

Stichwort Phishing - Welche Gefahren bestehen beim Online-Banking?

Wenn Sie Ihre Bankgeschäfte über das Internet abwickeln, sollten Sie sich bewusst sein, dass Sie innerhalb eines weltweiten Datennetzes sensible persönliche Daten versenden. Daher sollten Sie bei der Weitergabe Ihrer Daten auf höchste Sicherheit bedacht sein, denn nicht nur am Geldautomaten können Kriminelle Ihren PIN ausspähen und damit Ihr Konto leer räumen, auch beim Online-Banking laufen Sie Gefahr, dass Ihnen bei der Eingabe von PIN und TAN jemand „über die Schulter schaut“.

Wie funktioniert Online-Banking? Das PIN/TAN-System

In den meisten Fällen erfolgt das Online-Banking über eine Kombination von PIN und TAN. PIN steht für persönliche Identifikationsnummer und ist eine Zahlenkombination die nur Ihnen persönlich bekannt ist. Mit Ihrer Kontonummer und Ihrer PIN, die nicht der PIN für Abhebungen am Geldautomaten entspricht, sondern separat bei Ihrer Bank beantragt werden muss, gelangen Sie zur Kontoübersicht und können die letzten Kontobewegungen prüfen. Um Überweisungen zu tätigen brauchen Sie zusätzlich die Transaktionsnummern (TAN), die Ihnen separat von Ihrer Bank zugeschickt werden. Jede TAN können Sie nur einmal verwenden. Um die Sicherheit zu erhöhen, haben einige Banken die TAN nummeriert und akzeptieren die Eingabe nur in dieser Reihenfolge.

Wie ist das Ausspähen im Internet möglich?

Phishing (eine Wortschöpfung die aus **password fishing** gebildet wurde) bedeutet, dass Sie durch die List eines Betrügers dazu bewegt werden sollen, Ihr Passwort und Ihre TAN herauszugeben. Der Betrüger fischt also nach diesen Daten, greift dann auf Ihr Konto zu und kann Ihr Geld auf sein Konto überweisen. Wie kommt der Betrüger an Ihre Bankdaten? Oft erhalten Sie als Bankkunde offiziell wirkende eMails, in denen Sie aufgefordert werden Ihre PIN und eine TAN anzugeben. Durch einen Link in der eMail werden Sie scheinbar auf Ihre Bankseite geführt. Tatsächlich wird die aufgerufene Seite so aussehen, wie die Internetseite Ihrer Bank. Es handelt sich jedoch nur um eine Fälschung, die dazu dient, Ihre Zugangsdaten und die TAN abzufragen. Die Gründe die vorgegeben werden, um Ihnen PIN und TAN zu entlocken sind vielfältig. Manchmal wird sogar in einer

Phishing-eMail vor Phishing gewarnt und dem Leser nahegelegt, sein Konto zu kontrollieren – tut er dies, so wird er selbst zum Phishing-Opfer.

Daneben können auch Viren und Würmer Ihren Rechner so manipulieren, dass Sie bei dem nächsten Online-Besuch Ihrer Bank auf eine Seite des Betrügers geraten, deren Tarnung so gut ist, dass es selbst erfahrenen Surfern nicht auffällt. Ihr Rechner kann sich z.B. über Anhänge in eMails infizieren. Es gibt auch Viren, die Ihre TAN nicht nur ausspähen, sondern zudem noch während der Eingabe manipulieren. Der Bankkunde erhält dann seitens der Bank eine Fehlermeldung wegen der falschen Eingabe, und der Betrüger kann die richtige TAN für seine Überweisung verwenden.

Wie kann ich mich vor Phishing schützen?

