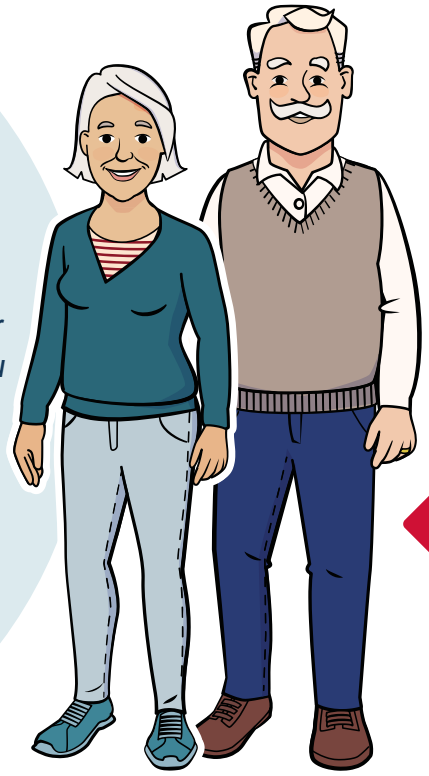
Kapitel 9
Bankgeschäfte online und mobil

Frau Neumann grübelt: „Bankgeschäfte sind sicher ziemlich kompliziert, gerade für uns Internet-Neulinge."

Herr Meister beruhigt sie: „Keine Angst, das begreift ihr schnell. Manche Banken haben ein Demo-Konto auf ihren Internet-Seiten, mit dem ihr ohne die Angaben eurer Privatdaten üben könnt. Du wirst sehen, bald wirst du dich fragen, warum du das nicht schon früher gemacht hast."

Frau Neumann fasst Mut. Sie und ihr Mann vereinbaren einen Termin mit ihrem Kundenberater, der ihnen das Online-Banking erklärt und Informationsmaterial bereithält.



Online-Banking[104] spart Zeit und Geld

Die Banken „belohnen" die Online-Kunden oft mit geringeren Kosten, sofern sie nicht sowieso gebührenfreie Girokonten anbieten. Die Banken sind sehr daran interessiert, die Zahl der arbeitsintensiven Papierunterlagen, wie Überweisungen u. ä. möglichst gering zu halten. Das zeitaufwendige Eingeben der Daten in den Zentralrechner überlässt man inzwischen gern der Kundschaft selbst. Das kennen Sie sicherlich

104 *Online-Banking, gesprochen: Onlein-Bänking, Kunstwort aus engl. Online und Banking, Bankwesen, Bankgeschäfte.*

Online-Banking

bereits in ähnlicher Form von den Geräten zur Selbstnutzung, die im Foyer Ihrer Bank stehen. Online-Banking hat den Vorteil, dass Sie jederzeit Ihren Kontoauszug einsehen oder die Rechnungen bezahlen können, ohne einen Fuß vor die Tür setzen zu müssen. Kostenersparnis und Bequemlichkeit sind sicher begrüßenswert. Allerdings muss natürlich verhindert werden, dass sich andere Menschen bequem von Ihrem Konto bedienen können.

Wie Sie selbst hat auch jedes Kreditinstitut großes Interesse daran, dass Kundengelder nicht in dunklen Kanälen verschwinden. Also haben die Banken verschiedene Sicherheitsbarrieren eingebaut. Im Gegenzug erwarten sie aber, dass sich ihre Online-Kundschaft ebenfalls an die Sicherheitsrichtlinien hält.

Schadenersatz

Falls Ihnen beim Online-Banking ein materieller Verlust entsteht, ist Ihr Kreditinstitut zu Schadenersatz verpflichtet. Dies gilt jedoch nur, wenn Sie sorgfältig sind und die Sicherheitsrichtlinien einhalten. Anderenfalls geht der Schaden zu Ihren Lasten. Achten Sie daher darauf, dass Sie Ihre Überweisungen verschlüsselt ausführen (ein sicheres Passwort ist hier ein Muss), Ihre Software auf dem aktuellsten Stand ist und Sie sich mit Hilfe von Schutzprogrammen gegen Versuche absichern, Ihre Passwörter auszulesen.

