CYBER-PRÄVENTION

ASSMANN Versicherungsmakler

Konten besser schützen.

Praxiswissen für dein Handwerk

Ein zweiter Faktor macht den Unterschied.

E-Mails, Kundendaten und digitale Kehrbücher gehören zu deinem Alltag. Ein gestohlenes Passwort kann vieles gefährden.

01 Was bedeutet Zwei-Faktor-Anmeldung?

Zwei-Faktor-Authentisierung (2FA) kombiniert zwei unterschiedliche Nachweise: zum Beispiel dein **Passwort** und einen **zeitlich begrenzten Code aus einer Authenticator-App**. Zwei verschiedene Passwörter allein sind keine zwei Faktoren. Mit der zweiten Anmeldehürde machst du Angreifern den Zugriff deutlich schwerer.

02 In vier Schritten einrichten

1. **Wichtige Konten zuerst.** Starte mit E-Mail, Cloud, Buchhaltung sowie Administrator- und Fernzugängen, sofern der Dienst 2FA unterstützt.
2. **Sicherheitseinstellungen selbst öffnen.** Wähle dort die zusätzliche Anmeldung. Nutze Passkeys oder Sicherheitsschlüssel, wenn der Dienst sie anbietet; sie können besser vor Phishing schützen als manuell eingegebene Codes.
3. **Authenticator-App verbinden.** Beispiele für iOS und Android sind Google Authenticator und Microsoft Authenticator. Lade die offizielle App, scanne den Einrichtungs-QR-Code des Dienstes und bestätige den ersten Code.
4. **Zugang testen und absichern.** Melde dich erneut an. Sichere Wiederherstellungscodes getrennt vom Smartphone und lege im Betrieb fest, wer im Notfall berechtigt auf den Zugang zugreifen darf.

Vorsicht bei unerwarteten Anfragen

Gib Anmelde- und Wiederherstellungscodes niemals weiter. Bestätige nur selbst gestartete Anmeldungen. App-Codes können auf gefälschten Login-Seiten abgefangen werden. Schütze dein Smartphone mit PIN oder Biometrie.

Dein kurzer Konten-Check

- ☐ E-Mail und wichtige Geschäftskonten zusätzlich abgesichert.
- ☐ Notfallcodes sicher abgelegt und Wiederzugang geklärt.

Assmann Versicherungsmakler GmbH | 02371 8266-0 | mail@assmann-makler.de
Barendorfer Bruch 2 · 58640 Iserlohn

CYBER-PRÄVENTION

ASSMANN Versicherungsmakler

Daten sicher verwahren.

Praxiswissen für dein Handwerk

Verschlüsseln. Schlüssel sichern. Weiterarbeiten.

Ein verlorenes Notebook muss nicht zum offenen Aktenschrank werden.

Vorher: Datensicherung und Notfallzugang

Erstelle ein aktuelles Backup. Bewahre den Wiederherstellungsschlüssel geschützt und getrennt vom Gerät auf. Kläre mit deiner IT-Betreuung, wie berechtigter Zugriff im Notfall möglich bleibt.

01 Windows: Geräteverschlüsselung oder BitLocker

Suche in Windows nach **„Geräteverschlüsselung“** oder **„BitLocker verwalten“** und prüfe den Status. Geräteverschlüsselung ist auf geeigneten Geräten auch mit Windows Home möglich. Die manuelle BitLocker-Laufwerkverschlüsselung gehört zu Pro, Enterprise und Education.
Wenn die Funktion fehlt oder zentral verwaltet wird: erst mit der IT-Betreuung abstimmen. Externe Datenträger sind nicht automatisch in jedem Fall mitgeschützt.

02 Mac: FileVault prüfen

Öffne **Systemeinstellungen → Datenschutz & Sicherheit → FileVault**. Prüfe den Status und richte den Wiederherstellungsweg sorgfältig ein. Bei Macs mit Apple Chip oder T2-Chip sind Daten bereits hardwareseitig verschlüsselt; FileVault bindet den Zugriff zusätzlich an die Anmeldung.

Verschlüsselung ist ein Baustein

Laufwerksverschlüsselung erschwert unbefugten Zugriff bei Geräteverlust. Sie ersetzt kein Backup und schützt nicht vor jedem Angriff auf ein entsperrtes Gerät. Systeme aktuell halten, Bildschirm sperren und getrennte/offline Sicherungen regelmäßig wiederherstellen und testen.

Technik absichern. Restrisiken mit uns besprechen.

mail@assmann-makler.de | 02371 8266-0

Mehr zum Cyber-Konzept auf unserer Website →

Offizielle Anleitungen zum Anklicken

BSI: Zwei-Faktor-Verfahren
Microsoft: Authenticator
Microsoft: BitLocker
Google: Authenticator einrichten
Microsoft: Geräteverschlüsselung
Apple: FileVault

Assmann Versicherungsmakler GmbH | 02371 8266-0 | mail@assmann-makler.de
Barendorfer Bruch 2 · 58640 Iserlohn