VR Bank Fulda eG

Partner der Region

Tipps zur Sicherheit beim OnlineBanking

Mit „Sicherheit“ durch Ihren Alltag“!

Als Ihr Finanzpartner sind wir technisch nicht in der Lage für Ihre Sicherheit auf Ihrem Endgerät (PC, Laptop, Tablet oder Smartphone) zu sorgen - das liegt allein in Ihrer Hand! Dieses Infoblatt liefert Ihnen wichtige Hinweise und Tipps, wie Sie sich vor Angriffen Dritter ganz einfach schützen können.

✓ **Erkennen Sie Sicherheitsprobleme auf Computer, Tablet und Smartphone und beheben Sie diese umgehend mit dem ComputerCheck (vrbankfulda.de/computercheck).**

✓ **Wir empfehlen Ihnen eine regelmäßige Änderung Ihrer PIN.**

✓ **Gleichen Sie bei jedem Zahlvorgang in Ihrem Online-Zugang, die Zahlungsverkehrsdaten, z.B. IBAN und Betrag bei Anzeige einer TAN bzw. eines Auftrages auf Ihrem Sm@rt-TAN photo Leser oder in der App VR SecureGo plus nochmals auf Korrektheit ab. Sofern die Angaben voneinander abweichen oder diese nicht zu dem von Ihnen erteilten Auftrag passen sollten, brechen Sie den Vorgang sofort ab und sperren Sie Ihren Online-Zugang (Sperr-Notruf +49 116 116).**

✓ **Weisen Sie eingehende Anrufe mit Aufforderung zur Bekanntgabe persönlicher Daten, wie z.B. Namen, Geburtsdaten, VR-NetKey oder PIN unverzüglich ab.**

✓ **Geben Sie TAN-Nummern per Telefon nach Aufforderung durch Dritte niemals weiter.**

Weitere wichtige Tipps, wie Sie für Ihre Sicherheit sorgen können:

1. Geben Sie Ihre Zugangsdaten wie PIN/TAN oder sonstige Kennwörter niemals an Dritte weiter.
2. Sämtliche Passwörter sollten aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen zusammengesetzt werden. Dies gilt nicht nur für die PIN, sondern beispielsweise auch für das Passwort Ihres Endgerätes. Verwenden Sie keine Geburtsdaten, Autokennzeichen etc.. Diese sind leicht herauszufinden. Bei dreimaliger Falscheingabe der PIN wird der OnlineBanking Zugang zu Ihrer Sicherheit gesperrt.
3. Es sollten keine Test-Versionen von Internet-Browsern verwendet werden. Diese so genannten Beta-Versionen können Sicherheitslücken enthalten oder Fehlfunktionen aufweisen.
4. Die Funktion „Autovervollständigung“ des Browsers sollte deaktiviert sein. Der Schutz für gespeicherte Benutzernamen und Passwörter auf der Festplatte ist hier gering.
5. Der Internet-Browser sollte regelmäßig aktualisiert werden. Die einzelnen Anbieter stellen auf ihren Webseiten Aktualisierungen, so genannte Updates und Patches, bereit. Diese schließen neue Sicherheitslücken. Alternativ kann die automatische Aktualisierung oder Erinnerung bei neuen Updates in den Einstellungen des Internet-Browsers aktiviert werden. Hierdurch ist der Browser immer auf dem aktuellen Stand.
6. Die Zusatzfunktion „ActiveX“ im Browser sollte deaktiviert sein. Hierüber können Dritte über das Internet unter Umständen unkontrolliert Programme installieren.
7. Bei Aufforderung des Browsers zur Bestätigung „nicht vertrauenswürdiger Zertifikate“ stimmen Sie nicht zu, sondern lehnen diese Zertifikate ab.
8. Prüfen Sie generell die Vertrauenswürdigkeit von fremden Angeboten und Anbietern vor deren Nutzung.
9. Installieren Sie nicht jede kostenpflichtige Software aus unbekannter Quelle (ggf. auf nicht produktivem System testen).
10. Prüfen Sie immer die Echtheit eines Angebotes. (Stimmen URL und Zertifikat?)
11. Sperren Sie Ihren Online-Zugang oder TANs bei Verdacht selbst, direkt nach Login im eBanking.
12. Halten Sie Ihr Betriebssystem, Virensoftware, Browser und Plug-ins immer auf dem aktuellen Stand und beziehen Sie Ihre Software - egal ob für Ihren Rechner oder Smartphone grundsätzlich nur über die Original-Herstellerseite. Weitere Infos zum Thema sichere Smartphones stehen auf der BSI-FUER-BUERGER-Seite https://www.bsi-fuer-buerger.de für Sie bereit.

