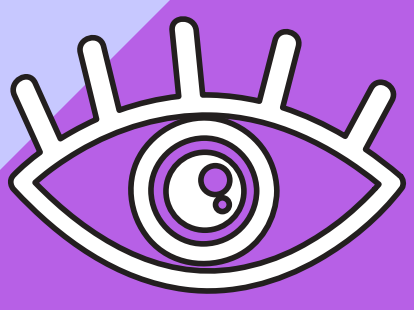
WELCOME TO THE GEMINI IBD INFOGRAPHICS NEWSLETTER

[Volume 2] 07-11-2017



HOW TO REPLACE YOUR PASSWORD WITH YOUR EYE

The Security Threats Posed By Passwords

THE PASSWORD OF TODAY HAS FOR THE LONGEST TIME BEEN THE MOST WIDELY USED LOGIN CREDENTIAL.

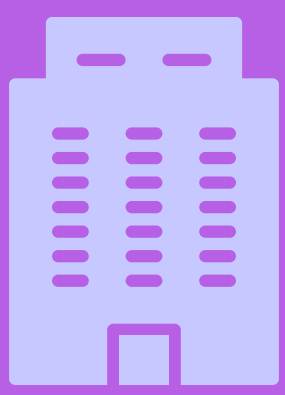
It is easy to use and can be easy to remember. But given the explosion of the Internet and other Web based applications, the individual must now remember hundreds of passwords, which can be very long and complex. Passwords have also become a grave security threat not just for people, but for businesses and corporations alike.

CONSIDER THIS.....

- 95% of all security breaches involve harvesting the password.
- 37% of the people in the United States and 42% of people in the United Kingdom have to change their passwords at least 50 times a year, because they have been a victim of a Cyberattack.
- Passwords are meant to be confidential. But, almost 60% of the employees share their passwords with others, whether they know them or not.
- 21% of US citizens use passwords which are over 10 years old; 47% of them have used the same password!!!
- Overall, 73% of people use the very same password for all of their online applications (such as email, bank accounts, corporate intranet, etc.).
- 65% of people use the same password for all of their applications, both personal and work related.
- 75% of people only change 1 character in their existing password in order to make it unique.
- 90% of all passwords created by employees can be cracked by a Cyber attacker in just under 6 hours.
- 85% of all employees either write their passwords down (such as on a Post It note) or stored electronically somewhere in a cleartext format.
- There are on average 1 Billion passwords that are stolen every year by Cyber attackers in Corporate America.

Does This Describe You?

THE FINANCIAL TOLL ON BUSINESSES AND CORPORATIONS



CONSIDER THIS.....

- It can cost an organization up to $300 per year per employee to reset a password.
- It can cost up to $200,000 for a business to recover from a Cyberattack which involved the hijacking of employee passwords. But the cost for each user rises to over $600 per year (14 tickets per year for fixing a password for one employee X $26 for the cost of each ticket + $300 per employee for a password reset).
- The consequences for not coming into compliance with password security mandated by HIPAA, Sarbanes-Oxley, etc. is a staggering $170 Million.
- 6 out 10 businesses surveyed in America claim that using passwords has a negative effect on productivity by 47%.

THE RESPONSES TO WEAK PASSWORDS

Because the password had become the prime choice of attack for the Cyber attacker, many corporations and businesses are not only hit hard financially after an attack, but they can also be hit financially in term of lawsuits after the fact.
In order to combat this “double whammy”, many organizations around the world are now adopting extremely stringent security policies when creating new passwords.

A NEW SECURITY POLICY EXAMPLE INCLUDES.....

“A strong password must be at least 8 characters long.
It should not contain any of your personal information—specifically your real name, user name, or your company name.
It must be very unique from your previously used passwords.
It should not contain any word spelled completely.
It should contain characters from the four primary categories, including: uppercase letters, lowercase letters, numbers, and characters.” (SOURCE: 5)

In the end, the password can come out looking something crazy like this:

eC<My!chO,quajôf)naD}uM}rIew>Ap[Ek}E*quaC.eib(Tyb

WHO IS GOING TO REMEMBER A CRAZY PASSWORD LIKE THAT?!?

As a result of these arduously long and complex passwords, employees often write them down on Post-It Notes, and attach to their workstation monitor, thus totally defeating the very entire purpose of a long and complex password. This phenomenon has become known as the “Post-It Syndrome” in Corporate America today. So what is Corporate America to do to protect itself???

CUE THE RISE OF BIOMETRIC TECHNOLOGY

Biometrics are fast becoming the norm now to replace the password in its entirety.

