COMMONWEALTH OFFICE OF TECHNOLOGY

AGENCY CONTACT MEMORANDUM 2023-0203

TO: **Agency IT Directors and Technical Staff**

FROM: **David Carter, Chief Information Security Officer**

DATE: **February 3, 2023**

SUBJECT: **MFA Enhancements**

Microsoft has announced that on February 27th, 2023, it will implement enhancements to the multifactor authentication process used in the **Microsoft Authenticator** mobile application. In an effort to allow for proper evaluation before these changes become mandatory, COT will enable these features for all employees on February 15th, 2023. This is applicable to the **Microsoft Authenticator** mobile application and the phone call methods of multifactor authentication verification. Employees using text messaging only as their verification mechanism will not be impacted. It is strongly recommended that all employees utilize the **Microsoft Authenticator** mobile application when possible because it is a much stronger method of multifactor authentication verification.

Beginning Wednesday, February 15th, all staff will see two new features for **Microsoft Authenticator** notifications: **Number Matching** and **Fraud Reporting**. Both are key security upgrades to traditional second factor notifications in **Microsoft Authenticator**.

Number Matching

When a user requests a **Microsoft Authenticator** push notification, they will be presented with a number. They need to type that number into the Authenticator app to complete the approval. See example screenshots below.

Additional information will also accompany the MFA push notification to include details about the application generating the request as well as the geo-location origin of the request. These details can be used by the user to confirm the request is from the user's authenticator or the request is fraudulent. It is important to note that the location information may not be accurate depending on the Internet service or mobile network provider. If you are using SMS text messaging or one-time passcodes (OTP) via another authenticator app (Google for example), this change will not impact your login process.

MFA Fraud Reporting

Receiving an unsolicited MFA notification indicates that a user's credentials may have been compromised by an attacker and steps need to be taken to investigate and mitigate. Reporting these events is critical for the security of not only the user's account but also to the organization.

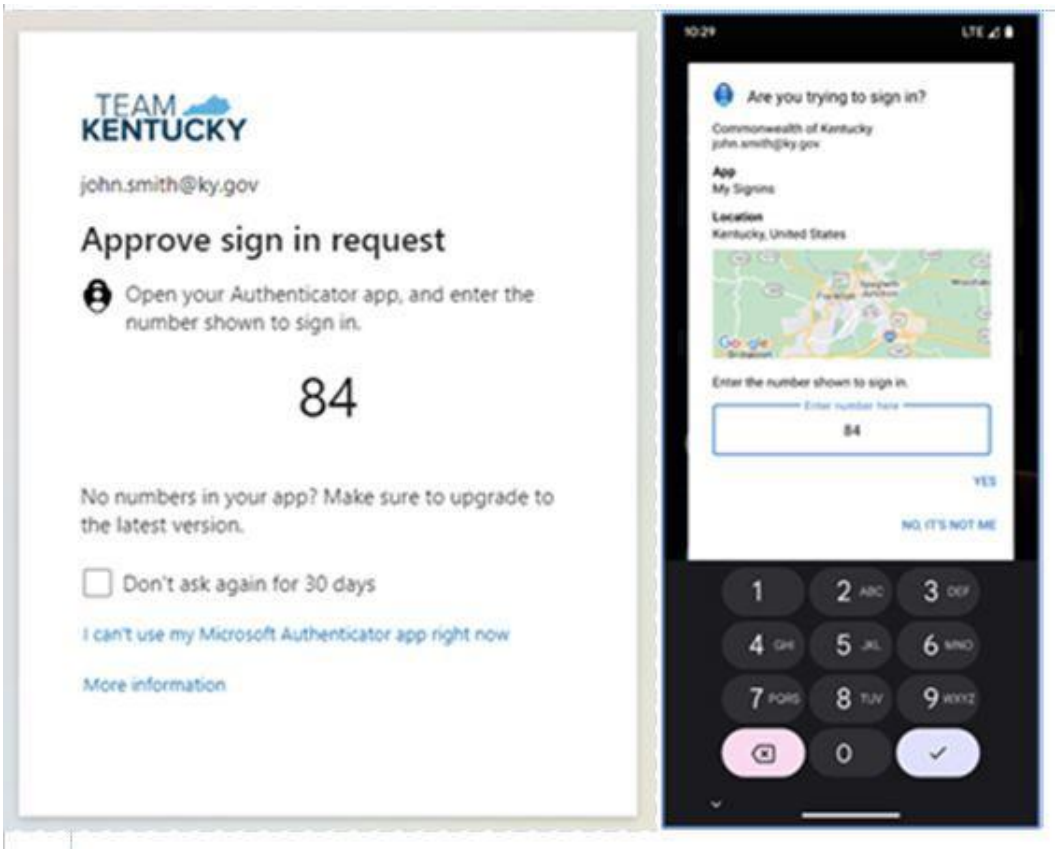
When a user receives a Microsoft Authenticator push notification or a phone call they will be given the chance to report the notification as fraudulent by selecting the option 'NO, IT'S NOT ME' in the Microsoft Authenticator or following the verbal prompts in the phone call.

A report should always be submitted if:

- The user was not expecting the request.
- The request appears to be for a different application than expected.
- The location is not near you or expected by you. ***

If you are using SMS text messaging and receive an unsolicited text code, you do not have the ability to report it directly via the text message. A report should always still be made to security operations (cotsoc@ky.gov) for investigation into any unsolicited MFA notifications.

Example Screen Shots



If you are not using the Microsoft Authenticator app already, it is highly recommended that you install and configure your account to use it. You can do this by visiting your Security Info page. Follow the link for enrollment and choose "Add method" and select "Authenticator App". Follow the instructions to setup the app. Additional instructions can be found in our SSPR and MFA setup guidance here: MFA-SSPR-Registration.

Should you have any question or concerns, please feel free to contact David Carter in the Office of the CISO at davidj.carter@ky.gov.