Zudem können Sie mit Ihrer Bank Tageslimits für das Online-Konto vereinbaren. Wenn Sie Ihre Bankgeschäfte beenden, verlassen Sie die Internet-Seite immer über den Knopf, der alle noch offenen Felder schließt und Sie abmeldet.

Kontoführungs-Programme

Beim Einstieg in das Online-Banking kann Ihnen nicht nur Ihre Hausbank auf ihrer eigenen Internet-Seite weiterhelfen. Verschiedene unabhängige Kontoführungs-Programme unterstützen Sie bei allen Bankgeschäften und verschaffen Ihnen einen Überblick über Ihren finanziellen Status. Sie können damit alle Ihre Konten (auch bei unterschiedlichen Banken) einheitlich verwalten und sich z. B. an Zahlungen, die zu festen Terminen fällig sind, erinnern lassen. Ihre Einnahmen und Ausgaben lassen sich nach Rubriken ordnen, wie etwa „Haus und Garten", „Urlaub", „Anschaffungen" etc. Als Beispiele seien genannt WISO Mein Geld, Star Finanz, StarMoney, Steganos Online-Banking.

Online-Zugang

Grundvoraussetzung ist ein aktuelles Antivirenprogramm mit einer Firewall und ein aktualisiertes Betriebssystem, d. h. mit regelmäßiger Ausführung von Updates. Ob Sie nun ein Kontoführungs-Programm oder die Internet-Seite Ihrer Hausbank verwenden, in beiden Fällen müssen Sie sich für das Online-Banking mit Ihrer Kontonummer/*UserID*[105] und einem Online-PIN/Passwort und ggf. mit einem Zugriffscode anmelden. Die PIN sollte möglichst sechsstellig sein und eine Kombination aus kleinen und großen Buchstaben und Ziffern enthalten. Speichern Sie die PIN nicht auf Ihrem Computer! Wenn Sie Ihr Passwort frei wählen können, beachten Sie bitte die Hinweise, die im Kapitel „Bestellen und bezahlen" aufgeführt sind. Wählen Sie außerdem für Ihre Bankgeschäfte immer ein anderes Passwort als z. B. für Ihr E-Mail-Konto. Sie werden nun mit Ihrem Namen und Ihren Kontoangaben begrüßt.

Beachten Sie: Nur wenn das Symbol eines kleinen Vorhängeschlosses links neben der Internet-Adresse im Browser zu sehen ist, sind Ihre Bankdaten sicher. Prüfen Sie zudem, ob in der Adresszeile an das übliche http:// ein „s" gehängt ist. Das ist ein Zeichen dafür, dass Sie sich jetzt auf einer Seite mit gesicherten Daten befinden. Ihre Eingaben werden ab sofort verschlüsselt übertragen.

Viele Banken ermöglichen ihrer Kundschaft ein sogenanntes Testprogramm/Demo. Damit können die Nutzerinnen und Nutzer zunächst die richtige Handhabung ausprobieren.

Demo-Konto

105 *UserID, gesprochen: Juser Eidi, engl., Benutzeridentifikation.*

Online-Banking-Verfahren am Computer

Für Überweisungen und andere Kundenaufträge benötigen Sie Transaktionsnummern (TANs). Das sind Zahlenkombinationen, die pro Überweisung nur eine einmalige Gültigkeit besitzen und danach „verfallen". Auch dies ist ein wichtiger Schritt zur Sicherheit Ihres Internet-Kontos. Zurzeit gibt es noch viele Verfahren nebeneinander, die sich in den nächsten Jahren wahrscheinlich angleichen werden. Um Ihnen einen Überblick zu geben, stellen wir Ihnen im Folgenden alle Möglichkeiten vor, die Sie am Computer durchführen können. Ihre Bank oder Sparkasse wird Ihnen eines der hier genannten Verfahren empfehlen.

iTAN-Verfahren

Bis September 2019 gab es das iTAN-Verfahren. Sie erhielten vorab eine (Papier-) Liste mit Zahlencodes. Während Sie eine Überweisung tätigten, bestimmte ein Zufallsgenerator der Bank, welche TAN aus der durchnummerierten (also indizierten) Liste eingegeben werden musste (daher der Name iTAN). Da das System zu unsicher ist, wurde das Verfahren abgeschafft.

mTAN-Verfahren

Die TAN wird auf Ihr Handy oder Smartphone geschickt (daher der Name mobilTAN oder sms-TAN) und ist nur für die aktuelle Buchung gültig.

