ONLINE-BANKING: Bankgeschäfte ohne Risiko

Tipps zum sicheren Online-Banking

Der Schaden bei einem ungenügend gesicherten Online-Konto geht schnell in die Tausende. So sichern Sie Ihre Bankgeschäfte im Internet und schützen sich vor Trickbetrügern.

Rund 35 Prozent aller Bankkunden erledigen ihre Geldgeschäfte mittlerweile online. Dabei laufen sie jedoch Gefahr, Opfer von Cyber-Kriminellen zu werden. Im schlimmsten Fall räumen diese das gesamte Online-Konto samt Dispokredit leer. Nur mit dem nötigen Wissen, den richtigen Tricks und sicherer Software lässt sich Online-Banking ohne Risiko durchführen.

Zu den häufigsten Angriffsmethoden gehört Phishing. Der Begriff setzt sich zusammen aus den Wörtern "Passwort" und "Fishing". Beim Phishing werden Surfer auf täuschend echt nachgemachte Webseiten gelockt. Mit den dort eingegebenen Daten – meist werden Account-Name, PIN sowie eine TAN verlangt – heben die Kriminellen dann Geld vom Konto des Internetnutzers ab. Der durchschnittliche Schaden von Phishing-Opfern lag bereits vor einem Jahr bei 7200 Franken – Tendenz steigend.

Lesen Sie, wie Sie Online-Betrug erkennen, bevor ein Schaden entsteht, und wie Sie Ihr Internetkonto effektiv schützen.

Online-Banking in der Praxis

Nur wenn die Verbindung zwischen Ihrem Computer und Ihrer Bank verschlüsselt ist, sollten Sie Ihre Kontobewegungen online durchführen. Im Zweifelsfall überprüfen Sie das Sicherheitszertifikat Ihrer Bank.

1. Sichere Browser-Verbindungen

Verdächtiges SSL-Zertifikat: Der Hinweis auf ein abgelaufenes Zertifikat deutet auf eine Phishing-Seite hin.

Normalerweise werden alle Daten beim Surfen im Klartext übertragen, das gilt prinzipiell sogar für Account-Namen und Passwörter. Damit jedoch niemand die Kommunikation zwischen Internet-Nutzer und Online-Bank ausspioniert, verschlüsseln alle Finanzinstitute die Verbindung mit SSL.

Sie erkennen eine mit SSL gesicherte Verbindung an der Gelbfärbung der Adresszeile sowie an dem geschlossenen Vorhängeschloss in der Adresszeile. Ausserdem handelt es sich um eine verschlüsselte Verbindung, wenn die URL in der Adresszeile mit "https://" beginnt.

2. SSL-Zertifikat überprüfen

Möglicherweise handelt es sich um eine Phishing-Seite, wenn Ihr Browser beim Besuch einer per SSL geschützten Webseite ein Fenster öffnet, in dem vor einem abgelaufenen oder einem für eine andere Seite ausgestellten Zertifikat gewarnt wird. Weitere Informationen zum Zertifikat erhalten Sie, wenn Sie auf den Button *Zertifikat überprüfen* klicken.

Kontaktieren Sie Ihre Bank, bevor Sie eine Transaktion über eine Seite mit einem dubiosen Zertifikat durchführen.

3. Phishing-Webseiten blockieren

Die Browser-Erweiterung Siteadvisor (**www.siteadvisor.com,** kostenlos) verhindert den Aufruf von gefälschten Webseiten. Jede Seite, die Sie besuchen wollen, wird dazu mit einer Datenbank bekannter Phishing-URLs verglichen.

Die McAfee-Tochter Siteadvisor testet die Adressen in der Datenbank mit mehreren Verfahren: So führt das Unternehmen Test-Downloads der angebotenen Dateien durch, meldet sich bei E-Mail-Verteilern an, um Spammer zu erkennen, und bewertet aggressive Pop-ups.
Sie finden Siteadvisor für Firefox sowie für den Internet Explorer zum Download unter **www.siteadvisor.com/**download.

4. Richtiger Umgang mit URLs

Klicken Sie nicht auf Links in E-Mails oder auf Webseiten, die vorgeben, zu Ihrer Online-Bank zu führen. Es könnte sich um eine Fälschung handeln. Rufen Sie die Adresse Ihrer Bank nur auf, indem Sie die URL selbst eintippen oder ein eigenes Bookmark verwenden.

