

Wichtige Verhaltensregeln im Online-Banking

Clariden Leu bietet die bestmögliche Sicherheit im Online-Banking und trägt dazu bei, das Computersystem der Bank und die elektronische Datenübermittlung zu schützen. Trotzdem ist es für die Online-Banking-Kunden von grosser Wichtigkeit, auch den eigenen PC zu schützen. Bitte beachten Sie deshalb die im Folgenden beschriebenen Verhaltensregeln im Online-Banking!

Die 10-Punkte-Checklist: Schützen Sie sich vor unberechtigten Zugriffen


- 1. Virenschutz und Firewall**
Schutzsoftware ([Antiviren-Software](#) und [Firewall](#)) installieren und regelmässig aktualisieren.

- 2. Eingeschränktes Profil verwenden**
Sie können die Sicherheit weiter erhöhen, wenn Sie nur unter einem [eingeschränkten Benutzerprofil](#) im Internet surfen und damit auch Online-Banking benützen.

- 3. Malware – böartige Links und Attachments in E-Mails**
Der Begriff «Malware» setzt sich aus den englischen Begriffen «Malicious» und «Software» zusammen. Oberbegriff für Software, die schädliche Funktionen auf einem Rechner ausführt (wie beispielsweise Viren, Würmer, Trojanische Pferde). Klicken Sie keine auffälligen Mails von unbekanntem Absendern an. Auf keine in E-Mails zugesandten Links klicken, die vorgeben, Sie zu Ihrem Online-Banking führen zu wollen. Vorsicht ist auch bei Attachments (d.h. allen angehängten Dateien in E-Mails) geboten. Sie können solche Mails direkt mit der Tastenkombination Shift/Delete löschen (in Microsoft Office Outlook).

- 4. Phishing**
Nie auf Anfragen und/oder Aufforderungen per Telefon oder E-Mail nach Ihren Zugangsdaten zum Online-Banking antworten. Ihre Bank fragt Sie nie danach. Installieren Sie keine Software aus unbekanntem Quellen; diese können Viren enthalten.

- 5. Zusammensetzung und Aufbewahrung Ihres Passworts**
Verwenden Sie kein Passwort, das aus Geburtsdatum, Telefonnummern oder gar Namen besteht.
Besser: Ein aus Buchstaben und Zahlen bestehendes Passwort kreieren.
Passwörter gehören nicht auf den Computer – weder auf die Festplatte noch auf ein Zettelchen am Bildschirm.

- 6. Zertifikat überprüfen**
Überprüfen Sie mit einem Doppelklick auf , ob das [Zertifikat](#) korrekt auf claridenleu.directnet.com lautet.

- 7. Systemunterbruch/ungewöhnliche Fehlermeldungen**
Kommt es beim Online-Banking während der Internetsitzung zu einem Systemunterbruch (z.B. plötzlich auftretender weisser Bildschirm) oder treten v.a. während dem Login ungewöhnliche Fehlermeldungen auf (z.B. «Das System ist derzeit überlastet. Bitte haben Sie etwas Geduld und probieren Sie es später noch einmal»), beenden Sie bitte sofort die Verbindung und benachrichtigen Sie unsere Spezialisten (Tel.-Nr. 0844 800 888, International: + 41 844 800 888 oder + 41 44 657 36 40).

- 8. Keine anderen Seiten öffnen**
Öffnen Sie beim Verbindungsaufbau zum Online-Banking der Credit Suisse und während der Benutzung von Direct Net keine anderen Internetseiten und keine E-Mails. Ausserdem empfehlen wir, Online-Banking nur von einem bekannten und sicheren PC zu benutzen (d.h. nicht in Internet Cafés).

- 9. Korrektes Beenden der Direct Net Sitzung**
Verlassen Sie Ihren Computerarbeitsplatz erst, wenn Sie die Online-Banking-Sitzung beendet haben. Direct Net immer mit der dafür vorgesehenen Funktion «Abmelden» schliessen und den Computer nicht einfach herunterfahren.

- 10. Browser-Cache leeren**
Leeren Sie nach jeder Abmeldung aus dem Online-Banking den Zwischenspeicher (Browser-Cache).
Die Anleitung (je Internetbrowser) wird jeweils direkt nach jedem korrekten «Abmelden» aus Direct Net angezeigt.

Beachten Sie auch die Informationen und Warnungen, welche von Kobik (nationale Koordinationsstelle des Bundes zur Bekämpfung der Internetkriminalität, www.kobik.ch) sowie Melani (Melde- und Analysestelle Informationssicherung des Bundes, www.melani.admin.ch) publiziert werden.