Bankhaus Mayer
Privatbank. Seit 1879

Informationen zum Thema Sicherheit im Umgang mit Ihrer Kreditkarte

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 des Kreditkarteneinsatzes im stationären Handel, an Geldautomaten, sowie in Online-Shops (E-commerce) ist neben der Vielzahl von Sicherheitsvorkehrungen, die durch Kreditinstitute und deren Kreditkarten-Zahlungsdienstleister umgesetzt wurden, die Sicherheit des Internetnutzer-PCs sowie die Sensibilisierung der Nutzer bei Internetzahlungen von hoher Bedeutung.

Gerade aktuelle Angriffsszenarien 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 E-commerce. 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/Online-Shops vor der Bezahlung im Internet:

- Vergewissern Sie sich, dass Sie es mit einem seriösen Anbieter zu tun haben. Bei großen, renommierten Veranstaltern sind Sie in der Regel auf der sicheren Seite.
- Bei Ihnen unbekannten Webseiten kontrollieren Sie die Anbieterinformationen im Impressum und achten auf Gütesiegel wie Trusted Shops oder TÜV Süd Safer Shopping.
- Bevor Sie Konto- oder Kreditkartendaten zur Bezahlung übermitteln, prüfen Sie stets, ob die Datenübertragung verschlüsselt erfolgt. In der

Regel erkennen Sie dies an der Kennung https am Beginn der Adresszeile Ihres Browsers.

- Immer wieder kommt es vor, dass Cyber-kriminelle E-Mails mit Sonderangeboten die Webseiten von seriösen Reiseanbietern imitieren, um Verbraucher mittels Phishing in die Falle zu locken. Deshalb ist es unerlässlich, die Absenderadresse einer E-Mail oder die Adresszeile einer Website dahingehend zu prüfen, ob sie tatsächlich echt ist. Auf der sicheren Seite sind Sie, wenn Sie die Internetadresse manuell in die Browserzeile eingeben – so landen Sie auch wirklich dort, wo Sie hin wollten.

3. Generelle Verhaltensregeln

- bei Erhalt des Pin-Briefes ist auf dessen Unversehrtheit zu achten
- Geheimhaltung von PIN für Bargeldabhebungen.
- Geheimhaltung von Kartennummer und 3-stelliger Prüfziffer (siehe Kartenrückseite)
- Karte nie aus Sichtweite geben (Gefahr von Duplikats-Anfertigungen)
- Keine Einkaufsbelege mit Kreditkartendaten wegwerfen.
- bei Verlust, sofort Kreditkartensperre veranlassen
- Reagieren Sie in keiner Weise auf E-Mails die Ihnen unaufgefordert zugestellt werden. Niemals wird ein Kreditinstitut seine Kunden per E-Mail auffordern, vertrauliche Daten preiszugeben. E-Mails mit Inhalten wie: "Ihre Kreditkarte wurde gesperrt/blockiert…“ sind i.d.R. so genannte Phishing Attacken! Hierbei versuchen Betrüger, Kreditkarten-Nutzer auf ihre Web-Seite zu locken, um Zugangsinformationen zu sammeln. I.d.R. befindet sich in diesen Mails ein Link, der direkt zur betrügerischen Internetseite führen soll. 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.

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

4. Empfohlene Sicherheitsvorkehrungen

- Sperren-Notruf-Hotline bereithalten
- MasterCard Abrechnungen regelmäßig prüfen
- Verfügungslimit für Bargeldabhebungen begrenzen (Cash-Limit)
- Separates eCommerce Limit einrichten
- 3 D Secure mobile Tan Verfahren nutzen (Siehe hierzu gesonderte Informationsblätter)

5. Kundeninformation und –kommunikation

- Kundeninformationen betreffend Neuerungen/Änderungen des bestehenden Kreditkartenvertrages finden über den jeweiligen Bankberater statt.

- Änderungen von Wohn- und Postadressen, Telefonnummern, Namen sollten von dem Karteninhaber dem zuständigen Berater zur Aktualisierung der Vertragsdaten mitgeteilt werden. Somit kann gewährleistet werden, dass die MasterCard-Abrechnungen pünktlich zugestellt und auf ihre Richtigkeit geprüft werden können.

- Auslandsaufenthalte sollten vor Antritt dem zuständigen Kundenbetreuer der Bank oder der Karteninhaberbetreuung der First Data Deutschland GmbH (Vertragspartner & Zahlungsdienstleiter MasterCard) gemeldet werden. Hintergrund ist die sensibilisierte Betrachtung von ausländischen Kartenumsätzen der MasterCard Missbrauchs-Präventionsabteilung.

- Der Kommunikationsweg seitens First Data Deutschland GmbH zu Karteninhabern findet auf dem Postweg statt. Niemals per Email! In dringenden Fällen auch per Telefon, wenn es nötig ist den Kunden umgehend erreichen zu können. Es empfiehlt sich bei Kartenantragsstellung eine Mobilnummer zu hinterlegen.

- Wichtige Informationen über Neuerungen oder Änderungen betreffend der Kartensicherheit werden den Kreditkarteninhaber frühzeitig über den Postweg mitgeteilt und zusätzlich auf der Bank-Homepage unter der Rubrik: „Kreditkarten“ veröffentlicht.

- Bearbeitung von Zahlungsreklamation: Der Karteninhaber kann sich telefonisch an die Karteninhaberbetreuung wenden oder persönlich mit seinem Bankbetreuer Kontakt aufnehmen, welcher die Bearbeitung in die Wege leiten wird.

6. Hotline und Support

- Karteninhaberbetreuung
  +49 (0)69 / 7933-2200

- 24h Karteninhaberservice 3-D Secure
  +49 (0)69 / 7933-2555

- 24h Internationaler Karten-Sperrnotruf:
  +49 (0)69 / 7933-1910

- Bankbetreuer zu Öffnungszeiten
  +49 (0)761/ 28200-0