Kennen Sie die 9 Säulen für sicheres Online-Banking?

Beim Online-Banking wird weniger und seltener Geld gestohlen als beim Bezahlen mit Bargeld. Soll heißen: Der Geldbeutel mit Bargeld fällt eher in die Hände von Dieben als dass es beim Online-Banking zu Diebstählen kommt. Da die Medien aber lieber über entleerte Konten als über gestohlene Portemonnaies berichten, ergibt sich bei vielen Bürgern ein anderes Bild.

Wir wollen die Statistik weiter verbessern und geben Ihnen 9 Säulen an die Hand, die nicht nur Ihr Online-Banking noch sicherer machen, sondern durch deren Befolgung Sie auch im Falle eines Diebstahls sicherstellen, dass die Haftung der Bank greift. Denn was viele nicht wissen: Wenn beim Online-Banking etwas schief läuft und man bestohlen wird, greift oft eine Versicherung der Bank und man erhält sein Geld zurück. Doch dafür müssen Sie diese 9 Dinge befolgen, um der Bank beweisen zu können, dass Sie alle notwendigen Sicherheitsvorkehrungen getroffen haben. Vor allem die Punkte 5 und 6 sind extrem wichtig!

1. SSL: Kontrolle der Adresse

Der erste Schritt beim Online-Banking ist immer, dass Sie die Adresse Ihrer Bank in den Browser eintippen. Hierbei ist auf zwei Dinge zu achten: Erstens tippen Sie die Adresse bitte wirklich immer neu mit der Tastatur ein. Nutzen Sie keine Lesezeichen und keine Links aus E-Mails. Auch dann nicht, wenn Sie das Lesezeichen selbst angelegt haben und wenn die E-Mail mit einem Link von Ihnen als sicher erachtet wird. Bitte immer die Adresse manuell neu eintippen. Und zweitens: nachdem Sie auf die Seite Ihrer Bank gewechselt sind, schauen Sie bitte erneut in die dünne Zeile ganz oben im Browser, die sogenannte Adresszeile, dort, wo Sie die Adresse zuvor eingegeben haben. Hier kontrollieren Sie bitte, ob ganz vorne ein Zeichen der SSL-Verschlüsselung zu erkennen ist. (Wenn Sie nicht wissen, was SSL ist, hilft Ihnen unser Erklärfilm zum Thema SSL weiter: **hier klicken**.) Und kontrollieren Sie bitte auch, ob immer noch der Name Ihrer Bank in der Adresszeile zu erkennen ist. Sollte hier etwas gänzlich anderes stehen, dann ist es Zeit, vorsichtig zu werden.

2. Anmeldename: Nicht die Kontonummer

Wenn Sie sich zum Online-Banking bei Ihrer Bank anmelden, so funktioniert dies mit einem Anmeldenamen, oft auch Benutzername genannt, und einem dazugehörigen Passwort. Natürlich sollte das Passwort möglichst sicher sein. Wie man sichere Passwörter erstellt, das erklären wir unter anderem in diesem Film: **hier klicken**. Aber auch der Anmeldename ist für die Sicherheit entscheidend. Bei einigen Banken darf man als Anmeldename die eigene Kontonummer verwenden. Das ist aber nicht ratsam! Bitte nutzen Sie einen gesonderten Anmeldenamen, der nicht mit Ihrem Vor- oder Zunamen und nicht mit Ihrer Kontonummer verknüpft ist, sofern dies bei Ihrer Bank möglich ist. Dies erhöht die Sicherheit!

3. Computer: Nur der eigene

Manchmal ist man gezwungen oder in Versuchung, eine dringende Überweisung von unterwegs zu tätigen, also nicht von zuhause, nicht vom heimischen Computer, nicht innerhalb des eigenen WLAN. Wenn Sie dies tun, gibt es zwei absolute Grundregeln, die Sie bitte niemals verletzen dürfen, sonst gefährden Sie die Sicherheit Ihres Bankkontos immens!

