Mastercard® Identity Check™ und Visa Secure

Jetzt schnell und einfach für Mastercard® Identity Check™ oder Visa Secure registrieren und sicher im Internet bezahlen.

Mastercard® Identity Check™ / Visa Secure für sicheres Bezahlen im Internet mit Ihrer Mastercard® oder Visa Karte

Sie kaufen gern bequem von zu Hause aus ein? Sie möchten jederzeit flexibel shoppen oder Ihre Reise buchen? Die Debitkarten und Kreditkarten Ihrer Volksbank Raiffeisenbank sind genau die richtigen Bezahlmittel dafür. Mit den Bezahl- und Authentifizierungsverfahren Mastercard® Identity Check™ und Visa Secure kaufen Sie bei teilnehmenden Online-Händlern sicher ein. Sie erkennen sie an der Verwendung dieser Zeichen:

Wie funktioniert das Bezahlverfahren?
Um Ihre Online-Zahlungen mit Ihrer Mastercard oder Visa Karte zu schützen, werden die Daten der Kauftransaktion via Push-Nachricht in der passenden App oder als SMS auf Ihr Mobiltelefon gesendet. Innerhalb der App kann die Freigabe der Transaktion direkt erfolgen. Entweder durch Eingabe des Freigabe-Codes oder per Face-ID oder Fingerabdruck. Die empfangene TAN aus dem SMS-Verfahren geben Sie während des Bezahlvorgangs im Online-Shop des teilnehmenden Händlers ein und bestätigen damit die Transaktion.

Registrieren Sie sich jetzt für mehr Sicherheit
Die Registrierung Ihrer Mastercard oder Visa Karte für das sichere Verfahren können Sie einfach und kostenlos auf der zentralen Internetseite **www.sicher-online-einkaufen.de** oder auf der Website Ihrer Volksbank Raiffeisenbank vornehmen. Egal, ob Sie ein neuer Nutzer oder bereits registriert sind – wir empfehlen Ihnen, dort das sichere Bezahlen über die VR SecureGo plus App zu wählen. Denn so sind Sie für alle zukünftigen technischen Weiterentwicklungen gerüstet.

Die Registrierung für das sichere Bezahlverfahren dauert nur wenige Minuten
Nutzen Sie die nebenstehende Kurzbeschreibung für den Registrierungsprozess oder die ausführliche Anleitung auf den Folgeseiten. Hier begleiten wir Sie Schritt für Schritt durch die Bildschirmmasken des Registrierungsprozesses.

Schnelle Registrierung in vier Schritten

1. Registrierungsseite aufrufen und Aktivierungscode anfordern

Fordern Sie Ihren Aktivierungscode über die zentrale Website www.sicher-online-einkaufen.de an. Alternativ finden Sie auch den Zugang über die Website Ihrer Volksbank Raiffeisenbank.

Falls Sie eine neue Mastercard oder Visa Karte (Debitkarte oder Kreditkarte) beantragt haben, wird Ihnen Ihr persönlicher Aktivierungscode automatisch wenige Tage nach Ihrer Mastercard oder Visa Karte zugesendet. Gleiches gilt, wenn Sie eine Erneuerungskarte erhalten und die Karte bisher nicht registriert hatten.

2. Aktivierungscode erhalten

Nach wenigen Tagen liegt Ihr persönlicher Aktivierungscode in der Post. Gehen Sie erneut auf die oben genannte Internetseite und geben Sie Ihre Kartennummer sowie den Aktivierungscode ein.

3. Wunschverfahren wählen

Wählen Sie Ihr sicheres Wunschverfahren.

App-Verfahren
Laden Sie sich die VR SecureGo plus App im App Store herunter. Öffnen Sie sie, legen Sie Ihren persönlichen Freigabe-Code fest und geben Sie auf der oben genannten Internetseite Ihre in der App angezeigte neue „Kreditkarten-Kennung“ ein.

SMS-Verfahren
Möchten Sie die zugesandte TAN für eine Kaufbestätigung per SMS erhalten, dann wählen Sie auf der oben genannten Internetseite das „SMS-Verfahren“ aus und hinterlegen dort Ihre Mobilfunknummer sowie eine gewünschte Sicherheitsfrage.

4. Bestätigen – fertig!

Im letzten Schritt bestätigen Sie bitte die Registrierung mit der TAN, die Sie unmittelbar als Nachricht erhalten. Jetzt können Sie bei teilnehmenden Händlern sicher im Internet einkaufen! Übrigens: Auf Wunsch können Sie auf unterstützten Geräten die VR SecureGo plus App auch per Fingerabdruck oder Gesichtserkennung entsperren.

Zu den App Stores gelangen Sie bequem über die folgenden QR-Codes:

