Big Tech Approaches To Streamline & Secure Passwords

cyber security

Summary: In Verizon's 2020 Data Breach Investigations Report, it was found that 81% of all breaches involved stolen or weak passwords. The human element in passwords is the main reason for the continuing frailty of passwords. Now, Apple and Google have new approaches to passwords. We guide you through them along with password managers and MFA to help keep your staff and customers safe.

The 1993 introduction of the E-ZPass electronic toll collection system changed the way people travel on major highways in the Northeast overnight, ending the practice of digging for coins or stopping to pay and get change. Today, the E-ZPass system, one of several electronic toll collection systems in the US, enables travelers to instantly pay tolls using a payment card without having to come to a stop. Much in the way that E-ZPass streamlined access through tolls, Apple and Google are working to streamline secure access to online accounts.

Passwords remain the main way that accounts are protected, yet they are often targeted by cyberthieves. So, these technology behemoths —Apple and Google— are honing the ways that their organizations secure passwords to make them both easier to use and more effective. Together, they power the majority of the world's smartphones and browsers, so if anyone can solve the password problem, they likely can.

Since community financial institutions help to keep their employees and customers' passwords safe every day, here are the latest password initiatives to protect against cybercriminals.

Continuing frailty of passwords

Though passwords remain the main way of securing information and accounts, they are still the easiest way for cyberthieves to gain access. As we have noted previously, the main reason passwords are so susceptible is the human factor. People have too many to remember, so they take shortcuts and use the same ones over and over. Or they use obvious combinations, including those incorporating sensitive information, such as their birth date.

Unfortunately, this has been going on for years. Aware of the fact that people aren't changing their behavior, cyberthieves don't need to change either. They use a variety of the same tactics that still work — from phishing emails to social media quizzes — for people to unknowingly reveal key details about themselves that can be used for password retrievals through security questions. Not surprising then that 81% of all breaches involved stolen or weak passwords, according to the 2020 Verizon Data Breach Investigations Report.

Apple & Google's approaches

Aware of the weakness of traditional passwords, Google is hoping to address the issue through its Chrome browser by bolstering it with Google's own password manager for users. Whenever a user logs onto a site or account with a password, not only will Chrome notify the individual if it has detected a breach where its password could be compromised, it will also provide a one-click option for changing that password to a more secure, randomly generated alternative. If someone chooses this "change password" option when the button

pops up, Chrome will locate the portion of that site where a password must be changed and automate the process for the user.

For its part, Apple is hoping to decrease cyberthieves' success rates by replacing traditional passwords with passkeys. These will be produced and stored in an iCloud Keychain, that will instantly synchronize on all of an individual's devices. Instead of relying on combinations of letters and numbers, Apple's passkeys will use biometric face scans to authenticate account owners for account or website access.

Unlike Google's approach which works for all websites and apps automatically, Apple's efforts will need the support of each organization to help integrate Apple's passkeys with the organization's apps and websites.

Password managers still help too

Besides the options from Google and Apple, password managers continue to help too. There are a wide variety of password managers in existence. These simplify the memorization of passwords by securing passwords in a virtual, secured vault that can be accessed using a single master password. While the features of password managers vary, the one thing that they all have in common is that they will automatically generate random, complex individual passwords for each and every account. Having passwords in this vault has significantly decreased the odds of cyberthieves making a blanket attack, known as "credential stuffing", on someone's accounts. Many password manager apps also offer the ability for people to auto-populate their passwords without ever having to type anything into their device.

Multifactor authentication secures passwords the best

Many financial institutions worry that passwords alone aren't enough. In fact, passwords coupled with multifactor authentication (MFA) are more secure than passwords alone and are highly recommended. Ways to authenticate along with a password include fingerprints, PIN codes, and security tokens.

Staying current on the new ways to safeguard passwords is an important part of cybersecurity. Discuss these new approaches with your IT team to see if anything needs to change with your institution's password policies and procedures. Your staff and customers count on you to keep them safe.

INTERNATIONAL SERVICES TO GROW WITH YOUR CUSTOMERS

Capture more customers and increase fee income with our international services. Contact us today to learn more.

ECONOMY & RATES

Rates As Of: 07/30/2021 04:40AM (GMT-0800)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.06	0.01	-0.03
6M	0.05	-0.01	-0.04
1Y	0.07	-0.01	-0.04
2Y	0.20	-0.05	0.07
5Y	0.70	-0.18	0.34
10Y	1.25	-0.22	0.33

30Y	1.89	-0.19	0.25
FF Market		**FF Disc**	**IORB**
0.10		0.25	0.15
SOFR		**Prime**	**OBFR**
0.05		3.25	0.08