

# Multi-Factor Authentication – Frequently Asked Questions (FAQ)

## What is Multi-Factor Authentication (MFA)?

Multi-Factor Authentication (MFA) refers to an additional layer of security that is added to the login process.

MFA relies on two forms of authentication: something you know, and something you have with you. The something you know is your password. The something you have with you can be a mobile device or USB Token. This means that even if your password is hacked, your account will remain secure.

## Who is currently impacted by MFA?

MFA is required for all faculty and staff. Students are not required to use MFA, as they do not have access to the school's information systems.

## What applications/systems are currently protected with MFA?

Microsoft email and SMUS network when accessed remotely.

## How often do I have to re-authenticate?

The current settings require reauthentication when you change your password – usually every 90 days.

You will need to re-authenticate on each device and each browser you use.

## What are my authentication options?

You will be able to choose a primary authentication method when you register, which you can change or update at any time. IT Department recommends using a smartphone to receive notifications and MFA codes – this is the most convenient way. There are other alternatives authentication options – Microsoft authenticator app, email, and security key. For further information on a USB Token refer to MFA Instructions on the Tech page on the Intranet.

Verification Method	Description
Text Messages	A text message with a 6-digit code is sent to your mobile device that you will input to complete the authentication process.
Phone Calls	A call is placed to your mobile phone asking you to verify you are signing in. Press the # key to complete the authentication process.
Security Key (Token)	You will be prompted to insert a registered security key to your computer.

### **What if I do not want to use my personal device or do not own a smart phone?**

Using a phone is the most secure and convenient way to receive authentication code. No personal information is stored or transferred for the purpose of authenticating access. Your phone number is also not available to SMUS. You may use a security key instead of your phone; however, you will be required to use your phone to register the security key. Contact the IT Help Desk at [help@smus.ca](mailto:help@smus.ca) for further information.

### **How do I change or update my authentication method?**

Go to <https://myaccount.microsoft.com/> to change your MFA settings. This link is accessible from the school and remotely.

### **I already have a strong password; can I opt out of MFA?**

No. You cannot opt out of MFA. Passwords can be obtained by cyber criminals via a variety of methods. Even if you choose a strong secure password and practice good cyber hygiene, your password can still be obtained by other means outside your control. MFA provides an additional layer of security – both are required.

### **What if I forget my mobile device at home?**

If you forget your mobile device at home, you can use your backup authentication method. If that does not solve the problem, please contact the IT Help Desk at [help@smus.ca](mailto:help@smus.ca).

### **Do I have to go through MFA steps when using computer in the office?**

Yes. You will be prompted to trust the device for up to 90 days if you choose to. Only do this if you trust the device and will be using it again. This will remember the sign in for around 90 days and then you will be asked to re-approve your log in.

If there is any suspicious activity detected on your account, you will also be asked.

### **Do I have to go through MFA steps to teach on a classroom computer?**

MFA will not be required on computers in classrooms, conference rooms, and labs except when the computer is using the Virtual Desktop or access the network remotely.

### **What if I am travelling?**

Access using MFA when abroad works the same way if you have access to your registered device and phone number.

### **What if I experience issues with MFA?**

You can contact the IT Help Desk at [help@smus.ca](mailto:help@smus.ca).