MELANI Melde- und Analysestelle Informationssicherung

Sicheres e-Banking

(Checkliste und Anleitung)

Dokument verfügbar unter: www.melani.admin.ch

Version 1.0
14.04.2005

Checkliste „Sicheres e-Banking“

Die einzelnen Punkte sind auf den folgenden Seiten Schritt für Schritt erklärt.

Generelle Massnahmen

Software-Updates durchführen

- Halten Sie Betriebssystem, Webbrowser und alle weiteren Programme auf dem aktuellsten Stand (aktivieren Sie dazu, falls vorhanden, die automatische Update-Funktion)

Antiviren-Software einsetzen

- Setzen Sie eine Antiviren-Software ein und halten Sie diese per Autoupdate auf dem aktuellsten Stand

Personal Firewall verwenden

- Setzen Sie eine Personal Firewall ein und prüfen Sie regelmässig, ob diese aktiviert ist

Vor dem Einloggen

Neues Browserfenster öffnen

- Öffnen Sie den Webbrowser für die e-Banking-Sitzung neu und halten Sie keine zusätzlichen Verbindungen offen

Adresse von Hand eingeben

- Folgen Sie keinesfalls Links in E-Mails oder auf Homepages von Dritten, um auf die e-Banking-Webseite zu gelangen
- Geben Sie die Adresse Ihrer Bank stets von Hand ein

Passwortregeln beachten

- Wählen Sie ein schwer zu erratendes Passwort und wechseln Sie dieses regelmässig
- Geben Sie das Passwort niemandem bekannt und schreiben Sie dieses nirgendwo auf

Während der e-Banking-Sitzung

Authentizität der e-Banking-Seite und Verschlüsselung überprüfen

- Überprüfen Sie anhand des Zertifikats die Authentizität der besuchten Webseite und kontrollieren Sie, ob die Verbindung verschlüsselt ist

Fehlermeldungen beachten

- Beachten Sie allfällige Fehlermeldungen oder Warnhinweise und kontaktieren Sie im Zweifelsfall Ihr Finanzinstitut

e-Banking-Sitzung beenden

Korrekt ausloggen

- Beenden Sie die e-Banking-Sitzung mit der dafür vorgesehenen Funktion „Abmelden“, „Logout“ oder „Beenden“

Temporäre Internetdateien löschen

- Löschen Sie nach der e-Banking-Sitzung die temporären Internetdateien Ihres Webbrowsers

INHALT

Einleitung

Die Meldungen über Betrügereien im Internet tragen zur Verunsicherung der Nutzer bei. Durch Beachtung einfacher Regeln kann die Abwicklung des Zahlungsverkehrs über das Internet (Internet-Banking oder e-Banking) jedoch sicher erfolgen.

Im Folgenden wird Schritt für Schritt aufgezeigt, wie die auf der vorangegangenen Checkliste aufgeführten Punkte umgesetzt werden können. Auf der letzten Seite finden Sie Links zu weiterführenden Informationen.

Anmerkung: Beachten Sie stets die Sicherheitsempfehlungen Ihrer Bank.

Generelle Massnahmen

Software-Updates durchführen

Auf Grund ständig neu identifizierter Sicherheitslücken ist unbedingt darauf zu achten, dass das Betriebssystem und der Webbrowser immer auf dem neuesten Stand gehalten werden. Die meisten Betriebssysteme bieten dafür eine automatische Update-Funktion, die Sie unbedingt aktivieren sollten. Halten Sie auch andere Applikationen (z.B. E-Mail-Programme, Media Player, Textverarbeitungsprogramme, Chat-Software usw.) auf dem aktuellsten Stand. Links zu den Software-Update-Seiten der Hersteller finden Sie unter:
http://www.melani.admin.ch/themen/00166/00169/index.html?lang=de

Antiviren-Software einsetzen

Setzen Sie eine aktuelle Antiviren-Software ein und halten Sie diese mittels automatischer Updatefunktion auf dem neusten Stand. Um einen möglichst hohen Schutz vor Spyware und Adware zu erreichen, empfiehlt sich zudem der Einsatz von Tools, mit denen Sie diese Schädlinge erkennen und entfernen können. Links zu Herstellern von Antiviren-Software finden Sie unter:
http://www.melani.admin.ch/themen/00166/00170/index.html?lang=de

