www.prismrisk.gov

RISK SIMPLIFIED

RESOURCES

[Cybersecurity & Infrastructure Security Agency]

[Synoptek – Managed IT Services]

QUESTIONS

Email PRISM Risk Control
or call 916.850.7300

Cyber Smart : Multifactor Authentication (MFA)

by Scarlett Sadler

Most agencies conduct some, if not all, of their daily business in a digital environment, which can increase vulnerability to cyber threat actors. Since cyber breaches are an ongoing risk in a digital environment and public agencies are increasingly digitized, they need to take more steps to implement safeguards to protect their information systems. There are many things an agency can do to decrease its cyber risk; however, one critical solution is the implementation of multifactor authentication (MFA).

MFA, sometimes referred to as access management, two-factor authentication, two-step authentication, or 2F, is a layered approach to securing online access. MFA is a security control that combines two or more authenticators to verify a user's identity before granting access to a network or information system.

When MFA is enabled, it is more difficult for unauthorized threat actors to gain access to networks, information systems such as remote access technology, billing systems, and email. In addition, when MFA is enabled, and a password is compromised, an unauthorized user will have a harder time accessing the network or information systems without the second-factor authentication.

Most MFA logins require a user to present a combination of the following:

- something you know; a password or a personal identification number (PIN)
- something you are; a biometric factor such as a fingerprint, palm print, or voice recognition
- something you have; an authentication application, a confirmation text on your phone, a smart card, or a mobile token

Many people have experience with MFA and may not even realize it, for example, when using a bank card at an automated teller machine. In order to access an account, the person has to insert a bank card into the card reader, the first factor (something you have), and then enter a PIN, the second factor (something you know). An unauthorized user in possession of the physical card but not the PIN would likely be unable to access the account associated with the bank card. Likewise, without the physical bank card, a user with the PIN cannot access the associated account.

There are multiple options for authentication factors, and an agency can customize the authentication factors that work best for their employee population. For example, some departments might have access to an authentication factor on their smartphone application and a password; others may utilize a fingerprint scanner and a PIN. Two factors may be sufficient for some use cases, while others may require all three types of authentication factors. MFA authentication factors do not have to be a one size fits all use.

Since many agencies do not have the time or resources to manually manage usernames and passwords, tools, such as MFA, are necessary to verify a user's identity. MFA is not unhackable; however, some solutions are more resilient to hacking. MFA can protect against phishing, social engineering, and password brute-force attacks where cyber threat actors use trial-and-error to gain system access. Using MFA can prevent cyber related incidents, and agencies are encouraged to review their authentication factors and determine if MFA can increase cybersecurity. For questions regarding MFA or cyber security, please contact Risk Control.