January 19th, 2026
More information: media@surfshark.com

Surfshark introduces post-quantum protection and evaluates the quantum-resistance of top apps: only 8% are resilient

Surfshark, a cybersecurity company, is becoming future-proof and has launched post-quantum protection on WireGuard. This cutting-edge security is now available for major platforms, including macOS, Linux, and Android, with plans to expand to iOS and Windows platforms soon. As quantum computing raises significant concerns and only 8% of the most popular everyday-used apps are resilient, this development is crucial for protecting individuals, businesses, and governments against future technology that could compromise digital security.

“Quantum computing is advancing rapidly, and it poses a threat to current encryption methods used to secure data online. Although nowadays it is used in very limited capabilities, soon it could become powerful enough to compromise today’s encryption systems, leading to significant digital security threats. Therefore, creating cryptographic methods that can withstand quantum computing is essential for any business, especially a cybersecurity company,” comments Donatas Budvytis, Chief Technology Officer at Surfshark.

Why is it important to outrun quantum computers?

While a classical computer might require thousands or even billions of years to solve a very difficult prime factorization problem, a powerful quantum computer can often find a solution in just a few hours. The expert provides an easy explanation of how this might harm a person.

Budvytis highlights that hackers are currently able to store large amounts of encrypted data, which is secure against today's technology but not immune to future developments in quantum computing. As quantum computing becomes more accessible to the general public, sensitive information like passwords, financial data, private conversations, and other encrypted data will become much easier to decrypt quickly. If businesses, governments, and institutions do not take precautionary measures to implement post-quantum cryptography (PQC), it will pose significant privacy challenges for everyone.

“Imagine someone making a bank transfer. Even if they use a VPN with post-quantum protection that encrypts the entire process, their data remains vulnerable if the bank itself lacks similar protection. Hackers equipped with quantum computing capabilities could easily decipher the data, though the process itself might remain secure. This may lead to major financial losses both for the individual and the bank,” explains Budvytis.

To better understand readiness for the post-quantum era, Surfshark selected the most popular apps in banking, shopping, social media, and messaging categories to assess their adoption of PQC.

Only 8% of analyzed apps currently utilize PQC

We analyzed a total of 40 commonly used apps across social media (9), messaging (11), banking (10), and shopping (10) categories. The data reveals that:

- PQC implementation is still in its early stages, with only 8% of analyzed apps currently utilizing PQC. Approximately 30% of the analyzed app developers are researching or have prepared plans to become quantum-resistant. About 65% of analyzed apps have no public information available regarding PQC adoption plans;
- Among the most popular banking apps, none have yet implemented PQC, and only 20% have taken proactive steps to become quantum-resistant. The same situation applies to shopping apps;
- In the social media apps category, TikTok is the only one that is quantum-resistant;
- Messaging apps are the only category of analyzed apps that already feature PQC, with 18% being quantum-resistant, 27% researching quantum resistance, and 55% having no plans regarding PQC. However, both Google, which owns Google Messages, and Meta, which owns WhatsApp and Messenger, have acknowledged potential threats from quantum computers and have taken proactive measures to protect against their future decryption capabilities.

To enhance your future readiness, Budvytis advises taking proactive steps today: stay informed with the latest news, pursue continuous education, and adopt quantum-resistant technologies as soon as possible.

ABOUT SURFSHARK

Surfshark is a cybersecurity company offering products including an audited VPN, certified antivirus, data leak warning system, private search engine, and a tool for generating an online identity. Recognized as a leading VPN by CNET and TechRadar, Surfshark has also been featured on the FT1000: Europe's Fastest Growing Companies ranking. Headquartered in the Netherlands, Surfshark has offices in Lithuania and Poland. For more research projects, visit our research hub.