ROCKY MOUNTAIN
School District #6

Tech Systems Support
Last Modified: 12/05/2024

Microsoft 365

Multi Factor Authentication (MFA)

There are 2 methods to setting up Multi Factor Authentication (MFA):

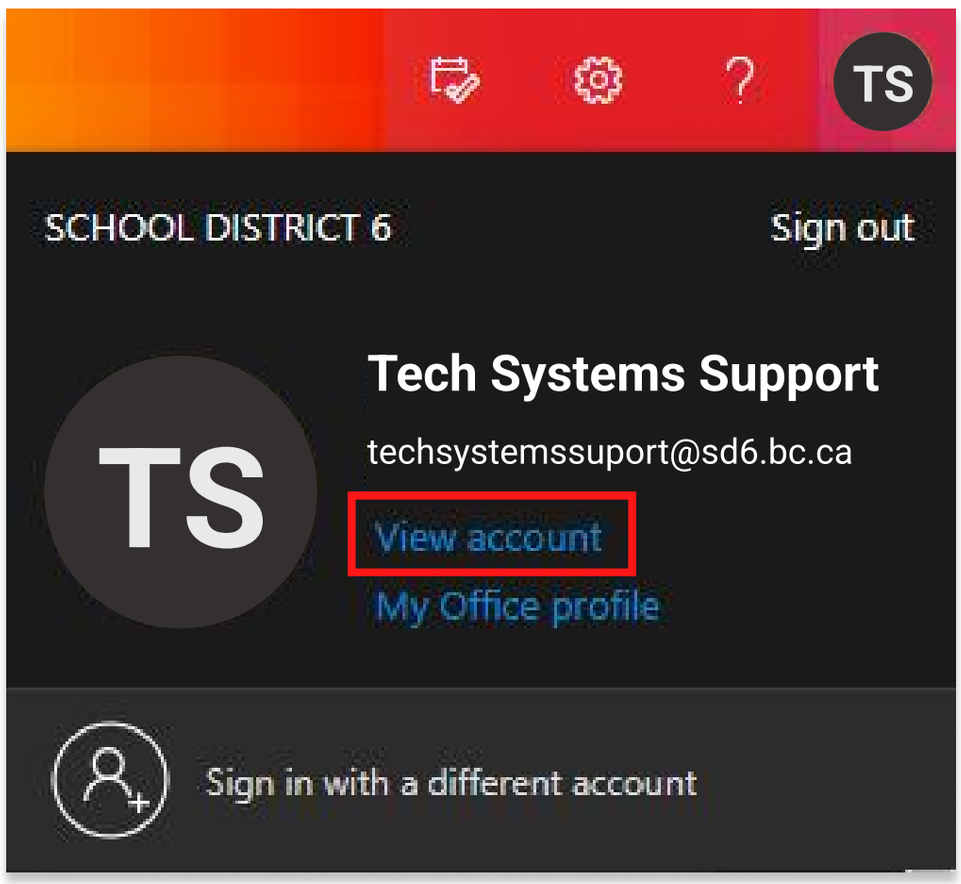
1. Microsoft Authenticator App
2. SMS/Voice Notification

