Bankhaus Mayer
Privatbank. Seit 1879

## Informationen zum Thema Sicherheit

Das Internet hat sich zu einem selbstverständlichen Medium entwickelt, dessen Bedeutung stetig zunimmt. Neben den positiven Möglichkeiten des Internets ergeben sich jedoch auch eine Reihe von Sicherheitsrisiken, denen durch geeignete Maßnahmen entgegengewirkt werden muss.

Für die Sicherheit der Online-Filiale ist neben der Vielzahl von Sicherheitsvorkehrungen, die durch das Bankhaus Mayer in Zusammenarbeit mit der Fiducia & GAD IT AG als IT-Dienstleister unseres Kreditinstituts umgesetzt wurden, die Sicherheit des Internetnutzer-PCs sowie die Sensibilisierung der Online-Banking-Nutzer von hoher Bedeutung.

Gerade aktuelle Angriffszenarien zielen immer öfter nicht nur auf die Ausnutzung von System- und Anwendungsschwachstellen und nutzen gezielt bestimmte Verhaltensmuster der Anwender. Durch den sensiblen Umgang mit den gegebenen technischen Möglichkeiten lassen sich jedoch die meisten Angriffe abwehren.

## Folgende Punkte sind von wesentlicher Bedeutung:



## 1. Sicherheit am Internet-PC

Der vertrauenswürdige Zustand Ihres PCs ist die Voraussetzung für sicheres Banking und Brokerage. Um die Sicherheit Ihres PCs zu gewährleisten, sind folgende Maßnahmen von wesentlicher Bedeutung:

- Nutzen und installieren Sie nur Software aus vertrauenswürdigen Quellen.

  Überlegen Sie immer, ob Sie eine Software wirklich brauchen und ob Sie dem Anbieter (Hersteller und Download-Quelle) wirklich vertrauen. Generell sollten Sie keine Dateien von unbekannten Servern bzw. E-Mail-Anhänge unbekannten Ursprungs öffnen, herunterladen oder ausführen. Sollte dies jedoch erforderlich sein, so ist zumindest eine Überprüfung der Dateien mit einem aktuellen Virenscanner sinnvoll.

- Schutz vor Viren, Würmern und "Trojanischen Pferden".

  Einmal auf Ihrem System befindliche Viren, Würmer oder "Trojanische Pferde" haben weitreichende Möglichkeiten. Sobald eine solche Schadsoftware auf Ihrem System vorhanden ist, kann der Schutz Ihrer Daten und die korrekte Funktion von Betriebssystem, Virenscanner und Anwendungen prinzipiell nicht mehr gewährleistet werden.

  Um eine optimale Abwehr von Schadsoftware zu erreichen, ist die Installation eines **Virenscanners** und einer **Personal Firewall** erforderlich bzw. sinnvoll. Wesentlich für die Wirksamkeit dieser Komponenten ist zudem eine regelmäßige, möglichst tägliche Aktualisierung.

- Sicherheitsaktualisierungen für Betriebssystem, Browser und Browser-Plugins

  Zum Teil nutzen Angreifer und Schadprogramme Sicherheitslücken im Betriebssystem und Programmen wie dem Browser, um sich unbemerkt in Ihrem PC einzunisten. Um das Angriffspotential über offene Schwachstellen zu minimieren, sollten Aktualisierungen für Betriebssysteme, Browser, Browser-Plugins und Sicherheitskomponenten (wie Personal Firewall oder Virenscanner) umgehend installiert werden. Die meisten Programme bieten für diesen Zweck automatische Update-Funktionen, die in regelmäßigen Abständen auf den Herstellerseiten nach Aktualisierungen der Produkte suchen und diese ggf. installieren.

- Auf folgenden Seiten finden Sie weiterführende Informationen zur Sicherheit im Internet:

  www.bsi-fuer-buerger.de

  www.buerger-cert.de

## 2. Prüfung der Authentizität des Online-Angebots

Die Authentifizierung ist der Nachweis eines Kommunikationspartners, dass er tatsächlich derjenige ist, für den er sich ausgibt. Die Authentizität wird in der Online-Filiale durch Einsatz des SSL-Protokolls gewährleistet. Hierbei wird über ein Zertifikat die Authentizität des Anbieters bestätigt. Eine erste und einfache Möglichkeit der Prüfung ist zudem anhand der angezeigten Internet-Adresse (URL) im Browser möglich.