Links zu Herstellern von Spyware- / Adware-Tools finden Sie unter:
http://www.melani.admin.ch/dokumentation/00126/index.html?lang=de

Personal Firewall verwenden

Verwenden Sie eine Personal Firewall, um unerwünschte Internetverbindungen zu verhindern. Einige Betriebssysteme (z.B. Windows XP, Mac OS X usw.) verfügen standardmässig bereits über ein solches Tool. Zudem stehen Personal Firewalls kostenlos im Internet zum Download bereit. Links zu Herstellern von Personal Firewalls finden Sie unter:
http://www.melani.admin.ch/themen/00166/00168/index.html?lang=de

Vor dem Einloggen

Vor dem Öffnen des Browsers Desktopsuch-Programme deaktivieren

Wenn Sie Desktopsuch-Programme, wie beispielsweise „Google Desktop Search“, „Yahoo Desktop Search“, „MSN Desktop Search“, „Blikx“, „Copernic“, „ISYS Search“, „X1“ usw., einsetzen und Sie sich an einem von mehreren Personen genutzten Computer befinden, sollten Sie die Indexierfunktion deaktivieren oder solche Programme ganz ausschalten. Mehr Informationen dazu finden Sie unter:
http://www.melani.admin.ch/dienstleistungen/archiv/00490/index.html?lang=de

Neues Browser-Fenster öffnen

Für die e-Banking-Sitzung ist der Browser stets neu zu öffnen. Dabei ist zwingend zu beachten, dass während der Sitzung keine weiteren Webseiten geöffnet werden.

Gewisse Browser unterstützen so genanntes „Tabbed Browsing“, d.h. die Möglichkeit, in einem Browser-Fenster mehrere Verbindungen zu öffnen (z.B. Opera, alle Browser der Mozilla-Familie wie Mozilla und Firefox, aber auch Safari unter Mac OS X). Anhand der Tab-Leiste lässt sich bei solchen Browsern am oberen Rand des Browser-Fensters erkennen, ob mehrere Tabs geöffnet sind (Beispiel: Firefox):

Abbildung 1: Falsch – Mehrere Tabs geöffnet in einem Browser-Fenster

Ein Browser-Fenster mit nur einem geöffneten Tab ist in Abbildung 2 zu sehen (ebenfalls am Beispiel des Webbrowsers Firefox):

Abbildung 2: Korrekt – Keine Tabs offen im Browser-Fenster

Adresse von Hand eingeben

Geben Sie nach dem Öffnen des Browsers die Adresse Ihrer Online-Bank stets von Hand ein. Klicken Sie niemals auf Links in E-Mails oder auf Homepages von Dritten,

die Sie angeblich zur gewünschten Webseite führen (selbst wenn diese von Ihrer Bank zu stammen scheinen).

Passwortregeln beachten

Die Finanzinstitute verlangen von ihren Online-Kunden mehrstufige Authentifizierungsverfahren (z.B. Vertragsnummer, Streichliste und Passwort oder Ähnliches). Meist ist ein einzugebendes Passwort vom Kunden frei wählbar und könnte allenfalls leicht erraten werden. Wählen Sie ein schwer zu erratendes Passwort bestehend aus Buchstaben, Zahlen und Sonderzeichen (mind. 8 Zeichen) und wechseln Sie dieses regelmässig. Geben Sie Ihr Passwort niemals einer Drittperson oder dem Finanzdienstleister bekannt. Ihre Bank wird Sie niemals zur Bekanntgabe Ihres Passwortes auffordern. Schreiben Sie das Passwort nirgends auf und speichern Sie es auf keinen Fall auf Ihrem Rechner.

Während der e-Banking-Sitzung

Authentizität der e-Banking-Seite und Verschlüsselung überprüfen

Nach dem Einloggen lassen sich die Verschlüsselung der Verbindung sowie die Authentizität der besuchten Webseite mit Hilfe eines so genannten Zertifikats überprüfen. Führen Sie dazu einen Doppelklick auf das geschlossene Schlosssymbol aus, das sich in der Statuszeile ganz unten im Browser-Fenster befindet (siehe Abbildung 3).

