Using Strong Authentication

About Authentication

Authentication is the process of verifying a user is who they say they are before granting the user access to requested resources.

There are multiple ways to verify someone is who they claim to be. These are most often split into three categories.

SOMETHING YOU KNOW
This could be a password, pin, social security number, etc.

SOMETHING YOU HAVE
This could be a code generated by a token, an authenticator mobile app, a text message or phone call sent to your mobile device, etc.

SOMETHING YOU ARE
This is commonly referred to as “biometrics” and could be achieved through a fingerprint reader, facial recognition, iris scanner, etc.

Single-Factor

Single-factor authentication occurs when you would only need to provide one method of verification.

The most common form of single-factor authentication happens when someone would provide only a username and password to sign into an account.

In this scenario, the user would only need to know the password to gain access. This is inherently insecure because if the password gets compromised, the whole account can get compromised.

If single-factor authentication is used, a compromised password can lead to issues such as a loss of money, installation of malware, data theft or destruction, or loss of reputation.

Multi-Factor

Multi-factor authentication (MFA) is considered a much stronger and more secure authentication option.

MFA occurs when you require more than one form of authentication to access a system.

For example, instead of just providing a username and password, you would also need to enter a code you received on your phone.

This is helpful because it means that even if your password gets compromised, an attacker would still need to have physical access to your mobile device to get into your account.

BOTTOM LINE
Single-factor authentication is not considered secure enough to protect your most valuable assets. Enable MFA wherever you can, but especially on your high-risk accounts like internet banking, payments apps, email, online shopping, and social media.

Contact Us

We encourage you to use strong authentication, like multi-factor authentication (MFA), to secure all your accounts.

To learn more about how you can enable MFA on your internet banking accounts, contact your financial institution.

CENTERA BANK
ORGANIZATION NAME

620-675-8611
PHONE NUMBER

WEBADMIN@CENTERABANK.COM
EMAIL ADDRESS

CENTERABANK.COM
WEB ADDRESS

Learn More

To learn more about about cybersecurity awareness and using strong authentication, visit any of the following websites:

- OnGuardOnline.gov
- StaySafeOnline.org
- BBB.org/Data-Security
- CISA.gov