MERCK FINCK
A QUINTET PRIVATE BANK

ONLINE-BANKING SICHERHEITSHINWEISE

Damit Sie Ihre Bankgeschäfte nicht nur bequem, sondern auch sicher erledigen können, haben wir für Sie einige Sicherheitshinweise zusammengestellt. Bitte berücksichtigen Sie unsere Sicherheitshinweise zum Merck Finck Online-Banking.

Grundsätzlich gilt,

- dass Merck Finck Ihnen keine E-Mail zusendet, die direkt zu Internetseiten verlinkt, die Zugangsdaten oder persönliche Daten abfragt oder die einen Link zum Merck Finck Online-Banking enthält, die Sie auffordert, Zugangsdaten oder persönliche Daten (Mobilfunknummer, Kunden-/Teilnehmer-/Kontonummer, Passwort, PIN, TAN, EC- PIN, Kreditkartennummer, etc.) einzugeben bzw. zurückzusenden.

- dass durch Merck Finck weder eine Abfrage der für das Online-Banking hinterlegten Mobilfunknummer, noch des verwendeten TAN-SMS-Empfangsgeräts, bzw. Mobilfunkgeräts stattfindet.

- dass durch Merck Finck keine Aufforderung zu einem Software-Update durch sog. „ServiceSMS“ oder ähnlich an Ihrem Mobilfunkgerät stattfindet.

Sollten Sie derartige Abfragen, E-Mails oder Aufforderungen erhalten, so folgen Sie diesen Aufforderungen auf keinen Fall und informieren Sie uns unter der Tel. +49 89 2104-2222 bzw. senden Sie uns eine E-Mail an folgende Adresse: e-Services@merckfinck.de

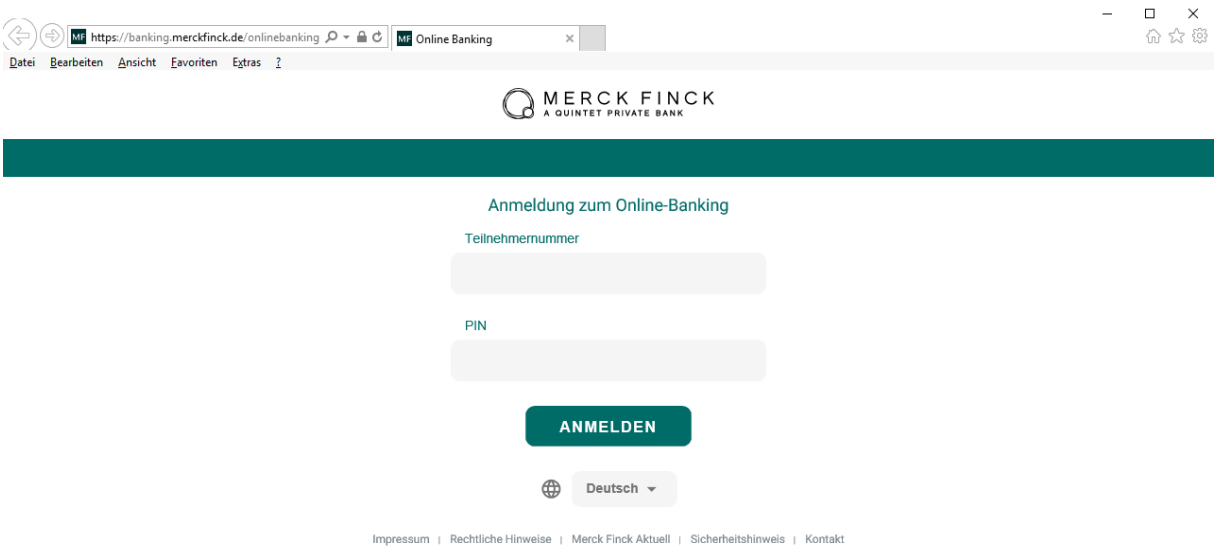
Wichtig beim Umgang mit dem Online-Banking:

- Bitte beachten Sie, dass beim mobileTAN-Verfahren das für den SMS-Empfang angegebene Mobiltelefon oder Smartphone nicht für die Anmeldung am Online-Banking Portal oder die Einreichung von Überweisungen genutzt werden darf! Bitte lesen Sie dazu auch unsere „Bedingungen für das Online-Banking“ unter den rechtlichen Hinweisen auf unserer Internetseite.