Abbildung 3: Beispiele von Verschlüsselungssymbolen in den Statuszeilen der gängigsten Browser

Dadurch öffnet sich ein Fenster, in dem die Eigenschaften des Zertifikats angezeigt werden. Überprüfen Sie, ob das Zertifikat auf den Namen Ihrer Bank lautet. Überprüfen Sie auch den so genannten Fingerprint/Fingerabdruck des Zertifikats. Stimmt dieser mit dem auf der e-Banking-Webseite publizierten Fingerprint überein, ist eine verschlüsselte Verbindung auf die richtige Seite sichergestellt. Die folgenden Bilder zeigen Beispiele der Eigenschaftsfenster von Zertifikaten:

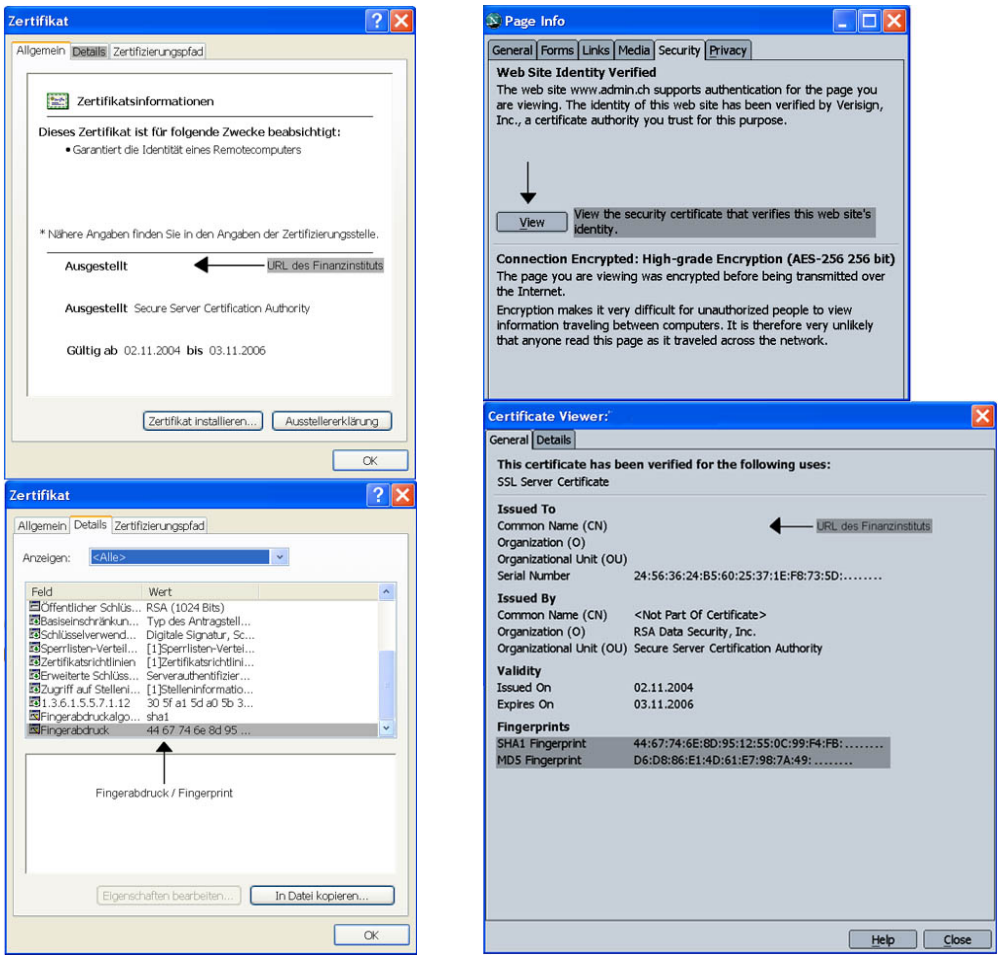

Abbildung 4: Die Zertifikatsfenster im Internet Explorer (links) und im Netscape (rechts)

Die Zertifikatsfenster anderer Browser sehen ähnlich aus, so dass die Fenster in Abbildung 4 sinngemäss auch für diese gelten.

