JOIN THE #NOPASSWORDS REVOLUTION

MAKE THE INTERNET MORE SECURE. ELIMINATE PASSWORDS.

BY ORI EISEN
FOUNDER & CEO, TRUSONA

Trusona™
WHEN YOU TRULY NEED TO KNOW

> “The only thing necessary for the triumph of evil, is for good men and women to do nothing.”
>
> – Edmund Burke

#NoPasswords Revolution

This article is not simply meant to be read. It is meant to be read and ***acted upon.***

I am here to recruit you.

If you think the Internet is secure and everything is "ok", you can stop reading here.

I, however, think there is a ***major problem*** and doing nothing is simply not an option…not anymore.

I have dedicated my life to fighting online crime. One day, while serving as the Worldwide Director of Fraud at a top bank I asked the question: "Where does the stolen money go? What is it being used for? By whom?"

Unfortunately, I learned the answers. And once you learn it, you cannot sit by and do nothing. You must take action.

Money stolen over the Internet funds the following: narcotics, weapons, terrorism, human trafficking, child exploitation.

We must protect online businesses so these funds are not handed over to the criminals for their nefarious activities.

Current cybersecurity solutions are just not cutting it. Passwords were invented in the early 1960's and have not had one single innovation since.

It is time to move on.

The Problem

During history, weapons were developed to both attack and defend. If you wanted to defend yourself from bows and arrows, you could use a steel shield

But what do you do when the attackers are more powerful than your defenses? Inability to protect yourself will surely lead to your destruction. Weapons are only effective until their rival is created.

The Internet is no different. The Internet was not designed with security in mind. In the early days, username and passwords were very useful. They were used to help grant access to a network for academic research – not to protect multimillion dollar wire transfers.

Just like the padlock on your front door is "good enough" to keep your neighbors from waltzing into your home. Username and passwords just help keep honest people honest.

What if there is a master key available for $1 that can open your front door – would you worry? Would you admit to yourself and others that your security is not "ok"? Most importantly, would you DO something about it?

We now conduct almost every aspect of our lives online. Yet the security measures have not changed. 99% of sites still use username and password as the first line of defense.

According to Privacyrights.org, over 900 million user records have been breached since 2005[1]. There are just over 300 million active Internet users in the US alone[2]. You do the math. Chances are the $1 key to open your online accounts is out there.

What Are the Implications of Using Passwords?

This paper is not intended to alarm you. Just by reading the news, you already have seen the headlines:

8/15/2016	***"Twenty U.S hotels hit by massive data breach"***
8/14/2016	***"Financial malware attacks increase"***
8/13/2016	***"IRS warns citizens of new phishing scheme"***
8/12/2016	***"Russian cyber-attack that targeted Democrats much larger than first reported"***
8/11/2016	***"Researchers expose Iranian cyber-attacks against hundreds of activists"***
8/10/2016	***"Volkswagens Susceptible to Hack"***
8/9/2016	***"National Cybersecurity Commission Seeks Assistance from Public"***
8/8/2016	***"U.S. Cyber Command Could Become Its Own Military Branch"***
8/7/2016	***"Researchers Discover Advanced Malware that Remained Hidden for Five Years"***
8/6/2016	***"Hackers Make the First-Ever Ransomware for Smart Thermostats"***
8/5/2016	***"Russians Hack Oracle's MICROS"***
8/4/2016	***"U.S. gears up for voting cyber-attacks"***
8/3/2016	***"Banner Healthcare breach"***
8/2/2016	***"$72M in Bitcoin stolen in Bitfinex breach"***
8/1/2016	***"Ohio healthcare system attacked"***

This is what I call the Breach of the Day. Each of these is an example of why passwords are no longer effective.

When a company is breached, the soft costs are customer trust, brand reputation and customer loyalty. The obvious, hard costs are breach investigation, credit monitoring, customer attrition, legal fines and fees etc.

[1] http://www.privacyrights.org/data-breach/new

[2] http://www.internetlivestats.com/internet-users-by-country/

But some of the costs of using passwords are a bit more hidden:

1. Call center calls about forgotten passwords
2. Services to reset them (KBA, SMS 2FA, Phone Call 2FA)
3. Losses attributed to weak passwords
4. Losses attributed to fraudulent password resets
5. Losses attributed to malware or breaches stealing passwords

So What Can be Done?

Many companies started using multi-factor authentication solutions only to realize the bitter truth. Using solutions such as SMS one-time passwords to protect data and networks can be completely circumvented. The crooks easily take over your phone line by convincing the telephone company they are you.

Case in point, is the social media account of DeRay Mckesson. On 6/10/2016 the following news broke: "Black Lives Matter activist DeRay Mckesson's Twitter hacked." In the article, Mckesson describes what many of us knew all along...

> *"At 10:31 am, someone called @verizon impersonating me and successfully changed my SIM & unsuccessfully attempted to change my phone number," McKesson tweeted. "By calling @verizon and successfully changing my phone's SIM, the hacker bypassed two-factor verification which I have on all accounts."*

This story epitomizes the point – not all multi-factor authentication solutions are created equal. To the perpetrators of this attack, SMS was nothing more than a turnstile in the middle of the desert...they simply went around it.

"All the forces in the world are not so powerful as an idea whose time has come."

– Victor Hugo

The Solution

What if we were to take static passwords out of the security paradigm altogether?

What if each time your account is used, you need to affirm that it is you on the other end?

What if your affirmation was wrapped in a unique value, so it cannot be used again by any perpetrator?

What if we only have user IDs and never use static passwords again?

This would solve the real problem and kill two birds with one stone.

#1: More security.

By ridding the world of passwords, there will be no incentive for crooks to steal passwords. Malware that steals passwords will lose its power, as passwords will have no value. By affirming it is really them on the other end, users can play a part in their own security. Users will know each time their account is accessed, and affirm or reject the transaction.

#2: More convenience.

By ridding the world of passwords, users no longer need to remember passwords, make them longer and complex, or change them. Password resets will be a thing of the past.

In the US alone, 70% of people have smartphones[3]. So why are we not utilizing these mini-computers in our pockets to improve our security? Users can authenticate themselves via their smartphones. No need to rely on telco providers; no need to worry about malware.

We can fight fire with fire, and use technology to raise the bar on online criminals. We can do this.

Enough is enough. Let's reclaim the Internet. The cost of doing nothing has shown its ugly face.

I am here to recruit you to put a dent in the universe. Heed the call and join the #NoPasswords Revolution.

We at Trusona are passionate about this topic. We will freely provide our app and service to any company and Internet user. We call on the rest of the industry to do the same and offer free methods to rid the internet of passwords. This way we raise the bar together.

[3] http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/

+1 480 454 2380 • info@trusona.com • www.trusona.com

Trusona™
WHEN YOU TRULY NEED TO KNOW