5. Online-Banking unterwegs

Verzichten Sie auf Online-Banking an einem öffentlichen Computer, beispielsweise in einem Internet-Café. Selbst wenn die Verbindung verschlüsselt ist, kann doch ein heimlicher Keylogger auf dem Computer installiert sein.

Kartenleser: Eine Smartcard erhöht die Sicherheit.

Dieser schneidet alle Tastatureingaben inklusive Ihrer Kontonummer und Ihrer PIN mit.

6. Zugangsdaten ändern

Ändern Sie Ihre PIN regelmässig, sofern Ihre Bank diese Funktion anbietet. Loggen Sie sich dazu in Ihrem Online-Konto ein. Sie finden die Option unter Einstellungen oder einem ähnlichen Punkt.

Beachten Sie die Sicherheitshinweise Ihrer Bank. Meist sind neben Ziffern auch grosse und kleine Buchstaben möglich. Durch eine Mischung erhöhen Sie die Sicherheit Ihrer PIN. Verwenden Sie keine Wörter, die sich in einem Lexikon finden.

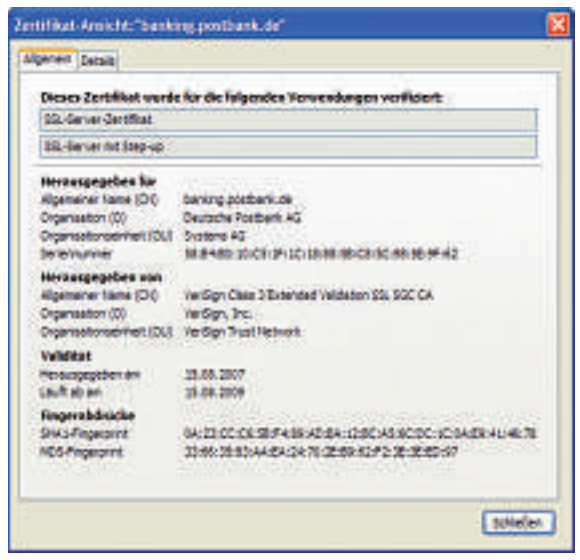
Profi-Tipps

Das herkömmliche TAN-Verfahren gilt als nicht mehr zeitgemäss. Welche Verbesserungen die Banken heute anbieten, lesen Sie in den folgenden Abschnitten.

7. SHA1-Check

Mit dem SHA1-Fingerprint lässt sich die Echtheit eines SSL-Zertifikats überprüfen. Der SHA1-Wert ist ein eindeutiger Fingerabdruck, der die Echtheit einer besuchten Webseite garantiert. Sie finden ihn auf den Support-Seiten Ihrer Bank.

Um ihn zu überprüfen, rufen Sie eine mit SSL geschützte Webseite Ihrer Online-Bank auf und klicken doppelt auf das Schloss-Symbol unten rechts. Unter Firefox wechseln Sie anschliessend zum Reiter *Sicherheit* und klicken auf *Anzeigen*. In der vorletzten Zeile sehen Sie den *SHA1-Fingerprint*. Beim Internet Explorer findet sich der SHA1-Fingerprint auf dem Reiter *Details* in der letzten Zeile hinter *Fingerabdruck*.



SHA1-Fingerprint: Der SHA1-Wert in der vorletzten Zeile muss mit den Angaben Ihrer Bank übereinstimmen.

8. Smartcards einsetzen

Einige Online-Banken setzen bereits auf HBCI. Für dieses Verfahren benötigt der Kunde nicht nur wie bisher seine Zugangsdaten, sondern zusätzlich einen Chipkartenleser sowie seine persönliche Smartcard.

Dies ist jedoch mit Zusatzkosten für den Kunden verbunden, der die Hardware meist für etwa 20 bis 80 Franken selbst kaufen muss.

Andreas Th. Fischer

Symantec Sicherheitstipp

Sicherheitstipp von Virenforscher Candid Wüest

Norton from symantec

Bergen Hot-Spots Gefahren?