- Bitte vergleichen Sie vor der Bestätigung (und somit Freigabe der Transaktion) die Übereinstimmung der in der TAN-SMS angezeigten Daten (z. B. bei einer Überweisung, der Betrag, die Empfänger IBAN, die transaktionsgebundene TAN sowie die Gültigkeitsdauer) mit den für die Transaktion vorgesehenen Daten. Bei Sammelüberweisungen werden Ihnen die entsprechenden Summen angezeigt.

- Starten Sie das Online-Banking, indem Sie auf der Originaladresse der Startseite der Bank www.merckfinck.de die Schaltflächen → „Login“ → Online-Banking „Zum Login“ anklicken.

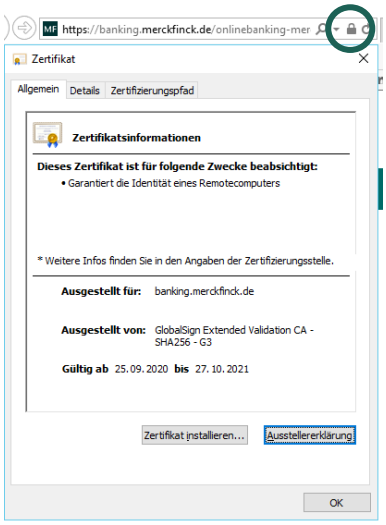
Seiten mit anderen Kombinationen oder Zusätzen sind keine Originalseiten von Merck Finck! Rufen Sie keine Internet-Seite auf, deren Adresse aus einer IP-Adresse besteht (z.B. http://123.456.789.101).



- Seien Sie misstrauisch, wenn Sie im Online-Banking auf einer vorgeschalteten Seite Daten eingeben sollen, zu deren Eingabe Sie sonst nicht aufgefordert werden. Fragen Sie im Zweifelsfall sofort bei der Bank nach.

- Die Datenübertragung wird seitens Merck Finck, wo möglich, überall mit einer 256-Bit-SSL-Verschlüsselung mit AES versehen, um die Daten vor Manipulation und Einsichtnahme Dritter zu schützen.

- Weiterführende aktuelle Zertifikatsinformationen zur Echtheit der Seiten erhalten Sie im Browser durch Klick auf das Schloss-Symbol und der Auswahl „Zertifikate anzeigen“.



Mit diesem Seitenzertifikat können Sie sicher sein, dass die Seiten, die nach Merck Finck aussehen, auch wirklich von Merck Finck stammen. Diese Zertifikate sind eine Art "Digitaler Personalausweis", die nicht gefälscht werden können.

- Benutzen Sie immer die Funktion „Abmelden“, um das Online-Banking zu beenden und löschen Sie nach Beendigung immer den Zwischenspeicher (Cache) Ihres Internet-Browsers (z.B. beim Internet Explorer: Extras→Internetoptionen→Allgemein→Browserverlauf→Löschen).

- Beim so genannten „Phishing“ wird die E-Mail-Absender-Adresse bekannter Unternehmen vorgetäuscht. Der Empfänger wird entweder direkt in der E-Mail dazu aufgefordert seine Zugangsdaten für das Online-Banking anzugeben, oder ein enthaltener Link führt zu einer gefälschten Internetseite, die optisch wie die Originalseite aussieht. Dort soll der E-Mail-Empfänger seine persönlichen Informationen oder Zugangsdaten (PIN, TAN, EC-PIN, Kreditkartennummern, Mobilfunknummer, etc.) preisgeben. Diese werden dann missbräuchlich weitergeleitet. Wichtig: Wenn Sie glauben, dass Sie Opfer einer „Phishing“ E-Mail geworden sind und Ihre Anmeldedaten preisgegeben haben, sperren Sie umgehend Ihre PIN mit der Funktion „PIN sperren“ unter dem Menüpunkt „Administration“ im Merck Finck Online-Banking oder veranlassen Sie die Sperrung des Zugangs unter Tel. +49 89 2104-2222 (Montag bis Freitag 8.00 Uhr bis 16.00 Uhr) bzw. Tel. 0201 3101-163 (Montag bis Freitag 16.00 Uhr bis 8.00 Uhr und an Wochenenden oder Feiertagen) oder per E-Mail an: e-Services@merckfinck.de.