ChipTAN, Flicker-TAN, Sm@rt-TAN

Bei diesem Verfahren, das unter mehreren Namen eingesetzt wird, kaufen Sie bei Ihrem Geldinstitut für ca. 15 € ein besonderes Lesegerät, in das Sie Ihre Kontokarte einführen. Das halten Sie beim Überweisungsvorgang an den Bildschirm und bestätigen damit Ihre Buchung. Der Vorteil: Ohne Lesegerät und Kontokarte können keine Geldtransfers erfolgen, also selbst dann nicht, wenn jemand betrügerisch Zugang zu Benutzerkonten erhält.

HBCI 100 mit Chipkarte

Auch bei diesem Verfahren erhalten Sie von Ihrem Geldinstitut eine Chipkarte zusammen mit einem Lesegerät. Wie am Automaten in der Bankfiliale führen Sie nun zu Hause Ihre Karte in das Gerät ein und erledigen Ihre Geldgeschäfte. Auch hier ist eine Finanztransaktion nur mit Ihrer Karte möglich, mit der Sie eine elektronische Signatur erzeugen.

Foto-TAN oder Photo-TAN

Dies ist ein vergleichsweise modernes System, das nicht von allen Banken angeboten wird. Das Verfahren funktioniert ähnlich wie das ChipTAN-Vorgehen, nur dass Sie den Code nicht mit einem Lesegerät abscannen, sondern mit Ihrem Smartphone. Dieses generiert Ihnen dann die TAN, die Sie für die Überweisung nutzen können. Sie brauchen für das Vorgehen ein Smartphone und die entsprechende App Ihrer Bank.

Barrierefreies Online-Banking

Manche Kreditinstitute bieten ihren blinden und sehbehinderten Kundinnen und Kunden besondere Zugänge an, damit sie ihre Konten online führen können. So können Schriftgröße und Kontraste individuell angepasst und die Seiten mit einem Screenreader ausgelesen werden.

Mobiles Banking (M-Banking, mBanking) am Smartphone

Sie können Ihre Bankgeschäfte auch an Ihrem Smartphone oder Tablet erledigen. Sie benötigen dafür nur die App Ihrer Bank.

Allerdings unterscheidet sich der Funktionsumfang je nach Institut erheblich. Um die App dann tatsächlich nutzen zu können, müssen Sie zunächst die Freischaltung zum Online-Banking beantragen. Die Daten, mit denen Sie sich anschließend über den Browser einloggen können, werden einfach in die App übertragen und schon kann es losgehen.

Sollten Sie mehrere Konten bei unterschiedlichen Banken nutzen, können Sie auch bankenunabhängige Apps verwenden wie finanzblick Online, Banking 4, OutBank.

Mobiles Banking auf dem Smartphone ist so sicher wie Online-Banking am Rechner. Darauf weist die Stiftung Warentest in einem Testbericht von je-

weils 19 Banking-Apps für Android und iOS hin („Test"-Ausgabe 10/18). Banking-Apps sollten aus Sicherheitsgründen jedoch nur aus den offiziellen App Stores installiert und wie das Smartphone-Betriebssystem stets aktuell gehalten werden. Die Banking-Anwendungen müssen die Nutzerinnen und Nutzer mit einem sicheren, mindestens achtstelligen Passwort oder per Fingerabdruck schützen.

