Frequently Asked Questions (FAQ)

Häufig gestellte Fragen zur Multi-Faktor-Authentifizierung (MFA)

Wieso ist MFA nötig und jetzt aktiviert worden?

Der Schutz des Zugangs zu Online-Anwendungen und darin verwendete Informationen einzig mittels *Benutzername* und *Passwort* reicht heute oft nicht mehr aus. Der Zugriff auf Microsoft 365 Cloud-Dienste von www.schulen.li (Outlook, Teams, OneNote, OneDrive oder SharePoint) ist seit Herbst 2023 deshalb nur noch mit Einrichtung der Multi-Faktor-Authentifizierung (MFA) möglich. MFA und 2FA sind in der digitalen Welt weit verbreitet und wurden nach den allgemein üblichen Sicherheitsstandards durch das Amt für Informatik nun auch im Schulnetz eingeführt.
(MFA betrifft spezifisch die *Microsoft Cloud-Dienste* und hat vorerst keine Auswirkungen auf die lokale Anmeldung auf deinem Schulgerät.)

Ich habe MFA noch nicht aktiviert. Was muss ich tun?

Als Benutzer/in eines **Windows Notebook** der Schule lade auf deinem Smartphone die **Microsoft Authenticator App** aus dem Apple App Store oder aus dem Google Play Store herunter und installiere und aktiviere sie **selbst** gemäss Schritt-für-Schritt-Anleitung.
Nach erfolgreicher Registrierung kann zusätzlich auf dem Notebook die Anmeldevariante "Windows Hello" genutzt werden, welche die MFA nochmals vereinfacht mittels mindestens einem der weiteren Faktoren (PIN, Fingerabdruck oder Gesicht). [Link]
Für Benutzer/innen eines **Apple iPad** der Schule ist die Microsoft Authenticator App bereits *automatisch im Hintergrund installiert* worden. Aktiviere **selbst** zusammen mit deiner Lehrperson die Authenticator App auf deinem Schul-iPad gemäss Schritt-für-Schritt-Anleitung. [Link]

Muss ich die Authenticator App auf Smartphone *und* iPad einrichten?

Nein, es braucht nur eine Authenticator App. Diese gilt dann für alle Geräte. Lehrerinnen und Lehrer, sowie Schulamtsmitarbeitende und andere Lehrpersonen, die *zusätzlich auch* ein iPad benutzen, müssen die Authenticator App nur einmal auf ihrem Smartphone aktivieren und dieses benutzen.

Die separate Anleitung zum Einrichten der Authenticator App auf Schul-iPads gilt grundsätzlich nur für Schülerinnen und Schüler der Primarschulen!

Ich habe einen Link zu Inhalten im Schulnetz an eine externe Person (z.B. Elternteil) versandt. Muss dafür MFA auch aktiviert werden?

Ja, auch externe Personen (ohne Mailadresse @schulen.li) müssen für den Zugriff auf Microsoft 365 Cloud-Dienste von www.schulen.li seit den Sommerferien 2023 die Multi-Faktor-Authentifizierung (MFA) aktivieren. Für diesen Fall wurde ein Merkblatt und eine separate Anleitung erstellt, welche an externe Personen zur Unterstützung versandt werden kann. [Link]

Ist die Verwendung von MFA aus Datenschutzgründen bedenklich?

Nein, es bestehen keine Datenschutzbedenken bei Verwendung von MFA. Das Schulamt und das Amt für Informatik haben diese Frage eingehend geklärt und die Liechtensteinische Datenschutzstelle erachtet die Verwendung der Multi-Faktor-Authentifizierung im Schulnetz als zulässig.
Insbesondere von biometrischen Daten wie Fingerabdruck oder Gesicht wird kein Foto, sondern nur eine nummerische Information (Hash-Wert) auf dem eingebauten TPM-Chip lokal auf dem Gerät gespeichert. Es steht zudem allen Nutzenden frei, überhaupt den eigenen Fingerabdruck oder das Gesicht als ergänzenden Faktor neben Authenticator App oder PIN festzulegen.
Nachdem ein Schulgerät retourniert wurde, wird, neben der Festplatte, auch der TPM-Chip zurückgesetzt.

Muss ich innerhalb vom Schul-WLAN nun immer MFA benutzen?

Mit einem **Schulgerät** (Windows-Notebook oder Apple iPad der Schule) wird innerhalb vom Schul-WLAN (WILI_INT) keine regelmässige MFA-Abfrage erfolgen.

Mit einem **eigenen Gerät** ("Bring Your Own Device") im separaten WLAN (WILI_BYOD) wird ebenfalls keine regelmässige MFA-Abfrage erfolgen.

In Ausnahmefällen kann auch innerhalb vom Schulnetz eine Aufforderung zur Multi-Faktor-Authentifizierung erscheinen, wenn Microsoft beispielsweise verdächtige Zugriffe von ausserhalb des Schulnetztes feststellt.

Was bedeutet MFA?

MFA ist die Abkürzung für "Multi-Faktor-Authentifizierung" und beschreibt den Vorgang, bei dem Benutzer ihre Identität mit mindestens zwei verschiedenen Faktoren nachweisen müssen, bevor sie Zugriff auf eine Website bzw. ein Online-System erhalten. Damit wird es Angreifenden erschwert, unbefugten Zugriff auf Daten zu erlangen, weil sie zwei Barrieren überwinden müssen.