Apple App Store

Google Play Store

Anschaulich erklärt

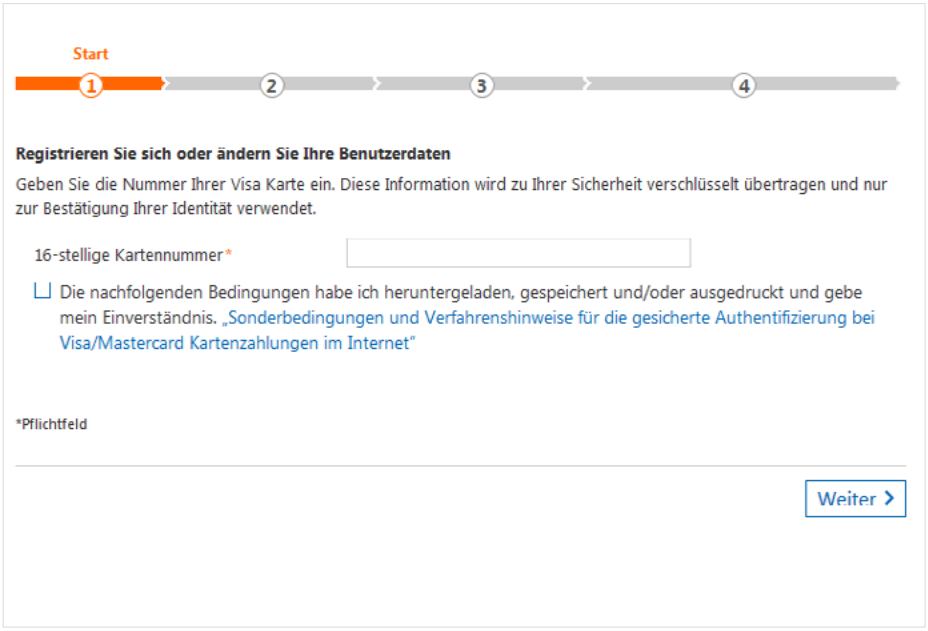
Besuchen Sie doch mal die zentrale Website www.sicher-online-einkaufen.de oder die Internetseite Ihrer Volksbank Raiffeisenbank und erleben Sie Registrierung und Einkauf mit dem sicheren Bezahlverfahren in bewegten Bildern.

Auf den folgenden Seiten führen wir Sie einfach und verständlich durch die Registrierungsmasken für die Bezahl- und Authentifizierungsverfahren Mastercard® Identity Check™ und Visa Secure. So kommen Sie schnell und bequem zu mehr Sicherheit beim Online-Shopping.

Schritt 1: Start auf der Registrierungsseite

Besuchen Sie die Registrierungsseite für Mastercard® Identity Check™ oder Visa Secure auf der Internetseite Ihrer Volksbank Raiffeisenbank oder starten Sie die Registrierung über die zentrale Website www.sicher-online-einkaufen.de.

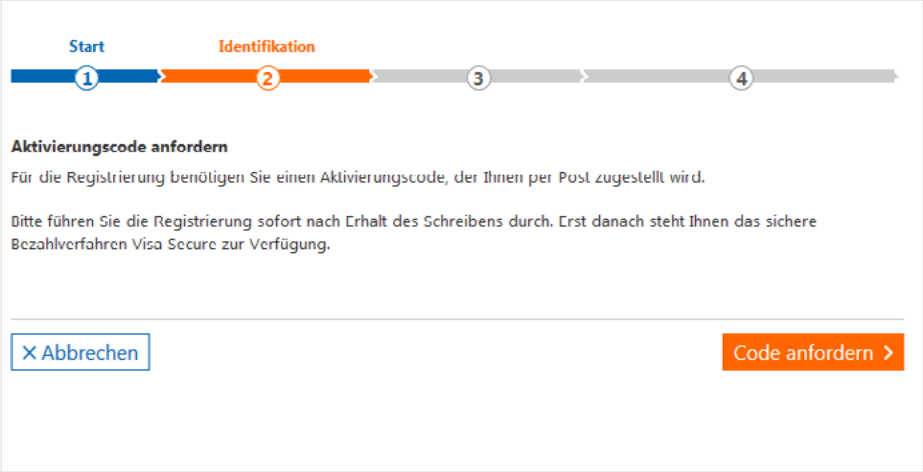
Die nachfolgenden Bildschirmmasken sind für Mastercard® Identity Check™ und Visa Secure inhaltlich identisch.



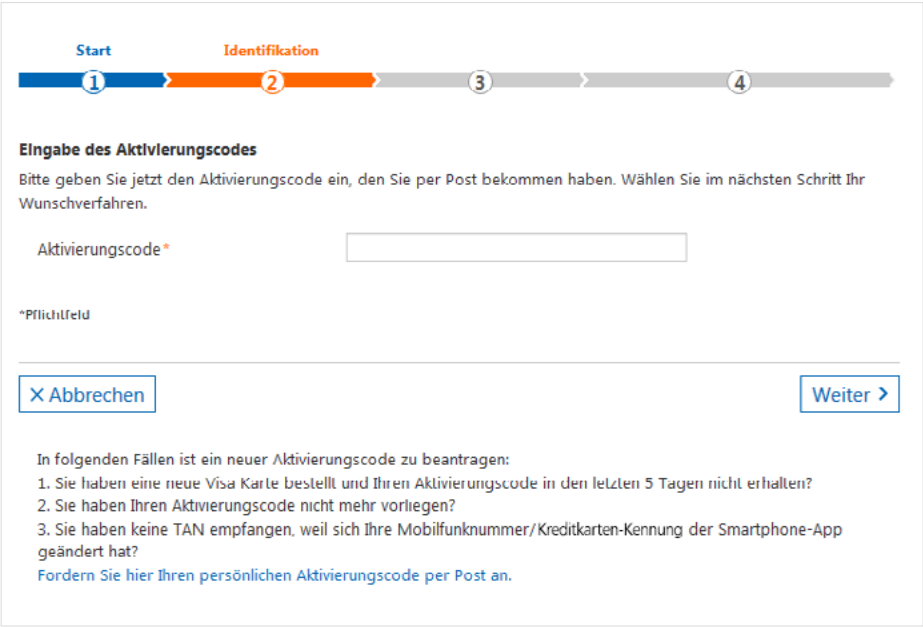
Nach Eingabe Ihrer Kreditkartennummer setzen Sie bitte ein Häkchen im entsprechenden Kasten, wenn Sie sich mit den Sonderbedingungen für die Teilnahme am Verfahren einverstanden erklären.