Erstens: Nutzen Sie mit Ihrem Laptop, wenn Sie unterwegs sind, niemals ein völlig fremdes WLAN, wenn Sie Online-Banking betreiben. Alle Daten, die über ein ungesichertes oder fremdes WLAN laufen, können mitgelesen und aufgezeichnet werden. Sie wissen nämlich über das WLAN nichts Genaues, ob und wie es verschlüsselt und gesichert ist, wer gerade noch alles in dem WLAN angemeldet ist und welche Einstellungen der Router hat, der das WLAN-Signal aussendet. Nur, wenn Sie den Besitzer des WLAN sehr gut kennen, beispielsweise im Haus eines guten Freundes, dann wäre die Gefahr weitestgehend gebannt.

Zweitens: führen Sie niemals Online-Banking an einem völlig fremden Computer durch, zum Beispiel in einem Internetcafé oder in der Lobby eines Hotels. Die Gefahren hier sind sehr vielfältig, solche Computer könnten auf verschiedenste Arten manipuliert sein. Bitte merken Sie sich einfach: Online-Banking immer nur am eigenen Computer, niemals an einem fremden Computer.

4. Grenze: Überweisungslimit einrichten

Für den schlimmsten Fall, dass mal etwas schief laufen sollte, können Sie eine Obergrenze (Limit) für ausgehende Überweisungen einrichten. Dadurch kann pro Tag nur noch diese von Ihnen festgelegte Euro-Summe überwiesen

werden. So wäre es den Kriminellen maximal möglich, diesen Betrag von Ihrem Konto zu stehlen. Aber bedenken Sie: diese Obergrenze dürfen auch Sie selbst mit Ihren Überweisungen nicht überschreiten. Eine sehr niedrige Obergrenze von 80 Euro wäre somit unpraktisch 

5. Absichern: Virenscanner ist Pflicht

Natürlich darf der Hinweis nicht fehlen: Ohne Virenscanner helfen alle Tipps und Tricks nichts. Wenn der Computer durch einen Trojaner befallen ist, können die Kriminellen nicht nur mitlesen, sondern Ihren Computer auch fernsteuern, ohne dass Sie etwas davon mitbekommen. Heutige kostenfreie Virenscanner von allen Herstellern sind in der Regel gut genug, um uns für den normalen Alltag abzusichern. Es gibt aber immer noch Millionen Computer, die keinen Virenscanner installiert haben – man mag es kaum glauben.

Und falls Sie nicht wissen, ob Sie wirklich einen Virenscanner besitzen, dann fragen Sie uns, wir helfen Ihnen und stehen Ihnen ratsam beiseite. **Hier zeigen wir, wie man einen Virenscanner installiert.**

6. Vorsorgen: Updates im Betriebssystem

Der Virenscanner hilft, um mögliche Bedrohungen auf dem Computer zu erkennen und zu beseitigen. Er ist also vergleichbar mit der Feuerwehr, die antritt, wenn das Feuer ausgebrochen ist. Doch noch besser ist es, dafür zu sorgen, dass überhaupt erst gar kein Feuer ausbricht, sprich dass überhaupt keine Schadprogramme wie Viren oder Trojaner auf den Computer gelangen.

Dafür sind zwei Dinge ausschlaggebend: Einerseits benötigt der Anwendung , also der Mensch vor dem Bildschirm, eine nötige Erfahrung und Sicherheit in der Computernutzung. Dafür sorgen wir mit Levato, unsere Mitglieder sind deutlich besser gegen mögliche Betrugsversuche gewappnet. Andererseits ist das Installieren neuer Updates im Betriebssystem ein absolutes Muss. Auch der Browser, über den das Online Banking betrieben wird, muss mittels Updates auf dem aktuellsten Stand sein. Diese beiden Voraussetzungen gelten sogar als rechtliche Grundlage, für die der Bankkunde sorgen muss. Nur, wenn der Kunde diese Grundlagen der Updates erfüllt, kann er im Betrugsfall auf die Haftung der Bank (Schutzpflicht) hoffen und somit von der Bankenversicherung profitieren, die das Geld des Opfers erstattet.

