May 2019
Volume 14, Issue 5

Securing Online Accounts with Multi-factor Authentication

MS-ISAC
Multi-State Information Sharing & Analysis Center

Enterprise Information Security Program

Tacoma

From the Desk of Ron Jimerson, Chief Information Security Officer

Have you noticed how often security breaches, stolen data, and identity theft are consistently front-page news these days? Perhaps you, or someone you know, are victims of cyber criminals who stole personal information, banking credentials, or more. As these incidents become more prevalent, you should consider using multi-factor authentication, which is often also called strong authentication, or two-factor authentication. This technology may already be familiar to you, as many banking and financial institutions require both a password and one of the following to log in: a call, email, or text containing a code. By applying these principles of verification to more of your personal accounts, such as email, social media, and more, you can better secure your information and identity online!

What it is

Multifactor authentication (MFA) is defined as a security process that requires more than one method of authentication from independent sources to verify the user's identity. In other words, a person wishing to use the system is given access only after providing two or more pieces of information which uniquely identifies them.

How it works

There are three categories of credentials: something you either know, have, or are. Here are some examples in each category.

Something you know	Something you have	Something you are
Password/Passphrase	*Security Token or App*	*Fingerprint*
PIN Number	*Verification Text, Call, Email*	*Facial Recognition*
	Smart Card	*Voice Recognition*

In order to gain access, your credentials must come from at least two different categories. One of the most common methods is to login using your user name and password. Then a unique one-time code will be generated and sent to your phone or email, which you would subsequently enter within the allotted amount of time. This unique code is the second factor.

When should it be used?

MFA should be used to add an additional layer of security around sites containing sensitive information, or whenever enhanced security is desirable. MFA makes it more difficult for unauthorized people to log in as the account holder. According to the National Institute of Standards and Technology (NIST) MFA should be used whenever possible, especially when it comes to your most sensitive data – like your primary email, financial accounts, and health records. Some organizations will require you to use MFA; with others it is optional. If you have the option to enable it you should take the initiative to do so to protect your data and your identity.

Activate MFA on your accounts right away!

To learn how to activate MFA on your accounts, head to the Lock Down Your Login site, which provides instructions on how to apply this fantastic form of security to many common websites and software products you may use. Lock Down Your Login is a resource created by the National Cyber Security Alliance and the U.S. Department of Homeland Security through their Stop Think Connect campaign to empower citizens with cybersecurity knowledge and practices.

If any of your accounts are not listed on that resource site, look at your account settings or user profile and check whether MFA is an available option. If you see it there, consider implementing it right away!

Conclusion

User name and password are no longer sufficient to protect accounts with sensitive information. By using multifactor authentication you can protect these accounts and reduce the risk of online fraud and identify theft. Consider also activating this feature on your social media accounts!

Resources:

https://www.lockdownyourlogin.org/

https://www.us-cert.gov/ncas/tips/ST05-012