



# Sicherheitshinweise

---

## 1. Schutz Ihrer vertraulichen Daten

Zur Identifikation auf unserer Online-Banking-Plattform benötigen Sie Ihren Anmeldenamen, Ihre PIN und TANs. Sie haben dafür Sorge zu tragen, dass keine andere Person Kenntnis von diesen Daten erhält. Insbesondere sollten Sie Folgendes zur Geheimhaltung dieser vertraulichen Daten beachten:

- Geben Sie Ihren Anmeldenamen, Ihre PIN und TANs niemals an Dritte weiter. Mitarbeiter der TRUMPF Financial Services GmbH werden Sie niemals nach derartigen Daten fragen.
- Sie müssen die von uns zugeschickte PIN nach der Erstanmeldung auf eine individuelle PIN ändern. Verwenden Sie dabei keine einfachen, leicht zu erratenden Begriffe. Die PIN zur Erstanmeldung verfällt zu Ihrer eigenen Sicherheit nach 180 Tagen.
- Informieren Sie uns bitte umgehend, wenn die von uns zugeschickten Umschläge offen oder beschädigt sind, Abdeckungen der PIN verletzt oder verformt sind oder die PIN bereits vor dem Abziehen sichtbar ist.
- Bitte speichern Sie Ihren Anmeldenamen, Ihre PIN oder TAN-Liste niemals elektronisch ab.
- Bitte geben Sie Ihren Anmeldenamen, Ihre PIN und TANs nur auf von uns autorisierten Zugangswegen ein.
- Halten Sie Ihre TAN-Liste immer unter Verschluss und stellen Sie sicher, dass niemand sie unbemerkt entwenden kann.
- Kontrollieren Sie regelmäßig die Umsätze auf Ihrem Konto und Referenzkonto, um rechtzeitig unberechtigte Abbuchungen zu erkennen und uns informieren zu können. Falls Sie den Verdacht haben, dass mit Ihrer Online-Anwendung etwas nicht in Ordnung ist, sperren Sie Ihren Zugang und kontaktieren Sie uns umgehend auf den von uns mitgeteilten Kommunikationswegen.

## 2. Browser Software / Anti-Virus-Maßnahmen / Firewall

Bitte setzen Sie für die Online-Anwendung nur vom jeweiligen Hersteller freigegebene Versionen eines Internet-Browsers ein und achten Sie darauf, dass Sie die eingesetzte Browser-Software aus vertrauenswürdigen Quellen bezogen haben.

Setzen Sie immer einen aktuellen Virenschanner ein, um Ihren Computer von Viren, Trojanern und anderer Schadsoftware in empfangenden oder vorhandenen Daten zu schützen. Lassen Sie regelmäßig Ihren gesamten Datenbestand auf Ihrem Computer durch den Virenschanner überprüfen.

Zusätzlich sollten Sie eine aktuelle Firewall einsetzen, um unerwünschte Zugriffe aus dem Internet auf Ihren Computer und von Ihrem Computer ins Internet zu unterbinden.

Achten Sie bei der Beschaffung derartiger Sicherheitssoftware ebenfalls auf vertrauenswürdige Quellen.

Öffnen Sie niemals E-Mails oder Dateianhänge von Absendern, die Ihnen nicht bekannt sind. Die TRUMPF Financial Services GmbH wird niemals persönliche oder sicherheitsrelevante Kontodetails per E-Mail bei Ihnen abfragen.

Weitere Sicherheitshinweise finden Sie auch unter [https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home\\_node.html](https://www.bsi-fuer-buerger.de/BSIFB/DE/Home/home_node.html).

## 3. Nutzung der Original-Website

Achten Sie darauf, dass die technische Verbindung zum Onlinebanking der TRUMPF Financial Services GmbH nur über die Internetseite der TRUMPF Financial Services GmbH (<https://www.trumpf-banking.com>) erfolgt.

Für den sicheren Datentransfer nutzen wir eine SSL-Verschlüsselung, die den Missbrauch von Daten oder Datendiebstahl verhindern soll. Eine SSL-verschlüsselte Verbindung erkennen Sie an dem Schlosssymbol in der Adresszeile und daran, dass in der Adressleiste Ihres Browsers der Link der Seite mit „https“ beginnt. Bitte achten Sie darauf, dass während der gesamten Verbindungsdauer mit unserem Online-Banking dieses Symbol ungebrochen dargestellt wird.

## 4. Sichere Abmeldung

Um das Online-Banking ordnungsgemäß zu beenden, wählen Sie bitte immer den Button „Abmelden“. Wenn Sie 15 Minuten keine Eingabe tätigen, werden Sie automatisch aus dem Online-Banking abgemeldet.

## 5. Sichere Kommunikation

Wir bitten Sie, uns bei Verdacht auf betrügerische Zahlungen oder anderweitige Sicherheitsvorfälle umgehend zu kontaktieren. Hierfür können Sie unsere Servicehotline nutzen oder uns per Email ([trumpf-banking@kundenserviceteam.de](mailto:trumpf-banking@kundenserviceteam.de)) darüber informieren.

Wir werden Ihnen dann auf einem dieser Kommunikationswege antworten.

Ebenfalls werden wir Sie nur mittels der bekannten Kommunikationswege über etwaige betrügerische Transaktionen in Kenntnis setzen. Bitte kontaktieren Sie uns im Zweifelsfall immer.