SwissBanking

September 2009

Secure e-Banking

1 Sicheres e-Banking

Das e-Banking ist ein etablierter, kosteneffizienter Kommunikationskanal zwischen Privat- oder Geschäftskunden und ihrer Bank. Es bietet beiden Seiten Vorteile: Der Kunde muss sich nicht mehr für eine Überweisung oder die Abfrage seines Kontostandes zur Bank begeben. Diese Basisdienstleistungen stehen ihm unabhängig von den Öffnungszeiten ständig online zur Verfügung. Die Banken wiederum verfügen über ein rund um die Uhr nutzbares Kommunikationsinstrument zum Kunden. Damit trägt das e-Banking auch für Sie zur Qualität Ihrer Bankbeziehung bei.

Doch nebst diesen Vorteilen, die das Internet bietet, sind mit dessen Nutzung auch verschiedene Sicherheitsrisiken, wie zum Beispiel Mitlesen, Verändern oder Löschen von Daten bei der Übertragung und das Erschleichen von Daten durch Vorgabe falscher Tatsachen durch Unbefugte, verbunden.

Mit diesem Informationspapier möchten wir Sie als e-Banking-Kunden auf die Sicherheitsrisiken hinweisen und Ihnen aufzeigen, welche Massnahmen gegen die gängigsten Bedrohungen und Gefahren im Internet zu ergreifen sind.

Sicheres e-Banking ist dann gewährleistet, wenn Sie genügend Kenntnis über die Bedrohungen im Internet haben, um gemeinsam mit Ihrer Bank gegen die zunehmende Internetkriminalität vorzugehen.

Damit Sie sich vor Manipulationen beim e-Banking schützen können, sollten Sie grundsätzlich im Umgang mit dem Internet ein sicherheitsbewusstes Verhalten pflegen und regelmässig Ihre Kontobewegungen überprüfen. Wenn Sie den Verdacht haben, Opfer von Internet-Kriminellen geworden zu sein, sollten Sie den Online-Zugang zu Ihrem Bankkonto sofort sperren lassen und nicht nachvollziehbare Kontobewegungen umgehend Ihrer Bank melden.

2 Gefahren und Bedrohungen im Internet

Die Gefahren und Bedrohungen im Internet sind kontinuierlichem Wandel unterzogen und ändern sich teilweise rasant. Zu den häufigsten Gefahren im Internet gehören Viren, Würmer, Trojanische Pferde, Phishing, Pharming, Drive-By-Infektion. Nachfolgend möchten wir Ihnen die Bedeutung dieser Begriffe näher erläutern und Ihnen aufzeigen, was Sie dagegen tun können.

2.1 Viren

Viren haben ähnliche Merkmale wie Krankheitsviren, können sich selbst verbreiten und besitzen das Potenzial, grossen Schaden anzurichten. Bei einem harmlosen Virus können Dateiinhalte verändert werden und im schlimmsten Fall zur vollständigen Löschung Ihrer Festplatte führen. Viren gelangen über e-Mail oder infizierte Dateien, die vom Internet heruntergeladen werden, auf die Festplatte des Computers. Wenn die Viren einmal aktiviert werden, können sie sich via e-Mail oder Internet rasant verbreiten.

2.2 Würmer

Würmer zeigen ein ähnliches Schadensbild wie Viren, sind aber eigenständige Programme, d.h. sie benötigen kein Wirtprogramm zur Aktivierung. Vielmehr nutzen sie Sicherheitslücken oder Konfigurationsfehler in Betriebssystemen bzw. Anwendungen (e-Mail, Internet), um sich selbstständig von Computer zu Computer auszubreiten.

2.3 Trojanische Pferde

Trojanische Pferde oder „Trojaner“ sind eingeschleuste Programme, die häufig durch das Internet heruntergeladen werden, um – von Ihnen unbemerkt – Schaden auf Ihrem Computer anzurichten. Ziel der meisten Trojaner ist es, sensible Daten, wie z.B. Passwörter, auszuspähen und sie an den Eigentümer des Trojaners zu senden oder Ihre Transaktionen direkt zu manipulieren. Der Trojaner ermöglicht seinem Eigentümer, auf fremde Rechner zuzugreifen und somit die Fernkontrolle über Ihren Computer zu übernehmen. Die Trojaner tarnen sich in der Regel für den Benutzer als nützliche Anwendung oder Datei.

2.4 Phishing

Beim Phishing, einer Zusammensetzung aus den englischen Wörtern „password“ und „fishing“, werden Sie von Betrügern aufgefordert, Ihre vertraulichen Zugangsdaten zum e-Banking auf der Internetseite Ihres Instituts zu aktualisieren oder erneut einzugeben. Die Aufforderung dazu kann sowohl mittels einer e-Mail als auch durch manipulierte Internetseiten erfolgen. Dadurch wird versucht, Ihre vertraulichen Daten, wie zum Beispiel die e-Banking-Zugangsdaten oder den Kontostand, auszuspähen.