Ihr kennt es vermutlich vom privaten Online-Banking, wo man sich beim Einloggen in die Online-Anwendung (zusätzlich zu E-Mail-Adresse und Passwort) mit einem *zweiten Faktor* anmelden muss.

Als verschiedene Faktoren werden bei der Anmeldung allgemein unterschieden:

a) etwas, das man **kennt**	(Benutzername und Passwort - 1. Faktor)
b) etwas, das man **hat**/**besitzt**	(Authenticator App, Token - 2. Faktor)
c) etwas, das man **ist**	(Fingerabdruck, Gesicht - 3. Faktor)

Was bedeutet 2FA?

2FA ist die Abkürzung für "2-Faktor-Authentifizierung" bzw. "Zwei-Faktor-Authentifizierung" und im Wesentlichen das Gleiche wie MFA.

Was ist der Unterschied zwischen MFA und 2FA?

Der Hauptunterschied zwischen den beiden Begriffen besteht darin, dass MFA (Multi-Faktor) ein allgemeinerer Begriff ist, der eine beliebige Anzahl von Authentifizierungs-Faktoren umfasst, wohingegen 2FA (2-Faktor) sich speziell auf ein System bezieht, das nur zwei Faktoren zur Authentifizierung verwendet.

In der Praxis werden die Begriffe häufig austauschbar verwendet, und beide werden üblicherweise zur Beschreibung derselben Sicherheitsmassnahme verwendet, bei der die Benutzerinnen und Benutzer zwei oder mehr Formen der Authentifizierung angeben müssen, um ihre Identität zu überprüfen und Zugriff auf ein System oder eine Anwendung zu erhalten.

Welche zweiten Faktoren sind empfohlen?

Aktuell empfiehlt Microsoft die **Authenticator App** zu installieren, da dies die komfortabelste und sicherste Methode darstellt. Die App kann aus dem Apple App Store oder aus dem Google Play Store heruntergeladen werden.
Wer aus besonderen Gründen die App nicht auf das Smartphone herunterladen kann, hat auch die Möglichkeit, beim Amt für Informatik einen separaten TOTP-Token anzufordern. Dessen Einrichtung ist jedoch aufwendig und soll nur im Ausnahmefall erfolgen.

Welche dritten Faktoren können verwendet werden?

Mit der empfohlenen *Microsoft Authenticator App* werden *"etwas, das man kennt"* und *"etwas, das man hat"* abgedeckt. **Alternativ** oder zusätzlich kann auf Windows Notebooks als dritter Faktor noch *"etwas, das man ist"* aktiviert werden, indem man selbst **Windows Hello** aktiviert und entweder *PIN*, *Fingerabdruck* oder *Gesichtserkennung* einrichtet - oder eine Kombination davon.

Windows Hello kann für sich selbst nicht als MFA-Faktor eingerichtet werden und es muss immer zuerst ein MFA-Faktor mittels Authenticator App erfasst worden sein, um Windows Hello verwenden zu können. Nachdem Windows Hello aber korrekt eingerichtet ist, gilt es trotzdem als "starke Authentifizierung" und man muss für die meisten Authentifizierungsvorgänge die Authenticator App nicht mehr jedes Mal verwenden.

Was bedeutet TOTP-Token?

TOTP steht für "Time-based One-Time Password" und erzeugt zeitlich limitierte Einmalkennwörter. Ein solches Einmalpasswort ist üblicherweise maximal 30 Sekunden lang gültig, bis ein neues generiert wird. Unter einem TOTP-Token versteht man ein kleines Gerät ("Hardware") mit einem Display und langlebiger Batterie, welches entweder laufend diese Einmalpasswörter anzeigt oder jeweils nur beim Drücken einer kleinen Taste den nächsten Zahlencode für 30 Sekunden anzeigt.
Es handelt sich dabei um bewährte Technologie, welche z.B. auch beim Online-Banking, zur Anwendung kommt. Die Einrichtung der Token ist jedoch aufwendig und soll nur im Ausnahmefall erfolgen.

Ich habe ein neues Smartphone. Wie kann ich die Authenticator App erneut einrichten?

Lade zuerst auf dem neuen Gerät die **Microsoft Authenticator App** aus dem Apple App Store oder aus dem Google Play Store herunter und installiere sie. Melde dich danach auf deinem Schul-Notebook (mit Windows Hello) auf deiner Microsoft-Konto-Seite https://myaccount.microsoft.com an und klicke auf den Bereich "Sicherheitsinformationen", wo Du über die Option "Methode hinzufügen" dein neues Smartphone bzw. eine neue Authenticator App zusätzlich hinzufügen kannst.
Nachdem das neue Smartphone bzw. die neue Authenticator App erfolgreich eingerichtet wurde, kannst Du *die vorherige Registrierung mit dem alten Handy aus der Liste der angezeigten Geräte löschen.*
Falls die obigen Schritte nicht erfolgreich sind, wende dich (über deine Lehrerin oder deinen Lehrer) an das Amt für Informatik, damit die MFA-Einstellungen für dein Benutzerkonto zurückgesetzt werden können.

Ich habe meinen (TOTP-)Token verloren. Was muss ich tun?

Wende dich an deine Lehrerin oder an deinen Lehrer und melde ihr/ihm den Verlust. Die Lehrperson kann anschliessend über das Support System "4me" beim Amt für Informatik einen Ersatz-Token beantragen. Lehrerinnen und Lehrer, sowie Schulamt-Mitarbeitende, die einen Token verloren haben, eröffnen gleich selbst ein Ticket oder wenden sich an die Medien-Koordinatoren.