Sicherheit beim OnlineBanking

Damit Sie OnlineBanking sicher nutzen können, beachten Sie bitte unbedingt die nachfolgenden Sicherheitshinweise:

I. SYSTEMSICHERHEIT

A. Nutzung vertrauenswürdiger Computer

Vergewissern Sie sich, dass nur Personen Ihres Vertrauens das Computersystem nutzen oder administrieren. Wickeln Sie niemals Bankgeschäfte über nicht vertrauenswürdige Computer ab.

B. Verwendung sicherheitsoptimierter Betriebssysteme und Browser

Nur gepflegte und gewartete Computersysteme verwenden - das Betriebssystem sollte jedenfalls in regelmäßigen Abständen mit den neuesten Erweiterungen der Sicherheitssoftware versorgt werden. Gleiches gilt selbstverständlich für Ihren Browser. Aktivieren Sie die automatischen Updates und den Phishing-Filter im Internet-Browser. Nähere Informationen hierzu erhalten Sie bei Ihrem Software-Betreuer oder Lieferanten.

C. Einsatz von Virenschutz und Firewall

Verwenden Sie ein aktuelles Virenschutzprogramm mit regelmäßigen automatischen Updates gegen Spyware, Viren und Trojaner bzw. aktivieren Sie eine Personal Firewall zum Schutz Ihres Computersystems.

II. SICHERES VERHALTEN

A. Vertraulichkeit der persönlichen Identifikationsmerkmale

Geben Sie Ihre persönlichen Identifikationsmerkmale, wie z.B.: **P**ersönliche **I**dentifikations **N**ummer (PIN), PIN2 und Geheimfragen, niemals an Dritte weiter und nur auf der geschützten Internetseite der AutoBank mit verschlüsselter Verbindung ein. Diese Seite erkennen Sie unter anderem daran, dass die URL mit https:// beginnt. Niemals dürfen diese vertraulichen Daten in E-Mails, Formularen oder unbekannten Internet-Banking-Systemen eingegeben werden.

B. OnlineBanking-Adresse https://einlagen.autobank.at nur manuell eingeben

Folgen Sie niemals Links aus E-Mails oder von anderen Internet-Seiten zum (vermeintlichen) OnlineBanking-Portal der AutoBank. Auch die Verwendung von Bookmarks (Favoriten, Lesezeichen) birgt Gefahrenpotenzial, da sie von Hackern manipuliert werden können.

C. Verschlüsselung im OnlineBanking

Die Internetseite der AutoBank verwendet ein 128 Bit-SSL-Verschlüsselungsverfahren mit dem Einsatz von EV-SSL Zertifikaten (erweiterte SSL-Zertifikate). Sicherheitszertifikate dienen dazu, den Übertragungsweg im Internet abzusichern um sicherzustellen, dass Daten nicht von Unbefugten eingesehen oder abgefangen werden können.
Achten Sie daher auf die korrekte Eingabe der OnlineBanking-Adresse der AutoBank https://einlagen.autobank.at (genau lesen und gegebenenfalls aufschreiben, damit Sie beim nächsten Login wiedererkannt wird), eine sichere verschlüsselte Verbindung zum OnlineBanking der Autobank und überprüfen Sie das SSL-Zertifikat auf Echtheit (durch Anklicken des Schlosssymbols oder der farbigen Markierung in der Adressleiste auf Ihrem Browser). Die Detaildaten des SSL-Zertifikates der AutoBank lauten wie rechts abgebildet:

D. Persönliche Identifikationsmerkmale (Verfügernummer, PIN, PIN2 und Geheimfragen) getrennt voneinander aufbewahren und nicht auf dem Computer speichern

Verwahren Sie Ihre persönlichen Identifikationsmerkmale getrennt voneinander an einem sicheren Ort auf. Da die Daten auf einem PC ausgespäht werden können, raten wir von einer Speicherung auf dem PC dringend ab.

III. MÖGLICHE GEFAHREN BEACHTEN

A. Vorsicht bei angeblichen E-Mails von Banken

Die AutoBank versendet keine E-Mails, in denen Kunden aufgefordert werden, Ihre persönlichen Identifikationsmerkmale (Verfügernummer, PIN, PIN2 und Geheimfragen) bekannt zu geben. Bei dieser Art von E-Mails handelt es sich immer um Betrugsversuche.