Schritt 2: Aktivierungscode anfordern und eingeben

Fordern Sie über den Button „Code anfordern“ Ihren Aktivierungscode an. Dieser wird Ihnen per Post oder bei Nutzung der elektronischen Umsatzaufstellung in Ihrem elektronischen Postfach zugestellt. Sofern Sie eine neue Mastercard oder Visa Karte (Debitkarte oder Kreditkarte) beantragt haben oder eine Erneuerungskarte erhalten, wird Ihnen Ihr Aktivierungscode automatisch zugestellt. Sie führen die Registrierung im nächsten Schritt fort. Mithilfe des Codes können Sie Ihre Karte registrieren und das gewünschte Sicherheitsverfahren auswählen.



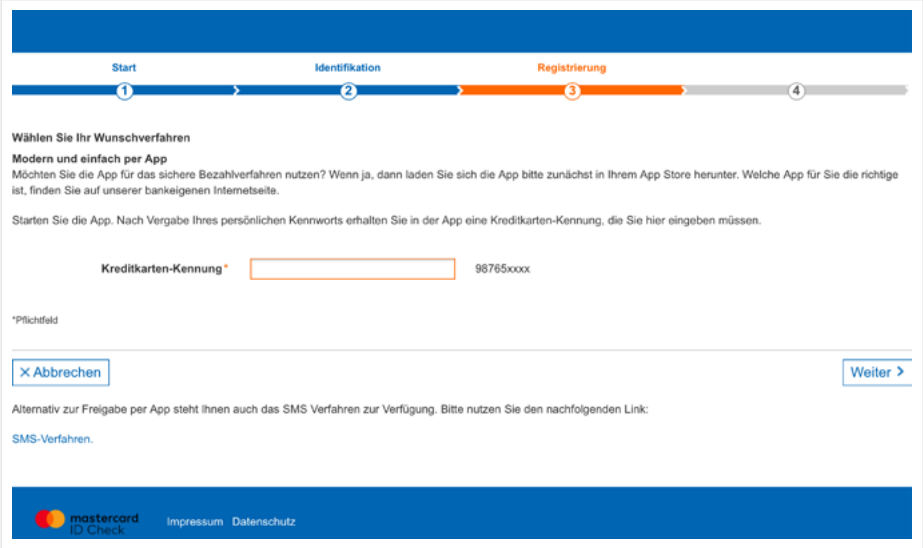
Registrieren Sie sich schnellstmöglich, nachdem Sie den Aktivierungscode erhalten haben, um direkt für Ihren nächsten Online-Einkauf bei teilnehmenden Händlern startklar zu sein. Der Aktivierungscode wird einmalig benötigt und ermöglicht Ihnen die Hinterlegung Ihrer Kreditkarten-Kennung für die VR SecureGo plus App oder Ihrer Mobilfunknummer und Sicherheitsfrage für das SMS-Verfahren. Nach der Registrierung wird der Aktivierungscode nicht mehr benötigt. Sie haben Ihren Aktivierungscode bereits angefordert, aber nicht mehr zur Hand? Kein Problem – über diese Seite haben Sie die Möglichkeit, einen neuen anzufordern.



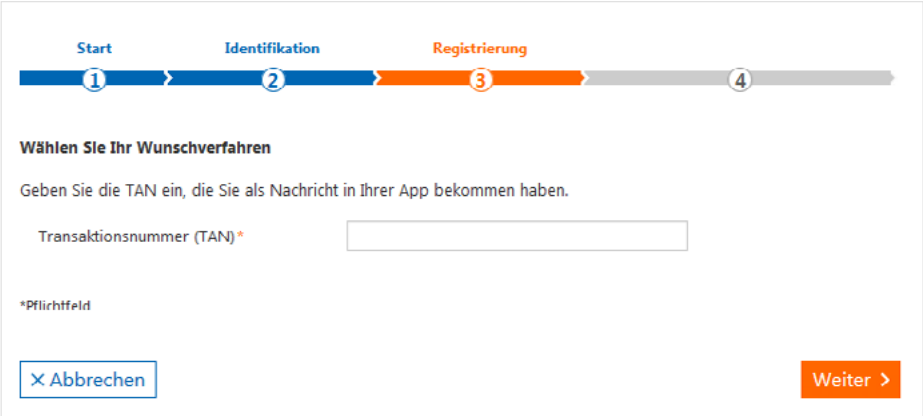
Für den Fall, dass Sie den Aktivierungscode selbst angefordert haben, beginnt die Aktivierung genauso wie die Registrierung in Schritt 1. Geben Sie noch einmal Ihre Kartennummer ein und bestätigen Sie, dass Sie die Sonderbedingungen akzeptieren. Sie werden danach automatisch auf die nebenstehende Maske geführt und geben den Aktivierungscode ein, den Sie per Post oder in Ihrem elektronischen Postfach erhalten haben.

Schritt 3 bei Verwendung des App-Verfahrens: Eingabe der Kreditkarten-Kennung

Wenn Sie ein Smartphone nutzen, empfehlen wir Ihnen die Verwendung der VR SecureGo plus App, die Sie sich bequem aus dem App Store herunterladen können. Nutzen Sie dazu ganz einfach die QR-Codes auf Seite 3.



