can remain secure with larger key sizes.

The immediate concern is [public-key cryptography](#), which supports secure web browsing, authentication, digital signatures and key exchange, the process that helps two systems securely agree on how to communicate. Because these technologies are built into many parts of the digital ecosystem, organizations should already be preparing for the transition to post-quantum cryptography, which is designed to provide the same security protections, even in the presence of powerful quantum computers.

Q: You mentioned “harvest now, decrypt later,” where attackers steal encrypted data today in hopes of unlocking it in the future. How real is this threat? What kinds of data or organizations are most at risk?

A: It is a real and, in my view, underappreciated threat. An adversary does not need a working quantum computer today to benefit later. They just need to capture encrypted traffic or stolen data now and store it until the technology catches up.

The organizations most exposed are the ones holding information that has to stay confidential for a long time, such as government agencies and defense contractors with classified or sensitive communications, health care systems with medical records, financial institutions with transaction

and account data, and any company protecting long-lived intellectual property or genomic data. If that information needs to remain secret in 2035 or 2040, protecting it with quantum-vulnerable encryption today is already a real security vulnerability gap, even though no attacker can exploit it this year.

Q: What is post-quantum cryptography, or PQC, and how does it help prepare digital systems for a future where quantum computers are more powerful?

A: My team and I have worked on this for more than a decade, including through the [National Institute of Standards and Technology's](#) process, to evaluate and standardize post-quantum cryptography. Post-quantum cryptography is a new generation of algorithms designed to stay secure even against powerful quantum computers. Rather than relying on mathematical problems that a quantum computer could eventually solve, these algorithms are built on different types of problems that researchers believe are hard for both classical and quantum computers to crack.

In 2024, NIST finalized its first post-quantum cryptography standards, marking an important step toward the broader transition. But an algorithm being quantum-safe on paper does not mean a given implementation is secure, and that gap is a big part of what my group focuses on. That includes an open-source platform we built with industry partners so small and midsize organizations can safely experiment with and transition to PQC.

Q: How is artificial intelligence, or AI, changing the landscape here?

A: AI is affecting this in a few different ways at once. It is accelerating quantum computing research itself, from qubit design to error correction, which could shorten the timeline to a capable quantum machine. It is also being used to search for weaknesses in cryptographic algorithms, both old and new, which is part of why NIST's standardization process involved years of public cryptanalysis before finalizing PQC standards.

At the same time, AI is creating a new category of information worth protecting: The data used to train models, proprietary model weights and sensitive datasets often need to stay confidential for a long time, which makes them attractive targets for harvest-now, decrypt-later attacks. And because AI systems increasingly run on specialized hardware, securing that hardware is just as important as securing the software layer above it.

Q: Phoenix recently announced a Quantum Strategy, with ASU helping lead the effort. What role can universities play in preparing the region for quantum technologies, especially when it comes to cybersecurity, workforce development and building trusted systems?

A: The [Phoenix Quantum Strategy](#), announced by Mayor Kate Gallego, is an effort to position Phoenix as a national hub for quantum computing, communication and sensing. ASU is playing a key role in that work, with [Sethuraman Panchanathan](#), University Professor of Technology and Innovation at ASU and former director of the [National Science Foundation](#), helping guide the strategy. That matters because quantum readiness requires more than scientific discovery. It also requires secure infrastructure, workforce development, industry partnerships and trusted systems that can support these technologies responsibly.

Q: In the STAM Center, how are you training students to understand and respond to the cybersecurity challenges that quantum computing may create? What skills will they need to help organizations make the transition to quantum-safe systems?

A: A lot of it comes down to giving students hands-on experience rather than just theory. One of the biggest challenges we run into across the field is that many engineers and organizations have little to no understanding of the mathematical underpinnings of PQC, or of the software and hardware vulnerabilities a poor implementation can introduce.

An algorithm being quantum-safe does not mean an implementation of it is secure. At the STAM Center, students implement post-quantum algorithms in real hardware and software, evaluate how they perform on constrained systems, and study how these systems can be attacked through side channels.

With support from the National Science Foundation, we have been [running a workshop series](#) that brings together top researchers from academia, government and industry to study implementation vulnerabilities in PQC. Our students take part in that effort and work alongside industry and government partners, because the classroom and the lab can only teach so much. Working in real deployment environments, under real scenarios, is what builds the transferable skills that matter.

One example is [Isa Cohen](#), a recent ASU graduate and [Foreign Affairs Information Technology Fellow](#) with the [U.S. Department of State](#). Students like Cohen show how that combination of research experience and applied problem-solving prepares them to help organizations manage this transition, whether they go on to work in industry, government or academia.

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

Main image



Michel Kinsy in the Secure, Trusted, and Assured Microelectronics, or STAM, Center. Kinsy 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 also serves as director of ASU's STAM Center, a research consortium that includes the Adaptive & Secure Computing Systems Laboratory, which studies post-quantum cryptography. Photo by Erika Gronek/ASU