Wer ungeschützt einen der zahlreichen Hot-Spots in Cafés, Hotels oder an Bahnhöfen nutzt, setzt sich einem hohen Risiko aus: Im Extremfall liest der Nachbar mit. Dabei hilft eine Sicherheitssoftware mit Firewall und Virenschutz. Für Online-Banking oder -Shopping empfiehlt sich zudem ein VPN (Virtual Private Network).

Vorsicht ist auch daheim angesagt: Diejenigen, die sich zuhause ein drahtloses Funknetz (WLAN) einrichten, sind vom Grundsatz her den gleichen Gefahren ausgesetzt wie an öffentlichen Hot-Spots. Daher sollte neben den genannten Sicherheitsfunktionen im privaten WLAN eine Verschlüsselung zu jeder Zeit aktiviert sein und ein cleveres Passwort gewählt werden.

Mit geringem Aufwand ist eine sehr hohe Sicherheit erreichbar – so macht Mobilität wirklich Spass!

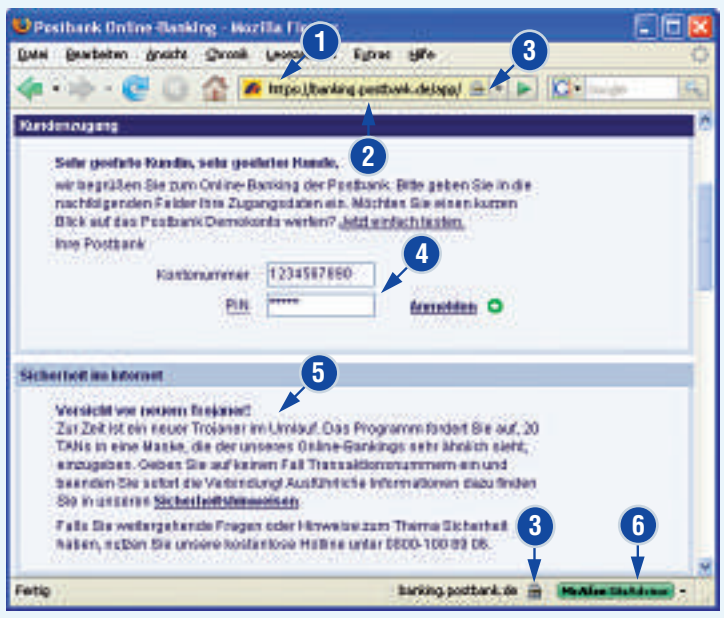
Norton 360 Version 2.0

- Rundumschutz: PC-Sicherheit, Optimierung, Backup und Wiederherstellung
- Keine Einbussen der Computerleistung
- **Schützt vor Online-Identitätsdiebstahl**
- Phishingschutz macht Transaktionen sicher
- **Überwacht den Sicherheitsstatus des drahtlosen Netzwerks**
- Browserschutz blockt Schadcode von infizierten Webseiten
- **Verwaltet und verschlüsselt Passwörter**
- Verhaltensbasierte Technologie erkennt unbekannten Schadcode und gefälschte Webseiten

www.norton.ch

ONLINE-BANKING: SO ERKENNEN SIE DIE ORIGINALSEITE IHRER BANK

Nur wenn Sie Ihre Online-Geschäfte über verschlüsselte Verbindungen durchführen, können die Kontobewegungen unterwegs nicht ausspioniert werden. An folgenden Merkmalen erkennen Sie in Firefox, ob die Verbindung sicher ist.



1. **SSL-Verschlüsselung:** Die Internetadressen von verschlüsselten Webseiten beginnen mit "https://".
2. **Gelbe Adressleiste:** An der Gelbfärbung der Adressleiste erkennen Sie am schnellsten eine SSL-Verbindung.
3. **Schloss-Symbol:** Die geschlossenen Vorhängeschlösser zeigen ebenfalls, dass die Verbindung mit SSL gesichert ist.
4. **Kontonummer und PIN:** Falls schon beim Einloggen zusätzlich eine TAN verlangt wird, handelt es sich um eine Phishing-Seite.
5. **Sicherheitshinweis:** Lesen Sie immer die aktuellen Infos Ihrer Bank. Oft finden sich hier Informationen über aktuelle Gefahren.
6. **Siteadvisor-Erweiterung:** Siteadvisor ist ein kostenloses Add-on für Firefox. Die grüne Farbe des Buttons zeigt, dass die Webseite nicht gefälscht ist.