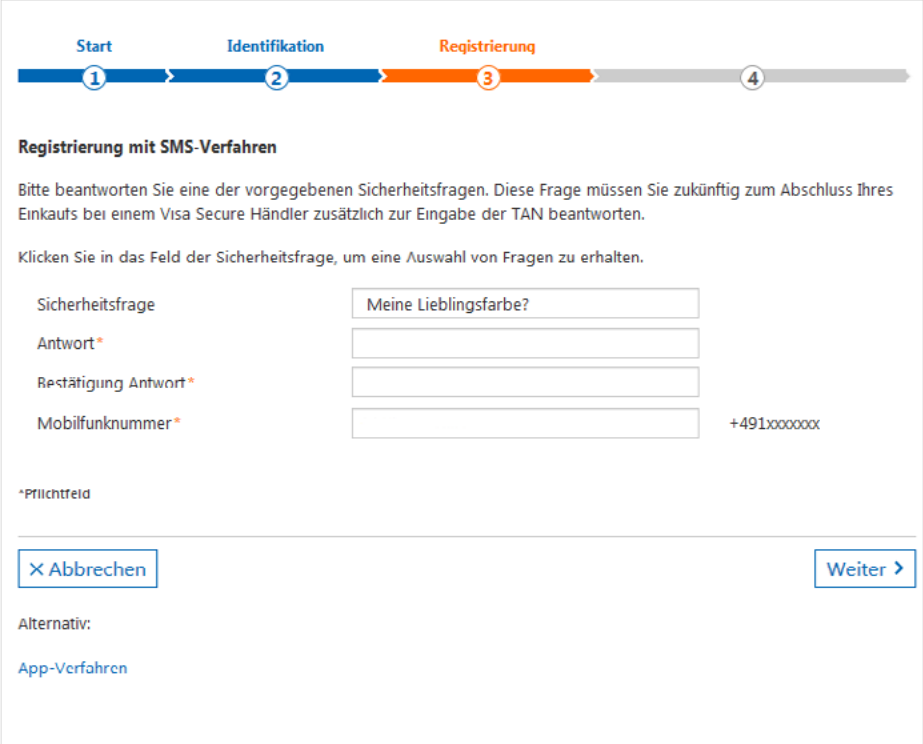
Geben Sie die „Kreditkarten-Kennung ", die Ihnen in der App angezeigt wird, in der vorgesehenen Schreibweise ein.



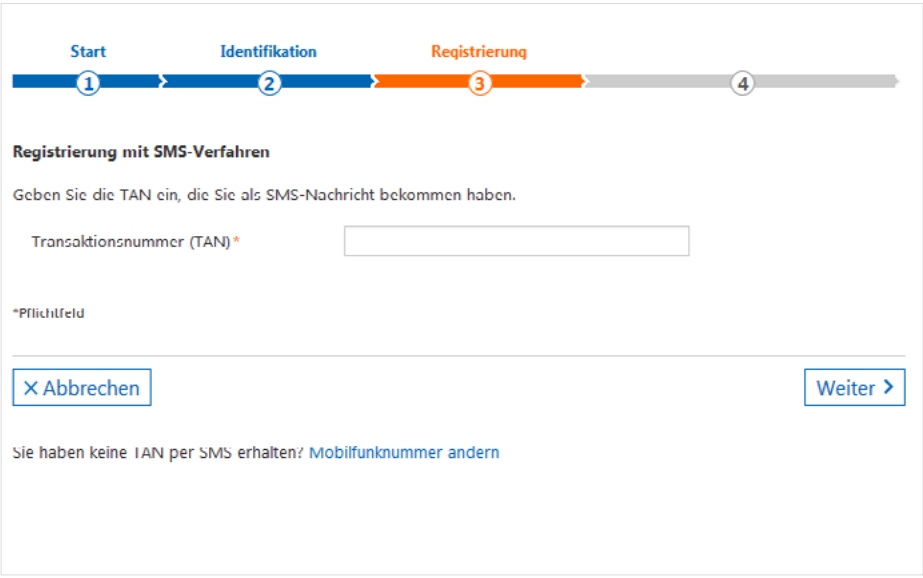
Zur Bestätigung erhalten Sie eine TAN in Ihrer VR SecureGo plus App. Prüfen Sie die angezeigten Informationen und geben Sie die TAN im Eingabefeld ein.

Schritt 3 bei Verwendung des SMS-Verfahrens: Auswahl der Sicherheitsfrage

Sollten Sie kein Smartphone, sondern nur ein einfaches Mobiltelefon besitzen, nutzen Sie bitte das SMS-Verfahren.



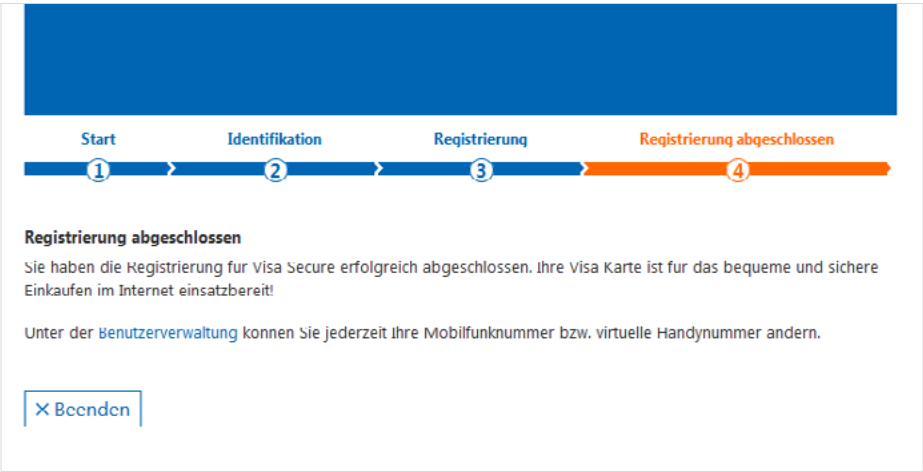
Klicken Sie in das Feld der Sicherheitsfrage und wählen Sie eine für Sie passende Frage aus. Beantworten Sie die Frage und bestätigen Sie die Antwort. Tragen Sie nun noch Ihre Mobilfunknummer in der vorgesehenen Schreibweise ein. Sie erhalten jetzt eine TAN per SMS.



