

Mehr Passwort Sicherheit durch MFA

Verwendung von eigenen Passwörtern

In Zukunft sollen die Notebook-Benutzer ihr Passwort selbständig verwalten können und mit geeigneten Mitteln die Sicherheit unserer Systeme verstärkt zu schützen.

Jeden Tag werden Tausende von Benutzerkonten gehackt, weil Passwörter zu einfach, gestohlen oder durch Phishing-Angriffe kompromittiert wurden.

Hacker nutzen verschiedene Methoden, um Zugang zu Konten zu erhalten:

- **Brute-Force-Angriffe:** Automatisierte Programme testen Millionen von Passwort-Kombinationen in kürzester Zeit.
- **Phishing:** Betrügerische E-Mails oder Webseiten verleiten Benutzer dazu, ihre Zugangsdaten preiszugeben.
- **Datenleaks:** Viele Nutzer verwenden dasselbe Passwort für mehrere Dienste – wird eines kompromittiert, sind alle Konten gefährdet.
-

Nachfolgend erfährst du, wie wir gemeinsam mehr Sicherheit erreichen wollen.

Multifaktor Authentifizierung (MFA)

Was ist die Multifaktor-Authentifizierung?

Die Multifaktor-Authentifizierung (MFA) ermöglicht den Schutz von Benutzerkonten vor unberechtigtem Zugriff. Zusätzlich zum ersten Authentifizierungsfaktor (Username und Passwort) wird das Benutzerkonto durch eine Authentifizierung über eine Smartphone-App (Authenticator) geschützt (SMS-Code). Und dazu musst du dein Smartphone benutzen.

Windows Hello

Zusätzlicher Schutz mit Windows Hello

Es ermöglicht den Notebook-Benutzern, sich sicher und einfach mit verschiedenen Methoden anzumelden, ohne ein Passwort einzugeben. Zu den unterstützten Authentifizierungsoptionen gehören:

- **Gesichtserkennung:** Windows Hello kann die Gesichtszüge des Nutzers erkennen und so eine schnelle Anmeldung ermöglichen, sofern eine entsprechende Kamera vorhanden ist.
- **Fingerabdruck:** Bei Geräten, die einen Fingerabdrucksensor unterstützen, kann man sich durch das Scannen des Fingers anmelden.
- **PIN-Code:** Zusätzlich zu den biometrischen Optionen bietet Windows Hello auch die Möglichkeit, sich mit einer persönlichen Identifikationsnummer (PIN)

anzumelden, die lokal auf dem Gerät gespeichert wird und daher schneller und sicherer ist als ein Passwort.

Windows Hello bietet mehr Sicherheit und Komfort, da die Anmeldedaten (z. B. Gesichtsm Merkmale oder Fingerabdruck) lokal auf dem Gerät verarbeitet werden und nicht auf Servern gespeichert werden. Es ist also eine benutzerfreundliche Alternative zu klassischen Passwörtern.

Steps zur Einführung von MFA und Windows Hello

1. MFA Aktivieren

Aktiviere die MFA bis **Freitag, 11.4.2025, 14:00** mit der Anleitung «MFA-Aktivieren» ([Downloaden](#)) oder diesem [Video](#).

2. Neues Passwort setzen

Nach erfolgreicher Aktivierung der MFA kannst du dein Notebook im Online-Betrieb neu starten und beim Login mit «Ctrl-Alt-Del» und «Passwort neu setzen» dein Passwort ändern.

Die neue Richtlinie verlangt neben MFA auch eine neue Passwortlänge von 12 Zeichen, dafür ohne Komplexität (keine Gross-Kleinschrift, keine Vorgaben über Zahlen und Sonderzeichen). Wähle dazu ein einfaches, aber krasses Passwort am besten ein Dialektwort, wie zum Beispiel:

Striitpareid, Chuchichäschtle oder Badwanneäntli.

Auf dem Geschäfts-Notebook musst du zum MFA weiter nichts mehr machen.

Auf all deinen nicht SHV-Geräten, musst du dich nun alle 30 Tage, neu mit MFA einloggen. Dazu wird dir ein Code per SMS gesendet.

3. Windows Hello einrichten

Nach erfolgreichem Login wirst du ab **Montag, 14.4.2025 14:00** aufgefordert, auf deinem SHV-Gerät einen PIN für Windows Hello zu setzen.

Danach kannst du auch die anderen Login Methodiken, wie Fingerprint oder Gesichtserkennung einrichten.

Hier geht es zur [Anleitung](#) von Microsoft zu Windows Hello

Fragen

- Bedeutet dies, dass wir von nun an zwingend das Handy nicht zuhause vergessen dürfen, damit wir uns am Laptop einloggen können, weil wir die App benötigen?
➔ Das Handy kann problemlos zu Hause vergessen werden, es wird nicht zum Einloggen am SHV-Notebook benötigt

- Wie ist dies, wenn ich im Büro vom Laptop weggehe, dann Sperre ich eigentlich immer den Bildschirm (habe dies so gelernt), müsste ich mich dann jeweils dann ebenfalls wieder mithilfe der App einloggen?
➔ Das Entsperren wie auch das Einloggen geht dann mit deinem 4-stelligen PIN, der Gesichtserkennung oder dem Fingerprint mit Windows Hello

Support

- Bei Fragen oder Problemen, wendet euch bitte an diese Mail-Adresse:
support@swiss-support.net