Fürst Fugger Privatbank

Überblick

In diesem Dokument erhalten Sie wichtige Sicherheitshinweise, die Sie unbedingt einhalten sollten. Folgende Themen werden angesprochen:

Sicherheitsrelevante Themen

- Browser-Software / Betriebssystem
- Anti-Virus-Maßnahmen / Firewall
- SSL-Protokoll
- Abmelden / Automatische Zeitüberwachung
- Benutzerautorisierung durch PIN/TAN
- Geheimhaltung
- Zugangswege

Browser-Software / Betriebssystem

Bitte setzen Sie für die Online-Anwendung nur vom jeweiligen Hersteller freigegebene Versionen eines Internet-Browsers ein, z. B.

- Mozilla Firefox
- Microsoft Edge
- Apple Safari
- Google Chrome

Hinweise:
Achten Sie darauf, dass Sie die eingesetzte Browser-Software aus vertrauenswürdigen Quellen bezogen haben, so dass sichergestellt ist, dass es sich um unveränderte Originalsoftware handelt.

Nutzen Sie zudem die aktuelle Version Ihres Internet-Browsers. Nur die jeweils aktuellen Versionen der gängigen Browser können die bestmögliche Sicherheit gewährleisten.

Zudem bieten Hersteller von Betriebssystemen stets neue Updates an. Informieren Sie sich deshalb regelmäßig über die neuesten Entwicklungen und halten Ihr Betriebssystem durch Updates auf dem jeweils aktuellen Stand.

Weitere nützliche Tipps zum Thema 'Sicherheit im Internet' finden Sie auch unter https://www.bsi-fuer-buerger.de/.

Anti-Virus-Maßnahmen / Firewall

Stellen Sie bitte sicher, dass Ihr PC virenfrei ist. Dies ist am besten durch einen regelmäßigen Virencheck mit einem der bekannten Virenscan-Programme zu erreichen.

Überprüfen Sie dabei stets die Aktualität Ihrer sog. 'Virenbibliothek' und laden Sie regelmäßig die neuesten Updates auf Ihren PC.

Zusätzlich sollten Sie eine Firewall verwenden. Diese soll den Rechner vor Angriffen von außen schützen und verhindern, dass bestimmte Programme, zum Beispiel sog. Spyware, unkontrollierten Kontakt zum Internet aufnehmen.

Weitere nützliche Tipps zum Thema 'Firewall' sowie eine Auswahl kostenloser Sicherheitssoftware finden Sie auch unter https://www.bsi-fuer-buerger.de/

SSL-Protokoll

Grundlage der sicheren Internet-Verbindung ist die Verwendung des SSL-Protokolls für die Übertragung der Daten.

Das Bestehen einer sicheren SSL-Verbindung wird Ihnen durch ein geschlossenes Schloss-Symbol angezeigt.

Bitte achten Sie darauf, dass während der gesamten Verbindungsdauer mit unserem Online-Anwendungsrechner dieses Symbol ungebrochen dargestellt wird.

Durch einen Klick auf das jeweilige Symbol werden Ihnen weitere Informationen angezeigt. Die Darstellung ist abhängig von der von Ihnen eingesetzten Browserversion.

Abmelden / Automatische Zeitüberwachung

Um die Online-Anwendung ordnungsgemäß zu beenden, wählen Sie bitte immer die Schaltfläche rechts oben neben Ihrem Namen.

Wenn keine Eingabe erfolgt, werden Sie nach **fünf Minuten** nach vorhergehender Abfrage automatisch von der Anwendung abgemeldet.

Benutzerautorisierung durch PIN/TAN

Zur Identifikation gegenüber unserer Online-Banking Anwendung benötigen Sie von uns zu Ihrer Zugangskennung (VR-NetKey) eine PIN und TANs.

Die PIN ist nur Ihnen bekannt und Sie erhalten diese in einem verschlossenen Umschlag.

