E-BANKING ABER SICHER

PCtipp hat sich die Schweizer E-Banking-Lösungen angeschaut: Wie funktionieren sie? Welche sind sicher? Plus: wichtige Sicherheitstipps fürs Onlinebanking.

VON GABY SALVISBERG

Schon fast jeder vierte Bankkonto- oder Postkontobesitzer in der Schweiz nutzt E-Banking. Die Sicherheitsanforderungen an eine derart heikle Internetanwendung steigen angesichts der wachsenden Cyberkriminalität. So zeigte etwa ein kürzlich von der TV-Sendung Kassensturz durchgeführter Test, wie sich sogar ein relativ sicheres System aushebeln lässt. Die vom Kassensturz angestellten «Hacker» der ETH Zürich konnten ihre Konten bei der Migros Bank, Raiffeisenbank und bei der Berner Kantonalbank um einige Hundert Franken erleichtern. Das gelang ihnen aber nur mithilfe eines Trojaners. Die Schad-Software meldete sich bei den Angreifern, sobald der Benutzer auf seinem PC eine E-Banking-Sitzung startete. Die Hacker waren in der Lage, auf ihren Monitoren den Bildschirminhalt des Opfers darzustellen. Nach dem erfolgreichen Login-Vorgang lenkten sie das Opfer mit einem gefälschten Update-Fenster ab. Das gab ihnen Zeit, im Hintergrund eigene Zahlungsaufträge zu erfassen.

Mit wenigen Sicherheitsmassnahmen sind E-Banking-Nutzer gegen solche Gaunereien geschützt. Denn die Angreifer müssen zum Plündern des Bankkontos einige Hürden nehmen – von der Installation des Trojaners bis hin zum Verbergen der Zahlungsmanipulation.

Fachbegriff

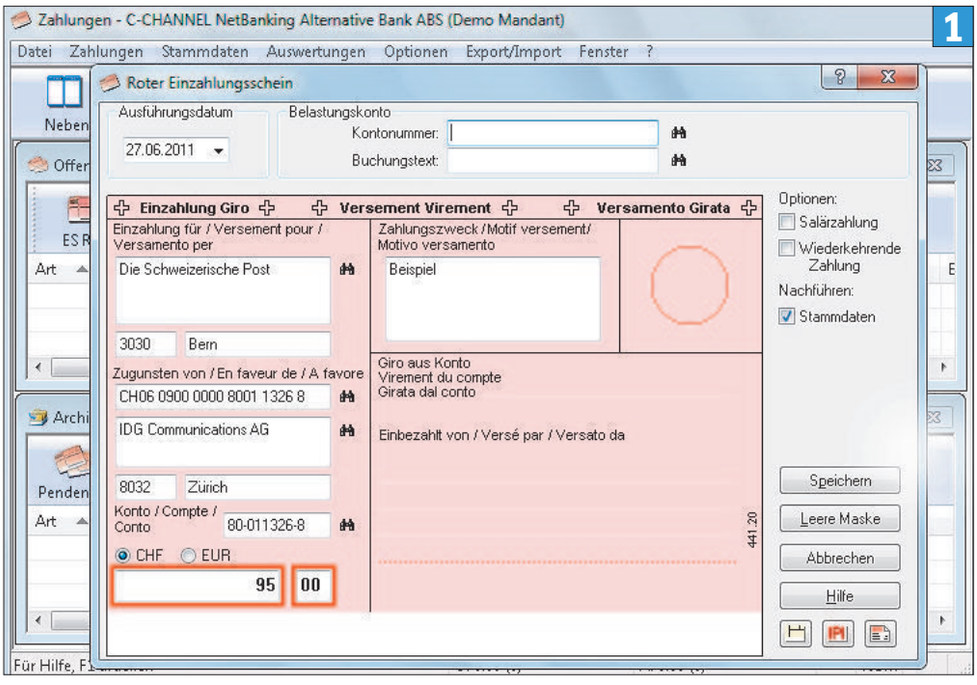
TAN > Steht für Transaktionsnummer. Bei vielen E-Banking-Systemen wird entweder zum Einloggen oder zum Bestätigen einzelner Buchungen eine TAN in Form eines mehrstelligen Codes verlangt. Die TAN kann von einer nummerierten Liste stammen (iTAN: Indexed TAN), per SMS eintreffen (mTAN: mobile TAN) oder auf einem USB-Stick erscheinen.

PCtipp zeigt Ihnen, wie E-Banking funktioniert, welche Systeme es in der Schweiz gibt und wie sicher diese sind. Beim Sicherheitscheck half uns die Schweizer Sicherheitsfirma OneConsult. In der Box auf S. 27 finden Sie zudem die wichtigsten Tipps für ein sicheres Onlinebanking.