13. Geben Sie die Web-Adresse Ihrer Bank stets selbst im Browser ein.
14. Banken verschicken keine Mails, in denen Sie zum Eingeben von Daten in Online-Formularen aufgefordert werden. Deshalb sollten Sie auf solche Links nie klicken.
Löschen Sie am besten Mails ohne Voransicht, deren Absender Ihnen nicht bekannt ist.
Des Weiteren versendet die Bank keine Sicherheitszertifikate, Verschlüsselungs- oder Sicherheitssoftware um diese auf dem Smartphone oder Tablet zu installieren. Dies ist eine neue Masche bei Betrügern, um Ihr TAN-Verfahren auszuhebeln. Wenn Sie den Verdacht haben, dass auf Ihrem Smartphone Schadcode installiert wurde, sollten Sie keine TANs mehr anfordern und das Gerät einem Fachmann zur Überprüfung geben.
15. Führen Sie kein OnlineBanking an einem Endgerät durch, das auch von anderen Benutzern verwendet wird (z.B. in Firma, Schule oder gar Internetcafé). Die Gefahr durch Keylogger wäre zu groß.

Wir als Bank sorgen dafür, dass die von uns angebotenen Zugangsverfahren und Anwendungen im OnlineBanking höchste Sicherheit gewährleisten.

Sicherheit beim Telefon-Banking:
Nach dem Telefonat mit der Bank muss unbedingt der Nummernspeicher überspielt werden (z. B. durch Eingabe einer beliebigen Nummer über die Tastatur). Dadurch wird verhindert, dass ein Dritter durch Nutzung der Wahlwiederholungsfunktion Kenntnis von der zuvor eingegebenen Kontonummer und PIN erhält bzw. missbräuchlich Zugang zum OnlineBanking erhält.

Wir empfehlen Ihnen:
Ein OnlineBanking-Tageslimit können Sie mit Ihrem Berater oder direkt im OnlineBanking unter Service & Mehrwerte-> „Überweisungslimits“ hinterlegen. Wählen Sie Ihr OnlineBanking-Tageslimit nur so hoch, dass es für Ihre normalen Bedürfnisse ausreicht!

Maßnahmen bei Verdacht auf Missbrauch:
Verdächtige Vorfälle oder Betrugsversuche melden Sie bitte umgehend bei unserem KundenServiceCenter - 0661 289-0 (Mo. - Fr. 8:00 Uhr bis 20:00 Uhr).
Bitte beachten Sie, dass Sie gemäß der Sonderbedingungen für das OnlineBanking umgehend eine Sperrung des OnlineBanking-Zugangs vorzunehmen haben, falls Sie einen Verdacht auf Missbrauch Ihres Online-Zugangs haben. Sie können dies auf einem der folgenden Wege veranlassen:
- KundenServiceCenter 0661 289-0 (Mo. - Fr. 8:00 Uhr bis 20:00 Uhr)
- Sperrhotline: 116 116 (24 Stunden, 7 Tage in der Woche)
- im Online-Zugang Klicken Sie oben rechts auf Ihren Namen im Menü auf "Onlinezugang & Sicherheit" --> "Online-Zugang sperren"

Security – Hotline Tel. 0800 50 53 111:
Die Security - Hotline Tel. 0800 50 53 111 *(14 Cent/Minute aus dem Festnetz; Mobilfunkhöchstpreis 0,42 Euro/Minute)* bietet täglich 8-24h die Möglichkeit sich über Prävention von Phishing - Attacken und Maßnahmen bei erfolgtem Phishing zu informieren.
Auf folgenden Seiten finden Sie weiterführende Informationen und Sicherheitstipps für Ihr OnlineBanking: www.vrbankfulda.de/sicherheit ; www.bsi-fuer-buerger.de ; www.buerger-cert.de