Tragen Sie die erhaltene TAN ein und bestätigen Sie Ihre Eingabe, indem Sie auf den Button „Weiter" klicken. Sollten Sie keine SMS erhalten haben, überprüfen Sie bitte die eingegebene Mobilfunknummer. Über „Mobilfunknummer ändern" können Sie Ihre Rufnummer ändern.

Schritt 4: Sie sind jetzt startklar für Ihre Einkäufe im Internet!

Ihre Registrierung ist nun abgeschlossen. In der Benutzerverwaltung können Sie jederzeit das Verfahren wechseln oder Ihre Mobilfunknummer bzw. Ihre Kreditkarten-Kennung ändern.



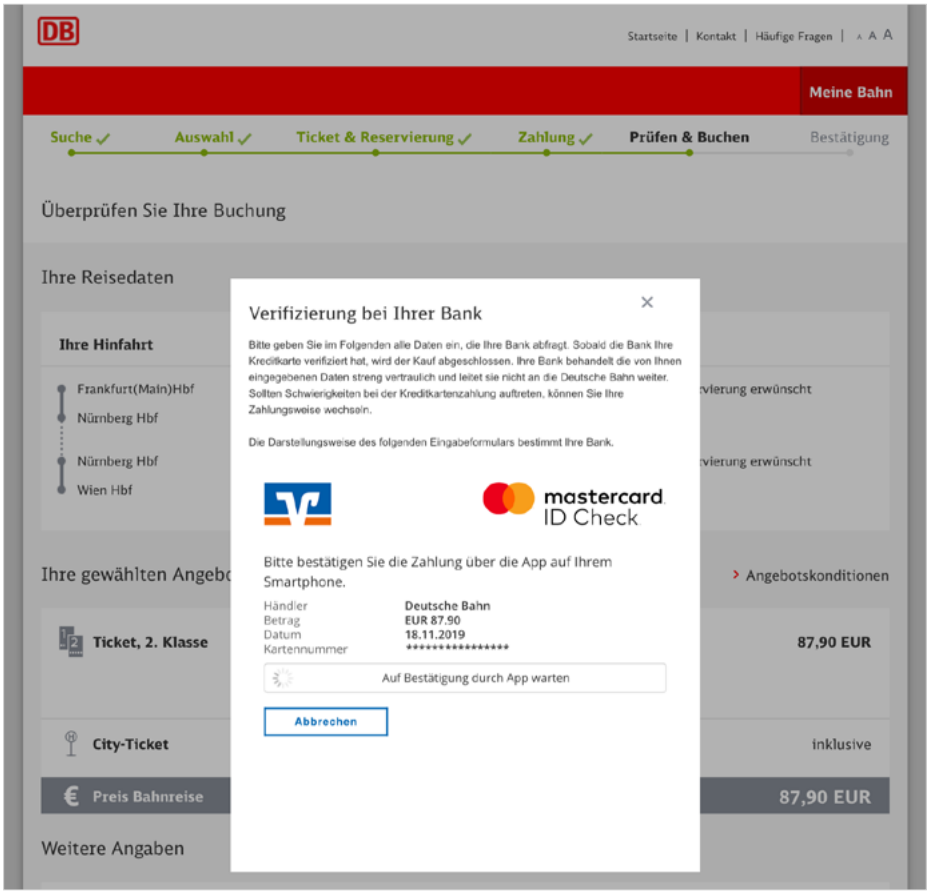
So schließen Sie Ihren Online-Einkauf sicher ab

In der Internetwelt ist es besonders wichtig, dass sich Käufer und Händler gegenseitig vertrauen können. Dafür sorgen die sicheren Bezahlverfahren Mastercard® Identity Check™ und Visa Secure mit einer eindeutigen Authentifizierung. Mit Ihrer erfolgreichen Registrierung erfahren Sie ab jetzt bei teilnehmenden Händlern volle Sicherheit beim Bezahlvorgang. In nur vier Schritten schließen Sie Ihren Einkauf sicher ab:

1. Kartennummer eingeben
Geben Sie Ihre Kartennummer im Online-Shop eines Händlers, der das Verfahren unterstützt, ein, um die sichere Authentifizierung zu initiieren.

2. Transaktion prüfen
Sie erhalten nun eine Nachricht mit den Transaktionsdaten via VR SecureGo plus App oder per SMS inklusive der individuellen TAN auf Ihr Mobiltelefon. Prüfen Sie sorgfältig, ob die Daten mit denen des von Ihnen beabsichtigten Kaufs übereinstimmen (siehe Musterabbildungen rechts).

3. TAN eingeben
Wenn die Daten richtig sind, bestätigen Sie die Zahlung in der VR SecureGo plus App oder geben Sie Ihre TAN in die Freigabemaske ein. Als Nutzer des SMS-Verfahrens werden Sie außerdem gebeten, Ihre Sicherheitsfrage zu beantworten. Anschließend werden Sie zurück zum Online-Shop des Händlers geleitet.

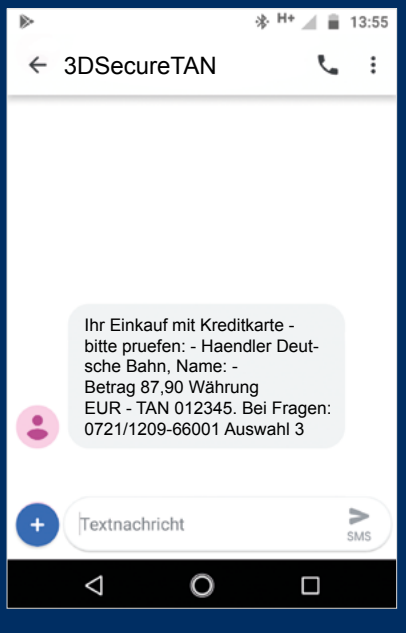


4. Zahlung freigeben
Geben Sie nun Ihre Zahlung frei. Damit ist Ihr Einkauf sicher abgeschlossen.

Prüfen Sie die Transaktionsdaten auf Ihrem Mobiltelefon für einen sicheren Einkauf im Internet.

