RESULTS Multi-Factor Authentication

Keep your business safe.

Has your Cybersecurity Insurance Provider told you to get MFA yet? Has your regulator? If not, it's only a matter of time. Cyber attacks have been at an all-time high since early 2020 and the problem is only getting worse. All it takes is one compromised credential or legacy application to cause a data breach. Now is the time to step up your security.

Multi-Factor Authentication (MFA) is a security system that verifies a user's identity by requiring multiple credentials. Typically, this means providing an additional way for a user to verify who they are beyond the usual username and password. This additional factor should be one that is not easily captured or hacked by a bad actor.

Most of today's applications support some level of MFA. It is important to investigate what options are available for your applications.

RESULTS successfully completes the AICPA's SSAE 18 SOC 2, Type 1 compliance audit annually. This is the gold standard for the validation of a service organization's operations and procedures. RESULTS is audited in nine specific areas including all aspects of data and physical security, data backup, network monitoring, change management and systems maintenance.

What is Multi-Factor Authentication?

Something you know.
a unique username or password

Something you have.
A smartphone with an app to approve the authentication request

Something you are.
Biometrics, like your fingerprint or a retina scan.

According to a joint study conducted by Google, New York University, and University of California San Diego, the use of MFA "blocked 100% of automated bots, 99% of bulk phishing attacks and 66% of targeted attacks.

RESULTS Multi-Factor Authentication

Keep your business safe.

1. Email Code. The application sends a code to your pre-registered email address. The code must be entered within a limited window of time.

- **Costs:** No costs, but the end user must have access to the designated email account at login time.
- **Why is this secure?** This adds an additional factor for authentication with a limited time code. This method doesn't require any special device or application.
- **What are the potential problems?**
  - ◊ Email accounts are vulnerable to hacking so the code could be captured as well.
  - ◊ If the email account is compromised, the hacker doesn't need any special device or application either.
  - ◊ Email should be protected by MFA as well, so you need another way to add multi-factor authentication to the email account.

2. Text Code. The code is texted to your registered mobile phone number

- **Costs:** This is a cheap and easy option because almost everyone has a text-capable phone.
- **Why is this more secure?** The application sends a limited time code to a specific mobile phone device held only by the user via text message. A lost phone is easier to identify and report than a hacked email account.
- **What are the potential problems?** SIMM swapping is a known way for hackers to capture texts from mobile phones, but is still much less common than email hacking.

3. Mobile App. The code is accessed from a dedicated mobile app.

- **Costs:** There may be a monthly cost for the app. Some apps (like Google Authenticator) are available at no cost, but may have limited scope.
- **Why is this more secure?** With the addition of a mobile app, the SIMM swapping problem is eliminated. A hacker would have to have physical access to both your phone and credentials for the app to access the code.
- **What are the potential problems?** The end user must have a smart phone capable of running the app.

4. Hardware Token. The code comes from a hardware token that displays a time sensitive code or can be plugged into a USB port.

- **Costs:** There is an upfront cost to purchase the tokens and management software.
- **Why is it more secure?** Tokens are owned and managed by your company and don't rely on end-user phones. Hackers would need physical access to the token to make use of them.
- **What are potential problems?** No token, no login without IT support.

Biometrics (finger print or facial recognition) can be added to any of the methods above to enhance security, but is not strongly secure as implemented on phones and laptops It can be a convenience and often better than remembering and entering a complex password, but typically does not count toward MFA by itself.

RESULTS can help you to determine the most effective strategy for your business. Contact us today. 913.928.8300 or info@resultstechnology.com

RESULTS TECHNOLOGY

www.resultstechnology.com | 913.928.8300 | info@resultstechnology.com
12022 Blue Valley Parkway, #524, Overland Park, KS 66213

V03292022