Referat für Schule und Sport

M365 / WebUntis
Zwei-Faktor-Authentisierung (2FA)

Hilfestellung zur Einrichtung

Zum Schuljahr 2023/24 wird verpflichtend die Zwei-Faktor-Authentisierung für M365 und WebUntis eingeführt. Hier finden Sie eine Anleitung zur Einrichtung der 2FA mit der Microsoft Authenticator App sowie zur Nutzung der 2FA mit der App oder mit dem Hardware-Token.

Hinweis: Die Wahl, welche App Sie nutzen möchten, liegt bei Ihnen. **Für städtische Dienst-iPhones empfiehlt sich die SafeNet-App MobilePass+**, da diese geprüft und im Unternehmensportal verfügbar ist. MobilePass+ im Apple App-Store. Anleitungen zur Einrichtung dieser Apps finden Sie i.d.R. im Internet, das Vorgehen ist aber meist ähnlich!

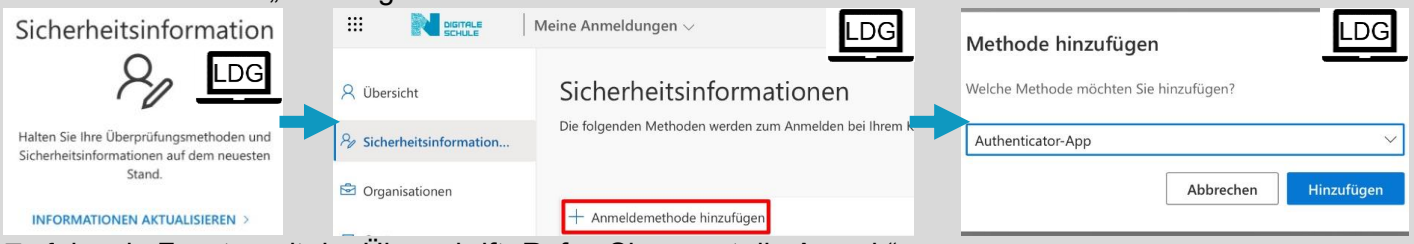
Bitte beachten Sie, dass einzelne Schritte und Ansichten bei Ihnen abhängig von den genutzten Systemen und Geräten ggf. anders aussehen könnten. Auch sind Änderungen im Ablauf durch Programmupdates denkbar. Eine ggf. aktualisierte Version dieser Anleitung ist daher auf der Homepage der digitalen Schule verfügbar.

Inhaltsverzeichnis

Wie richte ich die MS Authenticator App als zweiten Faktor ein?

Rufen Sie im Browser ihres Dienstgeräts myaccount.microsoft.com auf und loggen sich mit Ihren Zugangsdaten (@schulen.nuernberg.de) ein. (Sie können sich auch normal unter portal.office.com anmelden und rechts oben auf Ihre User-Kachel klicken – hier finden Sie den Link auf Ihre Accountverwaltung.)

Wählen Sie in der Kachel „Sicherheitsinformationen“ den Punkt „INFORMATIONEN AKTUALISIEREN“. Klicken Sie dort auf „+ Anmeldemethode hinzufügen“ und wählen Sie aus der Liste die „Authenticator App“ aus. Klicken Sie auf „Hinzufügen“.



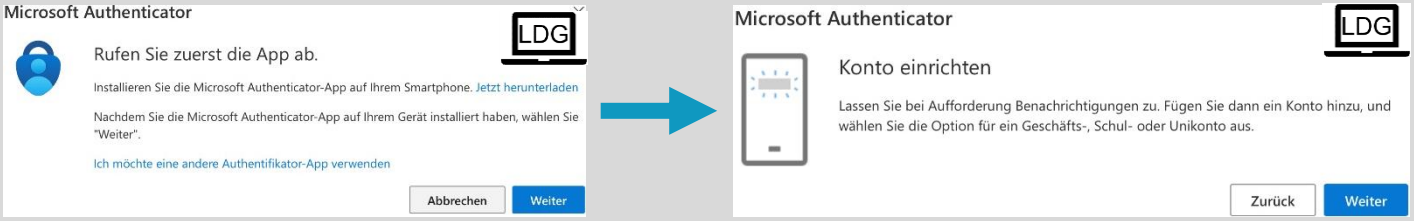
Es folgt ein Fenster mit der Überschrift „Rufen Sie zuerst die App ab“.

