SwissBanking

Basel, 31.03.2005

# Sicherheit im Zahlungsverkehr
# Information der Schweizerischen Bankiervereinigung

In letzter Zeit sind Bank- und PostFinance-Kunden vermehrt Opfer von Betrügereien und Betrugsversuchen geworden. Dies veranlasste die Schweizerische Bankiervereinigung (SBVg) - in Absprache mit den Mitgliedsinstituten und der Schweizerischen Post - eine Informationskampagne "Sicherheit im Zahlungsverkehr" zu starten.

## Manipulation von Papieraufträgen

Die Ermittlungen der Strafbehörden zeigen, dass die Täterschaft bei der Manipulation von schriftlichen Zahlungsaufträgen vielfach nach demselben Tatmuster vorgeht:

- die schriftlichen Zahlungsaufträge werden aus Briefeinwürfen entwendet
- Einzahlungsscheine werden ausgewechselt
- der Zahlungsauftrag wird wieder in den Briefeinwurf geworfen

Da bei diesem Vorgehen die Originalunterschrift des Kunden wie auch die Anzahl Einzahlungsscheine und der Totalbetrag oft unverändert erhalten bleiben, ist es für die Finanzinstitute nicht möglich, diese Manipulationen zu erkennen.

Um der Täterschaft das Handwerk zu erschweren, haben die meisten Schweizer Banken und die Schweizerische Post bei ihren 2'500 Poststellen ihre Briefeinwürfe mittels baulichen Massnahmen sicherer gemacht. Dies verunmöglicht oder erschwert ein Entnehmen von eingeworfenen Briefen.

**Um von einer sicheren Zahlungsverkehrsabwicklung profitieren zu können, empfiehlt die SBVg, die Sicherheitshinweise der Schweizer Finanzinstitute und der Schweizerischen Post zu beachten:**

- Kontoauszüge und schriftliche Zahlungsaufträge nicht Unberechtigten zugänglich machen.
- Papiere mit Bank- bzw. Karteninformationen gehören nicht ins Altpapier (idealerweise benutzen Sie einen Aktenvernichter; mindestens sind die Unterlagen aber zerkleinert in den Abfall zu geben).
- Totalbetragsfeld auf den schriftlichen Zahlungsaufträgen linksbündig mit durchgestrichenen Nullen oder Doppelstrich ergänzen, damit keine Ziffern davor gesetzt werden können.
- Sämtliche Postsendungen mit sensiblem Inhalt (z.B. schriftliche Zahlungsaufträge) direkt am Postschalter abgeben oder in einen besonders gesicherten Briefeinwurf bei einer Poststelle einwerfen. In Gemeinden mit Hausservice können Briefe mit Zahlungsaufträgen dem Briefträger mitgegeben werden.

Die Schweizerische Post hat ihre Empfehlungen unter www.post.ch publiziert.

## Internet-Banking

Noch sicherer als Papieraufträge ist die immer beliebtere Abwicklung des Zahlungsverkehrs mittels Internet-Banking. Zudem eröffnet sich ein sehr umfangreiches Dienstleistungsangebot, welches weit über die Zahlungsabwicklung hinausgeht:

- Konto- und Depotinformationen
- Kontoüberträge
- Zahlungsverkehr (Einzel- und Daueraufträge innerhalb der Schweiz und ins Ausland)
- Kursinformationen (Noten, Devisen, Wertschriften)
- Börsenaufträge

Das Internet ist ein offenes, weltweit vernetztes Kommunikationssystem. Um die Sicherheit bei Internet-Banking Aktivitäten zu gewährleisten, setzen die Schweizer Finanzinstitute modernste Technologien ein. Für die Sicherheit des persönlichen Computers gibt es einige Grundsätze zu beachten:

**So schützen Sie Ihren Computer:**

- Benützen Sie in jedem Fall auf Ihrem Computer eine aktuelle Firewall und Virenschutzsoftware.
- Installieren Sie keine Programme von nicht vertrauenswürdigen Anbietern.
- Öffnen Sie keine e-Mails unbekannter Herkunft oder mit fremden Anhängen.
- Verwenden Sie die empfohlenen Browser- und Betriebssystemversionen mit den neusten Sicherheitsupdates.

**Wichtige Tipps zur Sicherheit im Internet-Banking:**

- Sicherheitsmerkmale (Passwörter/Codes) nicht aufschreiben oder Dritten zugänglich machen.
- Schliessen Sie sämtliche Browserfenster und starten Sie den Browser neu, bevor Sie sich ins Internet-Banking einloggen. Vor und während der Arbeit mit Internet-Banking sollten keine anderen Internet-Seiten angewählt werden.
- Melden Sie sich mit den Identifikations-Daten nur auf den offiziellen Login-Pages der Finanzinstitute an.
- Überprüfen Sie nach der Erfassung Ihrer Zahlungs- und Börsenaufträge diese auf Korrektheit direkt im Internet-Banking.
- Reagieren Sie auf keine e-Mails oder Links, welche Sie auffordern, Ihre Sicherheitsmerkmale einzugeben, auch wenn der Absender angeblich Ihr Finanzinstitut sein soll.
- Beenden Sie Ihre geschützte Internet-Banking Session immer mit der dafür vorgesehenen Programmfunktion "Beenden", bevor Sie das Browser-Fenster ganz schliessen. Leeren Sie den Cache des Browsers nach dem Verlassen des Internet-Banking.

## Card-Banking

Wertvolle Tipps im Umgang mit Karten und PIN-Code:

- Unterschreiben Sie Maestro-, Postcard oder Kreditkarten sofort nach Erhalt auf der Rückseite.
- Bewahren Sie Karten stets an einem sicheren Ort auf und überprüfen Sie regelmässig, ob sie noch in Ihrem Besitz sind.
- Wenn Ihnen Ihr PIN-Code oder eine Karte abhanden gekommen ist, sei es durch Verlust, Diebstahl oder Einzug an einem Automaten, lassen Sie diese in jedem Fall umgehend sperren.

**Das Wichtigste zu Ihrem PIN-Code:**

- Vermeiden Sie einfach zu erratende Kombinationen wie Geburtsdaten, Auto- oder Telefonnummern oder leicht nachvollziehbare Kombinationen wie z.B. 123456.
- Lernen Sie Ihren PIN-Code auswendig, und geben Sie ihn niemals weiter (auch nicht bekannten Personen oder Bankmitarbeitern).

**Der sichere Karteneinsatz:**

- Lassen Sie sich beim Bargeldbezug am Automaten nicht ablenken. Versichern Sie sich, dass Sie beim Eingeben Ihres PIN-Codes nicht beobachtet werden, und nehmen Sie keine Hilfestellung von fremden Personen an.
- Überprüfen Sie innerhalb von 30 Tagen (ab Datum der Erstellung) auf Ihren Kontoauszügen beziehungsweise auf Ihren Kreditkartenabrechnungen Ihre Ausgaben und Bezüge mit Ihren Karten.
- Melden Sie Ihrem Finanzinstitut, falls Sie etwas Ungewöhnliches rund um einen Geldbezugautomaten feststellen.

Für weitere Fragen im Zusammenhang mit der Zahlungsabwicklung wenden Sie sich bitte an Ihr Finanzinstitut. Ihre Kundenbetreuerin oder Ihr Kundenbetreuer wird Sie gerne beraten.