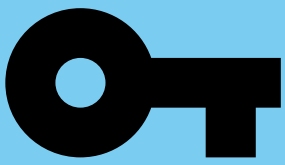
MULTI-FACTOR AUTHENTICATION

Getting Started

WHAT IS IT?

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 that person.



HOW IT WORKS

There are three categories of credentials: something you either know, have, or are. 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 then enter within the allotted amount of time. This unique code is the second factor.

1) SOMETHING YOU KNOW

- Password/Passphrase
- PIN Number

2) SOMETHING YOU HAVE

- Security Token or App
- Verification Text, Call, Email
- Smart Card

3) SOMETHING YOU ARE

- Fingerprint
- Facial Recognition
- Voice Recognition

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.

The Southwest Kansas Library System