- Installieren und aktivieren Sie Schutzprogramme: Wer Online-Banking ohne aktiviertes Virenschutzprogramm und Firewall betreibt handelt fahrlässig. Beide Schutzprogramme gehören auf jeden internetfähigen Computer und müssen beim Surfen aktiviert sein.

- Aktualisieren Sie Programme regelmäßig: Viren-Schutzprogramme nützen nur, wenn sie regelmäßig aktualisiert werden. Ebenfalls sollten Sie den Internet-Browser, das Computer-Betriebssystem und andere Programme wie z.B. Adobe Acrobat Reader stets auf dem neuesten Software-Stand halten. Täglich erscheinen neue Schadprogramme (Malware), die vor allem ältere Sicherheitslücken ausnutzen. Verwenden Sie das Online-Banking nicht, wenn Sie die Vermutung haben, dass der verwendete Computer oder das Endgerät mit einem Virus oder einem „Trojanischem Pferd“ befallen sein könnte.

- Verschlüsseln Sie Ihr WLAN: Wer mit WLAN surft, sollte auf die Verschlüsselung der Hotspots achten: Internet-Verbindungen nur über den WPA2-Standard starten.

- Arbeiten Sie mit eingeschränkten Benutzerrechten: Für sicheres „Surfen“ sollte jeder PC-Nutzer ein zusätzliches Benutzerkonto ohne Administrator-Rechte auf dem Rechner einrichten. So verhindern Sie, dass sich beim Surfen Schadprogramme automatisch im System einnisten. Denn nur im Administrator-Konto lässt sich Software installieren und ausführen.

- Meiden Sie öffentliche Computer: Betreiben Sie Ihre Bankgeschäfte am besten nur am eigenen Computer. Auch wenn Computer in Internet-Cafés, Büchereien oder Hotels für mobile Kunden praktischer scheinen, können Sie mit Schadprogrammen infiziert sein.

Wichtig beim Umgang mit internetfähigen Mobiltelefonen (Smartphones)

- Ein Smartphone benötigt dieselben Sicherheitsvorkehrungen wie ein PC.
- Seien Sie bitte misstrauisch, wenn Sie im Online-Banking auf einer vorgeschalteten Seite Daten eingeben sollen, zu deren Eingabe Sie üblicherweise nicht aufgefordert werden. Fragen Sie im Zweifelsfall sofort bei der Online-Banking-Hotline +49 89 2104-2222 von Merck Finck nach.
- Merck Finck wird Sie niemals nach vertraulichen Informationen wie Kontodaten, Telefonnummern oder persönlichen Daten per E-Mail oder Telefon fragen.
- Folgen Sie weder auf dem Computer noch auf dem internetfähigen Mobiltelefon oder Smartphone Verlinkungen aus unbekannten Quellen, vor allem wenn Ihr Gerät Updates zulässt. Dahinter kann sich Schadsoftware verbergen.
- Bitte verwenden Sie für den Empfang der TAN-SMS keine Smartphones, bei denen durch „Jailbreak“ oder ähnliche Verfahren die originale Betriebssystem-Software verändert wurde, oder generell die Schutzmechanismen des Geräteherstellers entfernt wurden.
- Bitte verwenden Sie für den Empfang der TAN-SMS (nach Möglichkeit) kein Gerät, das mit einem Android Betriebssystem ausgestattet ist. Die Verwendung solcher Geräte wird in Zusammenhang mit dem mobileTAN-Verfahren aus sicherheitstechnischen Gründen nicht empfohlen.

Weitere Informationen zum Thema Sicherheit im Internet finden Sie auf folgender Seite:

- Auf dem Portal des Bundesamtes für Sicherheit in der Informationstechnik: https://www.bsi-fuer-buerger.de/