Beispiel für das App-Verfahren

Beispiel für das SMS-Verfahren



Gern stehen wir Ihnen für weitere Informationen zur Seite. Nachstehende Tipps helfen bei der Beantwortung möglicher Fragen.

Sichere Freigabe Ihres Online-Einkaufs

Kontrollieren Sie die mit der Nachricht übermittelten Daten zum Händler und zum freizugebenden Umsatz stets sorgfältig. Sollte die Nachricht mit der Bestätigung nicht die Transaktionsdaten enthalten, die Sie erwarten, lehnen Sie die Zahlung in der App ab bzw. geben Sie die per SMS übermittelte TAN nicht ein, sondern wenden Sie sich an unseren 24 Stunden erreichbaren Kartenservice oder die Karten-Hotline unter der Telefonnummer 0721 1209-66001.

Sollten Sie unerwartet Bestätigungsnachrichten zur Freigabe von Transaktionen erhalten, die Sie nicht veranlasst haben, lassen Sie Ihre Karte sofort nach einem Anruf unter der gleichen Rufnummer sperren. Es handelt sich in einem solchen Fall vermutlich um den Versuch einer missbräuchlichen Verwendung.

Haben Sie Ihre TAN für das sichere Bezahlverfahren mehr als dreimal falsch eingegeben? In diesem Fall wird Ihre Kennung gesperrt. Bitte wenden Sie sich dann zwecks Entsperrung telefonisch an unseren Service zu den sicheren Bezahlverfahren oder an die Filiale Ihrer Volksbank Raiffeisenbank.

Zustellungsverfahren oder Endgerät ändern
Sie können jederzeit zwischen dem App- und SMS-Verfahren über die Benutzerverwaltung in den Registrierungsmasken wechseln. Bei Hinterlegung einer Mobilfunknummer und Sicherheitsfrage erhalten Sie Transaktionsdaten und TAN per SMS, bei Hinterlegung Ihrer Kreditkarten-Kennung werden Ihnen die Transaktionsdaten zur Freigabe in die VR SecureGO plus App zugestellt.

Möchten Sie von der VR-SecureCARD auf die VR SecureGo plus App wechseln?
- Installieren Sie die VR SecureGo plus App auf dem (neuen) Gerät.
- Melden Sie sich über die Website Ihrer Bank oder über sicher-online-einkaufen.de an. Die erforderliche TAN erhalten Sie in Ihrer existierenden VR-SecureCARD App.
- Rufen Sie den Punkt „Registrierung verwalten/Verfahren ändern" auf.
- Hinterlegen Sie nun die Kreditkarten-Kennung, die in der VR SecureGo plus App unter den Einstellungen angezeigt wird.
- Geben Sie die erhaltene TAN ein, um die richtige Zuordnung Ihrer VR SecureGo plus App zu bestätigen.
- Die VR-SecureCARD können Sie nun auf dem (alten) Gerät deinstallieren.

Bezahlen im Internet: damit das Verfahren sicher bleibt

Sicherer Karteneinsatz im E-Commerce. Information über das sichere Bezahlen im Internet
Sie können mit Ihren Debitkarten oder Kreditkarten von Mastercard oder Visa im Internet Waren und Dienstleistungen bezahlen. Gemäß den Vertragsbedingungen dürfen bei einer Zahlung mit Ihrer Mastercard oder Visa Karte im Internet nur folgende Daten angegeben werden: Ihr Name, die Kartenmarke (Mastercard/Visa), die Kartennummer, das Laufzeitende der Karte und die auf der Kartenrückseite genannte dreistellige Kartenprüfziffer.

Bitte geben Sie niemals die PIN an, die Sie für Zahlungen an Kassenterminals oder zum Geldabheben am Automaten erhalten haben! Unerwartete Nachrichten zur Zahlungsbestätigung in Ihrer VR SecureGo plus App lehnen Sie bitte stets ab. Eine E-Commerce-TAN, die Sie zur Authentifizierung der Zahlung auf Ihrem Mobiltelefon erhalten, geben Sie nur ein, wenn Sie die gleichzeitig mit dieser TAN eingetroffenen Daten zu Zahlungsempfänger, Betrag und Währung geprüft haben und sie mit den Angaben zur auszuführenden Zahlung übereinstimmen.

Allgemeiner Tipp für Ihre Endgeräte
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt unter https://www.bsi-fuer-buerger.de die nachfolgenden Maßnahmen zur Absicherung gegen Angriffe aus dem Internet:

