Microsoft Multi-Factor Authentication

Version 28

Published 12/17/2021 by Nadine Chautilal   Last updated 7/29/2024 1:10 PM by Tyler Stevens

About

- All students are required to set up Multi-Factor Authentication (MFA), also known as two-step verification.

- This is an extra step of verification when using your Seneca username and password to log into Seneca systems.

- For example, to access Microsoft Office 365 (such as Outlook, your Seneca student email), Learn@Seneca (Blackboard courses), Student VPN, and several academic services.

How it works

- MFA works by requiring something else, beyond just a password, to prove that you are who you say you are. This helps to prevent hackers from gaining access to your account.

- In addition to your password, your account will be protected by "something else you have," such as verification from another device (mobile phone or tablet).

- Please follow instructions below for setting up your Microsoft MFA.

Step 1 – Download Microsoft Authenticator mobile app

- The app can be used on mobile devices such as a smartphone and tablet.

- Download and install "Microsoft Authenticator" app from the Apple Store or Google Play Store.

Step 2 – Set up Microsoft Authenticator

- To set up, please have your computer and secondary device ready (such as mobile phone or tablet).

- [Follow written instructions](#) or watch video below:
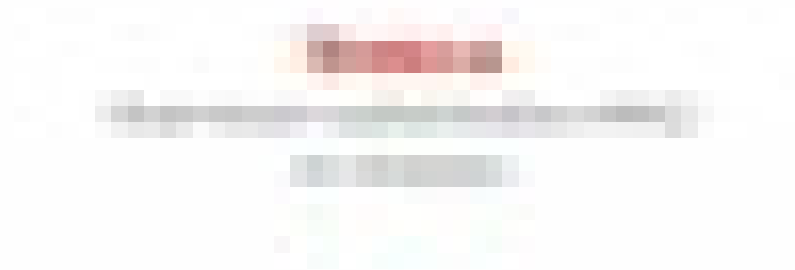
Frequently Asked Questions

For a complete list, please visit [MFA FAQs](#).

General

- [I don't always have internet access, can I still use the Microsoft Authenticator app?](#)

- [I don't have a smartphone, how can I verify?](#)

- [I don't have other devices, can I verify with my home phone?](#)

Troubleshooting

- [I am locked out](#)

- [I lost or broke my phone](#)

- [My phone number changed](#)

- [Verification codes are not being sent to my device](#)

For technical support, contact ITS

tags : mfa, multi-factor