- Prüfen der Internet-Adresse

Als Anwender sollten Sie darauf achten, dass Sie die korrekte Adresse (URL) für die Online-Filiale kennen. Bei jeder Sitzung sollten Sie die im Browser angezeigte URL auf Plausibilität prüfen. Jede unbekannte Internet-Adresse kann als nicht vertrauenswürdig eingestuft werden. Geben Sie bei fremden Adressen niemals persönliche Informationen und/oder Ihre Zugangsdaten der Online-Filiale ein.

- Der Zugang zur Online-Filiale sollte immer über die offizielle Homepage Ihrer Bank gestartet werden. Auf keinen Fall sollten Sie Links zur Online-Filiale verwenden, die über Web-Seiten oder E-Mails anderer Anbieter zur Verfügung gestellt werden.

## 3. Bedeutung und Kontrolle der wesentlichen Bestandteile der Internet-Adresse (URL) der Online-Filiale

- Die Adresse des Online-Bankings beginnt immer mit:

https:// - Kommunikation über das SSL-Protokoll (Verschlüsselte Kommunikation mit Authentizitätsnachweis des Anbieters) gad.de

internetbanking - Name der InternetBanking-Systeme bei gad.de

gad.de - Internet-Domain des IT-Dienstleisters GAD eG

## 4. Zertifikatsprüfung

Die SSL-Verbindung garantiert Ihnen, dass eine verschlüsselte Kommunikation mit der GAD eG, dem IT-Dienstleister Ihres Kreditinstitutes, stattfindet. SSL-Zertifikate enthalten hierfür generell den öffentlichen Schlüssel des Anbieters, sowie Angaben zur eindeutigen Identifikation.

Das SSL-Zertifikat der Online-Filiale ist auf den IT-Dienstleister GAD eG mit Sitz in Münster ausgestellt (Besitzer/Antragsteller).

Niemals sollte ein Zertifikat eines anderen Anbieters im Rahmen einer Sitzung in der Online-Filiale akzeptiert werden. Manuelle Bestätigungen des Zertifikats sind zudem in der Online-Filiale der GAD eG nicht erforderlich, da hierbei ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle zum Einsatz kommt.

Potentielle Angreifer nutzen i.d.R. eigenerstellte Zertifikate, welche vom Browser nur mit Bestätigung des Benutzers akzeptiert werden, da dieser die Authentizität nicht zweifelsfrei feststellen kann.

Bei Zertifikatsfragen des Browsers ist daher Vorsicht geboten, bevor fremde Zertifikate akzeptiert bzw. als vertrauenswürdig eingestuft werden.

Das Zertifikat des Anbieters sowie Angaben zur Stärke der Verschlüsselung Ihrer SSL-Sitzung können Sie überprüfen, indem Sie einen Doppelklick auf das Symbol "Vorhängeschloss" in der Statuszeile bzw. Symbol- oder Titelleiste des Browsers durchführen.

- Zertifizierungsstelle

Die Zertifizierungsstelle ist eine international anerkannte, unabhängige und vertrauenswürdige Instanz, die Zertifikate ausstellt. Bei der Zertifikatsausstellung ist ein spezieller Authentizitätsnachweis erforderlich, so dass später über das ausgestellte Zertifikat eine Authentizitätsprüfung möglich ist.

Die Online-Filiale der GAD eG verwendet "VR-Ident" als Zertifizierungsstelle.

Als weitere Möglichkeit steht Ihnen ein Abgleich des Fingerprints des SSL-Zertifikats zur Verfügung. Beachten Sie hierzu bitte die Hinweise im folgenden Absatz.

## 5. Abgleich des Fingerprints (SSL-Server-Zertifikat)

Weitergehend können Sie die Korrektheit und Authentizität des verwendeten Zertifikats überprüfen, indem Sie den sogenannten Fingerprint (Fingerabdruck) aufrufen.

Wenn Sie die Details des Zertifikats im Browser betrachten, wird Ihnen der unten aufgeführte Fingerprint angezeigt. Durch den Abgleich der angezeigten Daten mit den Informationen des Herausgebers können Sie sicher feststellen, dass es sich um das Originalzertifikat handelt, welches Sie nutzen möchten. Das SSL-Zertifikat sichert Ihnen zu, dass eine gesicherte Kommunikation mit dem gewünschten Gesprächspartner verschlüsselt erfolgt.

Das gängigste und derzeit sicherste Verfahren zur eindeutigen Authentizitätsbestimmung ist SHA-1.

Der Fingerprint nach SHA-1 für das InternetBanking-Zertifikat (https://internetbanking.gad.de/) :

0F:B3:22:6E:A8:A9:BC:A4:E7:6B:6E:DC:26:A5:4F:BF:FC:62:6D:00

## 6. Generelle Verhaltensregeln

- Geheimhaltung von PIN und TAN

  PIN und TANs dürfen nur im gesicherten Angebot der Online-Filiale verwendet werden. Niemals dürfen PIN und TAN per E-Mail übertragen oder auf anderem Wege Dritten anvertraut werden.