Fehlermeldungen beachten

Lesen Sie allenfalls angezeigte Fehler- oder Warnmeldungen aufmerksam durch. Wenden Sie sich im Zweifelsfall an die Hotline Ihrer Bank.

E-Banking-Sitzung beenden

Korrekt ausloggen

Beenden Sie die e-Banking-Sitzung immer mit der dafür vorgesehenen Funktion „Beenden“, „Logout“ oder „Abmelden“. Im Browser wird dann meist eine neue Seite als Bestätigung der korrekten Abmeldung anzeigt.

Temporäre Internetdateien löschen

Nach dem Ausloggen empfiehlt es sich, die temporären Internetdateien, den so genannten Cache des Browsers (quasi sein „Gedächtnis“), zu löschen. Auf diese Weise werden lokale Spuren der Online-Sitzung auf Ihrem Computer gelöscht.

Vorgehensweise Internet Explorer (Windows):

- Wählen Sie für den Internet Explorer unter Windows im Menü „Extras“ den Befehl „Internet-Optionen“ an. Es öffnet sich das in Abbildung 5 dargestellte Fenster. Darin klicken Sie auf „Cookies löschen“. Es öffnet sich ein weiteres Fenster, das Sie mit „OK“ bestätigen müssen und damit wieder zum Fenster aus Abbildung 5 zurückkehren.

- Klicken Sie dann auf „Dateien löschen“, worauf sich erneut ein Fenster öffnet. Darin setzen Sie bei „Alle Offlineinhalte löschen“ ein Häkchen und bestätigen dies mit „OK“. Schliessen Sie das Fenster von Abbildung 5 abschliessend mit „OK“.

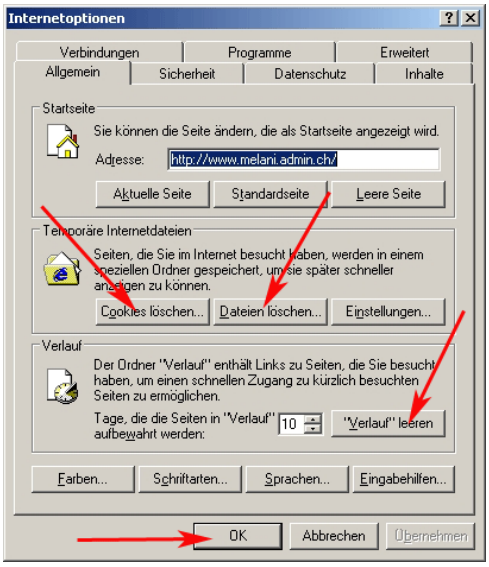

Abbildung 5: Cookies, Offline-Dateien und Verlauf im Internet Explorer löschen (Windows)

Vorgehensweise Firefox (Windows):

- Wählen Sie im Menü „Extras“ den Befehl „Einstellungen“ an. Im sich öffnenden Fenster klicken Sie links auf das mit „Datenschutz“ beschriftete Schlosssymbol (siehe Abbildung 6).

- Anschliessend klicken Sie auf der rechten Feldseite den Knopf „Alles löschen“ an. Bestätigen Sie im sich öffnenden Fenster mit einem Klick auf „Alle Daten löschen“. Danach können Sie das Einstellungsfenster mit „OK“ wieder schliessen.

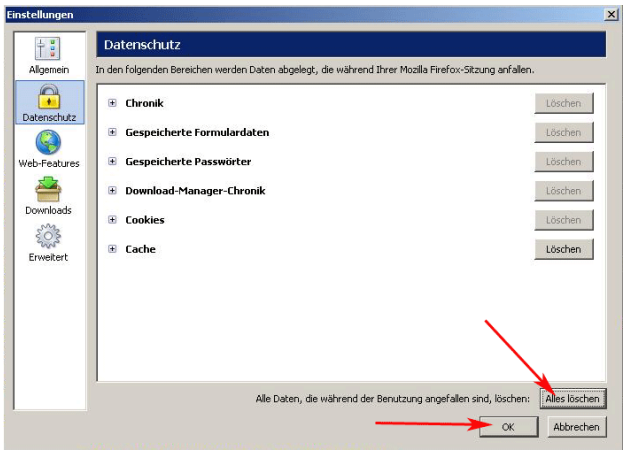

Abbildung 6: Löschen des Cache in Firefox (Windows, Mac OS X)

Vorgehensweise Safari (Mac OS X):

- Klicken Sie das fett dargestellte Menü „Safari“ gleich rechts vom Apfel-Menü an. Wählen Sie darin den Befehl „Cache leeren“ aus (siehe Abbildung 7).

