Bulletin #112/21

DATE: June 30,2021

TO: All Locations

FROM: Joanna Bonneville

RE: E-mail - Multi-Factor Authentication

Hello everyone,

We are taking precautions against the all-time high Cybercrime activity currently and will be setting all @smittys.ca emails up with multi-factor authentication in the upcoming weeks.

Set-up Schedule:
- British Columbia and Ontario – Week of July 5th
- Alberta – Week of July 12th
- Manitoba and Atlantic – Week of July 19th
- Saskatchewan – Week of July 26th

Individual emails will be sent out on the day of your location's activation and will include the attached instructions. Once the authentication is active on your account, you will need to set it up in order to access your account again.

Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. MFA is a core component of a strong identity and access management (IAM) policy. Rather than just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack.

Why is MFA Important?
The main benefit of MFA is it will enhance your organization's security by requiring your users to identify themselves by more than a username and password. While important, usernames and passwords are vulnerable to brute force attacks and can be stolen by third parties. Enforcing the use of an MFA factor like a thumbprint or physical hardware key means increased confidence that your organization will stay safe from cyber criminals.

If you have any questions or concerns, please do not hesitate to reach out at jbonneville@smittys.ca

Yours truly,
SMITTY'S CANADA INC.

Joanna Bonneville

Joanna Bonneville
Office Manager and Executive Assistant

# MS Office 365

MFA Multifactor Authentication Setup

1. **Microsoft Authenticator App:**

   The easiest verification method and security purpose is to use Microsoft Authenticator. It's just one click instead of typing in a 6-digit code, and if you travel, you won't incur roaming fees when you use it.

   Download and install the Microsoft Authenticator app for Android, iOS or Windows Phone.

2. **Configure your preference:**

   a. Type this link **https://aka.ms/MFASetup** into any browser or wait for the prompts when you log into your office account

   b. Sign into your Microsoft account using your email address and your Office 365 password.
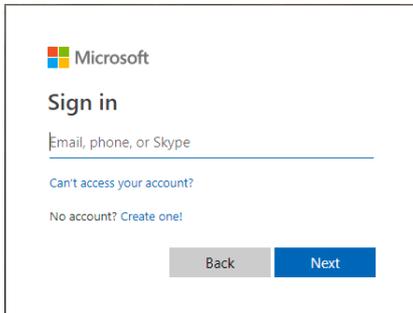
   c. If you already setup MFA to send text code you may need to enter the code provided.

   d. Click yes to the Stay signed in message box

e. In the Additional security verification screen:

    1. Select "Notify me through app"

    2. Checkbox Authenticator app or Token

    3. Click on "Set up Authenticator app"

Additional security verification   App Passwords

When you sign in with your password, you are also required to respond from a registered device. This makes it harder for a hacker to sign in with just a stolen password.
View video to know how to secure your account

what's your preferred option?

We'll use this verification option by default.

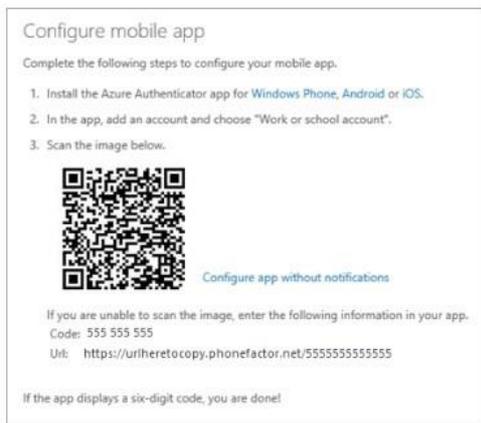| Notify me through app ▼ |

how would you like to respond?

Set up one or more of these options. Learn more

☑ Authentication phone	United States (+1) ▼	1234567890
☐ Office phone	Select your country or region ▼	
	Extension	

f. Wait for the configure mobile app to pop-up. You should see a window on your computer that looks like this.

Configure mobile app

Complete the following steps to configure your mobile app.

1. Install the Azure Authenticator app for Windows Phone, Android or iOS.

2. In the app, add an account and choose "Work or school account".

3. Scan the image below.

Configure app without notifications

If you are unable to scan the image, enter the following information in your app.
Code: 555 555 555
Url: https://urlheretocopy.phonefactor.net/5555555555555

If the app displays a six-digit code, you are done!

g. Switch to your Microsoft Authenticator App

1. Open the Microsoft Authenticator app on your phone.

2. Tap the "+" button to add account and select "Work account".
3. You will need to scan the scan the QR code that will display on your screen.

      h. Switch back to your computer and click "Done".
      i. Now wait for the Checking activation status text to finish configuring your phone
      j. When it's complete, you'll be able to click the Next me button on the right.

Note: If configuration fails just delete retry the previous steps again.

Additional security verification

Secure your account by adding phone verification to your password. View video to know how to secure your account

Step 1: How should we contact you?

| Mobile app | ▼ |

┌─ How do you want to use the mobile app? ──────────────┐
│ ◉ Receive notifications for verification
│ ○ Use verification code
└───┘

To use these verification methods, you must set up the Microsoft Authenticator app.

| Set up | Mobile app has been configured for notifications and verification codes.

[Next]

      k. Switch back to your phone and you'll see a notification for approval. Tap "Approve" to allow it.

      l. Back on the computer, follow any prompts such as additional verification.

Now you should be done setting up MFA using the Authenticator App.