Installation der App: Der MS Authenticator ist auf Android- und iOS-Geräten verfügbar. Scannen oder klicken Sie den QR-Code, um zum App Store Ihrer Plattform zu gelangen, bzw. öffnen Sie den App Store und geben Sie im Suchfeld den App-Namen ein. Folgen Sie zur Installation den Anweisungen auf Ihrem Smartphone. **Lassen Sie ggf. Benachrichtigungen und den Zugriff der App auf die Kamera zu.** Direkt nach der Installation führt Sie das Programm bereits durch die Einrichtung eines ersten Kontos. Brechen Sie dies ab und starten Sie die App neu, falls Sie genau dieser Anleitung folgen wollen.

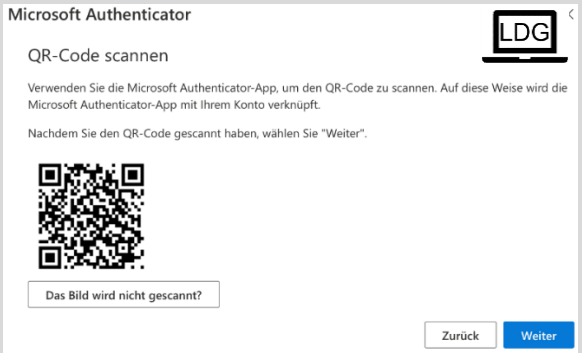
QR-Code scannen – Android: Öffnen Sie die Kamera-App und richten Sie sie auf den Code. Sollte Ihnen kein klickbarer Link angezeigt werden, so müssen Sie ggf. *Modi* und dann *Lens* wählen.

QR-Code scannen – Apple: Richten Sie die Kamera auf den QR-Code und klicken Sie den Link, der Ihnen angezeigt wird.

Nach der Installation können Sie im Browser Ihres Dienstgeräts auf „Weiter“ klicken. Wählen Sie auch im nächsten Fenster „Weiter“.



Ihnen wird nun ein Fenster „QR-Code scannen“ angezeigt. Lassen Sie dieses geöffnet und öffnen Sie die Authenticator App auf Ihrem Smartphone. **Klicken Sie noch nicht auf „Weiter“.**



MS Authenticator App: Klicken Sie in der App auf Ihrem Smartphone auf das „+“-Symbol. Wählen Sie anschließend „Geschäfts- oder Schulkonto“ und „QR-Code scannen“.

In der Authenticator App öffnet sich dann ein Fenster, mit dem Sie den QR-Code scannen können, der auf Ihrem Dienstgerät angezeigt wird. Sie werden abschließend darüber informiert, dass das Konto erfolgreich hinzugefügt wurde.

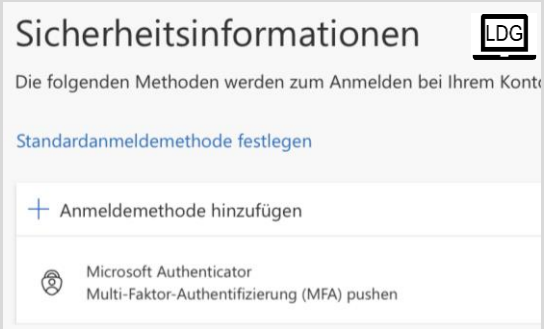
MobilePass+ App: Klicken Sie in der App auf Ihrem Smartphone auf das „+“-Symbol. Es öffnet sich ein Fenster, mit dem Sie den QR-Code scannen können, der auf Ihrem Dienstgerät angezeigt wird. Sie werden abschließend darüber informiert, dass das Konto erfolgreich hinzugefügt wurde.

Klicken Sie jetzt auf Ihrem Dienstgerät im Fenster „QR-Code scannen“ auf **„Weiter“.** Microsoft wird nun eine Benachrichtigung an die Authenticator App auf Ihrem Smartphone senden, die Sie bestätigen müssen. Dies kann z.B. wie folgt aussehen:

Alternativ wird Ihnen auf dem Smartphone ein 6-stelliger Zahlencode angezeigt, den Sie auf dem Dienstgerät eingeben können. Die Vorgehensweise wird von den Anzeigen auf den Geräten aber immer erklärt.