B. Informationen der AutoBank beachten und Vorfälle der AutoBank umgehend melden

Bei sicherheitsrelevanten Vorfällen sollten Sie Ihre persönlichen Identifikationsmerkmale unverzüglich sperren und die AutoBank informieren.

Servicenummer: +43.1.60190.190
Servicezeiten: Mo. bis Do. 8:30-17:00 Uhr, Fr. 8:30-15:00 Uhr
E-Mail: einlagekonto@autobank.at (außerhalb der Servicezeiten)

Geben Sie keinerlei Daten bekannt!

C. Kontoauszüge regelmäßig prüfen

Überprüfen Sie in regelmäßigen Abständen Ihre Kontoauszüge auf Unregelmäßigkeiten.

IV. AKTUELLE WARNHINWEISE

Phishing Warnung

Was versteht man unter Phishing?

Unter Phishing versteht man einen Versuch, mit gefälschten Internet-Adressen, E-Mails oder Kurznachrichten an Daten eines Internet-Nutzers, wie z.B. Zugangsdaten zum OnlineBanking zu gelangen und mit diesen Daten kriminelle Handlungen zu begehen.

Wie können Sie sich schützen?

- Seien Sie stets vorsichtig und wachsam!
- Weder gut konfigurierte Firewalls noch aktuelle Antiviren-Programme können Sie vor Phishing-Attacken schützen.
- Achten Sie auf die E-Mail-Adresse des Absenders, die meist ähnlich, aber nicht ident mit der E-Mail-Adresse der AutoBank ist.
- In E-Mails werden oft Links zu gefälschten Internet-Seiten eingebaut, die fast oder manchmal sogar gleich aussehen, wie die echten Internet-Seiten der jeweiligen Bank. Bedenken Sie, dass Internet-Seiten und Logos leicht kopiert werden können.
- Geben Sie die Adresse zum OnlineBanking-Portal der AutoBank https://einlagen.autobank.at/ immer händisch ein und geben Sie Ihre Zugangsdaten ausschließlich auf dieser Seite ein. Das ist die wirkungsvollste Methode, um zu verhindern dass Sie auf eine gefälschte Seite gelockt werden.

Was können Sie beim Verdacht eine Phishing-E-Mail erhalten zu haben tun?

Folgen Sie keinesfalls der Aufforderung, Informationen dem E-Mail-Absender bekannt zu geben. Die AutoBank wird Sie NIEMALS auffordern, Informationen per E-Mail bekannt zu geben.

Folgen Sie keinesfalls dem in dieser E-Mail-Nachricht eingefügten Link auf eine Internet-Seite.

Informieren Sie umgehend die AutoBank:

Servicenummer: +43.1.60190.190
Servicezeiten: Mo. bis Do. 8:30-17:00 Uhr, Fr. 8:30-15:00 Uhr
E-Mail: einlagekonto@autobank.at (außerhalb der Servicezeiten)

Gefälschte SMS

Bitte beachten Sie, dass wir niemals SMS an Sie versenden. Gefälschte SMS täuschen einen seriösen Absender vor, um so an vertrauliche Informationen von Kunden zu gelangen. Oft wird als Rückrufnummer eine Telefonnummer angegeben, die mit hohen Gebühren verbunden ist. Bitte antworten Sie niemals auf diese Kurznachrichten und rufen Sie keinesfalls die darin angegebene Telefonnummer an.

Informieren Sie umgehend die AutoBank:

Servicenummer: +43.1.60190.190
Servicezeiten: Mo. bis Do. 8:30-17:00 Uhr, Fr. 8:30-15:00 Uhr
E-Mail: einlagekonto@autobank.at (außerhalb der Servicezeiten)

Schadsoftware

Unter Schadsoftware versteht man Computerprogramme, deren Ziel die Ausforschung sensibler Daten, wie z.B. (Verfügernummer, PIN, PIN2 und Geheimfragen), ist. Für gewöhnlich sind diese Programme gut getarnt und laufen unbemerkt im Hintergrund.

Bitte beachten Sie in diesem Zusammenhang unsere Sicherheitshinweise unter dem Punkt Systemsicherheit.