Passwords Are Scarily Insecure. Here Are a Few Safer Alternatives.

Here’s what comes next to authenticate users and protect networks.

March 7, 2018 8 min read

Opinions expressed by *Entrepreneur* contributors are their own.

The password, the most common way to authenticate users around the globe, has been in slow decline for over a decade. Bill Gates famously asserted at an RSA conference in 2004, “There is no doubt that over time, people are going to rely less and less on passwords … they just don’t meet the challenge for anything you really want to secure.”

To maintain acceptable security standards that protect company assets and employees, businesses need to start seriously considering how to implement alternatives to their password-based systems.

The main problem with passwords is twofold: For starters, passwords just aren’t that secure. Every company in the world uses them to authenticate users to confirm they are who they say they are, but a recent Verizon study showed that a majority of hacks leverage weak or guessable passwords. Additionally, passwords are susceptible to being stolen or extracted by hackers using various methods, like impersonating someone you know or trust to gain login information or personal details.

Careless practices such as exposing hard or digital copies of

passwords are also a major contributor to their becoming compromised. Think about that the next time you write down your work account password on a piece of paper and stick it in a desk drawer at the office.

There are numerous examples that demonstrate the vulnerabilities of passwords to theft. In 2017, online image sharing community Imgur made headlines when it had troves of user passwords stolen from the company database because of weak security protocols. The hack left 1.7 million accounts compromised.

In 2018, flaws were exposed that had been embedded on Intel processors for years, allowing hackers to gain device memory access and authentication credentials. Even more recently, US researchers identified the re-circulating of the Zyklon virus, a malware program that exploits vulnerabilities in Microsoft applications to steal passwords and other personal details. The list goes on.

A second aspect to the problem is that passwords require users to remember numerous letter/number/character combinations for most accounts, which if we're honest, is totally unrealistic. Limiting the variety of passwords by, say, simply repeating the same password for multiple accounts only increases security risk.

While passwords are still used across almost all industries and companies, a slew of alternative tools have begun to make their way into our daily routine and will, one day in the not so distant future, replace passwords altogether.

Here are some of the pros and cons of the most popular password alternatives that may be right for your company, since all passwords are going the way of the dodo.

Security tokens

Tokens, both soft and hard, provide a reasonable level of security in that they require any user to possess a specific item at the time of login. Tokens are not connected to a network, but rather generate one-time passwords based on a ‘seed record’ synchronized with a central server. Many current token technologies don’t even require a user to manually type a password but rather transmit them to a PC or laptop via a device’s near field communications.

Related: The Dos and Don’ts of Cyber Security Measures to Help You Protect Your Business and Assets

One company making headway in this industry is the New York-based Tokenize. The product allows a full range of operations and devices to be synced to a small wearable ring-token, from credit card purchases to unlocking computers.

However, tokens present a serious logistical challenge to businesses for a number of reasons. First off, a token-based system is expensive to deploy, since every user is required to have their own device. Additionally, the method requires users to have their tokens with them any time they want to log on while also needing to safeguard them from loss and theft.

Biometrics

Biometrics are identifiers like fingerprint and facial scans. This method has become increasingly popular among users, with applications like Apple’s Touch ID and Face ID now extremely common. What gives biometrics a leg up from a security perspective is that the technology is based on something that the user “is.” A fingerprint, for instance, can’t be lost or hacked the same way that other authenticators can be. Biometrics also tend to offer a better user experience as well, since many metrics are quick and easy to authenticate.

Many tech leaders have begun to offer scalable biometric solutions to authentication. Microsoft Hello for PCs now features fingerprint and face recognition options, and increasingly, more devices compatible with the application will be made available by the company in the future.

Biometrics has its drawbacks, though. Many common biometric systems still suffer from accuracy issues and may be prohibitively expensive. Biometrics are also vulnerable to hackers. Findings by Japanese researchers last year showed that biometric markers can be forged by simply using high resolution photographs.

More important, the infrastructure supporting biometrics has been decentralized in recent years to avoid a central database of biometric information that may be stolen by attackers. As a result, the authentication actually boils down to a private/public key-based exchange – which means that merely stealing a key allows stealing a user's identity, even without forging or possessing any biometric data at all.

With all of these risk factors in mind, it's no surprise that the National Institute for Standards and Technology has recommended against the use of biometrics as a lone method of authentication.

Phone-based authenticators

Phone authenticators are quickly becoming the leading solutions within the tech world. There are currently three methods that utilize mobile phones for authentication.

Related: How Digital Wallets and Mobile Payments Are Evolving and What It Means for You

Push notification apps work by a user sending an access request to a server, which responds immediately with either a security challenge or a message that authentication has taken

place. One of the big advantages of this approach is that it offers a smooth user experience, since there's no need to look up one-time passwords or carry an otherwise redundant device.

Additionally, user experience is good since there's no need to remember passwords or carry an additional device. Push only requires the response to an app's notifications, which are sent straight to the user's mobile device.

Secret Double Octopus leverages secret sharing encryption to provide password-free, high-assurance access to a user's online platforms, internet applications and networks such as Active Directory.

Software tokens, or soft tokens for short, are similar in concept to hard tokens. However, instead of carrying around an extra piece of hardware, it uses a smartphone to calculate the one-time code using the smartphone's clock and the algorithm contained in an app's software installed on the device.

Among the leaders in authentication software is the Dutch company CM.com. CM offers a range of one-time-password generating apps specifically designed to be applied at the enterprise level.

Soft tokens have a downside, though. Because soft token one-time passwords are located on a network-connected device, they become inherently more vulnerable because they are left open to the threat of hackers remotely intercepting and copying the app's passwords.

Related: Here Are the 25 Worst Passwords of 2017

Text messaging a one-time password is known as SMS authentication. Initially, SMS was used in addition to passwords. However, since the password itself can be reset with the acceptance of an SMS, the value of the password diminished, and more applications began using SMS as a password alternative. The biggest advantage of SMS one-time

passwords is that they do not require the installation of any app on the user’s mobile device.

Gemalto, a digital security company operating out of Belcamp, Maryland, offers a user-friendly, business-compatible solution for SMS password delivery. The company’s one-time-password application allows users to configure settings that optimize security based on the business environment and can be synced with a PC or laptop.

The downside is that SMS messages are weak on security. Passwords delivered via SMS can be compromised in any one of three ways: impersonating a phone’s owner, hacking a cellular network and secreting malware onto a mobile device itself.

A coming paradigm shift

All the signs are pointing to a shift away from password authentication. Big tech firms have been busy producing innovative alternatives, and users are also beginning to demand replacements. Armed with the knowledge of the pros and cons of different methods, companies and individual users can find the authentication solution that best fits their needs.

https://www.entrepreneur.com/article/309054