7. Passwort: Mensch als Schwachstelle

So gut der Computer auch abgesichert sein mag, durch teure Virenscanner und andere Schutzprogramme, und so sehr einem die möglichen Schwächen des PIN-TAN-Verfahrens in Medienberichten als problematisch erscheinen, wenn man von technischen Raffinessen der Cyber-Kriminellen in bedrohlich anmutenden journalistischen Berichten von aktuellen Betrugsfällen hört und liest: die größte Schwachstelle ist der Mensch. Das war schon immer so und es wird auch lange so bleiben.

Nur, wer am Computer selbst aufmerksam ist, kann den Betrügern entwischen. Und das größte Risiko sind die von uns Menschen erdachten Passwörter, die den kompletten Vorgang absichern. So ist natürlich auch beim Online-Banking ein sicheres Passwort das A und O. Bei allen Passwörtern gilt: 12 Zeichen lang, Großbuchstaben, Kleinbuchstaben, Ziffern, Sonderzeichen. Nur wenn diese fünf Eigenschaften erfüllt sind, ist ein Passwort sicher genug für unseren aktuellen digitalen Alltag. Mehr Infos zu sicheren Passwörtern und dem Verwalten von oftmals vielen Passwörtern erfahren Sie in unserem Kurs “Passwörter”: **bitte hier klicken**. Zudem sollten Sie das Passwort für Ihr Online-Banking nicht im Browser speichern lassen.

8. Spuren: Browser als “Inkognito” nutzen

Ein sinnvoller Tipp für das Online-Banking ist die Nutzung des Inkognito-Modus. Dieser “private Modus” ist eine Funktion des Browser, der die Aufzeichnung des sogenannten “Browserverlaufs” für eine bestimmte Zeit stoppt. Das erhöht die Sicherheit während des Online-Banking.

Wie der Inkognito-Modus aktiviert wird und weitere Informationen zu dieser Sicherheitsmaßnahme erfahren Sie in unserem Beitrag “ **Inkognito – Mehr Privatsphäre auf Knopfdruck**“.

9. Kontrolle: Der tägliche Blick aufs Konto

Das Online-Banking bietet eine weitere tolle Möglichkeit: man kann jederzeit, so oft man will, mehrfach täglich in das eigene Konto hineinschauen. Das erlaubt es uns, jederzeit in Echtzeit den Kontostand abzufragen. Und dadurch würden wir sofort mitbekommen, ob es eine betrügerische Kontobewegung gibt. Das Wissen, immer und in Sekundenschnelle einen Blick auf das eigene Konto werfen zu können, kann nicht nur beruhigen, sondern ist als echte Waffe gegen Betrüger zu betrachten.

Wenn Sie täglich in Ihr Konto schauen, kann eine betrügerische Überweisung sofort erkannt werden und durch einen Anruf bei der Bank unterbunden

werden. Oftmals können die Banken noch am selben Tag einer Betrugsüberweisung das Geld “zurückholen”. Zudem ist es ein ganz wesentlicher Faktor, dass Sie einen Betrug schnellstens erkennen und mitteilen. Denn wenn Sie Ihrer Bank mitteilen, dass vor langer Zeit eine Betrugsüberweisung auf Ihrem Konto geschehen ist, können selbst die für solche Fälle versicherten Banken nicht mehr viel tun. Wenn Sie Ihrer Bank eine Mitteilung über einen Cyber-Diebstahl innerhalb weniger Stunden oder Tage machen, und sich über alle weiteren 8 oben stehenden Punkte abgesichert wissen, dann haben Sie berechtigte Hoffnung, dass die Schutzpflicht der Bank in Kraft tritt und Sie selbst nicht für den Schaden haften müssen: Sie bekämen Ihr Geld zurück.