Sicherheit geht vor

Keylogger[106] sind Schadprogramme, die Tastatureingaben bei einem Computer aufzeichnen und damit protokollieren. Im Internet versuchen Datendiebe auf diesem Weg, Passwörter oder Identifikationsnummern auszulesen. Ihren Virenschutz und Ihre Firewall sollten Sie daher immer eingeschaltet haben. Beinahe „einfacher" verläuft das „*Phishing*[107]", mit dem Ihre Passwörter ebenfalls „abgefischt" werden sollen. Eine beliebte Methode ist es, Kundinnen und Kunden gefälschte E-Mails des Geldinstituts zuzusenden und sie aufzufordern, vertrauliche Daten im Netz einzugeben. Diese Schreiben stammen nie von der Bank Ihres Vertrauens. Sie sollten sie am besten sofort löschen. Falls an eine solche E-Mail eine Datei angehängt ist: Öffnen Sie diese nicht! In der Regel verbirgt sich dahinter ein Schadprogramm, wie z. B. ein Trojaner. Lassen Sie sich nicht einschüchtern, falls Ihnen in der E-Mail mit einer Kontosperre gedroht oder mitgeteilt wird, dass Ihr Konto bereits deaktiviert wurde. Das ist eine beliebte und leider wohl auch funktionierende Masche, um die Angeschriebenen dazu zu bewegen, diese Dateien aufzurufen und auf diesem Weg Schadprogramme zu installieren. Nehmen Sie bei Nachfragen persönlich oder telefonisch Kontakt zu Ihrer Bank auf. Was Sie tun sollten, um einem Ernstfall vorzubeugen, können Sie auf den Seiten des Bundesamtes für Sicherheit in der Informationstechnik (www.bsi-fuer-buerger.de) nachlesen. Weitere Sicherheitstipps erhalten Sie bei Ihrer Bank oder Sparkasse, fragen Sie das Beratungspersonal danach. Denn auch wenn Ihr Wohnzimmer nun Ihre eigene Filiale ist, sollten Sie durchaus öfter einmal im Haupthaus vorbeischauen. Auf diese Weise sind Sie gut informiert und geschützt.

Bitte beachten Sie, dass Sie Ihre Online-Banking-Geschäfte am sichersten von zu Zuhause aus betreiben. Nutzen Sie dafür kein öffentliches WLAN, wie beispielsweise in Cafés und Bahnhöfen.

106 Keylogger, gesprochen: Kielogger, engl., Tasten-Aufzeichner.

107 Phishing, gesprochen: Fisching, Kunstwort aus engl. Password + Fishing, Passwort „abfischen".

Mobiles Bezahlen

Mittlerweile können Sie auch an einigen Kassen mit Ihrem Smartphone bezahlen. Dafür benötigen Sie eine spezielle App, entweder Ihrer Bank oder eines anderen Anbieters wie Apple oder Google, und ein *NFC*[108]-fähiges Smartphone. NFC-fähige Kassen erkennen Sie an dem Wellensymbol, das in der Regel in der Nähe der Kasse oder am Bezahlterminal angebracht ist. Aktivieren Sie an der Kasse das Display Ihres Smartphones und halten Sie es an das Terminal. Der Bezahlvorgang wird durch ein akustisches Signal bestätigt. Beim mobilen Bezahlen handelt es sich um eine gewöhnliche Kartenzahlung. Der Betrag wird von der Karte abgebucht, die Sie hinterlegt haben.

Zum NFS-Vorgehen gibt es auch Alternativen: Einige Anbieter arbeiten mit QR-Codes, die an der Kasse eingescannt werden, oder Zahlenreihen, die man an der Kasse benennt. Diese Systeme sind eher bei Supermarktketten verbreitet.

Für alle Vorgehensweisen gelten folgende Sicherheitshinweise:

- Überprüfen Sie genau, welchen Anbieter Sie nutzen möchten.
- Halten Sie die Gerätesoftware Ihres Smartphones immer auf dem aktuellen Stand, nutzen Sie am besten automatische Updates.
- Richten Sie einen PIN als Zugangsschutz ein.

Mobiles Bezahlen

- Kontrollieren Sie regelmäßig Ihre Kontoauszüge und Abrechnungen.
- Sollte Ihr Smartphone verloren gehen, sollten Sie die hinterlegte Karte sofort sperren lassen.

Zudem sollte man immer bedenken, dass das mobile Bezahlen nicht in allen Geschäften möglich ist.

Digital Kompass

Grundkenntnisse im Umgang mit dem Online-Banking vermittelt Ihnen die Anleitung „Bankgeschäfte online – bequem von zu Hause aus“ von Nicola Röhricht auf der Internet-Seite: www.digital-kompass.de.

108 NFC, Abkürzung für Near Field Communication, engl., Kommunikation über eine kurze Entfernung, in diesem Fall ein Datenaustausch.