pushTAN: Ersteinrichtung

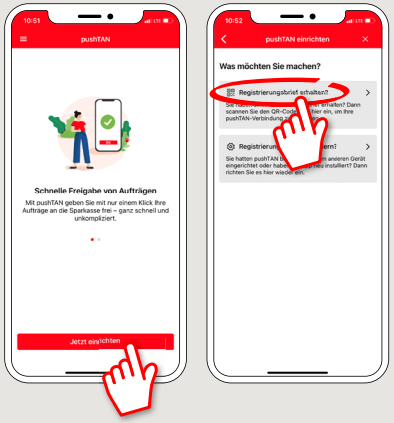
www.sparkasse-hanau.de/pushtan

Sparkasse Hanau

Starten Sie die nachfolgend beschriebene Registrierung erst, wenn Ihnen der **Registrierungsbrief** und Ihre **Zugangsdaten** für das Online-Banking (Eröffnungs-PIN und Anmeldename) vorliegen. Wenn Sie Ihr bisheriges Verfahren auf pushTAN umgestellt haben, behalten Sie Ihre gewohnten Zugangsdaten. Andernfalls erhalten Sie getrennt per Post einen PIN-Brief, der Ihre neuen Zugangsdaten enthält.

1 Laden Sie die S-pushTAN-App auf Ihr Smartphone.

2 Starten Sie die App und tippen „**Jetzt einrichten**“ → „**Registrierungsbrief erhalten**“ → „**Weiter**“ → „**Weiter**“ um die Zustellung von Push-Nachrichten zu erlauben.

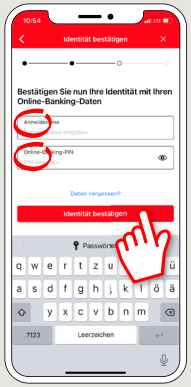


3 Im nächsten Schritt vergeben Sie ein Passwort für die App und bestätigen dieses durch wiederholte Eingabe.

Anschließend geben Sie an, ob Sie die App alternativ auch per TouchID oder FaceID öffnen wollen.

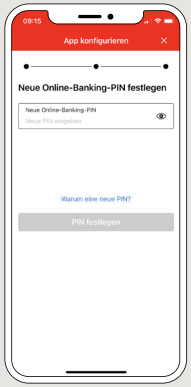
4 Erlauben Sie der App nun den Zugriff auf Ihre Kamera, um den QR-Code des Registrierungsbriefes zu scannen.

5 Im nächsten Schritt erfassen Sie Ihre Zugangsdaten für das Online-Banking.

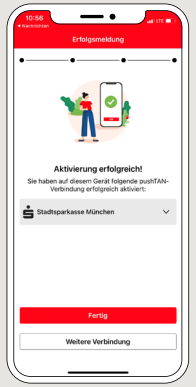


6 Wenn Sie von uns Erstzugangsdaten für das Online-Banking erhalten haben, ist nun die Änderung der mitgeteilten PIN nötig. Bestätigen Sie diese PIN anschließend durch wiederholte Eingabe.

Merken Sie sich diese PIN gut! Sie benötigen diese PIN auch für den Login via App „Sparkasse“ und www.sparkasse-hanau.de



7 Ihre pushTAN Verbindung wurde nun erfolgreich eingerichtet!



HABEN SIE NOCH FRAGEN? WIR HELFEN IHNEN GERNE WEITER.

Zentrale Service-Rufnummer: Unter **06181 298-0** sind wir **Mo-Fr von 8-19 Uhr** für Sie da.

Weiterführende Informationen zum pushTAN-Verfahren erhalten Sie unter: **www.sparkasse-hanau.de/pushtan**

Sparkasse Hanau | Am Markt 1 | 63450 Hanau | Telefon: 06181 298-0 | E-Mail: info@sparkasse-hanau.de | www.sparkasse-hanau.de

November 2022

Sparkasse Hanau
Telefon: 06181 298-0
www.sparkasse-hanau.de

Hinweise für mehr Sicherheit im Internet

Bevor Sie Online-Banking nutzen oder Ihre Kreditkarte im Internet einsetzen, nehmen Sie sich bitte einige Minuten Zeit für die nachfolgenden wichtigen Informationen.