- ▶ Kontrollieren Sie die Internetseiten Ihrer Bank regelmäßig auf aktuelle Sicherheitshinweise.
- ▶ Führen Sie in Internet-Cafés oder über öffentliche zugängliche Computer keine Bankgeschäfte durch. Möglicherweise können die übertragenen Daten mitgeschnitten werden.
- ▶ Wenn Sie eine eMail Ihrer Bank erhalten, melden Sie sich im Zweifelsfall telefonisch bei der Bank, um die Richtigkeit des Inhalts zu prüfen.
- ▶ Bedenken Sie: Ihre Bank wird Sie niemals außerhalb eines Überweisungsauftrages dazu auffordern, PIN oder TAN einzugeben.
- ▶ Nutzen Sie niemals einen Link aus einer Mail, um ein Bankgeschäft zu tätigen. Es ist sicherer, selbst die Adresszeile Ihrer Bank einzugeben.
- ▶ Wenn die Verbindung während eines Online-Banking-Vorganges abbricht, informieren Sie sofort Ihre Bank, ändern Sie möglichst schnell Ihre PIN oder falls dies nicht möglich ist, blockieren Sie den Onlinezugang bewusst durch die Eingabe einer falschen PIN.
- ▶ Kontrollieren Sie regelmäßig Ihr Konto, vereinbaren Sie gegebenenfalls mit der Bank ein Tageslimit für Überweisungen.
- ▶ Leiten Sie mögliche Phishing-eMails an die Kriminalpolizei weiter.
- ▶ Überwachen Sie Ihren eMail-Eingang: Löschen Sie im Zweifel unerwartete Nachrichten mit Dateianhang, da diese Viren oder Trojaner enthalten könnten.
- ▶ Speichern Sie PIN und TAN NIEMALS auf Ihrem PC.
- ▶ Bewahren Sie Ihre TAN-Liste an einem sicheren Ort auf.
- ▶ Verwenden Sie einen Virens scanner und Sicherheitssoftware und aktualisieren Sie diese regelmäßig.
- ▶ Prüfen Sie die Adressleiste Ihres Browsers, ob sie mit Ihrer Bankadresse übereinstimmt oder verdächtige Anhänge hat.
- ▶ Achten Sie darauf, dass Ihre Kontodaten nur verschlüsselt übertragen werden. Ob eine Verschlüsselung vorliegt, erkennen Sie an dem Kürzel „https“.
- ▶ Prüfen Sie die Sicherheitszertifikate durch einen Doppelklick auf das Schlosssymbol auf der gesicherten Website darauf, ob der Urheber der Seite tatsächlich Ihre Bank ist.

Was kann ich tun, wenn ich auf einer „Phishing“-Seite meine Daten eingegeben habe?

- ▶ Setzen Sie sich sofort mit Ihrer Bank in Verbindung! Berichten Sie von der Überweisung und bitten Sie den Bankangestellten, die Überweisung noch abzufangen oder eine Rückbuchung vorzunehmen. In diesem besonderen Fall können Sie dem Bankangestellten Ihre weitergegebene TAN nennen, da es hiermit der Bank möglich ist, die Überweisung noch abzufangen. Aber auch zu diesem Zeitpunkt nennen Sie niemals Ihre PIN!!
- ▶ Ändern Sie sofort Ihre PIN!!
- ▶ Leiten Sie der Bank und der Polizei die eMail, die Sie zur Eingabe der Daten veranlasst hat weiter. Die eMail kann wichtige Hinweise auf den Täter liefern!
- ▶ Erstellen Sie Strafanzeige! Betrug ist strafbar und auch schon bloße Vorbereitungshandlungen hierzu führen zur Strafbarkeit aufgrund Versuchs. Zwar stellen sich oft praktische Schwierigkeiten für die Strafverfolgungsbehörden, wenn der Täter aus dem Ausland agiert, doch können die Behörden insbesondere in der Europäischen Union mit den ausländischen Ermittlungsbehörden zusammenarbeiten.
- ▶ Informieren Sie auch Ihre Verbraucherzentrale, damit diese für andere Nutzer entsprechende Warnhinweise rausgeben kann!

Viele Bankinstitute sind bisher zur Entschädigung ihrer betrogenen Kunden bereit, wenn der Kunde trotz sorgfältigen Handelns, Opfer einer Phishing-Attacke geworden ist. Denn nur solange die Kunden das Vertrauen in die Sicherheit des Online-Banking nicht verlieren, lohnen sich die hierfür gemachten Aufwendungen der Banken. Zudem fehlt auch eine Alternative, denn weder für die Bank noch für den Kunden ist die Rückkehr in die Zeit vor der Vernetzung reizvoll.

Wo kann ich weitere Unterstützung erhalten?

Seit Anfang 2006 bietet die **Bochumer Arbeitsgruppe Identitätsschutz im Internet** eine Hotline für Opfer von Phishing und anderen Formen des Identitätsmissbrauchs an. Die Hotline ist montags und donnerstags in der Zeit von 14 bis 17 Uhr über die Telefonnummer 0234 / 32 280 58 zu erreichen. Außerdem kann das Online-Portal der Arbeitsgruppe Identitätsschutz über www.a-i3.org erreicht werden.

Weitere Informationen erhalten Sie beim **Bundesamt für Sicherheit in der Informationstechnik** (www.bsi-fuer-buerger.de bzw. www.buerger-cert.de), bei der **Initiative Deutschland sicher im Netz** (www.sicher-im-netz.de) und beim **Verbraucherzentralen Bundesverband** (www.vzbv.de).

© Euro-Info-Verbraucher e.V., Kehl, www.euroinfo-kehl.com Rehfusplatz 11, 77694 Kehl
Für die Richtigkeit der in diesem Faltblatt enthaltenen Angaben können wir trotz sorgfältiger Prüfung keine Gewähr übernehmen. Stand dieser Informationen: Mai 2006