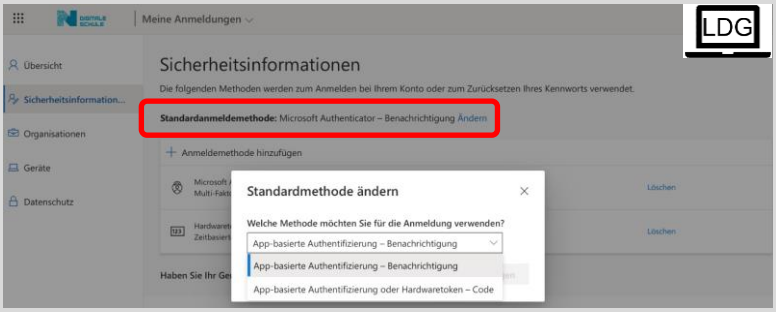
Unter „Sicherheitsinformationen“ auf myaccount.microsoft.com sollte nun die 2FA-App angezeigt werden. Dort können Sie außerdem alle für Ihr Konto eingerichteten Token einsehen.

Sie können den Vorgang auch für ein weiteres Smartphone wiederholen und natürlich alte Token löschen, z.B. bei Diebstahl oder Smartphonewechsel. Denken Sie daran, bei einem Wechsel des Smartphones **vor** dem Rücksetzen des Altgeräts auf dem neuen Gerät einen Token einzurichten – neue Token müssen nämlich mit dem bestehenden bestätigt.



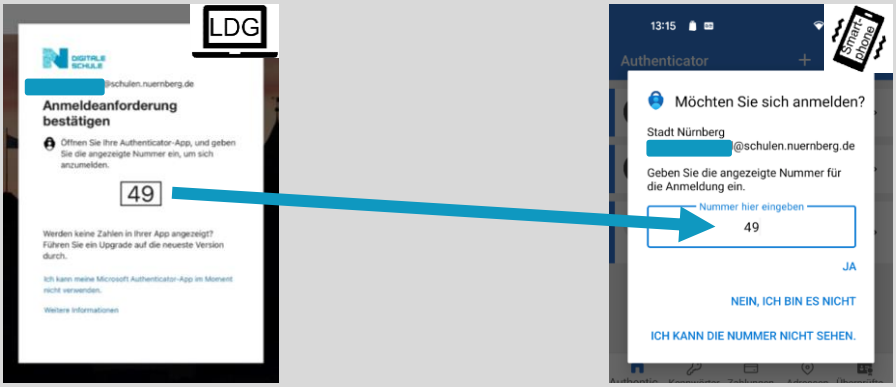
Wie melde ich mich mit der 2FA bei M365 an?

Unter „Sicherheitsinformationen“ auf myaccount.microsoft.com können Sie zwischen verschiedenen Verfahren wählen, mit denen Sie die Authenticator App als zweiten Faktor nutzen können. Die Wahl des Verfahrens steht Ihnen frei, Sie können diese jederzeit wie beschrieben ändern.

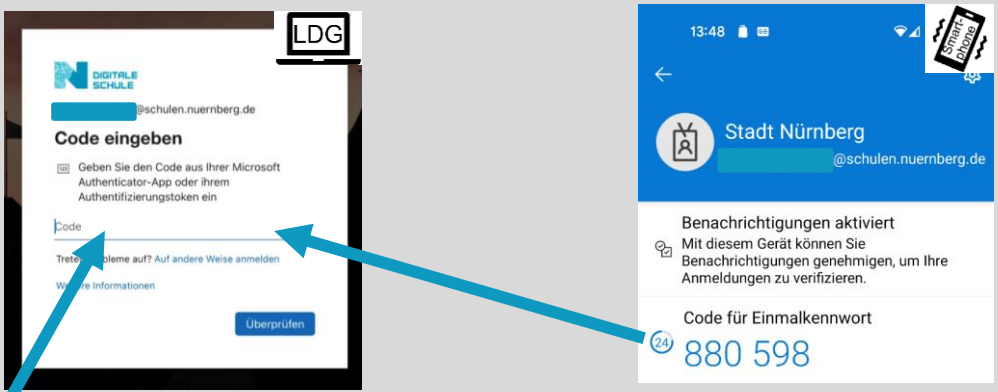


Achtung – abhängig davon, welche 2FA-App Sie wählen, können die Alternativen eingeschränkt sein!

