Die Verbraucherzentrale NRW informiert:

Online-Banking – wie funktioniert es und ist es sicher?

Online-Banking hat große Vorteile und wird von vielen Kunden genutzt. Insbesondere sind die Kunden nicht mehr von den Öffnungszeiten der Bank abhängig und können jederzeit auf das eigene Konto zugreifen. Online-Banking hat aber auch Schattenseiten. Dies liegt vor allem daran, dass Kriminelle in schöner Regelmäßigkeit versuchen, Schwachstellen zu finden, um an das Geld der Bankkunden zu kommen.

Im Folgenden erläutert Annabel Oelmann die grundsätzliche Funktionsweise von Online-Banking, die derzeit angebotenen gängigen Verfahren und geht schließlich auf Sicherheitsregeln ein, die beim Online-Banking auf jeden Fall eingehalten werden müssen.

Dr. Annabel Oelmann
Verbraucherzentrale NRW

So funktioniert Online-Banking

Online-Banking bedeutet vom Grundsatz her, dass Kunden ihre Bankgeschäfte größtenteils von zu Hause, aber mit mobilen Geräten auch von unterwegs aus erledigen können. Sie loggen sich einfach in ihr Onlinekonto ein und können zu jeder Tages- und Nachtzeit den Kontostand oder einzelne Buchungen kontrollieren, Geld überweisen, Daueraufträge überprüfen und vieles mehr.

Um sich in das eigene Girokonto einzuloggen, erhalten Kunden die sogenannte PIN. PIN steht für persönliche Identifikationsnummer oder im Englischen für personal identification number. Mit der PIN alleine könnten sich Kunden alles in ihrem Konto anschauen, aber noch kein Geld überweisen. Hierzu ist neben der PIN auch eine sogenannte TAN nötig. TAN steht für Transaktionsnummer. Bildlich gesehen ist eine TAN ein Einmalpasswort, mit der ein Kunde eine Überweisung freigeben kann. Die TAN ersetzt sozusagen die Unterschrift – genau wie es die PIN für die Girokarte am Geldautomaten tut. Eine TAN kann nur einmal verwendet werden. Will ein Kunde mehrere Überweisungen durchführen, benötigt er für jede einzelne Überweisung eine separate TAN.

Ein internetfähiges Gerät mit einer Online-Verbindung, PIN und TAN sind daher die Voraussetzungen, um nicht nur passiv (Kontostände prüfen etc.) am Online-Banking teilnehmen zu können, sondern um auch aktiv Geld vom Konto zu überweisen. PIN und TAN dürfen niemals Dritten mitgeteilt werden. Denn das wäre so, als ob man jemandem einen Blankoscheck ausstellt, mit dem dieser einfach das Konto leeren könnte.

Wer sich für Online-Banking entscheidet, muss bestimmte Sicherheitsstandards einhalten, um böse Überraschungen zu vermeiden. Denn alle elektronischen Geräte vom Computer bis zum Smartphone sind ein beliebtes Angriffsziel. Sollte es Kriminellen gelingen, sich den Zugang zu verschaffen, haben sie unter Umständen auch Zugriff auf Ihr Girokonto.

Foto: vege/Fotolia.com

Welche Verfahren gibt es beim Online-Banking?

TAN-Listen

Diese Variante des Online-Banking kennt man unter dem Namen PIN/TAN-Verfahren oder iTAN-Verfahren. Der Kunde bekommt neben der PIN eine Liste, auf der viele verschiedene TANs stehen. Wenn er einen Geldbetrag überweisen will, muss er neben der PIN eine TAN eingeben. Je nach Bank kann es eine beliebige TAN der Liste sein oder aber eine ganz bestimmte. Dann muss er beispielsweise aus der Liste mit 50 Nummern die TAN angeben, die hinter Nummer 27 steht. Diese TAN-Listen waren in der Vergangenheit zahlreichen betrügerischen Angriffen ausgesetzt. Der Grund ist einfach: Wenn ein Krimineller im Besitz von PIN und TAN ist, ist er in der Lage, Geld vom Konto des Kunden zu überweisen. Daher wurden diese unsicheren TAN-Listen nach und nach aus dem Verkehr gezogen. Heute gibt es kaum noch eine Bank, die mit solchen Listen arbeitet. Falls ausgerechnet Ihre eigene Hausbank oder Haussparkasse ausschließlich dieses Verfahren anbietet, sollten Sie entweder auf Online-Banking verzichten oder das Kreditinstitut wechseln.

mTAN

Auch beim mTAN-Verfahren, auch mobileTAN-Verfahren oder smsTAN-Verfahren genannt, muss der Kunde die PIN und eine TAN eingeben, wenn er von seinem Konto Geld online überweisen will. Nachdem er sich mit der PIN in sein Konto eingeloggt hat und die Überweisungsdaten eingegeben hat, bekommt er die TAN auf sein Mobiltelefon geschickt. Mit dieser TAN kann er die Überweisung freigeben – und nur diese, denn die TAN kann nicht für eine andere Überweisung als die im Telefondisplay angezeigte genutzt werden.

Der Vorteil: Wenn Kriminelle an das Geld auf dem Konto wollen, müssten sie also zwei Geräte hacken – den Computer und das Mobiltelefon. Die Tatsache, dass zwei voneinander getrennte Geräte im Einsatz sind, reduziert die Gefahr eines Missbrauchs. Das heißt aber auch, dass Kunden das Smartphone nicht gleichzeitig nutzen dürfen, um ins Internet zu gehen und um die TAN zu empfangen. Denn dann müssten die Kriminellen mit dem Smartphone nur ein Gerät manipulieren und der Sicherheitsgewinn wäre verpufft. Deswegen sollte das Handy für das Online-Banking nicht internetfähig sein und darf auch nicht über Kabel oder Bluetooth mit dem Computer verbunden werden.