Die TANs sind ebenfalls nur Ihnen bekannt. Sie erhalten diese, abhängig davon, welches Verfahren bei Ihnen eingesetzt wird, in folgender Form:

- als SecureGo plus TAN oder Freigabe in Ihrer SecureGo plus App
- als Sm@rt-TAN plus auf Ihrem TAN-Generator

Bitte beachten Sie im Umgang mit PIN und TANs unbedingt Folgendes:

- Geben Sie die PIN und die TANs an **niemanden** weiter.
- Auch Bankmitarbeiter sind nicht berechtigt, derartige Daten von Ihnen zu erfragen.
- **Niemals** wird Ihre Bank Sie per E-Mail auffordern, diese vertraulichen Daten in ein Formular einzugeben. Sollten Sie eine solche E-Mail erhalten, löschen Sie diese bitte umgehend.

Die PIN (Personal Identification Number) dient als 'elektronischer Ausweis', zusammen mit Ihrer Zugangskennung (VR-NetKey) oder dem Alias, um über unsere Online-Banking Anwendung Zugang zu Ihrem Konto zu erhalten.

- Sie müssen die von uns erhaltene PIN bei der Erstanmeldung in eine persönliche PIN abändern.
- Verwenden Sie für Ihre individuelle PIN dabei keine einfachen, leicht zu erratende Begriffe wie den eigenen Vornamen, Geburtsdaten oder ähnliche Begriffe.
- Mit der PIN erhalten Sie Zugriff auf Ihre Kontendaten und können Informationen über Ihre aktuellen Kontenstände bzw. über Ihre Kontoumsätze abfragen.

Alle Vorgänge im Online-Banking, die zu einem signierpflichtigen Geschäftsvorgang führen, wie z. B. Überweisungen, werden zusätzlich noch durch die Eingabe einer TAN bzw. Freigabe in der SecureGo plus App abgesichert.

Durch die Verwendung von PIN und TAN ist sichergestellt, dass nur Sie mit Ihrer Zugangskennung (VR-NetKey) oder Ihrem Alias Bankgeschäfte mit der Online-Banking Anwendung durchführen und vertrauenswürdige Informationen abfragen können.

Beachten Sie:

- Auf eine TAN-Eingabe kann dann verzichtet werden, wenn der Zahlungsbetrag nicht über 30 Euro liegt oder die Höchstanzahl von fünf aufeinanderfolgenden Zahlungen die Gesamtsumme von 100 Euro nicht überschreitet.
- Ebenso werden im Betrag unbegrenzte Überweisungen von Konten der gleichen juristischen oder natürlichen Person innerhalb der gleichen Bank ohne TAN-Eingabe ausgeführt, wenn Ihre Bank sich dazu entschlossen hat, diesen Service anzubieten.

Geheimhaltung

Bitte achten Sie unbedingt darauf, dass Sie Ihre Zugangskennung (VR-NetKey) und/oder Ihren Alias, Ihre PIN und Ihre TANs immer unter Verschluss halten und kein unberechtigter Dritter Zugriff auf diese Daten bekommt. Behandeln Sie diese sensiblen Daten wie Bargeld.

Zugangswege

Bitte geben Sie die PIN und TAN nur auf den Ihnen von uns mitgeteilten und autorisierten Zugangswegen ein.

Vergewissern Sie sich immer, dass Sie auch auf einer echten Seite Ihrer Bank sind. Dies überprüfen Sie im ersten Schritt durch einen Abgleich der Internet-Adresse im Browser, der sogenannten URL.

Bereits minimale Abweichungen weisen auf eine gefälschte Internetseite hin.

Bitte prüfen Sie, ob die Internet-Adresse (URL) zum kontaktierten Finanzinstitut gehört. Die URL finden Sie in der 'Vereinbarung über die Nutzung des Online-Bankings'. Alternativ können Sie diese auch bei Ihrer Bank erfragen.

Falls Sie eine andere Adresszeile vorfinden, beenden Sie die Verbindung sofort.

Bei Fragen wenden Sie sich bitte an Ihren Berater oder unser Team Online-Banking.