Mindestanforderungen für sichere Zahlungen im Internet

Das Internet stellt viele Möglichkeiten zur Verfügung. Es ist immer und nahezu überall verfügbar. Da liegt es nahe, auch die persönlichen Bankgeschäfte online zu erledigen. Im weltweiten Netz tätigen Sie zum Beispiel einfach und bequem Ihre Überweisungen oder rufen zu jeder Tageszeit Ihren Kontostand ab. Aber das Internet birgt auch Gefahren. Vermehrt warnen Experten und Medien vor Risiken wie z.B. Phishing-Attacken, neuen Viren oder Würmern. Trotzdem können Sie die Vorzüge des Online Bankings gesichert nutzen, wenn Sie die Gefahren kennen und wissen, wie Sie die Abwehr Ihres Computers, Tablets oder Smartphones stärken.

Sicherheits-Tipps

Es ist wie bei Ihrer Haustüre: Diese lassen Sie nicht unbeaufsichtigt offen stehen.

✓ **Regel 1:**
Schützen Sie Ihr Gerät mit geeigneter Software, wie z.B. aktueller Antivirus-Software und Firewall.

✓ **Regel 2:**
Erlauben Sie keinem Fremden den Zugang zu Ihrem Computer.

✓ **Regel 3:**
Machen Sie sich mit möglichen Gefahren vertraut.

Pharming

Beim Pharming werden Sie während des Surfens im Internet auf eine gefälschte Seite gelotst. Dabei setzen die Betrüger auf Manipulation der technischen Abläufe beim Aufrufen der Seite. Ziel ist es, vertrauliche Informationen zu stehlen. Es handelt sich hierbei um eine Fortentwicklung des klassischen Phishings. Sie schützen sich am besten vor diesen Betrugsversuchen, indem Sie Ihre Sicherheitssoftware immer auf dem neuesten Stand halten.

Viren, Würmer und Trojaner

Immer wieder gibt es Schlagzeilen zu neuen Varianten von Viren, Würmern oder Trojanern. Diese infizieren beim Surfen im Internet unbemerkt Computer, Tablet und Smartphone oder werden als Links oder Anhänge von E-Mails verbreitet.

Ist Ihr Gerät erst einmal infiziert, ist es schwer, diese Internet-Parasiten wieder loszuwerden.

Wenn Sie jedoch die Funktionsweise von Viren, Würmern und Trojanern kennen, können Sie sich mit einigen Sicherheitsregeln entspannt im Internet bewegen: Öffnen Sie grundsätzlich keine Links oder Anhänge in E-Mails, sondern rufen Sie beispielsweise Rechnungen oder Bestellbestätigungen über die jeweiligen Unternehmensportale auf.

Kommunikationswege Ihrer Volksbank Stuttgart eG
Wir kommunizieren mit Ihnen hinsichtlich der sicheren Nutzung der Internetzahlungsdienste über sichere Wege. Dies sind der Postversand, das elektronische Postfach im Online Banking bzw. der papierhafte Kontoauszug.

Sie können sich ganz sicher sein: Ihre Bank wird Sie nie per E-Mail oder Telefon nach Ihren Online-Banking-Zugangsdaten fragen.

Phishing

Beim Password-Fishing, kurz Phishing, versuchen Kriminelle über das Internet oder Telefon an Ihre persönlichen Zugangsdaten für das Online Banking zu gelangen. Sie erhalten in der Regel eine E-Mail, die angeblich von Ihrer Bank oder einem Ihnen vertrauten Unternehmen stammt. Darin werden Sie aufgefordert, einem Link zu folgen und dort ihre persönlichen Daten einzugeben.

Waren es anfangs noch einfache Mailtexte, die in holprigem Deutsch den Empfänger zur Preisgabe seiner persönlichen Identifikations- (PIN) und Transaktionsnummer (TAN) aufforderten, so gehen die Täter heute mit mehr Raffinesse ans Werk:

Die Mails sehen aus wie offizielle Schreiben, z. B. Ihrer Bank. Sie tragen also das Firmenlogo, benutzen dieselbe Schriftart und dieselben Gestaltungsrichtlinien. Im Text ist oft die Rede von „Sicherheitsüberprüfungen" oder anderen wichtigen klingenden Maßnahmen.

Alle Phishingmails verfolgen das gleiche Ziel: Sie zu einer Formularseite weiterzuleiten auf der Sie Ihre Geheimzahlen eintragen sollen. Diese Seiten sind ebenfalls perfekt den offiziellen Web-Seiten nachgebaut. Auch wenn Sie die Link-Adresse als die richtige identifizieren, ist Vorsicht geboten – denn sie ist trotzdem gefälscht.

Eine weitere Version des Phishings ist der Anruf eines angeblichen Servicemitarbeiters, der unter einem Vorwand telefonisch persönliche Daten erfragen möchte.

