MULTIMEDIASUPPORT

Riccardo Dizioli
Tödistrasse 121
CH-8800 Thalwil

# Tipps für sicheres Onlinebanking

Jeder Tipp ist für sich alleine eine Verbesserung der Sicherheit, je mehr Tipps umgesetzt werden, umso mehr nimmt die Sicherheit zu. Die unten aufgelisteten Tipps haben keine bestimmte Reihenfolge, sie sind auch nicht alle zwingend notwendig. Auch können sie nach und nach umgesetzt werden. Wichtig ist, dass sie immer einer neuen Situation angepasst werden.

- ➔ Lassen sie die tägliche Bezugshöhe bei ihrer Bank limitieren. Erlauben Sie via Onlinebanking nur Zugriff auf Konten die Sie wirklich benötigen. (Andere Konten können Sie auch nur anzeigen lassen, ohne Zugriffsmöglichkeit)

- ➔ Schützen Sie das Administratorkonto mit einem Passwort nach dem Einrichten des Laptops / PCs. Erstellen Sie ein neues Konto mit Standardrechten für das tägliche arbeiten zum Surfen und für den Mailverkehr. Erstellen Sie ein zweites Passwortgeschütztes Konto mit Standardrechten nur für das E-Banking.

- ➔ Achten sie darauf, dass bei neuen Zahlungsaufträgen und höheren Beträgen auf bestehenden Zahlungsvorlagen ein Bestätigungs-Code auf Ihr Handy gesendet wird. (Je nach Bank verschieden)

- ➔ Arbeiten sie mit für das Online-Banking mit einem alternativen Browser, nicht mit IE8 oder 9. (ZB. Firefox, Chrome, Safari) den Sie sonst nicht benutzen.

- ➔ Bevor Sie ihre Bankseite aufrufen, sollten sie alle Programme und offenen Webseiten schliessen. Öffnen sie nun die Bankseite in einem neuen Fenster. Nutzen sie die sicheren Modi der Browser. Führen Sie zuvor einen Scan mit Malwarebytes als Administrator aus. https://de.malwarebytes.com/ Für Firefox: "Ein neues privates Fenster öffnen" In Chrome: «Neues Inkognito Fenster» öffnen, Edge: «Neues InPrivate-Fenster» öffnen.

- ➔ Benutzen sie nicht die Favoriten oder Lesezeichen um die Loginseite für das Online-Banking aufzurufen, gehen sie zuerst auf die Hauptseite ihrer Bank und erst danach mit dem angegebenen Link auf die Loginseite. Oder tippen sie die URL von Hand ein.

- ➔ Benutzen sie nicht die Passwortspeicherung ihres Browsers für ihre Loginseite.

- ➔ Nach dem Login sollte in ihrem Browser der URL-Anfang von http auf https wechseln. Im Edge, Firefox und Chrome erscheint ein grünes Schloss links vom Link. Über das Schlosssymbol können sie sich auch das Zertifikat anzeigen lassen. In den neuesten Browsern wird die Adressleiste grün eingefärbt.

- ➔ Schliessen sie den Browser sofort, wenn sie eine ungewöhnliche URL entdecken.

- ➔ Verwenden sie eine Antiviren-Software die sich täglich über das Internet aktualisiert. Prüfen sie Ihr System von Zeit zu Zeit mit einer ergänzenden Schutz-Software. (ZB. Ad-Aware, Malwarebytes und einem beliebigen Online-Scanner)

- ➔ Kommt ihnen die Loginseite ungewöhnlich vor, geben sie absichtlich einen falschen Tan-Code ein. Eine Illegale Seite kann die Richtigkeit ihres Codes nicht überprüfen. Anhand der Fehlermeldung wissen sie, ob sie auf der richtigen Website sind. Danach geben sie den richtigen Code ein. (Phishing)

- ➔ Ändern sie von Zeit zu Zeit ihr Passwort / Pin-Nummer. Ein Sicheres Passwort besteht aus Gross-Kleinschreibung, Zahlen und Sonderzeichen. Mindestlänge 12 Zeichen.

- ➔ Reagieren sie nie auf Mails, die angeblich von ihrer Bank kommen. Ihre Bank wird sie nie per Mail kontaktieren. Geben sie nie Passwörter und andere Logindaten Preis. Benachrichtigen Sie bei Betrugsmails Ihre Bank.

- ➔ Melden Sie sich immer korrekt ab und schliessen Sie den Browser. Löschen sie nach jeder Online-Banksitzung ihre persönlichen Daten im Browser. (IE8/9: "Extras/ Internetoptionen/Allgemein/Löschen". Firefox: Im Menü Extras, die Position "Private Daten löschen" anklicken oder "Extras/Neueste Chronik" löschen) Oder machen Sie nach dem Abmelden einen Scan mit dem Systemreinigungs-Programm CCleaner. http://www.piriform.com/ccleaner/download

- ➔ Achten sie darauf, dass ihr Computer immer alle neuen Betriebssystem-Aktualisierungen von Microsoft installiert und ihr Browser auf dem neuesten Stand ist. Vermeiden Sie wenn möglich Freeware-Programme. Sie beinhalten oft Malware. (Spionagecode)

- ➔ Benutzen sie wenn möglich ihren eigenen PC für ihr Online-Banking. Wenn sie sich über WLAN ins Internet begeben, achten sie darauf, dass diese Verbindung richtig installiert und sicher ist. (WPA Verschlüsselung, Passwort, SSID). Benutzen sie nie PCs in Internetcafés oder dergleichen, auch nicht um E-Mails abzufragen, da ihre Logindaten einfach abgefangen werden können, ausser die Seite für die Passworteingabe ist verschlüsselt. Sie wissen jedoch nicht ob die Tastatureingabe aufgezeichnet wird.

- ➔ Installieren sie einen Router neuster Technologie, auch wenn sie Zuhause nur mit einem PC arbeiten. Bevorzugen sie immer eine Kabelverbindung zwischen PC / Laptop und Router.

- ➔ Wenn Sie es noch sicherer machen wollen, nehmen Sie einen älteren Laptop / PC nur für das E-Banking (Sie dürfen damit keine Mailabfragen machen und nicht im Internet surfen). Nehmen Sie für den Code Empfang ein Prepaid-Handy das keinen Internetzugang hat. So kann das Handy nicht manipuliert werden.