2.5 Drive-By-Infektion

Unter einer Drive-By-Infektion versteht man die Infektion des Computers mit Malware (Schadprogramme), die allein durch den Besuch einer Webseite herbeigeführt wird. Vielfach beinhalten diese Webseiten seriöse Angebote, sind jedoch für die Verteilung von Schadprogrammen kontaminiert worden. Damit schleusen Kriminelle Schadcodes auf die Webseite ein. Das alleinige Surfen auf einer betroffenen Webseite genügt, um einen Computer zu infizieren.

2.6 Pharming

Beim Pharming handelt es sich um eine Betrugsmethode, bei der Ihre Internet-Verbindung auf eine gefälschte Webseite umgelenkt wird. Sie geben also die richtige Internetadresse im Browser ein, gelangen jedoch auf eine gefälschte Webseite.

3 Massnahmen zum Schutz Ihres e-Banking

Öffnen Sie nur e-Mails von Ihnen bekannten Personen oder Unternehmen und öffnen Sie keine Anhänge in e-Mails, deren Absender Sie nicht kennen. Im Zweifelsfall fragen Sie beim Absender nach. Setzen Sie eine aktuelle Virenschutzsoftware und eine persönliche Firewall ein. Es ist zudem wichtig, die Virenschutzsoftware stets auf dem neusten Stand zu halten. Dies können Sie tun, indem Sie die verfügbaren Updates umgehend von den Seiten Ihres Softwareanbieters herunterladen und installieren oder einen automatischen Updateservice nutzen.

Achten Sie zudem darauf, dass Sie stets ein aktuelles Betriebssystem sowie eine aktuelle Version des Browsers inkl. der dazugehörigen Plugins installiert haben. Auch sollten Sie stets die aktuellen Sicherheitsupdates Ihrer Anwendungsprogramme installieren, andernfalls könnten neu bekannt gewordene Schwachstellen durch Kriminelle für Angriffe auf Ihren Computer ausgenutzt werden.

3.1 Kein e-Banking auf einer bankfremden Internetadresse!

Geben Sie Ihre e-Banking-Zugangsdaten nur ein, wenn Sie sicher sind, dass Sie sich tatsächlich auf der geschützten, autorisierten Internetseite Ihrer Bank befinden und eine verschlüsselte Verbindung nutzen. Eine verschlüsselte Verbindung können Sie daran erkennen, dass dem http ein s (= secure, dt. sicher) in der URL der Verbindung angehängt wird. Dies heisst, dass für diese Webseite ein Sicherheitszertifikat eingesetzt wurde (z.B. https://www.sba.ch). Die Authentizität dieses Sicherheitszertifikats können Sie überprüfen, indem Sie wie folgt vorgehen: Doppelklicken Sie auf das geschlossene Schlosssymbol, das sich in der Statusleiste ganz unten im Browser-Fenster befindet. Im anschliessend geöffneten Zertifikats-Dialogfenster sollte der Name Ihrer Bank aufgeführt sein. Ferner setzen die meisten Banken Extended Validation SSL-Zertifikate ein. Diese sind daran zu erkennen, dass ein Teil der URL-Adressleiste mit dem Namen der Bank grün hinterlegt ist. Wenn Sie auf den grünen Balken klicken, erscheint ein Dialogfenster, in dem der Name des Bankinstituts im Zertifikat sowie die Zertifizierungsstelle angezeigt werden. Wenn dies gewährleistet ist, können Sie von einer vertrauenswürdigen Internetseite ausgehen. Leider unterstützen noch nicht alle Browser Extended Validation SSL.

Beim Online-Shopping sollten Sie Ihre persönlichen Zugangsdaten weder auf der Shopping-Seite noch auf den Seiten eines Online-Überweisungsdienstes eingeben. Geben Sie Ihre geheimen Zugangsdaten niemals auf einer anderen Internetseite als derjenigen Ihrer Bank und auch sonst nicht einem Dritten preis. Teilen Sie Ihre e-Banking-Zugangsdaten anderen Unternehmen mit, verstossen Sie damit gegen die Sorgfaltspflichten aus Ihrem e-Banking-Vertrag mit Ihrem Bankinstitut.

3.2 Schützen Sie Ihre sensiblen Daten

Schützen Sie Ihre Zugangsdaten zum e-Banking vor unberechtigtem Zugriff und Entwendung. Speichern Sie sensible Daten (Passwörter, e-Banking-Zugangsdaten, Kreditkartennummern etc.) nicht auf Ihrem Computer ab. Dies könnte sonst an Computern, die nicht ausschliesslich von Ihnen benutzt werden, wie z.B. am Arbeitsplatz, dazu führen, dass Dritte diese Daten einsehen.

