## An Open Letter To Bill Gates

Dear Bill:

I saw a year-old news item detailing how Microsoft spends *over $1 Billion a year on cybersecurity*. Since that article published in January 2017, cybercrime has escalated by *$1 Trillion*. You've got a lot of catching up to do. But, by the time you spend another billion, cybercrime will increase by *$2 trillion*.

Cybercrime is escalating at record rates, year after year, and the criminals aren't getting advanced degrees—they're succeeding because it's *easy to do!* **You're buying solutions from the same people who made the problems.**

Here's a scary technical example of cryptography's failure to provide solutions:

1. Out of the currently proposed 5 network security protocols for LPWA (the soon-to-be heart-n-soul of IoT), *not one* can provide end-to-end security
2. The new proposed version of TLS (V1.3) is attempting to speed up by performing authentication *even less often than it is used today*

All cryptography today is exactly like this: it is *not* fundamentally sound and *not* fundamentally secure. It *is* the *fundamental reason why cybercrime is alive and well*. Since it doesn't work from end-to-end, cybercriminals just patiently keep attacking as *you* pay to patch up all the holes in the dam*.*

Unbreakable encryption exists, and it has *zero* attacks. **The method for producing unbreakable encryption is faster, more efficient, smaller and simpler than any other**. Yet it isn't used anywhere, in any current protocol, any authentication mechanism, any security policy, practice, method or system.

Here is Current Crypto: Hard Math Problem basis; such as the 'Factoring Problem'.

$$a * b = 21, \text{ which is the given Public Key}$$

This is trivial to solve, of course, so one must use Large Primes. This is moronic, because it *only works at a scale imperceptible from the current perspective***. Change the perspective, it is <u>always trivial</u>**.

Here is Unbreakable Crypto: An Underdetermined System basis.

$$a + b = 7, \text{ which is the ciphertext}$$

This is impossible to solve, from every perspective, including Quantum Computers. It's perfect, because it *works at any scale, from every perspective—now, tomorrow, and forever.* **It is <u>always unsolvable</u>.**

Cybercrime would have no place to attack and no way to attack, so the great majority of it would stop. Yet this doesn't exist in anyone's tech—and not a single cryptographer alive is looking for ways to implement it, use it, or rely on it. Except me.

I have cryptography that solves these fundamental problems by using a provably unbreakable basis. It's called **Qwyit**. Everything about it is transparent, as shown on our [website](#). It's faster, simpler, more efficient, more flexible—and it uses the 100-year old provably unbreakable One-Time-Pad encryption. End-To-End. I have a complete business plan for QwyitTalk™ (unbreakable network communications), QwyitStore™ (unbreakable data at rest), and QwyitCash™ (unbreakable financial transactions that remove credit cards, and all the readers).

***I'd like to issue a basic challenge***: Have your team perform whatever due diligence they need to answer *your* questions: What's Wrong With Qwyit and Why Shouldn't We Use It? And, when they realize they cannot break it, call me.

If they turn me down, ask them *why* and listen carefully: they won't actually say *anything* about what we do. They'll start with a 'hand-waving dismissal', then move to 'trust model problems', or 'unproven', or 'need more investigation', or any number of things: *NONE* of which have anything to do with the actual methods, results, or possibilities. In 22 years of attempting to get your attention, *several cryptographers have independently acknowledged its capabilities, and not a single cryptographer, engineer, scientist or anyone has ever found our method broken.*

So, put Qwyit to the test: put a couple engineers and coders on it for a month, and *see the future of security*. You have nothing to lose and the whole world to gain.

Sincerely,
Paul McGough, CTO, Qwyit LLC

Ps. I realize you might be busy, like with another guest appearance on *The Big Bang Theory*, but maybe you can show this to Messrs. Cook, Brin, Bezos, Ms. Rometty, or anyone you can think of who needs better security. Thanks! ☺