ELLWANGER.GEIGER
PRIVATBANKHAUS SEIT 1912

Sicherheitshinweise

In diesem Dokument erhalten Sie wichtige Sicherheitshinweise, die Sie unbedingt einhalten sollten.

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

Hinweis

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 http://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 http://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 den Button [Abmelden] rechts oben in der Marginalspalte.
Wenn Sie einmal vergessen haben sollten, die Anwendung zu beenden, oder längere Zeit Ihren Rechner unbeaufsichtigt lassen, müssen Sie sich keine Sorgen machen: Die eingebaute Zeitsperre bricht das Programm ab, sobald im festgelegten Zeitraum keine Eingabe erfolgt.

Benutzerautorisierung durch PIN/TAN

Zur Identifikation gegenüber unserem Online-Anwendungsrechner benötigen Sie von uns zu Ihrer Zugangskennung (E&G-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-TAN in Ihrer SecureGo-App oder
- als mobileTAN per SMS auf Ihr Handy oder
- 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 (E&G-NetKey) oder dem Alias, um über unseren Online-Anwendungsrechner Zugang zu Ihrem Konto zu erhalten.

- Sie müssen die erhaltene PIN nach der Erstanmeldung vom Vorgabewert auf einen individuellen Wert 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 Geschäftsvorgang führen, wie z. B. Überweisungen, werden zusätzlich noch durch die Eingabe einer TAN (Transaktionsnummer) abgesichert.

- Die TAN übernimmt dabei die Funktion einer 'elektronischen Unterschrift'.
- Jede TAN kann dabei nur für einen Vorgang verwendet werden. Nach Abschluss des Vorgangs wird die verwendete TAN ungültig.

Durch die Verwendung von PIN und TAN ist sichergestellt, dass nur Sie mit Ihrer Zugangskennung (E&G-NetKey) oder Ihrem Alias Bankgeschäfte mit der Online-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 (E&G-NetKey), 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 Ihre Bank.