Why is this so?

- With a simple scan of your fingerprint, or even your iris, your unique physiological trait can become your password.
- Either with a sensor embedded into your computer or wireless device, or even a via a simple USB connection, your fingerprint or iris can login you in just a matter of seconds versus the minutes it could take to enter and re-enter your password.
- The use of Biometrics is also known as “Single Sign On Solutions”. With one scan, you are logged in.
- There is no sharing of your fingerprint or iris, unlike a password. So, this alleviates the “Post It Syndrome”.
- Because of the sheer uniqueness of your fingerprint and/or iris, they cannot be used in a Cyber based attack. After all, what can a hacker do with your Biometric Template? NOTHING!!!
- By using your iris or your fingerprint, this totally eliminates any subsequent Identity Theft attacks. After all, these are just mathematical files, and a hacker has ABSOLUTELY NO WAY to rebuild your identity or claim your identity just by this, unlike using a credit card number.
- In the off chance that your fingerprint or iris scan has been compromised, it can just be quickly deleted and replaced again in just a matter of seconds. There are no resets involved unlike the password, thus 100% eradicating the $300 reset costs associated with passwords.
- Your iris or finger cannot be forgotten, stolen, or hijacked unlike your password- after all, they are a permanent of you!!!
- It has been scientifically proven that the fingerprint and iris are very rich in terms of uniqueness amongst individuals-thus making them much more robust than a password.
- Also, using your fingerprint or iris to initiate the login process is much easier to do rather than having to enter a long and complex password!

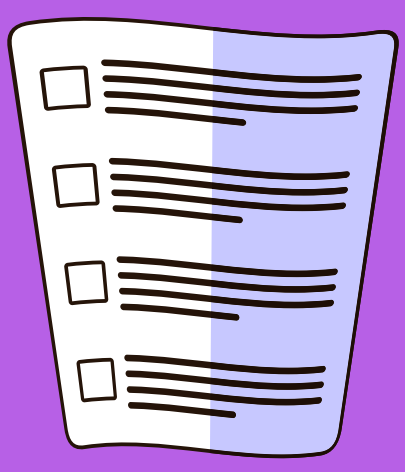
VOILA!!

MasterCard is one of the first major financial companies to implement the use of Biometrics on a large scale.

CONSIDER THIS.....

- 93% of customers favor using their fingerprint to login rather than having to use a password.
- 71% of customers would rather use their face as a means to login rather than using their own password.
- 72% of customers believe that using Biometrics as means to login is much more secure than whatever login tool that they are currently using.
- 73% of customers believe that using either their fingerprint or iris will actually reduce fraud, unlike passwords.
- 92% of customers want to use Biometrics overall in their login process than their password.
- 83% of customers feel that using Biometrics overall in the login process is much more secure than using a password.
- 93% of customers want to use either their fingerprint or iris to make a payment online.
- 67% of UK citizens would like to use some sort of Biometrics on their own Credit Card.
- 92% of customers want to use Biometrics to replace their own passwords for mobile app based banking.
- 60% of customers would suggest to their families or friends to use either their iris or fingerprint to replace their password.

In a recent survey of UK citizens.....



- **80% feel that Biometrics are much more secure than traditional password.**
- **52% want to use some sort of Biometrics on their Smartphone to avoid having to enter in a password.**
- **38% of UK citizens are currently using Fingerprint Recognition on their Smartphone.**
- **15% are using Voice Recognition on their Smartphone.**
- **11% are using Facial Recognition on their Smartphone.**

Apple is the pioneer for using Fingerprint Recognition for the iPhone as a replacement to the password. This particular system is called the "Touch ID", and it has demonstrated that there it is at least 5X more secure than using a password

Examples of Single Sign-On Solutions include the "Hamster Plus" from Secugen and the "IriShield" from IriTech, Inc.

Hamster Plus

IriShield

Sources

1) https://www.centrify.com/lp/are-you-protected-infographic/

2) https://www.entrepreneur.com/article/246902

3) https://www.digitalpulse.pwc.com.au/infographic-password-security/

4) https://www.heroictec.com/blog/passwords-hidden-costs-big-risks-infographic

5) https://www.digicert.com/blog/creating-password-policy-best-practices/

6) https://www.flickr.com/photos/mastercardnews/25043011184/sizes/l

7) https://betanews.com/2016/05/25/safer-password-alternatives/

8) https://www.veridiumid.com/blog/consumer-acceptance-biometrics-growing/

9) https://security.stackexchange.com/questions/144428/how-secure-is-a-fingerprint-sensor-versus-a-standard-password