Quantum Encryption and the Limits of Foolproof Security

Carl Lochstampfor Jr

Department of Cybersecurity, Old Dominion University,

CS 462 — Cybersecurity Fundamentals

February 28, 2026

Watch this TED talk

Watch this video titled “Can we make Encryption that’s Unbreakable?”

https://www.youtube.com/watch?v=q7zYnGjvpwc

The speaker shows a diagram at (2:09) of the records stolen since 2013 from the many famous companies around the world. What are your thoughts about it and the general idea of making encryption “Foolproof”? Share some other articles you searched online that gives any detailed information on the many attacks on those companies.

Quantum Encryption and the Limits of Foolproof Security

The graph Prisco shows at 2:09 is striking. Since 2013, hackers have stolen over 10 billion records from major companies, revealing that we are not keeping up with large-scale encryption standards. Yahoo reported 3 billion compromised accounts, and companies like Target, Equifax, and Marriott have also suffered breaches, even though they have highly skilled security teams in place (Swinhoe, 2024).

Prisco's solution, quantum key distribution (QKD), uses light and real physics to encrypt our data. It works by generating encryption keys from single photons. If someone tries to spy on the key and the photon, the quantum state of the photon changes, making the key useless to the eavesdropper and notifying both parties of the interference. QKD operates very differently from RSA encryption, which relies on hard mathematical problems and could be easily broken by quantum computers.

Still, I think it is unrealistic to call any encryption "foolproof." QKD technology can be strong, but most breaches happen because of other problems, not weak encryption algorithms. For example, the 2017 Equifax breach exposed 147 million records because the company failed to patch a known software flaw (Fruhlinger, 2020). The 2013 Target breach occurred through a third-party HVAC company that completely bypassed encryption (Kassner, 2014). These were operational failures, not cryptographic ones. Prisco is correct that we need quantum-resistant encryption to protect our data going forward. However, truly secure systems will need stronger encryption and better organizational practices, such as patch management, access controls, and employee training. Encryption is only as strong as the people and systems that support it.

References

Fruhlinger, J. (2020, February 12). Equifax data breach FAQ: What happened, who was affected, what was the impact? *CSO Online*. https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

Kassner, M. (2014, February 2). Anatomy of the Target data breach: Missed opportunities and lessons learned. *ZDNet*. https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

Leyden, J., Swinhoe, D., & Hill, M. (2025, June 12). The 20 biggest data breaches of the 21st century. *CSO Online*. https://www.csoonline.com/article/534628/the-biggest-data-breaches-of-the-21st-century.html