

SpecterAI Launches 'Quantum-Safe Security: Foundations' Course to Help the Financial Sector Prepare for the PQC Era

SpecterAI Launches "Quantum-Safe Security: Foundations" Course to Help the Financial Sector Prepare for the Post-Quantum Cryptography Era

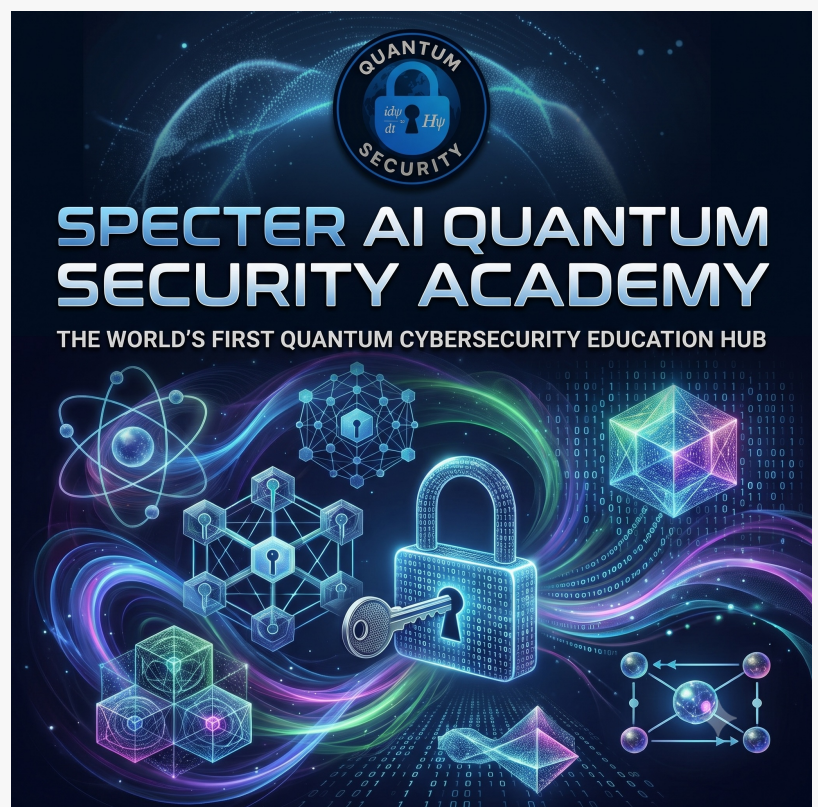
VIETNAM, July 15, 2026

/EINPresswire.com/ -- Specter AI Quantum Security Co., Ltd. (SpecterAI) — a provider of Post-Quantum Cryptography (PQC) migration solutions — has officially launched the “Quantum-Safe Security: Foundations” course. The program helps banks, insurers and financial institutions proactively prepare for the risk that data encrypted today could be decrypted once a cryptographically relevant quantum computer exists.

In the United States, NIST Interagency Report 8547 sets out a transition timeline that deprecates RSA and ECC in federal systems by 2030 and disallows them after 2035, while the NSA's CNSA 2.0 suite mandates post-quantum algorithms within the scope of U.S. national-security systems.

"Many organizations still believe they can wait until quantum computers actually arrive before taking action.

However, the risk is not in the future — it has already begun," said Dr. Peter Huynh, Chairman of SpecterAI APAC. "The collection of encrypted data for future decryption — a tactic known as



HỌC VIỆN ĐÀO TẠO BẢO MẬT LƯỢNG TỬ



Quantum-Safe Security Foundations

'Harvest Now, Decrypt Later' (HNDL) — has been flagged by CISA, NSA, and NIST in joint guidance issued in 2023, which recommends that organizations establish a quantum-readiness roadmap now and prioritize migrating systems that store data requiring long-term protection. For data with a lifespan of 25 to 30 years or more such as loan records, insurance contracts, and customer identification information — the risk from HNDL is clear."

The course applies Mosca's Inequality ($X+Y>Z$), a tool that helps decision-makers determine whether their organization has already entered the window of vulnerability to HNDL. The program comprises six modules: foundations of the quantum threat (including Shor's and Grover's algorithms); risk-timeline analysis using HNDL and Mosca's Inequality; the latest NIST post-quantum cryptography standards (FIPS 203–205: ML-KEM, ML-DSA and SLH-DSA); crypto-agile migration architecture; risk governance and development of a Return on Security Investment (ROSI) business case for Board approval; and a comparison of Quantum Key Distribution (QKD) with PQC.

The course is distinguished by its layered approach: participants develop both technical competence and the strategic perspective needed to present and defend cybersecurity investment decisions to senior leadership. Each lesson includes a knowledge check, and the course concludes with a scenario-based final assessment. Participants must achieve a minimum score of 70/100 to receive a certificate of completion.

"This is not a course focused solely on theory," Peter emphasized. "After completing the program, participants will understand what a Cryptographic Bill of Materials (CBOM) is, identify which data and systems should be prioritized for migration, and estimate the potential losses arising from delayed implementation. According to IBM's 2025 Cost of a Data Breach Report, the average cost of a data breach in the financial sector reached USD 5.56 million. These insights give organizations a solid basis for securing board approval of migration budgets."

The course is designed for Chief Information Security Officers (CISOs), Chief Technology Officers (CTOs), security architects, developers and compliance officers. By establishing a shared language for quantum risk, it helps shorten the approval cycle for cybersecurity investment decisions. The program is delivered online and is self-paced, making it suitable for the demanding schedules of both executives and technical specialists.

SpecterAI recommends that banks, insurers and financial institutions act early rather than waiting until compliance requirements become mandatory. "Quantum computing is not only a scientific breakthrough; it is also a catalyst for a fundamental shift in cybersecurity thinking. Organizations that prepare early will reduce risk, meet compliance expectations and gain a competitive edge in the transition to Post-Quantum Cryptographic infrastructure," Peter said.

About SpecterAI: SpecterAI is a pioneer in Post-Quantum Cryptography (PQC) migration, providing internationally aligned solutions for the finance, banking, insurance and telecommunications sectors. In addition to its proprietary SPECTER platform — backed by five

pending patents — SpecterAI is one of the first organizations to translate complex quantum-security knowledge into concise, practical training programs, helping leaders and cybersecurity professionals accurately understand quantum risk, assess its impact and build an appropriate migration roadmap.

Duc Mai (Mr.)

Specter AI Quantum Security

+84 93 421 14 84

duc.mai@specterai.vn

Visit us on social media:

[LinkedIn](#)

[Facebook](#)

[YouTube](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/925356610>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.