Auch spezielle Spionageprogramme, die auf Ihren Rechner gelangt sind, können solche Daten ausspähen und z.B. per e-Mail versenden. Wenn Sie zur Erhöhung der Sicherheit eine zusätzliche Ausrüstung, wie z.B. einen Chipkartenleser mit PIN-Eingabetastatur benutzen, geben Sie die dafür vorgesehenen, vertraulichen Daten nur dann ein, wenn Sie von diesem Gerät dazu aufgefordert werden. Speichern Sie vor allem Ihr Passwort nie ab.

Ihre Bank wird Sie niemals – weder per e-Mail noch telefonisch – kontaktieren und nach Ihren geheimen Zugangsdaten fragen. Beantworten Sie solche e-Mails nie und folgen Sie auch den angegebenen Instruktionen nicht, selbst wenn Ihnen mit negativen Konsequenzen, wie z.B. einer Kontosperre, gedroht wird. Informieren Sie Ihre Bank, wenn ein solcher Fall auftritt.

Für den umgekehrten Fall, dass Sie Ihre Bank selber kontaktieren, kann es im Rahmen von Phonebanking aber sehr wohl sein, dass die Bank Sie zwecks Identifikation nach Ihren geheimen Zugangsdaten fragt. Stellen Sie in jedem Fall sicher, dass Sie die richtige Nummer angerufen haben und dies dem entsprechend kommunizierten Vorgehen entspricht, bevor Sie solchen Aufforderungen nachkommen.

Stellen Sie sicher, dass Sie Ihre vertraulichen Zugangsdaten immer nur auf der echten Internetseite Ihres Bankinstituts eingeben. Achten Sie zudem auf Abweichungen im Erscheinungsbild des gewohnten e-Banking-Auftritts Ihrer Bank. Wenn Sie Ihre Bankseite schon oft aufgerufen haben, dann fällt Ihnen sogar eine minimale Veränderung – beispielsweise leichte Verschiebungen des Logos Ihrer Bank und den Überschriften – sofort auf.

3.3 Wählen Sie ein sicheres Passwort

Verwenden Sie ein gutes und sicheres Passwort für Ihr e-Banking. Ein solches zählt mindestens acht Stellen und besteht aus einer Mischung von Gross- und Kleinbuchstaben und Zahlen. Sie sollten weder Ihren Namen noch den Namen Ihnen bekannter Personen und auch nicht Ihr bzw. deren Geburtsdatum verwenden. Wechseln Sie regelmässig Ihr Passwort, insbesondere wenn Sie vermuten, jemand könnte dieses ausspioniert haben. Es gibt im Internet, evtl. auch auf der Internetseite Ihrer Bank, Beispiele für die Wahl eines guten und sicheren Passworts.

4 Allgemeine Vorkehrungen

Greifen Sie ausschliesslich von einem von Ihnen genutzten Computer aus auf das e-Banking zu. Bei einem nicht ausschliesslich von Ihnen genutzten Computer, z.B. in einem Internetcafé, wissen Sie nie genau, inwieweit der Zugang durch wirksame Sicherheitssoftware geschützt ist und welche Programme auf diesem PC ausgeführt werden. Auch die Tastaturen können manipuliert sein. Sicherheit können Sie hier nicht erwarten. Deshalb ist e-Banking an solchen Computern nicht empfehlenswert.

Wenn Sie e-Banking vornehmen, achten Sie darauf, dass Sie keine weiteren Browserfenster (auch keine Tabs) sowie kein Mailprogramm geöffnet haben.

Beenden Sie Ihre e-Banking-Sitzung stets mit der dafür vorgesehenen Funktion „Abmelden“, „Logout“ oder „Beenden“ und löschen Sie anschliessend die temporären Internetdateien Ihres Webbrowsers sowie die Cookies (eine Anleitung hierzu sollten Sie jeweils auf der Internetseite Ihrer Bank finden).

Weiterführende Links:

- www.swissbanking.org > Dossier: Informationen für Bankkunden
  http://www.swissbanking.org/home/dossier-bankkunden.htm

- Melde- und Analysestelle Informationssicherung MELANI
  http://www.melani.admin.ch/themen/00103/index.html?lang=de

- Bundesamt für Sicherheit in der Informationstechnik
  http://www.bsi-fuer-buerger.de/

Diese Broschüre ist auch erhältlich in den Sprachen Französisch, Italienisch und Englisch und kann bei der Schweizerischen Bankiervereinigung unter http://www.swissbanking.org/home/shop.htm bestellt werden.

Unter www.swissbanking.org/home/dossier-bankkunden.htm kann die Broschüre auch im PDF-Format heruntergeladen werden.

Schweizerische Bankiervereinigung
Aeschenplatz 7
Postfach 4182
CH-4002 Basel
T +41 61 295 93 93
F +41 61 272 53 82
office@sba.ch
www.swissbanking.org