App-basierte Authentifizierung – Benachrichtigung: Wenn Sie diese Methode wählen, wird Ihnen beim Login in M365 nach der Passworteingabe ein Fenster mit einer zufällig generierten zweistelligen Zahl angezeigt. Auf Ihrem Smartphone erscheint eine Push-Nachricht der Authenticator App, öffnen Sie diese. Danach können Sie dort die zweistellige Zahl eingeben und mit „JA“ den Login bestätigen.

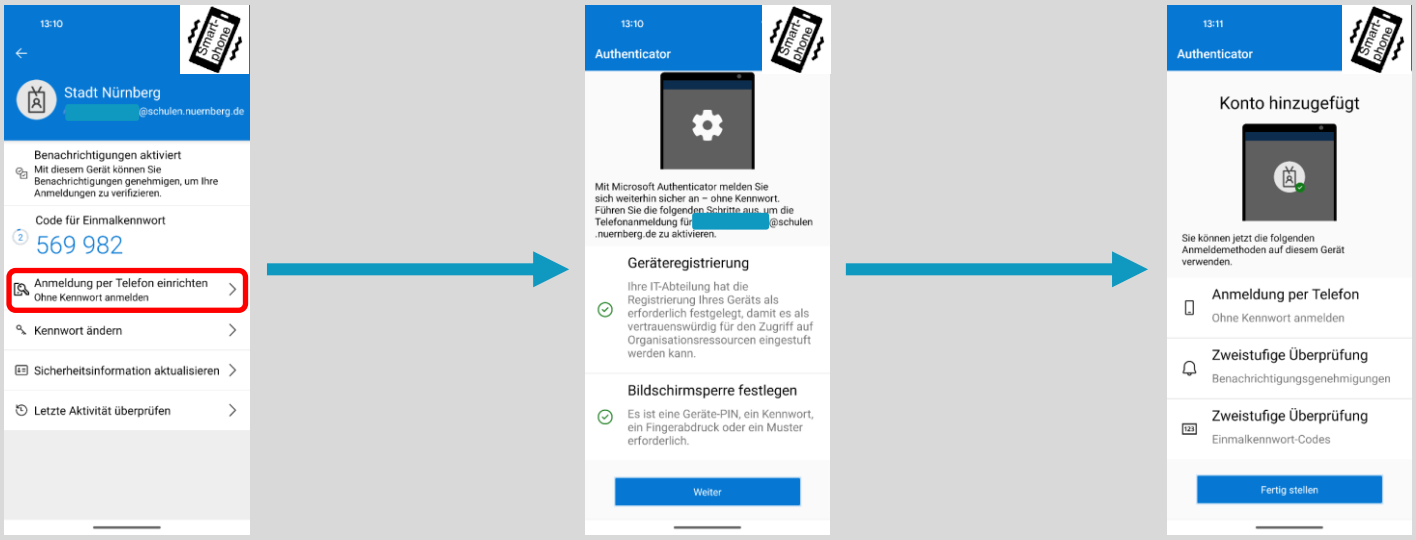


App-basierte Authentifizierung – Code: Bei dieser Methode müssen Sie nach Eingabe des Passworts einen Code eingeben. Öffnen Sie dafür die Authenticator App, wählen Sie das entsprechende Konto aus und geben Sie den dort angezeigten Code ein.