Abbildung 7: Löschen des Cache in Safari, Mac OS X

Vorgehensweise Internet Explorer (Mac OS X):

- Klicken Sie das fett dargestellte Menü „Explorer“ gleich rechts vom Apfel-Menü an (an derselben Stelle wie das Menü „Safari“ in Abbildung 7). Wählen Sie darin „Einstellungen“ aus, worauf sich das Einstellungsfenster öffnet (siehe Abbildung 8).

- Wählen Sie darin auf der linken Seite den Eintrag „Erweitert“ an. Klicken Sie dann auf der rechten Seite auf den Knopf „Jetzt leeren“ und anschliessend auf „OK“. Das Fenster schliesst sich wieder.

Abbildung 8: Löschen des Cache im Internet Explorer, Mac OS X

Vorgehensweise Firefox (Mac OS X):

- Klicken Sie das fett dargestellte Menü „Firefox“ gleich rechts vom Apfel-Menü an (an derselben Stelle wie das Menü „Safari“ in Abbildung 7). Wählen Sie darin den Befehl „Einstellungen“ aus. Es öffnet sich das Einstellungsfenster, das praktisch gleich aussieht wie unter Windows (siehe Abbildung 6).

- Klicken Sie darin auf der linken Seite auf das mit „Datenschutz“ beschriftete Schlosssymbol. Anschliessend klicken Sie auf der rechten Feldseite den Knopf „Alles löschen“ an. Bestätigen Sie im sich öffnenden Fenster mit einem Klick auf „Alle Daten löschen“. Danach können Sie das Einstellungsfenster mit „OK“ wieder schliessen.

Zusätzliche Informationen

Wer die in dieser Kurzanleitung beschriebenen Sicherheitsmassnahmen einhält, kann seine Bankgeschäfte bequem und sicher über das Internet erledigen. Dennoch lohnt es sich, die Gefahren und Risiken in diesem Umfeld genauer zu kennen.

Drohende Gefahren und Risiken:

- Viren:
  http://www.melani.admin.ch/themen/00103/00198/index.html?lang=de
- Würmer:
  http://www.melani.admin.ch/themen/00103/00199/index.html?lang=de
- Trojanische Pferde:
  http://www.melani.admin.ch/themen/00103/00200/index.html?lang=de
- Spyware und Adware:
  http://www.melani.admin.ch/themen/00103/00201/index.html?lang=de
- Social Engineering:
  http://www.melani.admin.ch/themen/00103/00202/index.html?lang=de
- Phishing:
  http://www.melani.admin.ch/themen/00103/00203/index.html?lang=de
- Informationen zu momentan kursierenden Phishing-Maschen:
  www.antiphishing.org

Unter den folgenden Links finden Sie weitere Informationen zu den erwähnten Massnahmen und noch einmal auf einen Blick die Links zu den Herstellern:

- Betriebssystem und Programme aktuell halten:
  http://www.melani.admin.ch/themen/00166/00169/index.html?lang=de
  Links zu den Software-Update-Seiten der Hersteller:
  http://www.melani.admin.ch/dokumentation/00126/index.html?lang=de
- Aktuelle Antiviren-Software einsetzen und regelmässig aktualisieren:
  http://www.melani.admin.ch/themen/00166/00170/index.html?lang=de
  Links zu Herstellern von Antiviren-Software:
  http://www.melani.admin.ch/dokumentation/00126/index.html?lang=de
- Nutzen Sie eine Personal Firewall
  http://www.melani.admin.ch/themen/00166/00168/index.html?lang=de
  Links zu Herstellern von Personal Firewalls:
  http://www.melani.admin.ch/dokumentation/00126/index.html?lang=de
- Deaktivierung von Desktopsuch-Programmen
  http://www.melani.admin.ch/dienstleistungen/archiv/00490/index.html?lang=de