Auch bei anderen Unternehmen sollten Sie bei der Weitergabe von Zugangsdaten sehr vorsichtig sein.

Finanzagent

Immer wieder gibt es Angebote, als sogenannter Finanzmakler tätig zu werden. Ihnen wird per E-Mail versprochen, sich mit diesem Job ein lukratives Zweiteinkommen zu sichern. Meist geht es darum, hohe Summen aus unbekannten Quellen zu empfangen und anschließend ins Ausland zu überweisen. Die Gelder stammen dabei unter anderem aus illegalen Phishing-Aktivitäten. Durch das Anwerben von Laien als Strohmänner wollen die Täter unerkannt bleiben. Verzichten Sie auf solche Angebote, denn Sie würden sich des Betrugs und der Geldwäsche mitschuldig machen.

Volksbank Stuttgart eG

Stärken Sie die Abwehr Ihres Computers, Tablets oder Smartphone mit einem Anti-Viren-Programm mit Firewall
Ein Anti-Viren-Programm durchforstet Ihr Gerät nach Schädlingen jeglicher Art, repariert infizierte Dateien bzw. löscht sie. Die Firewall schützt Sie vor Hacker-Angriffen, indem sie deren Zugriffsversuche blockiert. Ein solches Programm ist Pflicht für jeden PC. Kostenpflichtige Programme leisten meist mehr als kostenfreie. Ganz wichtig: Führen Sie regelmäßige Updates durch. Nur so erkennt das Anti-Viren-Programm auch die neuesten Gefahren.

Sicheres Online Banking

Neben der Erfassung von Zahlungsaufträgen in einer sicheren Umgebung – damit sind Computer mit aktuellem Softwarestand und Virenschutz gemeint – ist auch das Freigabeverfahren ein relevantes Kriterium für ein sicheres Online Banking.

Generell gilt:

- Jede Buchung wird durch eine Transaktionsnummer (TAN) freigegeben. Die jeweilige TAN ist nur für die aktuelle Transaktion gültig und kann nicht für andere Transaktionen missbraucht werden.
- Egal welches TAN-Verfahren Sie nutzen: Es werden stets relevante Transaktionsdaten als Kontrollmöglichkeit vor der Freigabe des Zahlungsauftrages angezeigt.

smartTAN

Mit den Sm@rt-TAN-Verfahren erledigen Sie Ihre Bankgeschäfte online direkt über unsere Website auf unserer Online-Banking-Plattform. Zusätzlich wird jeder Vorgang im Online-Banking durch das bewährte PIN-TAN-Verfahren verschlüsselt. So wird größtmögliche Sicherheit gewährleistet. Zum Erzeugen und Anzeigen der individuellen TAN wird lediglich ein TAN-Generator und Ihre girocard (Debitkarte) benötigt, der direkt mit der Anzeige auf Ihrem Bildschirm kommuniziert.

Sm@rtTAN optic

- Der Leser ist kompakt, leicht, arbeitet ohne externe Stromversorgung und muss nicht an den PC angeschlossen werden.
- Hohe Sicherheit durch das 3-Schritt-Verfahren:
  - Die Online-Banking-Plattform ist internetbasiert.
  - Die Zugangsdaten erhalten Sie per Post.
  - Die für jeden Vorgang individuelle TAN generieren Sie mit Ihrer girocard (Debitkarte) und dem Sm@rtTAN optic-Leser, in den Sie die Überweisungsdaten entweder manuell eingeben oder über eine optische Schnittstelle von Ihrem Bildschirm einlesen.

Und so geht's:

- Auftrag (z.B. Überweisung) am PC erfassen und girocard (Debitkarte) in den Sm@rtTAN-Leser einführen.
- „F"-Taste drücken und den Sm@rtTAN optic-Leser vor die animierte Grafik auf dem Monitor halten.
- Die übertragenen Daten z.B. mit der Rechnung abgleichen und nur bei Übereinstimmung mit der „OK"-Taste bestätigen.
- Die daraufhin angezeigte TAN in der Auftragsseite des Online Banking eintragen und den jetzt vollständigen Auftrag absenden.

Sm@rt-TAN photo

Bei Sm@rt-TAN photo werden im Vergleich zu Sm@rt-TAN plus mit der optischen Methode keine blinkende Balken sondern ein stehendes Bild (Farbmatrix-Code ähnlich eines QR-Code) zur Datenübertragung aus dem Online-Banking auf den TAN-Generator eingesetzt. Dadurch sind bei Sm@rt-TAN photo keine Größenanpassungen der Grafik oder weitere Einstellungen notwendig.