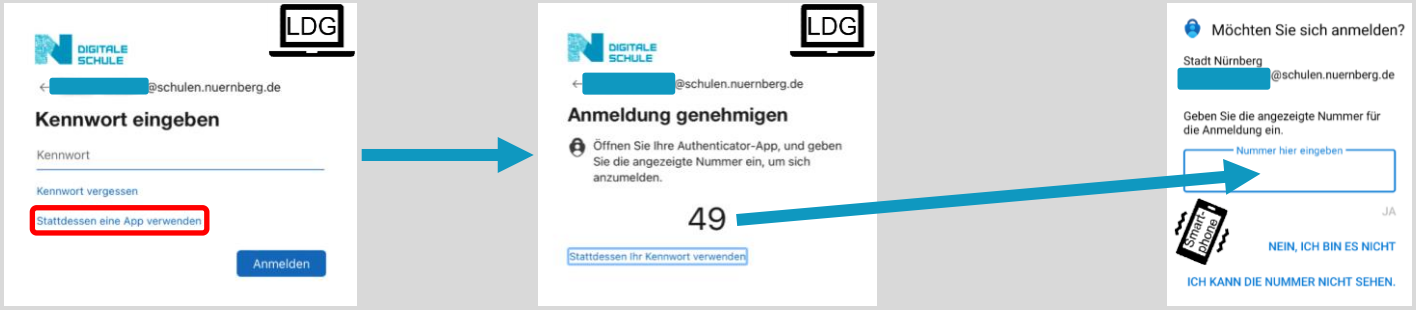


Anmeldung mit Hardware-Token: Mit dem Hardware-Token ist das Verfahren identisch zur App-basierten Authentifizierung mit Code, nur dass der Code in diesem Fall durch Drücken des roten Knopfs auf dem Hardware-Token generiert wird.

Passwortlose Anmeldung mit der MS Authenticator-App: Öffnen Sie in der MS Authenticator-App das Konto, für das Sie die passwortlose Anmeldung nutzen möchten. Klicken Sie dort auf „Anmeldung per Telefon einrichten / Ohne Kennwort anmelden“, „Weiter“ und „Fertig stellen“. Sie werden ggf. aufgefordert, Ihr Passwort einzugeben und z.B. Einstellungen zur Bildschirmsperre Ihres Smartphones anzupassen.



Bei der nächsten Anmeldung müssen Sie „Stattdessen eine App verwenden“ (entfällt bei weiteren Anmeldungen) auswählen und „Anmelden“ klicken. Im Browser wird Ihnen ein zweistelliger Code angezeigt. Auf dem Smartphone erhalten Sie eine Push-Nachricht der MS Authenticator-App. Öffnen Sie diese und tragen Sie dort den zweistelligen Code ein. Bestätigen Sie mit „Ja“.



Wichtig: Sie können diese Funktion erst einrichten, nachdem die 2FA zentral freigegeben wurde. Die Authenticator-App muss dennoch bereits im Vorfeld wie weiter oben beschrieben eingerichtet werden.

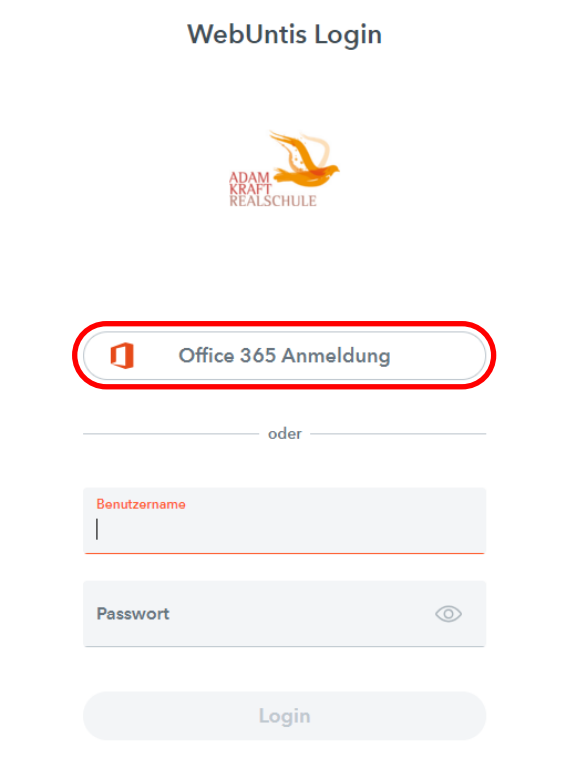
Wie melde ich mich bei WebUntis an?

Die Anmeldung bei WebUntis erfolgt zukünftig über einen sog. Single-Sign-On (SSO) mit Ihren M365-Zugangsdaten. Die notwendigen Einstellungen werden von Ihrem lokalen Untis-Administrator vorgenommen.

Im Browser erfolgt die Anmeldung dann ausschließlich über den Button „Office 365 Anmeldung“ – ist der User am Rechner bereits in Office angemeldet, öffnet sich WebUntis automatisch, ansonsten erscheint die übliche Anmeldemaske im Office-Portal.

Nach einem ersten Login erscheint auch in den Office-Apps ein direkter Link zu WebUntis. Die 2FA-Anmeldung ist hier dann verpflichtend. Die Anmeldung über das untere Untis-Anmeldefeld entfällt.

