GUS Canada MFA email #1- save the date
To GUS Canada staff and faculty
From making MFA@guscanada.ca
Subject: Multi-Factor Authentication Required for Microsoft Accounts

Dear Staff and Faculty,

To increase cyber security for all staff and faculty at GUS Canada <or insert brand name>, multi-factor authentication will soon be required for everyone with an @guscanada.ca <or insert brand domain> email address.

What is multi-factor authentication?

- Multi-factor authentication is an additional layer of protection for your Office 365 account.
- Multi-factor authentication combines something you know – your password – with something you have – typically, a mobile device like your smartphone.
- By responding to an app request on your phone or receiving an SMS text message with a code, you verify that the login request to your account is valid.
- With multi-factor authentication in effect, even if someone knows your password, they will not be able to access your account because they will be missing the multi-factor authentication component.

How do I set up multi-factor authentication?

Many staff and faculty have already voluntarily enabled multi-factor authentication, but multi-factor authentication will be reset for all users on <insert date for brand reset> to ensure the highest level of security for everyone with the most up-to-date information being used to authenticate your account.

You will receive another email after the system has been reset and can then enter or re-enter your multi-factor authentication. You are encouraged to set up multi-factor authentication as soon as possible after the reset on <insert reset date> to ensure there is no interruption to your access to email and other Microsoft apps.

One week after the reset, multi-factor authentication will become mandatory and you will not be able to access your email or Microsoft account until multi-factor authentication has been set up.

You can review the linked guide for step-by-step instructions on how to set up multi-factor authentication but please note that any changes you make before the reset date will need to be re-done after the reset is complete.

Recommended type of authentication

IT Services recommends receiving notifications from the Microsoft Authenticator app as it is quick to set up and easy to use. You can download it from the [Apple App Store](#) for iPhones or the [Google Play Store](#) for Android phones. You will also be required to set up at least one additional method of authentication after the reset and an SMS message authentication is the preferred secondary method of authentication.

When should I enable multi-factor authentication?

Starting on <insert reset date>, you will have one week to set up multi-factor authentication before access to your account will be impacted. That means you will have until <insert date and maybe time of when it is going mandatory> to set up your multi-factor authentication before it is mandatory to do so, and you will not be able to access your account until it's done. We estimate that it will take most users about three to five minutes to set up. However, you can download the Microsoft Authenticator app at any point to expedite the process.

Need help?

If you have any questions or require technical assistance, please [submit a ticket through the GUS Canada Help Desk](#) or email <insert brand helpdesk email>.

Kind regards,

GUS Canada Communications

GUS Canada MFA email #2- reset
To GUS Canada staff and faculty
From Brand Comms or MFA@guscanada.ca
Subject: You can now set up Multi-Factor Authentication for your Microsoft Account

Dear Staff and Faculty,

To increase cyber security for all staff and faculty at GUS Canada <or insert brand name>, multi-factor authentication will soon be mandatory for everyone with an @guscanada.ca <or insert brand domain> email address.

Multi-factor authentication was reset earlier today for all users, and you are encouraged to set it up as soon as possible to avoid any potential disruption to accessing your Microsoft account. Please use the linked guide for step-by-step instructions on how to set up multi-factor authentication.

What is multi-factor authentication?

- Multi-factor authentication is an additional layer of protection for your Office 365 account.
- Multi-factor authentication combines something you know – your password – with something you have – typically, a mobile device like your smartphone.
- By responding to an app request on your phone or receiving an SMS text message with a code, you verify that the login request to your account is valid.
- With multi-factor authentication in effect, even if someone knows your password, they will not be able to access your account because they will be missing the multi-factor authentication component.

How do I set up multi-factor authentication?

Many users had already voluntarily enabled multi-factor authentication, but multi-factor authentication was reset earlier today to ensure the highest level of security for everyone, with the most up-to-date information being used to authenticate your account. This guide includes step-by-step instructions for setting it up.

One week from today, multi-factor authentication will become mandatory and you will not be able to access your email or Microsoft account until multi-factor authentication has been set up.

Recommended type of authentication

IT Services recommends receiving notifications from the Microsoft Authenticator app as it is quick to set up and easy to use. You can download it from the [Apple App Store](#) for iPhones or the [Google Play Store](#) for Android phones. You will also be required to set up at least one additional method of authentication after the reset and an SMS message authentication is the preferred secondary method of authentication.

When should I enable multi-factor authentication?

Starting today, you will have one week to set up multi-factor authentication before access to your account will be impacted. That means you will have until <insert date when it is going mandatory> to set up your multi-factor authentication before you will not be able to access your account until it's done. We estimate that it will take most users about three to five minutes to set up.

Need help?

If you have any questions or require technical assistance, please [submit a ticket through the GUS Canada Help Desk](#) or email <insert brand helpdesk email>.

Kind regards,

GUS Canada Communications

GUS Canada MFA email #3- final warning
To GUS Canada staff and faculty
From Brand Comms or MFA@guscanada.ca
Subject: Last chance to set up Multi-Factor Authentication for your Microsoft Account

Dear Staff and Faculty,

To increase cyber security for all staff and faculty at GUS Canada <or insert brand name>, multi-factor authentication will be mandatory for everyone with an @guscanada.ca <or insert brand domain> email address starting tomorrow <insert date when it's mandatory>.

Multi-factor authentication was reset for all users last week so you need to set it up today to avoid any potential disruption to accessing your Microsoft account. Please use the linked guide <add hyperlink to guide> for step-by-step instructions on how to set up multi-factor authentication.

Starting tomorrow, multi-factor authentication will become mandatory and you will not be able to access your email or Microsoft account until it has been set up.

What is multi-factor authentication?

- Multi-factor authentication is an additional layer of protection for your Office 365 account.
- Multi-factor authentication combines something you know – your password – with something you have – typically, a mobile device like your smartphone.
- By responding to an app request on your phone or receiving an SMS text message with a code, you verify that the login request to your account is valid.
- With multi-factor authentication in effect, even if someone knows your password, they will not be able to access your account because they will be missing the multi-factor authentication component.

How do I set up multi-factor authentication?

Many users had already voluntarily enabled multi-factor authentication, but multi-factor authentication was reset last week to ensure the highest level of security for everyone, with the most up-to-date information being used to authenticate your account. This guide includes step-by-step instructions for setting it up.

Starting tomorrow, multi-factor authentication will become mandatory and you will not be able to access your email or Microsoft account until multi-factor authentication has been set up.

Recommended type of authentication

IT Services recommends receiving notifications from the Microsoft Authenticator app as it is quick to set up and easy to use. You can download it from the Apple App Store for iPhones or the Google Play Store for Android phones. You will also be required to set up at least one additional method of authentication after the reset and an SMS message authentication is the preferred secondary method of authentication.

When should I enable multi-factor authentication?

Today is the last day to set up multi-factor authentication before access to your account will be impacted. Starting tomorrow, you will not be able to access your account until it's set up. We estimate that it will take most users about three to five minutes to set up.

Need help?

If you have any questions or require technical assistance, please submit a ticket through the GUS Canada Help Desk or email <insert brand helpdesk email>.

Kind regards,

GUS Canada Communications