CONTENTS

Microsoft Authenticator App

1. Go to: **https://www.office.com/?auth=2** and sign in using your SD6 credentials.

2. At the top right corner of your screen, click on your profile and go to “View Accont”.



3. Navigate to Security Info, and select **Add sign-in method**.

4. Click the Choose a method dropdown and select: “Microsoft Authenticator”.

5. Download the Microsoft Authenticator using the QR codes below:

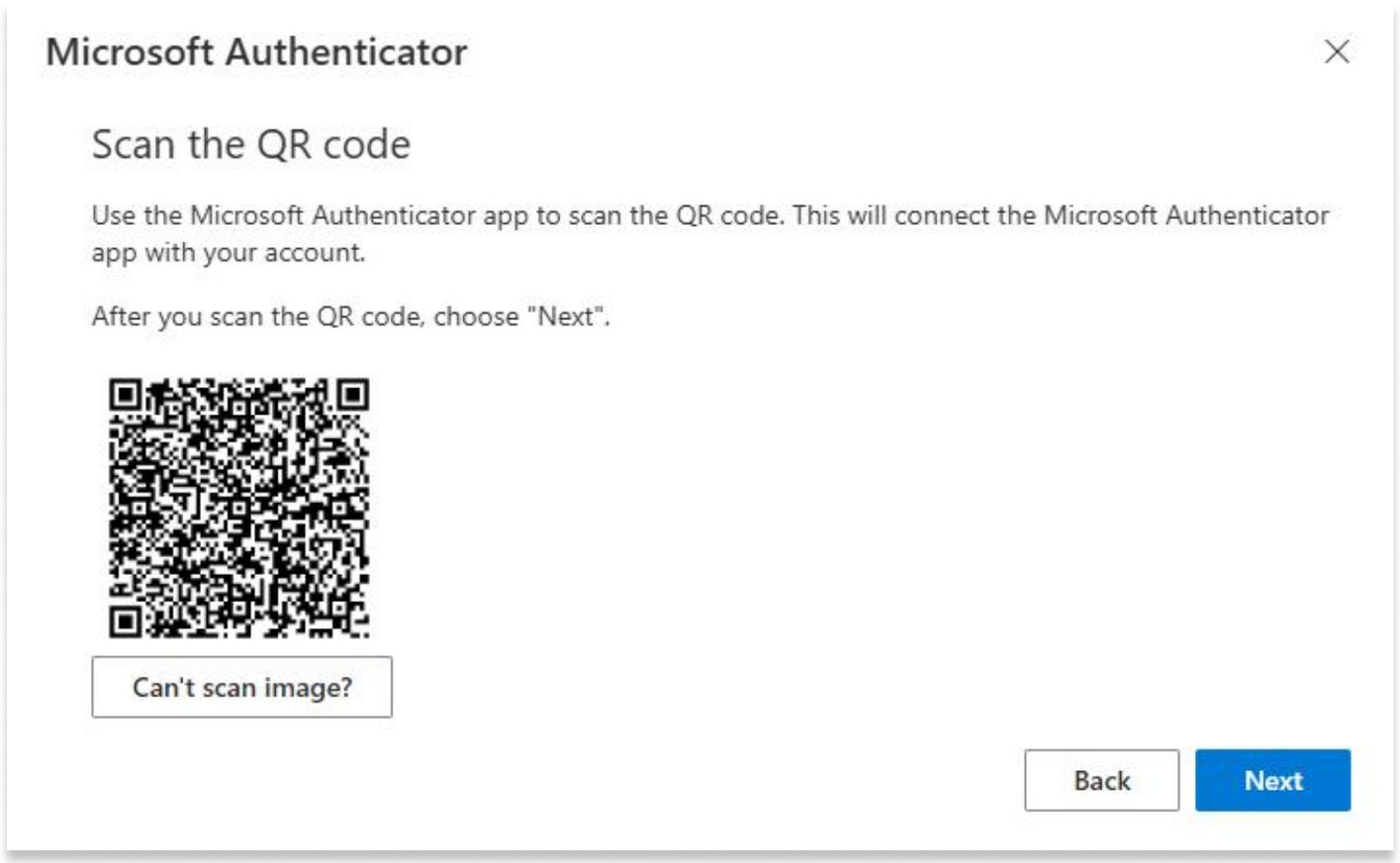
Google Play

App Store

6. Once downloaded, open the app and “Allow” notifications.

7. Click “Scan QR code”.

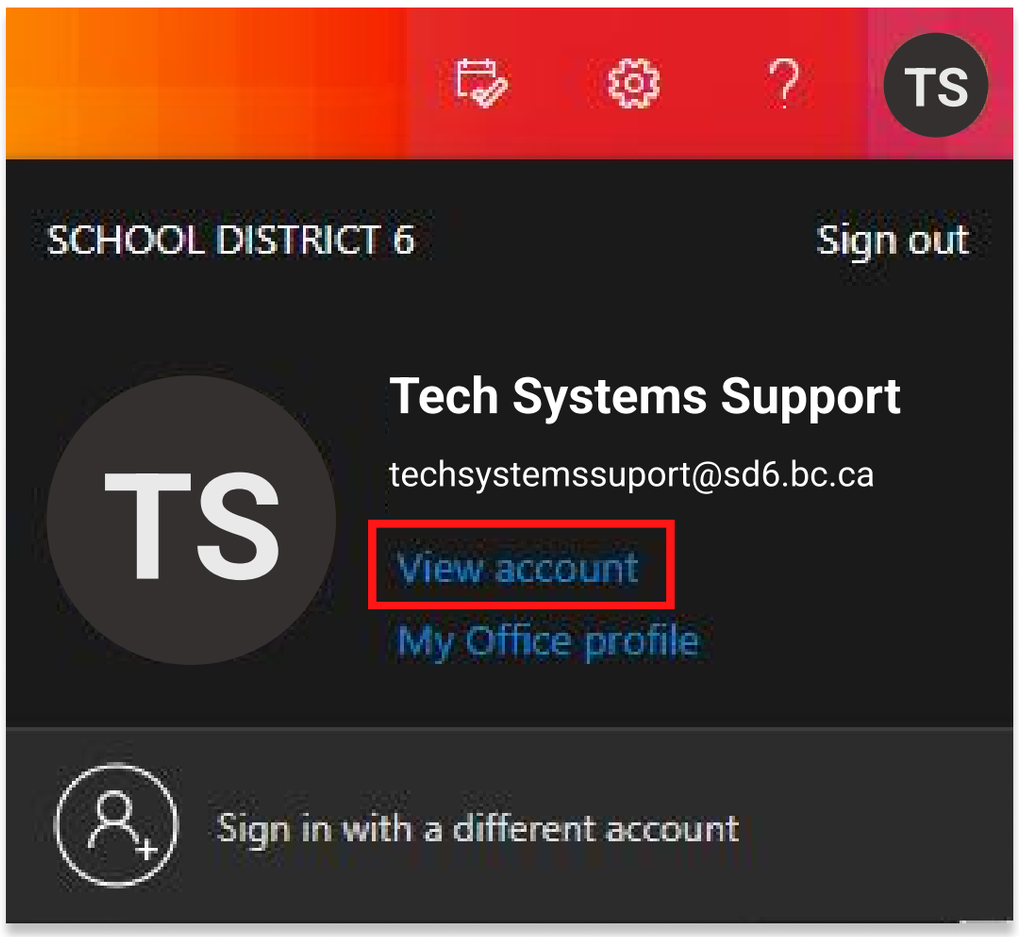
8. Now head back to the Security Info page on your computer and click “Next”, and “Next” again. This will then bring up a box with a QR code to scan using your phone.