Wie oben beschrieben kann je nach Einstellung und genutzter App der 2. Faktor unterschiedlich aussehen – entweder durch eine Push-Nachricht auf dem Zweitgerät, in der der Zugriff genehmigt werden muss, oder durch die Eingabe einer zufällig gewählten Zahl, die gerade am Browser angezeigt wird, oder durch die Eingabe einer 6-stelligen Ziffernfolge.



Empfohlene Einstellungen des Smartphones und der Authenticator App

Es ist allgemein empfehlenswert, das Smartphone mit einer Bildschirmsperre vor Zugriff zu schützen. (Aus der Zwei-Faktor- können Sie somit eine noch bessere Multi-Faktor-Authentisierung machen.)

In der 2FA-App selbst können Sie über die drei Punkte rechts oben und den Menüpunkt „Einstellungen“ das Verhalten der App anpassen. Bitte überlegen Sie selbst, welche Berechtigungen und Einstellungen Sie vornehmen möchten – wir empfehlen jedoch, App-Updates automatisch zuzulassen (zumindest bei bestehender WLAN-Verbindung) und keine Nutzungsdaten zur App-Verbesserung zu senden.

FAQ

Wie häufig muss ich den Soft- oder Hardwaretoken verwenden?

Sie müssen den Token nur in Situationen verwenden, in denen Sie bisher Ihr Passwort eingeben mussten. Also bei der Anmeldung unter portal.office.com oder bei WebUntis. Außerdem können auch die lokal installierten Apps sporadisch eine Bestätigung per 2. Faktor fordern. *Eine Ausnahme stellt die Anmeldung am Lehrerdienstgerät dar – hier ist i.d.R. kein 2. Faktor erforderlich.*

Ich habe keinen Zugriff mehr auf meinen Token – was kann ich tun?

Bitte erstellen Sie über Ihre örtliche Systembetreuung ein Ticket bei der Schul-IT. Teilen Sie uns bitte mit, falls es sich um einen dringenden Fall handelt, z.B. akuter Verlust der Kommunikationsmöglichkeit während einer Klassenfahrt o.Ä.. *I.d.R. können Sie die lokal installierten Office-Apps auch ohne 2. Faktor weiterverwenden – so lange, bis Sie ggf. zur Bestätigung per 2. Faktor aufgefordert werden.*

Welche Alternativen zum MS Authenticator gibt es?

MobilePass+, Google Authenticator und jede andere App, die hinreichend sicher erscheint (d.h. im Store über ein anständiges Impressum verfügt, von bekannten Entwicklern stammt, über mehrheitlich gute bis sehr gute Bewertungen verfügt usw.). Bitte lassen Sie bei der Auswahl eine gewisse Vorsicht walten.

Die obengenannten Apps sind kostenfrei und von uns getestet; eine Erstattung für kostenpflichtige Apps ist daher nicht möglich und wir können bei anderen Apps auch nur eingeschränkt bei Problemen helfen.

Nebenbei bemerkt: Einige 2FA-Apps verfügen neben der Authentisierungsfunktion auch über gute Password Safe-Funktionen und können Ihnen daher auch allgemein nützlich sein.

Wie richte ich meinen Hardware-Token ein?

Hardware-Token werden vom Team Digitale Schule für Sie eingerichtet, Sie müssen also selbst keine Einrichtung vornehmen.

Wie funktioniert die Passwortrücksetzung mit eingerichteter 2FA?

Hier ergeben sich keine Änderungen, ggf. werden Sie aber bei der Rücksetzung aufgefordert, Ihren zweiten Faktor zu verwenden.

Kann ich meine Telefonnummer als zweiten Faktor hinterlegen?

Haben Sie in der Vergangenheit z.B. zur Passwortrücksetzung eine Mobilnummer angegeben, wird diese auch hier als mögliches „Authentifizierungstelefon“ angezeigt. Unten auf der Seite steht ein Hinweis, dass Ihre möglicherweise angegebenen Telefonnummern nur zur Sicherheitsüberprüfung verwendet werden.
Die Nutzung eines Authentifizierungstelefons wird hier zwar angeboten, kann jedoch derzeit nicht (ausschließlich bzw. standardmäßig) genutzt werden. Die IT-Sicherheit schätzt die 2FA per SMS o.Ä. als nicht sicher genug ein.

Fragen? 2FA eingerichtet und nichts geht mehr?
Dann E-Mail an Hotline-SchulIT@stadt.nuernberg.de und/oder Anruf bei der Schul-IT-Hotline