JOSHUA: Hi, I'm Joshua and have you wondered, can my Facebook password be stolen from Facebook's databases? For example, if a hacker were to come into the Facebook network and get into the administrator's account, would he be able to steal my passwords, your passwords, everyone's passwords? Mua-ha-ha-ha. Would that be the end of the world?

Well, it turns out, no, because companies like Facebook or Google store your passwords not as passwords. In fact, this comes to one of the most important concepts in computer security and that is the concept of hashing. Well, so if companies like Facebook and Google don't store your information like passwords as passwords, what do they store in MS? Well, turns out they store in MS things called "hashers." And hashers are kind of like a little snapshot of the actual password.

So let's say this coffee is the password. So I just take a little snapshot and all I see is a 2D image of the password. So a hash is simply a representation of the password which proves that you know what the password is.

But you'll probably tell me, well, I can understand the idea of a photo but what about it in computer science? What about it in actual programming? How does it actually look? Well, the formal definition of a hash is kind of like what you understand as a one-way mathematical function. This is why we need to understand what a mathematical function is in the first place.

And so a mathematical function is a relationship between the inputs and the outputs. For example, f x equals to 2x and if x is 2, then 2x would be 4. It's just a mathematical relationship from the left side to the right side. But at the same time, you'll probably be wondering, well, that is not one-way.

So what "one-way" means-- well, "one-way" means that the input on the left-hand side cannot well determine what is on the right-hand side. But knowing the results on the right-hand side doesn't mean you know what the actual inputs were. For this case, if you see 2x and you see 4, you know for sure, oh, it's got to be 2 as an input.

So how do computers enable a one-way function? In other words, knowing what the inputs are to determine the outputs but just having the outputs would not be enough to determine the inputs? Well, it comes to the concept of the modulus operator.

So what's a modulus operator? A modulus operator is an operator the returns the remainder of a division. So an operator is just like a plus or a minus. You have, for example, 7 divided by 3. It would give you the answer of 2 with the remainder of 1. And so 7 modulus 3 would just be the answer 1, which happens to be just the remainder of a division operator.

Well, then you might say, how is that useful to become a hash function? Well, notice that 7 is not the only number that you can modulus by 3 to give you 1. You could use 4. You could use 1. In fact, there are many numbers that result in the modulus function returning 1. So just by telling you the answer is 1, you probably don't know what the input is. And hence, you can determine what the outputs are with the input but you cannot determine what the inputs are just with the output.

And so it seems that, is your password safe? Well, it's quite safe because most of your passwords are stored in hashers. And all the company just needs to do is to take your password whenever you log in and convert it into that same snapshot and to compare the snapshots to see whether the snapshots are equivalent. If they are, you logged in. If they're not, too bad for you.

So in that way, you are able to be secure. At the same time, if any hacker steals any of the hashers, they cannot determine what the passwords are in the first place. So in that sense, your passwords are safe. But however, in the same sense, a hacker could still brute force his way through trying any number of passwords and will eventually find your password some day.

So point or story-- is your password safe? Yes and not so because eventually, someday, someone will be able, if they try really hard, to find your password. So stay safe and change your passwords regularly. But other than that, your password is still safe with any company you put it with. Thank you.