From: Apon, Daniel C. (Fed)
To: Chen, Lily (Fed)
Subject: Re: Thought I"d point out some recent social media commentary to you
Date: Monday, August 5, 2019 4:56:28 PM

I guess we could always attach an appropriate family-friendly song to our future standard...

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

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Monday, August 5, 2019 4:43:20 PM
To: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Subject: RE: Thought I'd point out some recent social media commentary to you

Hi, Daniel,

Thanks for sharing what you saw. We have a long way to go to earn “trust” especially among the people who are not quite in the crypto inner circle. We might write a book called “Post-Quantum Cryptography for Dummies” or “Post-Quantum Everything”.

Lily

From: Apon, Daniel C. (Fed) <daniel.apon@nist.gov>
Sent: Monday, August 5, 2019 4:14 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Thought I'd point out some recent social media commentary to you

Hi Lily,

This is from reddit.com/r/crypto, from an anonymous user, 4 days ago. The thread was titled "Worried about quantum computers."

"I was recently told at a Unix group about an actual quantum computer that exists and works. As someone who's done light reading on cryptography (I've learned about Shor's algorithm) and personally uses RSA for everything simply because I understand it the best, I can't help but be concerned and worried about the future of cryptography.
I know I'm probably worrying about nothing, I have heard that the guys behind OpenBSD, OpenSSL, OpenSSH etc are working on something about quantum proof ciphers and I read a bit about the Post-Quantum Cryptography Standardization which does give me hope, though I don't trust NIST.
What quantum-proof asymmetric key ciphers exist, if any, that have withstood very rigorous tests? Are there any planned/exist GnuPG? Also, I read in a thread that GnuPG supposedly isn't secure. Does that claim hold any water?"

Thought you would find it interesting.

Comment 1: This is just one guy, and one data point.

Comment 2: This guy likely doesn't understand crypto very well, especially post-quantum crypto. But he's heard, probably, the initially-available, public advertisements of the problem.

Comment 3: He doesn't trust NIST! That's okay. We can convince him with our actions (many of which, recently, he probably hasn't heard of). (Moreover, I suspect there is some subset of the more serious r/crypto community that would correct him, or people like him -- at least partially -- on his view of NIST, especially if the PQC project goes well!) It is also worth pointing out that many of the most-upvoted comments on his thread specifically reference the NIST PQC process as the leading solution to his questions.

Comment 4: If there is an underlying desire of NIST's to be "liked" by the layman community, it never hurts to do a little (more?) outreach in additional public venues.. (Or, of course, it's always possible to just take the strategy of doing good work, letting it speak for itself, and allowing broader opinion to change over time to suit.)

Anyway, thought you would find this one-off observation interesting

--Daniel