Das mTAN-Verfahren bringt letztlich gegenüber den TAN-Listen zwar grundsätzlich einen deutlichen Sicherheitsgewinn, wenn auf die beiden voneinander getrennten Geräte geachtet wird. Aber auch hier haben trickreiche Kriminelle schon Mittel und Wege gefunden, das System zu knacken. So haben sie es schon geschafft, die Telefonnummer des Kunden gegen eine eigene auszutauschen. Dies gelang, indem sie unter der Telefonnummer des Kunden eine zweite SIM-Karte angemeldet hatten. Dann schickte die Bank die TAN nicht mehr an den Kunden, sondern an die Kriminellen.

Chip-TAN

Das Chip-TAN-Verfahren, auch TAN-Generator genannt, bietet eine zusätzliche Sicherheit durch den Einsatz von zwei getrennten Geräten. Was beim mTAN-Verfahren das Mobiltelefon ist, ist beim Chip-TAN-Verfahren der Generator. Dies ist ein elektronisches Gerät, das in der Regel ein Display, ein Ziffernfeld und einen Karteneinschub besitzt. Wenn der Kunde eine Überweisung tätigen will, loggt er sich mit der PIN in sein Konto ein und gibt

Foto: dessauer/Fotolia.com

Sicherheitsregeln

Damit Kriminelle keinen Zugriff auf Ihr Onlinekonto bekommen, ist es in der Tat wichtig, sich für ein Verfahren mit der größtmöglichen Sicherheit zu entscheiden. Das alleine reicht aber nicht. Um Kriminelle ins Leere laufen zu lassen, ist es zwingend notwendig, dass Sie bestimmte Sicherheitsregeln einhalten.

✔ Das Virenschutzprogramm, den Internetbrowser und das Betriebssystem stets auf dem neuesten Stand halten.

✔ Bei einer Überweisung mit mTAN-Verfahren oder Chip-TAN-Verfahren immer kontrollieren, wofür die TAN wirklich ist. Im Display des Mobiltelefons bzw. Generators stehen Betrag und zumindest Teile der IBAN, an die das Geld überwiesen werden soll. Falls etwas nicht stimmt, sollten Sie auf der Stelle abbrechen und keinesfalls die TAN eingeben.

✔ Geben Sie die Internetadresse zur Bank oder Sparkasse immer selbst per Hand ein. Die nur zweitbeste Lösung ist es, ein Lesezeichen anzulegen. Niemals sollten Sie einen Link nutzen, der in einer E-Mail enthalten ist. Denn solche Links werden oft von Kriminellen geschickt, die die Bankkunden auf eine nachgebaute Internetseite der eigenen Bank oder Sparkasse lotsen wollen.

✔ Nutzen Sie keinesfalls fremde Computer oder unbekannte WLAN-Verbindungen für das Online-Banking. Weder in Hotels oder Internetcafés noch bei Verwandten oder Freunden – denn man weiß nicht, wie diese Computer und Netze gesichert sind.

✔ Bei einer unerwarteten E-Mail bitte folgende drei Regeln einhalten:

- Niemals auf Links klicken!
- Keine Dateianhänge öffnen!
- Nicht auf diese E-Mail antworten! Wer sich unsicher ist, ob die E-Mail nicht doch echt sein könnte, kann beim echten Anbieter (Filiale, Homepage) nachfragen.

✔ PIN und TAN nur für die vorgesehene Überweisung eingeben, aber niemals zu angeblichen Kontrollzwecken – denn das würde ein echter Anbieter nie von Ihnen verlangen.

Mehr dazu unter: www.vz-nrw.de

die Überweisungsdaten ein. Bei den meisten Generatoren schiebt er dann seine Kunden- oder Girokarte in den Karteneinschub. Die TAN, mit der er die Überweisung abschließen kann, wird vom Generator zufällig ermittelt. Je nach Modell geschieht dies manuell oder dadurch, dass der Kunde den Generator vor eine flackernde Grafik auf dem Monitor hält.

Wie auch beim mTAN-Verfahren haben Kriminelle beim Chip-TAN-Verfahren das Problem, dass zwei verschiedene Geräte zum Einsatz kommen. Kriminelle müssten also nicht nur Zugriff auf den Computer haben, sondern dem Kunden auch den Generator und zusätzlich seine Kunden- oder Girokarte klauen. Damit ist das Chip-TAN-Verfahren deutlich sicherer als das mTAN-Verfahren. Denn da die Kriminellen auch die Kunden- oder Girokarte klauen müssten, müssen sie in der Nähe des Kunden sein – während sie sich beim mTAN-Verfahren irgendwo aufhalten können bei dem Versuch, beide Geräte zu hacken.

Fazit

Eine hundertprozentige Sicherheit gibt es beim Online-Banking nicht – bei keinem der vorgestellten Verfahren. Wer aber gewisse Regeln einhält, reduziert deutlich die Wahrscheinlichkeit, Opfer von Kriminellen zu werden. Von den aktuell gängigen Verfahren ist das Chip-TAN-Verfahren die sicherste Variante.

Foto: modern boomers/imagesource, Grafik: Matthias Enter/Fotolia.com