  Achten Sie darauf, dass Ihnen bei der Eingabe von PIN und TAN niemand "über die Schulter sieht" und speichern Sie nie Ihre PIN und TAN auf der Festplatte oder anderen Speichermedien Ihres Endgerätes. Deaktivieren Sie hierzu auch die automatische Passwort-Speicherung Ihres Browsers.

- Änderung der PIN bei Verdacht der Kompromittierung

  Sollten Sie versehentlich eine zweifelhafte Internet-Seite besucht und Ihre Daten preisgegeben haben, empfehlen wir Ihnen, die PIN zu ändern. Dies können Sie direkt in Ihrer Online-Filiale durchführen. Wenden Sie sich bei Problemen umgehend an Ihr Kreditinstitut.

- Prüfung der SSL-Verbindung

  Die Stärke der Verschlüsselung Ihrer SSL-Sitzung sowie das Zertifikat des Anbieters können Sie überprüfen, indem Sie einen Doppelklick auf das Symbol "Vorhängeschloss" in der Statuszeile bzw. Symbol- oder Titelleiste des Browsers durchführen.

  Nutzen Sie die Online-Filiale nur über die gesicherten SSL-Verbindungen zu Ihrer Bank bzw. zu deren Rechenzentrum der GAD eG.

  Achten Sie auf die korrekte Adresse der Online-Filiale (URL).

  Rufen Sie die Online-Filiale ausschließlich über die Homepage Ihres Kreditinstitutes auf.

- Reagieren Sie in keiner Weise auf E-Mails bzgl. Ihrer Online-Filiale, die Ihnen unaufgefordert zugestellt werden

  Niemals wird ein Kreditinstitut seine Kunden per E-Mail auffordern, vertrauliche Daten preiszugeben. E-Mails mit Inhalten wie: "Bitte prüfen Sie umgehend Ihren Online-Banking Zugang" weisen i.d.R. auf den Versuch einer so genannten Phishing Attacke hin. Hierbei versuchen Betrüger, OnlineBanking-Nutzer auf ihre Web-Seite zu locken, um Zugangsinformationen zu Online-Konten zu sammeln. I.d.R. befindet sich in diesen Mails ein Link, der direkt zur Online-Filiale führen soll. Die Internet-Adresse hat dabei meist nur marginale Abweichungen von der echten Adresse der Online-Filiale und der optische Eindruck der echten Seiten wird vollständig nachgeahmt. Nutzen Sie daher niemals Links, die Ihnen in Mails angeboten werden.

  Die Absenderadresse solcher E-Mails ist fast immer gefälscht, so dass eine Rückverfolgung dieser E-Mails sinnlos ist.

- Nutzen Sie die Funktion "Logout" zum Beenden einer Sitzung

  Erst mit dem Aufruf dieser Funktion wird Ihre Verbindung ordnungsgemäß getrennt. Die automatische Abmeldung erfolgt erst, wenn für die Dauer von fünfzehn Minuten (ohne aktiviertes Javascript fünf Minuten) keine Eingaben durch den Benutzer erfolgt sind. Sie werden in diesem Fall zur Neuanmeldung aufgefordert.

- Hinterfragen Sie immer kritisch, ob die auf einer Webseite geforderten Eingaben in Zusammenhang mit der von Ihnen gewünschten Aktion Sinn machen.

## 7. Kundeninformation und –Kommunikation **-gesicherter Kanal-**

- Für die laufende Kommunikation mit dem Kunden ist der elektronische Postkorb im Online-Banking als gesicherter Kanal vorgesehen

- Darüber hinaus können entsprechende Informationen von der Bank auf dem Postweg oder als Nachricht auf dem papierhaften Kontoauszug weitergegeben werde.

- Unsere Mitarbeiter werden zu keiner Zeit, weder persönlich, telefonisch noch per E-Mail, dazu auffordern, Zugangsdaten bzw. PIN und/oder TAN preiszugeben. Ebenso wird bei der Abfrage Ihrer Zugangsdaten niemals die Eingabe einer TAN verlangt.

## 8. Hotline , Support und Meldungen über Unregelmäßigkeiten im Zusammenhang mit Internetzahlungen

- Bei Fragen wenden Sie sich bitte an unsere Hotline-Nr. 0761 / 28200 22 oder schreiben Sie uns eine Nachricht über Ihren Postkorb.