So funktioniert Sm@rt-TAN photo mit der optischen Methode

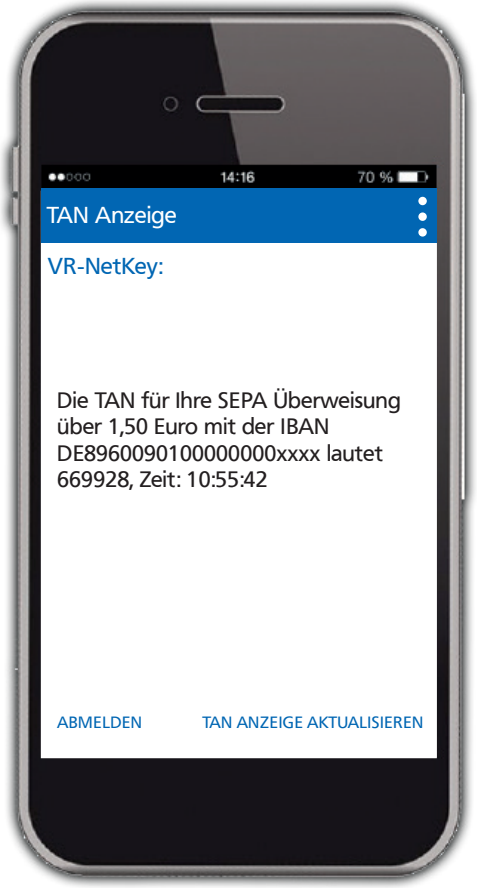
- Tragen Sie alle notwendigen Daten zum Beispiel in Ihr Online-Überweisungsformular ein. Wählen Sie anschließend „TAN-Eingabe durch Farbcode-Erkennung (Sm@rt-TAN photo)" aus.
- Die sogenannte optische Schnittstelle erscheint, ein stehendes Bild (Farbcode-Grafik, ähnlich eines QR-Codes) auf Ihrem Bildschirm.
- Schieben Sie Ihre girocard (Debitkarte) in den TAN-Generator. Drücken Sie die Taste „Scan". Halten Sie den TAN-Generator so vor die Farbcode-Grafik, dass der Farbcode in der Anzeige vollständig angezeigt wird. Prüfen Sie die Anzeige auf dem Display Ihres TAN-Generators und drücken Sie „OK".
- Im Display Ihres TAN-Generators werden nun alle wichtigen Daten Ihres Auftrages angezeigt, zum Beispiel die IBAN des Empfängers und der Betrag. Wichtig: Vergleichen Sie Ihre Daten mit denen auf dem Originalbeleg und bestätigen Sie diese jeweils mit „OK".
- Die TAN wird erstellt und erscheint auf dem Display Ihres TAN-Generators. Sie ist nur für diese Transaktion und für wenige Minuten gültig. Geben Sie die TAN in das entsprechende Feld im Online-Banking ein und bestätigen Sie Ihren Vorgang mit „OK" bzw. „Ausführen".

Volksbank Stuttgart eG

VR-SecureGo
Mit der TAN-App VR-SecureGo empfangen Sie Transaktionsnummern (TAN) jederzeit sicher und bequem auf Ihrem Smartphone oder Tablet. Die TAN-Benachrichtigungen sind vergleichbar mit dem mobile-TAN-Verfahren. Sie werden jedoch nicht per SMS versandt, sondern in der VR-SecureGo-App angezeigt. Dazu benötigen Sie lediglich ein Smartphone oder Tablet, auf dem die TAN-App VR-SecureGo installiert ist sowie eine Registrierung in der App und im Online-Banking Ihrer Volksbank Stuttgart eG.

So funktioniert die TAN-App VR-SecureGo

- Sie führen eine TAN-pflichtige Transaktion im Online-Banking, über HBCI/FinTS oder in der VR-BankingApp durch. Im Online-Banking wird beim Schritt „Eingabe prüfen" automatisch eine VR-SecureGo-TAN angefordert.
- Sie melden sich in der TAN-App VR-SecureGo an. Eine direkte Anmeldung ist auch über das Antippen der Push-Nachricht möglich. Dazu müssen Sie zuvor dem Empfang von Push-Nachrichten zugestimmt haben.
- Bitte prüfen Sie in der TAN-App VR-SecureGo die Transaktionsdaten auf Richtigkeit, wie zum Beispiel den Betrag und die IBAN des Empfängers.
- Wenn Sie die TAN-pflichtige Transaktion aus der VR-BankingApp heraus gestartet haben und die übermittelten Daten in der TAN-App VR-SecureGo richtig sind, klicken Sie bitte auf „An die VR-BankingApp übertragen". Die VR-SecureGo-TAN ist nur für diese Transaktion gültig. Wenn Sie die TAN-pflichtige Transaktion aus dem Online-Banking oder FinTS heraus gestartet und sich anschließend in der TAN-App VR-SecureGo angemeldet haben, wird Ihnen die TAN angezeigt. Sie müssen diese manuell übertragen. Für eine weitere TAN-pflichtige Transaktion klicken Sie bitte auf „TAN-Anzeige aktualisieren".
- Die direkte Übertragung in die VR-BankingApp ist nur möglich, wenn Sie beide Apps auf dem gleichen Smartphone oder Tablet installiert haben. Wenn Sie das browserbasierte Online-Banking oder HBCI/FinTS nutzen, müssen Sie die VR-SecureGo-TAN entsprechend manuell eingeben.



