How To Save $5.4Trillion in Cybercrime - Today

My recent move into a multicultural neighborhood has given me the opportunity to present a great 'teachable moment': How replicating physical world communications in the digital world would reduce cybercrime by 90% and *save $5.4Trillion in cybercrime*.

I arrived at this figure because physical-world over-all crime rates are ~3%, whereas cybercrime rates are 15-25%. If we made the cyber-world as safe as the physical one, we'd reduce the cybercrime rate to that same ~3% (no matter what security is in place, there are just some bad people!); which is a ~90% reduction in cybercrime. This saves *$5.4Trillion*…because there is an estimated *$6Trillion* going to be lost from 2017-2021.

Pretty big teachable moment! And the solution is so starkly simple, it's an absolute shame it hasn't been implemented:

Foreign languages.

Here's what that means: Imagine you can't speak the ancient, indecipherable Mexican language Olmec, and you've been transported into an Olmec town flea market. Now, everyone around you is talking – in Olmec; and while you don't understand a bit of it, you can infer some things – like the people trying food samples are talking about it…those laughing are happy, there's serious stuff going on as well. And there are cashiers taking money – that's a good place to steal value! But...even though you can create a map of activity, you can never be certain: Their entire world is unsolvable to you because *every single bit of communication is end-to-end indecipherable.* And because there is absolutely *no way to ever speak Olmec, you will never understand.*

Next, you notice that before anyone exchanges any money, or begins a conversation, they perform a greeting. And darn it, you can't ever make any sense of that greeting, because *it's different every time!* You've watched it a gazillion times, and it's never the same…yet everyone understands it! It's as if they all share secrets, they won't communicate until a secret is shared, they all understand it, and yet it's *different every time!* And then this too: You see and hear the *exact same exchange between two people, yet the Olmec is different! – as if the greeting is interwoven into the rest of every conversation or exchange!*

So…if you want to perform a crime, like opening the cash registers, or somehow getting into other's conversations, you've got two really big problems: you can't, and won't ever, understand the language; and you don't know the secrets as well as properly presenting them in every conversation – and of course, you're not entirely sure of *where* to commit your crime. So…you've got a really small chance of getting away with it…like, ~3% (heard that number before?!). And you absolutely are never operating *in Olmec* – you're an outsider, even if you got a job guarding the cash!

So why isn't the digital world just like Olmec, or any physical-world, communication system – where everything happens out in public, but you're not privy to it? And if you want to commit a crime, your risk is pretty high, your return is pretty low, and your methods have to be way outside the norm. *Why is there $6Trillion going missing?!*

It's simple: we're not digitally speaking Olmec! It isn't universally used, it isn't used all the time, and it most certainly doesn't have the proper greeting mechanism and inclusion.

If you're following our lesson, you know this is authentication (the greeting – *and* its subsequent use within every transmission), and unbreakable encryption (the never-deciphered ancient Olmec dialect.) Neither of these properties exist in *any cryptosystem in use today.* Again, *neither of these is used in the cryptography presented as secure today.* Which is why you can plainly see that cybercrime keeps increasing even though cybersecurity is being increased too. Before this lesson, you were improperly conditioned to expect this battle to continue – as if the cybercriminals are as smart, or smarter, than the cryptographers. Nothing could be further from the truth: criminals use simple shortcuts to arrive at value without obeying the rules: they are the furthest thing from smart. Which, unfortunately, means the cryptographers aren't very smart either: continuing to use their incompetent solutions that have yet to work, as if they suddenly will.

And yet, it's so simple: Olmec everywhere, all the time, with constant interwoven greetings throughout every conversation. This is using the true, already-proven, unbreakable 100-year-old One Time Pad (OTP) encryption technique for every single bit of digital plaintext (a new key bit for every message bit), with an authentication technique using the same, exact, unbreakable unique version for every use that is 'included' within the formulation of the OTP message keys. This exists, in the QwyitTalk® technology, but isn't used anywhere; and it has all of the required properties to answer the Extra Credit Question:

Why isn't the current cybersecurity the same as Olmec? Because the current 'languages' (cryptographic methods) are too big…too slow…too complicated…so they can't be used like Olmec – everywhere, all the time, under all circumstances. So…they aren't. And the cybercriminals keep attacking where the cybersecurity folks have dropped their guard. Then the cybersecurity folks change the game…and the cybercriminals find the new holes: *The Holes Don't Ever Stop Forming, no matter* ***how*** *the cybersecurity folks configure it – it's a losing game of Whack-A-Mole!* All the 'new stuff', like AI techniques to parse network data usage for 'irregular patterns' are a house-of-cards on top of quicksand: you can't possibly need to parse network data *when the only people on the network are authorized, and only where they are allowed to go!* The next time you hear $*Millions* being invested into 'new techniques' based on – not solving – existing problems, *you'll know right where the next $Billions will be stolen!*

The current crypto error list is limitless – like passwords being used incorrectly: the *entire purpose* of a password is an authentication 'greeting': they should *never be openly communicated, but integrated throughout the session* – exactly like the physical Olmec communication. Blind Olmec folks are still sure they are speaking to the same person throughout their entire conversation, not just at introduction. Current digital password methods aren't integrated into and throughout the conversation – since they are used improperly, they'll continue to be *63% of the cybercrime network intrusion problem*…they're like leaving the front door wide open! And when you hear about 'fixing passwords', you'll hear a bunch of nonsense about removing them, or changing their structure, etc.; you'll never hear about using them properly: integrated into every digital transmission. This is because no one has a technique to do this…except Qwyit®.

Thanks for attending class: There *is* a simple way to save *$5.4Trillion* in today's cybercrime: Olmec. And there is a simple way to implement it: QwyitTalk®.