Fit für das Internet

Wer die wichtigsten Grundregeln beachtet, kann sich gegen Angriffe aus dem Internet weitestgehend schützen. Erläuterungen, wie Sie Betrugsversuche erkennen, Ihren Computer und den Zugang zum Internet absichern sowie wichtige Hinweise zu aktuellen Betrugsversuchen erhalten Sie auf www.sparkasse-hanau.de/sicherheit

- Aktualisieren Sie regelmäßig Ihr Betriebssystem und Ihre eingesetzten Programme.
- Arbeiten Sie nicht mit Administratorrechten auf Ihrem Computer.
- Nutzen Sie eine Firewall und einen Virenscanner und halten Sie diese immer aktuell.
- Löschen Sie nach Geschäften über das Internet immer Browserverlauf und Cache.
- Erledigen Sie Bankgeschäfte oder Online-Einkäufe nie über ein fremdes WLAN.
- Hinterlegen Sie keine persönlichen Zugangsdaten auf fremden Portalen, geben Sie diese auch nicht an Dritte weiter.
- Achten Sie darauf, dass Sie Online-Geschäfte nur über eine verschlüsselte Verbindung tätigen.
- Für Online-Banking oder einen Einkauf im Internet geben Sie die Internet-Adresse immer von Hand ein.
- Öffnen Sie keine Dateianhänge in E-Mails von unbekannten Absendern.
- Folgen Sie nie Aufforderungen, die Sie per E-Mail oder Telefon erhalten, Zahlungsaufträge zu bestätigen.

Kein Mitarbeiter der Sparkasse wird Sie auffordern, Ihre Zugangsdaten zum Online-Banking preiszugeben – weder per E-Mail, per Fax, per Telefon noch persönlich.

Sicheres Online-Banking und Bezahlen im Internet

Diese Regeln sollten Sie unbedingt beachten:

Besser: vorsichtig sein

Mit dem Wischen des Buttons *Auftrag freigeben* bzw. der Eingabe einer TAN wird im Regelfall eine Überweisung von Ihrem Konto bestätigt. Denken Sie daran, wenn Sie nach Ihren Bankdaten gefragt werden oder aufgefordert werden, einen Auftrag freizugeben oder eine TAN einzugeben, ohne dass Sie eine Transaktion in Auftrag geben wollen.

Misstrauisch sein

Wenn Ihnen etwas seltsam vorkommt, brechen Sie im Zweifel lieber die Aktion ab. Ihre Sparkasse wird Sie z. B. niemals auffordern, Auftragsfreigaben oder eine TAN-Eingabe für Gewinnspiele, Sicherheits-Updates oder vermeintliche Rücküberweisungen zu erteilen.

Sorgfältig: Daten kontrollieren

Auf dem Display Ihres TAN-Generators oder Ihres Mobiltelefons werden Ihnen die wichtigsten Auftragsdaten angezeigt. Falls die Anzeigedaten nicht mit Ihrem Auftrag übereinstimmen, brechen Sie die Aktion ab.

Geschlossen: sichere Eingabe

Wenn Sie Ihre Anmeldedaten zum Online-Banking eingeben: Schauen Sie immer, ob das Schlosssymbol im Browser vorhanden ist.

Immer: aufmerksam bleiben

Kontrollieren Sie regelmäßig die Umsätze auf Ihrem Konto. Das geht im Online-Banking und mit Ihren Kontoauszügen. Nur so erkennen Sie unberechtigte Abbuchungen rechtzeitig und fristgerecht.

Eingrenzen: Tageslimit

Legen Sie ein Tageslimit für Ihre Transaktionen im Online-Banking fest. Mit Ihrem persönlichen Verfügungsrahmen schränken Sie die Möglichkeiten unberechtigter Zugriffe ein.

Im Zweifel: Zugang sperren

Falls Sie den Verdacht haben, dass mit der Banking-Anwendung irgendetwas nicht stimmt: Sperren Sie Ihren Zugang. Wenden Sie sich dazu entweder direkt an Ihre Sparkasse oder wählen Sie rund um die Uhr den Sperr-Notruf 116 116 – deutschlandweit kostenfrei. Auch aus dem Ausland ist der Sperr-Notruf erreichbar.