Volksbank Stuttgart eG

Grundlegende Sicherheitshinweise

- Geben Sie die Webadresse Ihrer Bank immer von Hand ein, niemals über den Link in einer E-Mail.
- Moderne Betriebssysteme machen es Ihnen leicht. Nutzen Sie die automatischen Updates und stellen Sie die Sicherheitsoptionen Ihres Browsers mindestens auf „mittel“.
- Speichern Sie keine persönlichen Zugangsdaten auf Ihrem Computer.
- Benutzen Sie möglichst immer Ihren eigenen Computer, denn fremde Rechner können Sicherheitslücken aufweisen.
- Starten Sie den Browser neu, bevor Sie das Online Banking aufrufen.
- Prüfen Sie das Vorhängeschloss der gesicherten https-Internetseite. Kennen Sie den Eigentümer oder den Zertifikatsaussteller nicht, brechen Sie die Sitzung ab.
- Gleichen Sie Ihre Kontoumsätze vor und nach jeder Transaktion ab.
- Fragen Sie sich immer, wann eine Dateneingabe sinnvoll ist.
- Folgen Sie keinen Links, die Sie auffordern, Ihr Passwort oder Ihre PIN preiszugeben.
- Öffnen Sie keine E-Mail-Anhänge, wenn Sie diese nicht angefordert haben.
- Beachten Sie die aktuellen Sicherheitshinweise und Warnmeldungen Ihrer Bank.
- Ändern Sie regelmäßig Ihre PIN.
- Durch Ihre Festlegung eines Online Banking-Limits erhalten Sie einen zusätzlichen Schutz vor unberechtigten Zugriffen im Online Banking. Ihr Online Banking-Limit wird bei der Beantragung zum Online Banking festgelegt, kann aber jederzeit von Ihnen angepasst werden. Eine Änderung können Sie selbst im Online Banking über die Funktion „Mitteilung an Ihre Bank“ ändern. Selbstverständlich können Sie sich auch jeder Zeit an Ihren Berater wenden.
- Verwenden Sie für Ihre PIN keine leicht nachvollziehbaren Zahlen- oder Buchstabenkombinationen (z. B. Geburtsdaten oder Namen).
- Sperren Sie unverzüglich Ihre Karte, sobald Sie den Verlust bemerken. Mit folgenden Telefonnummern können Sie auch Ihr Online Banking sperren lassen:

girocard (Debitkarte)	+ 49 1805 021 021*
Kreditkarten (Mastercard oder Visa)	+ 49 721 1209 66001
Einheitlicher Sperrnotruf	+ 49 116 116** (alternativ, sofern Sie die 116 116 aus dem Ausland nicht erreichen: + 49 30 40 50 40 50)
Sperrnotruf per Fax für sprach- und hörgeschädigte Menschen	+ 49 30 40 50 40 50

* 0,14 Euro pro Minute aus dem Festnetz, Mobilfunkhöchstpreis 0,42 Euro pro Minute.
** Telefonischer Vermittlungsdienst an die zuständige Sperrinstanz; bundesweit gebührenfrei.

Weitere Informationen finden Sie unter www.volksbank-stuttgart.de/kartesperren

- So sperren Sie Ihr Online Banking notfalls selbst: Geben Sie dreimal eine falsche TAN ein, um Ihre TANs zu sperren und danach zehnmal eine falsche PIN.

Schützen Sie Ihr Konto

Sind Sie bereits Opfer einer Phishingmail geworden, informieren Sie uns bitte unverzüglich unter **0711 181-0**.
Speichern Sie die gefälschte E-Mail zur Beweissicherung. Falls noch möglich, machen Sie Ihre alte PIN für den Trickbetrüger sofort unbrauchbar, indem Sie sie durch eine neue ersetzen.

Gehen Sie entspannt online

Sie wollen Ihre Bankgeschäfte schnell und sicher im Internet erledigen? Wir beraten Sie gerne zu allen Fragen des Online Bankings. Weitere Informationen und Meldungen zu aktuellen Sicherheitsfragen finden Sie auf unserer Internetseite:

www.volksbank-stuttgart.de/sicherheit

Volksbank Stuttgart eG