

An engineer works on a quantum computer in the US. Cybersecurity systems need to be upgraded to guard against the threat posed by the new generation of machines

REUTERS

CYBERSECURITY

## Battle begins to stop quantum computers smashing cyber defences

As new cryptography standards are approved in the United States, businesses can start to step up their systems to resist attacks from malicious users

Richard Tyler

Tuesday August 20 2024, 12.01am, The Times

[Share](#) [Save](#)

America has fired the starting gun for businesses to plan cybersecurity systems that can resist attack from malicious users of quantum computers.

Last week the National Institute of Standards and Technology, an agency of the US Department of Commerce, approved three algorithms for new post-quantum cryptography standards, the result of eight years of work by cryptography experts worldwide.

In the next phase, cybersecurity suppliers will develop ways to embed the technology in hardware, software and the applications that millions of people use every day.

The US government has said it expects companies supplying the federal government to begin protecting their systems between 2025 and 2030.


Britain's National Cyber Security Centre said in a guidance post from its high-threat technologies team that the standards meant the next step in the "national migration" in cybersecurity systems could begin. "For some sectors, we expect it to take more than a decade," they stated. "However, the scale of the effort means that work to prepare is a priority now. Larger organisations (and those that have bespoke IT or operational technology) should be planning."

ADVERTISEMENT

**THE CUPRA DRIVE EVENT**

Take a test drive and get an additional £1,000 off your new CUPRA.

[BOOK A TEST DRIVE](#)



**CUPRA BORN**

UK retail customers, 18+. Ordered and delivered between 13/08/24 and 30/09/24. £1,000 inc. VAT saving applied to manufacturer's direct on-the-road price on invoice. New stock vehicles only; subject to availability. See full T&Cs.

Ali El **Kaafarani**, the founder of PQShield, the Oxford-based quantum security specialist, said: "I don't have any doubt that in 2025 you will not see any major bank not having published publicly their road map to become post-quantum secure in two, three or four years."



PQShield's Ali El **Kaafarani** is confident that banks will soon have drawn up roadmaps to becoming "post-quantum secure in two, three or four years"

BT has said it is managing the threat to its communications infrastructure and that any changes to its systems "are tested before deployment in live networks".

Small businesses and consumers will see the software and devices they use refreshed as part of new product launches and updates.

The NCSC is encouraging companies to work with experts to avoid poorly managed and rushed migrations, and to have fully tested the algorithms before deploying them on live systems.

While a quantum computer capable of breaking existing security encryption is not yet known to exist, industry experts say hackers could steal encrypted data today and save it to be decrypted by a quantum computer in the future.

ADVERTISEMENT



The US government has already estimated that it will cost about \$7.1 billion to fund the migration on federal systems between 2025 and 2035.

Moody's, the credit rating agency, has said that the migration is comparable in scale and complexity to the changes made to computer systems to cope with the potential chaos in coding when the year changed from 1999 to 2000, known at the time as the Y2K bug.

Some of the largest technology firms have already begun deploying the technology, with Google updating its Chrome browser and Apple doing the same to its Swift programming language and operating system.

El Kaafarani said patching software with the new security algorithms would provide some protection. "It is better than not having post-quantum cryptography at all. But it will only give you a certain level of security guarantees if you don't have it in the hardware."

Business & Money > Entrepreneurs

- Technology
- United States
- Entrepreneurs

### Read more

#### Billionaires, bad deals and bold rivals: what went wrong at Asda?

August 19 2024, 10.34am  
Isabella Fish, Retail Editor

#### Lawyers set for record-breaking year as billings soar

August 19 2024, 5.00pm  
Jonathan Ames, Legal Editor

MARKET REPORT

#### FTSE 100 today: latest UK stock market news

August 16 2024, 7.25pm  
Jessica Newman

### Related articles

CYBERSECURITY

#### What I learnt ... about the security threat from quantum computing

July 02 2024, 6.00am  
Richard Tyler

#### Technology boss hoping to drive computing's next quantum leap

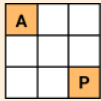

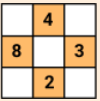
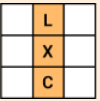
March 11 2024, 12.01am  
Katie Prescott, Technology Business Editor

TIMES ENTERPRISE NETWORK: RISING STARS

#### Start-up leads charge in widening access to quantum computing

August 02 2023, 10.15am  
Naomi Ackerman

### Today's puzzles

			
	Polygon	Sudoku	Lexica