Which Form of **MFA Is the Most Secure?** Which Is the Most Convenient?

MULTI-FACTOR AUTHENTICATION METHODS

By Rob Landis, Binary IT Solutions

With data and business processes now largely cloud-based, a user's password is the quickest and easiest way to conduct many different types of dangerous activities. How do you protect your online accounts, data, and business operations? One of the best ways is with multi-factor authentication (MFA). MFA provides a significant barrier to cybercriminals, even if they have a legitimate user credential to log in. This is because they most likely will not have access to the device that receives the MFA code required to complete the authentication process.

Let's take a look at three MFA methods:

SMS-BASED: The form of MFA that people are most familiar with is SMS-based. This method uses text messaging to authenticate the user.

ON-DEVICE PROMPT IN AN APP: Another type of multi-factor authentication will use a special app to push through the code. The user still generates the MFA code at login, but rather than receiving the code via SMS, it's received through the app.

SECURITY KEY: The MFA security key is typically smaller than a traditional thumb drive and must be carried by the user to authenticate when they log into a system.

A Google study looked at the effectiveness of these three methods of MFA at blocking three different types of attacks. The security key was the most secure overall.

Percentage of attacks blocked:

- SMS-based: between 76 – 100 percent.
- On-device app prompt: between 90 – 100 percent.
- Security key: 100 percent for all three attack types.

Looking for Help Setting Up MFA at Your Company? Let's come up with a solution together. Call 610.320.2628 or visit www.binaryitsolutiosn.tech.