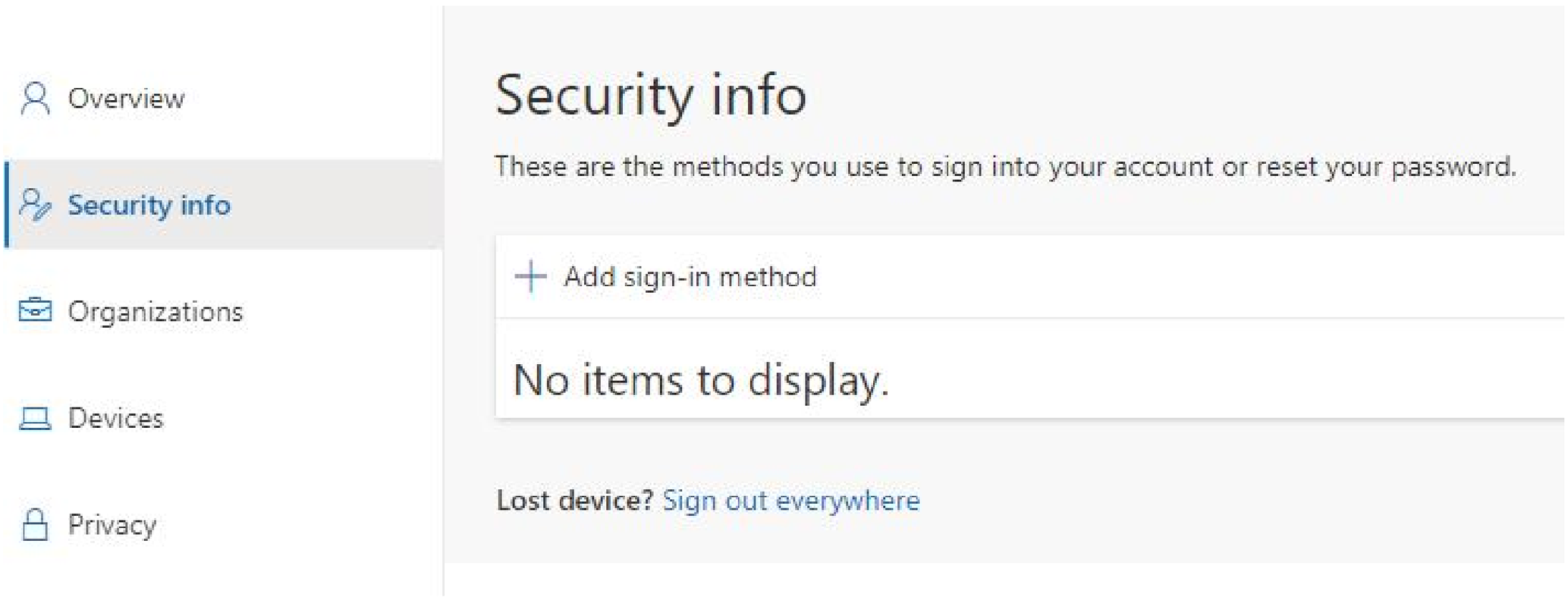
SMS/Voice Notification

1. Go to: **https://www.office.com/?auth=2** and sign in using your SD6 credentials.

2. At the top right corner of your screen, click on your profile and go to “View Accont”.



3. Navigate to Security Info, and select **Add sign-in method**.



3. Click the Choose a method dropdown and select: “Phone”. Press **Add**.

4. Select “Canada (+1)” and type your phone number.

5. Choose either “Text me a Code” or “Call Me”. Click **Next**.

> Shortly after pressing Next, you will recieve either a text or phone call with a 6 digit code.

6. Type your 6 digit code into the Enter Code field. Press **Next**.

7. Once verified, click **Done**.

MFA Background & FAQ

WHAT IS MULTI-FACTOR AUTHENTICATION (MFA)?

Multi-factor authentication (MFA) is a method of verifying a user's identity to access their district Microsoft 365 account. MFA requires the user to provide at least two pieces of evidence (or factors) that prove their identity. These factors can be something the user knows (such as a password or a PIN), something the user owns (such as a smartphone or a security token), or something physically unique to the user (such as a fingerprint or a face scan).

MFA - NEEDS & OBJECTIVES

MFA is necessary because it adds an extra layer of security to access Microsoft 365, which is used every day by School District employees and external contractors, and to other online applications. MFA makes it harder for hackers, cybercriminals, and identity thieves to gain unauthorized access to our digital information, much of which contains Personally Identifiable Information (PII) about us and our students. MFA helps prevent phishing, malware, and social engineering attacks that attempt to trick employees into revealing our passwords or other sensitive information.

KEY BENEFITS (THE WHY)

1. MFA can reduce the risk of data breaches and identity theft by making it more difficult for attackers to compromise our MS 365 accounts.
2. MFA can protect our privacy and confidentiality by preventing unauthorized access to our personal, district, and student information.
3. MFA can enhance our user experience and convenience by allowing us to use different factors that suit our preferences and needs.
4. MFA can increase our trust and confidence in the online services and accounts that we use by ensuring that they are secure and reliable.
5. The Freedom of Information and Protection of Privacy Act (FIPPA) states that public bodies ‘must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized collection, use, disclosure or disposal.’ MFA is widely considered to be one such ‘reasonable security arrangement’.

WHAT ARE THE RISKS ASSOCIATED WITH MFA?

1. Phishing Attacks: Attackers can use sophisticated phishing techniques to trick users into revealing MFA credentials or approving fraudulent authentication requests.
2. Social Engineering: Attackers may use social engineering tactics to manipulate users into providing MFA codes or approving access.