Kernmaßnahmen

1. **Halten Sie Ihre Software aktuell**
   Verwenden Sie eine aktuelle Version des Betriebssystems und der von Ihnen installierten Programme. Nutzen Sie wenn möglich die Funktion zur automatischen Aktualisierung, die oft die Standardeinstellung ist. Spielen Sie andernfalls umgehend die Sicherheitsupdates für Ihre Software ein, insbesondere für Ihren Webbrowser und Ihr Betriebssystem. Deinstallieren Sie nicht benötigte Programme. Je weniger Anwendungen Sie nutzen, desto kleiner ist die Angriffsfläche Ihres gesamten Systems.
2. **Nutzen Sie Virenschutz und Firewall**
   In den gängigen Betriebssystemen sind ein Virenschutz und eine Firewall integriert, die schon in der Standardkonfiguration Angriffe aus dem Internet erschweren. Aktivieren Sie diese oder verwenden Sie ein Virenschutzprogramm eines anderen Anbieters. Bedenken Sie, dass diese Maßnahme nur begleitend wirksam sein kann. Ihre Anwendung verringert nicht die Bedeutung der übrigen Tipps dieser Broschüre. Lassen Sie sich nicht durch einen aktivierten Virenschutz oder die Firewall zu Unvorsicht verleiten, sie garantieren keine vollständige Sicherheit.
3. **Legen Sie unterschiedliche Benutzerkonten an**
   Schadprogramme haben die gleichen Rechte auf dem PC wie das Benutzerkonto, über das sie auf den Rechner gelangt sind. Daher sollten Sie nur dann mit Administratorrechten arbeiten, wenn es unbedingt erforderlich ist. Richten Sie für alle Nutzerinnen oder Nutzer des PCs unterschiedliche, passwortgeschützte Benutzerkonten ein. Vergeben Sie für diese Konten nur die Berechtigungen, die die jeweilige Nutzerin oder der jeweilige Nutzer

für seine Arbeit braucht. So werden auch private Dateien vor dem Zugriff anderer Benutzerinnen oder Benutzer geschützt. Surfen Sie im Internet mit einem der eingeschränkten Benutzerkonten und nicht in der Rolle des Administrators.

4. **Seien Sie zurückhaltend mit der Weitergabe persönlicher Daten**
   Online-Betrüger steigern ihre Erfolgsraten, indem sie ihre Opfer individuell ansprechen: Zuvor ausspionierte Daten, wie etwa Surfgewohnheiten oder Namen aus dem persönlichen Umfeld, werden dazu genutzt, Vertrauen zu erwecken. Persönliche Daten gelten heute als Währung im Netz und so werden sie auch gehandelt. Auch die unbeabsichtigte Weitergabe persönlicher Daten in offenen Netzen sollte vermieden werden. Nutzen Sie in öffentlichen WLAN-Hotspots nach Möglichkeit ein mit Ihrem Heimnetz verbundenes VPN (Virtuelles Privates Netzwerk), da sonst unverschlüsselt übertragene Daten von Dritten mitgelesen werden können. Gleichzeitig schützt ein VPN auch vor einer Reihe weiterer Angriffe auf Ihren Rechner und die darauf gespeicherten Daten.

Ergänzende Maßnahmen

5. **Verwenden Sie einen aktuellen Webbrowser**
   Deaktivieren Sie Komponenten und Plug-ins in den Einstellungen Ihres Browsers. Weitere Einstellungen (unter anderem „privater Modus“, „Verlauf löschen“, „Cookies nicht für Drittanbieter zulassen“) verringern die Speicherung von vertraulichen Informationen, die Aufschlüsse über Sie und Ihr Verhalten im Web zulassen. Nutzen Sie ein Programm zum Blockieren von Werbung, um sich vor Malvertising, also der Verbreitung von Malware über Werbeeinblendungen, zu schützen. Tragen Sie die Adressen für besonders sicherheitskritische Webseiten, etwa für das Online-Banking, zunächst von Hand in die Adresszeile des Browsers ein und speichern Sie die so eingegebene Adresse als Lesezeichen, das Sie ab dann für den sicheren Zugang nutzen. Weitere Empfehlungen zur sicheren Konfiguration Ihres Browsers hat das BSI hier für Sie zusammengestellt.
6. **Nutzen Sie unterschiedliche Passwörter, die Sie bei Bedarf ändern**
   Bewahren Sie alle Passwörter und Benutzernamen sicher auf und ändern Sie schnellstmöglich alle Passwörter, die in falsche Hände geraten sein könnten. Verwenden Sie unterschiedliche, nicht erratbare Passwörter für die verschiedenen Anwendungen und ändern Sie die von den Herstellern voreingestellten Passwörter vor der ersten Nutzung. Es ist wichtig, dass Sie sich ein Passwort gut merken können. Grundsätzlich gilt: je länger, desto besser. Das Passwort sollte mindestens acht Zeichen lang sein, nicht im Wörterbuch vorkommen und aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern bestehen. Dort, wo eine Zwei-Faktor-Authentisierung angeboten wird, können Sie damit den Zugang zu Ihrem Account absichern. Ein Passwortmanager, wie zum Beispiel KeePass, kann die Handhabung unterschiedlicher Passwörter erleichtern. Geben Sie Ihre Passwörter nicht an Dritte weiter.
7. **Schützen Sie Ihre Daten durch Verschlüsselung**
   Übertragen Sie Ihre persönlichen Daten ausschließlich über eine verschlüsselte Verbindung, beispielsweise durch die Nutzung des sicheren Kommunikationsprotokolls https. Sie erkennen dies an der von Ihnen aufgerufenen Internetadresse, die stets mit https beginnt, und an dem kleinen geschlossenen Schloss-Symbol in der Adresszeile Ihres Webbrowsers. Schützen Sie Ihre vertraulichen E-Mails mit Verschlüsselung. Wenn Sie die Übertragungstechnologie Wireless LAN (WLAN) nutzen, achten Sie hier besonders auf die Verschlüsselung des Funknetzes. Wählen Sie in Ihrem Router den Verschlüsselungsstandard WPA3 oder, wenn dieser noch nicht unterstützt wird, bis auf Weiteres WPA2. Wählen Sie ein komplexes, mindestens 20 Zeichen langes Passwort.
8. **Seien Sie vorsichtig bei E-Mails und deren Anhängen**
   Verzichten Sie, wenn möglich, auf die Darstellung und Erstellung von E-Mails im HTML-Format, und seien Sie vorsichtig beim Öffnen von E-Mail-Anhängen. Besonders wichtig sind diese beiden Tipps bei E-Mails, deren Absender Ihnen nicht bekannt ist, denn Schadprogramme werden oft über in E-Mails integrierte Bilder oder Dateianhänge verbreitet. Im Zweifelsfall fragen Sie lieber beim Absender nach, ob der Anhang tatsächlich von ihm stammt. Nutzen Sie dabei aber nicht die in der E-Mail angegebenen Kontaktmöglichkeiten. Sie könnten gefälscht sein.
9. **Laden Sie Daten nur aus vertrauenswürdigen Quellen herunter**
   Seien Sie vorsichtig, wenn Sie etwas aus dem Internet herunterladen. Vergewissern Sie sich vor dem Download von Programmen, ob die Quelle vertrauenswürdig ist. Nutzen Sie nach Möglichkeit die Webseite des jeweiligen Herstellers zum Download.
10. **Fertigen Sie regelmäßig Sicherheitskopien an**
    Kommt es trotz aller Schutzmaßnahmen zu einer Infektion des PCs, können wichtige Daten verloren gehen. Um den Schaden möglichst gering zu halten, ist es wichtig, regelmäßig Sicherungskopien Ihrer Dateien auf externen Festplatten, USB-Sticks oder DVD zu erstellen. Diese Datenträger sollten nur bei Bedarf mit dem PC verbunden sein. Cloud-Dienste können für Sicherungskopien von verschlüsselten Daten herangezogen werden.

