GUARDSIGHT

https://www.guardsight.com

Selecting a Multi Factor Authentication Solution

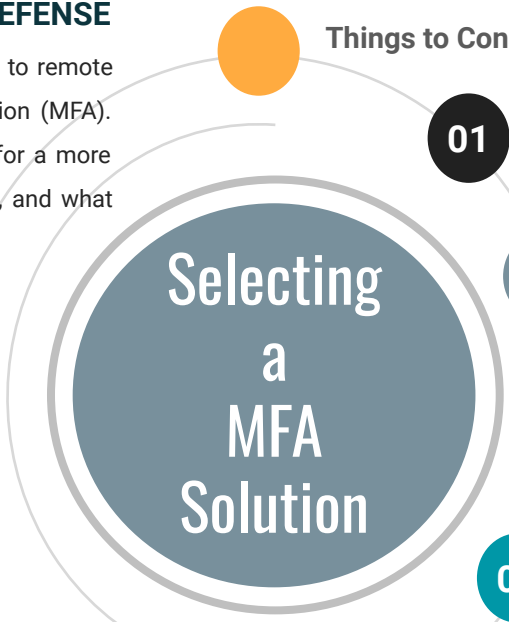
YOUR AWARENESS IS THE BEST DEFENSE

With the rise in remote work, companies are turning to remote security solutions such as Multi Factor Authentication (MFA). MFA allows you to present two pieces of evidence for a more secure verification: what you know (your password), and what you have (the app on your cell phone).

Examples of MFA Apps

Integration is as simple as scanning a QR code with the app. The following MFA apps are freely available for Android and iOS:

- Google Authenticator
- Okta Verify
- Duo Verify
- Microsoft Authenticator



Things to Consider When Selecting a MFA Solution

01 How It Works

Sites such as Gmail, Facebook, your bank's site, or your remote work environment will have a setting where you can toggle MFA if offered. This is where you would find step-by-step instructions on MFA setup.

02 What To Look For in a MFA Solution

Choose a MFA solution that is easy to integrate and provides different methods for verification. Security solutions should be versatile and as little as an inconvenience as possible.

03 What To Avoid

Avoid text based or voice based MFA solutions, if possible, as these are more easily spoofable than MFA apps. However, any MFA solution is better than none.

04 Why Use MFA

MFA protects by adding an additional layer of security, making it harder for bad guys to login as if they were you. Your information is safer because thieves would need to steal both your password and your phone.

05 The Login Process With MFA

- Log in to your email, bank, social media, work environment, etc. as normal.
- Depending on the MFA solution of your choice, you will be prompted by your MFA app to either authorize the login attempt or enter a verification code.
- If you enter the code correctly, or answer "yes" to the push notification, you will be allowed to log in.

For additional advice or to learn more contact us: info@guardsight.com