Sofern Sie den Verdacht haben, dass Ihre Kreditkartendaten auf Ihrem Computer ausgespäht wurden, sperren Sie Ihre Mastercard oder Visa Karte(n) sofort telefonisch unter der auf dem Übersendungsschreiben, der Kartenrückseite und der Umsatzaufstellung mitgeteilten 24-Stunden-Rufnummer 0721 1209-66001 (Sperrannahme-Service). Lassen Sie Ihre Karte(n) ebenfalls unverzüglich sperren, wenn Sie den Verlust der Karte(n) oder eine missbräuchliche

Nutzung der Karte(n), der Kartendaten oder eines Legitimationsmediums feststellen oder einen entsprechenden Verdacht haben (vgl. Ziffer 6.4 der Vertragsbedingungen). Informationen zur Beseitigung von Schadsoftware auf Ihrem Computer finden Sie ebenfalls auf der Website des Bundesamts für Sicherheit in der Informationstechnik (https://www.bsi-fuer-buerger.de) unter dem Stichwort „Infektionsbeseitigung". Darüber hinaus können Sie sich jederzeit auf der Internetseite des BSI über aktuelle Sicherheitswarnungen und Sicherheitsupdates informieren.

Telefonnummern und Versanddauer
Prinzipiell können für VR SecureGo plus und für das SMS-Verfahren sowohl deutsche als auch ausländische Mobilfunknummern erfasst werden. Bei der Verwendung des SMS-Verfahrens hängt die Dauer, die bei Roaming bzw. Versand ins Ausland für die Zustellung einer TAN benötigt wird, von den Netzbetreibern ab. Bei Verwendung der VR SecureGo plus App im Ausland benötigen Sie eine ggf. kostenpflichtige Datenverbindung über Mobilfunknetz oder WLAN, um die Nachrichten zur Freigabe Ihrer Zahlung zu empfangen.

Information über die Buchung von Umsätzen
Im Online-Banking haben Sie jederzeit die Möglichkeit, die gebuchten Umsätze und den Saldo Ihrer Karte(n) einzusehen. Darüber hinaus erhalten Sie, je nach Abrechnungsart Ihrer Mastercard oder Visa Karte, monatlich eine Umsatzaufstellung, die auf Unstimmigkeiten zu prüfen ist.

Information und Kontaktaufnahme im Fall von Missbrauchsverdacht oder neuen Sicherheitsmaßnahmen
Ihre genossenschaftliche Mastercard oder Visa Karte ist ein sicheres Zahlungsmittel. Vor Betrug schützen Sie auch unsere Präventions- und Monitoringsysteme, die darauf ausgerichtet sind, Auffälligkeiten beim Karteneinsatz frühzeitig aufzudecken. Als Kriterien dienen diesen Systemen allgemeine Erfahrungswerte, der Abgleich mit Vorfällen aus der jüngsten Zeit und Ihr bisheriger Karteneinsatz. Es kann daher in Einzelfällen vorkommen, dass eine beabsichtigte Transaktion einer Überprüfung bedarf oder nicht genehmigt wird. Je nach Ergebnis dieses Abstimmungsprozesses können Sie anschließend Ihre Karte wieder einsetzen, oder sie wird, bei Verdacht auf Missbrauch, gesperrt und durch eine neue ersetzt.

Unser Service für Sie
Wir informieren Sie bei Vorfällen, die die Sicherheit Ihrer Karte(ndaten) betreffen, telefonisch, per Brief, über eine Mitteilung auf dem Kontoauszug oder, sofern Sie ihn nutzen, über den elektronischen Postkorb in Ihrem Online-Banking.

Wichtig
Per E-Mail versenden wir keine sicherheitsrelevanten Nachrichten und fordern Sie auf diesem Weg auch niemals auf, Ihre Mastercard oder Visa Karte zu entsperren, Sicherheitsmerkmale zu ändern oder Ähnliches! Informationen zu allgemeinen Sicherheitsmaßnahmen (zum Beispiel Warnung vor gefälschten E-Mails, sogenannte „Phishing-E-Mails") erhalten Sie auch auf unserer Internetseite.

Auffälligkeiten, Unregelmäßigkeiten bei einer Transaktion über einen Internetzahlungsdienst oder einen Missbrauchsverdacht können Sie jederzeit über den Sperrannahme-Service unter der Nummer 0721 1209-66001 telefonisch melden.

November 2020