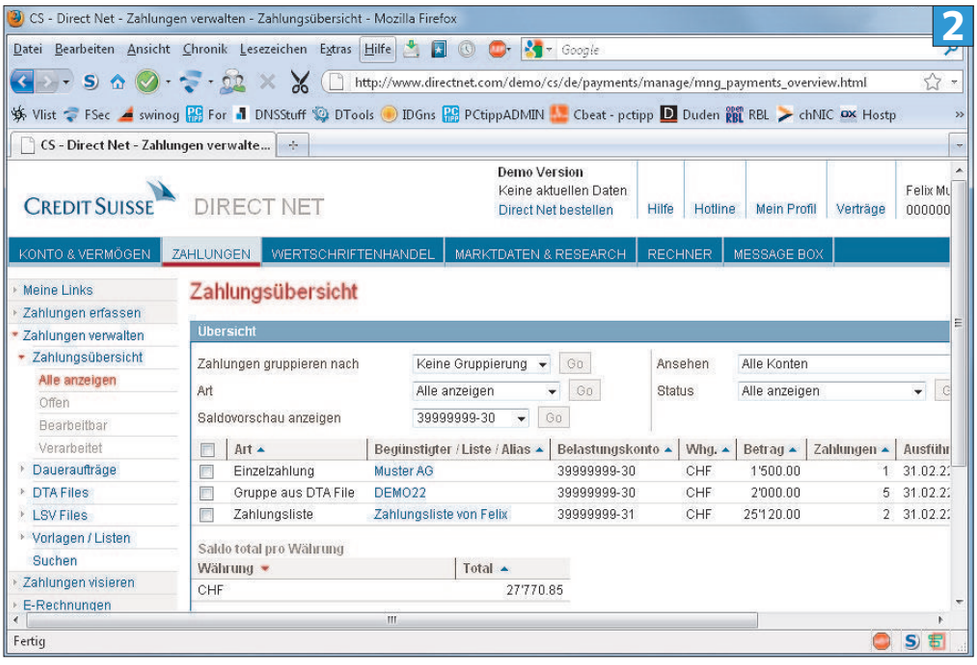
Wie funktioniert E-Banking?

Für die Anmeldung zum E-Banking leisten Sie die erforderlichen Unterschriften, danach erhalten Sie von Ihrer Bank alles, was Sie brauchen. Fortan surfen Sie für die Verwaltung Ihrer Konten, Zahlungen und Wertpapiere zu Ihrer Bankwebseite. Dort loggen Sie sich je nach Bank mithilfe von Vertragsnummer und PIN-Code ein. Es sind hierfür immer noch zusätzliche Elemente erforderlich, sei es ein Kartenleser, ein spezieller USB-Stick oder eine TAN. Die verschiedenen

FOTO ISTOCKPHOTO



Mit einer Software wie NetBanking erfassen Sie Ihre Einzahlungen zuerst bequem offline am PC



Die E-Banking-Lösung lässt sich meistens vorab im Web testen (hier Credit Suisse)

in der Schweiz gängigen Systeme stellen wir Ihnen ab S. 24 vor. Gleichzeitig finden Sie eine Beurteilung, wie sicher diese sind.

Alle Ihre Bankkonten sind in Ihrer E-Banking-Oberfläche versammelt. Damit sehen Sie die Kontostände auf einen Blick. Auch Umbuchungen zwischen den Konten sind ein Kinderspiel. Je nach Bank erstellen Sie bequem Zahlungsvorlagen für regelmässig fällige Überweisungen. Bei Bedarf richten Sie mit wenigen Klicks Ihre Daueraufträge ein. Wer eine Zahlungs-Software verwendet, lädt die daraus erzeugten Dateien in einem Rutsch direkt hoch, **Screen 1**. Welche Zahlungs-Software bei Ihrer Bank erhältlich ist und ob diese etwas kostet, zeigt die Tabelle, S. 26.

Ihre Belastungsanzeigen und sonstigen Belege erhalten Sie in Zukunft in elektronischer Form in Ihrer E-Banking-Oberfläche. Damit reduzieren Sie Ihre Bankspesen erheblich. E-Banking-Zahlungsaufträge im Inland sind bei fast allen Banken gratis. Einzig die UBS verlangt 30 Rappen pro Auftrag, aber auch nur, wenn das Gesamtvermögen unter 10 000 Franken liegt.

Alle Banken und immer mehr Unternehmen sowie Organisationen unterstützen ausserdem E-Rechnungen. Dazu gehören Versicherungen, Gemeinden, Elektrizitätswerke, Verkehrsbetriebe, Telekommunikationsanbieter etc. Welche das sind, erfahren Sie unter www.e-rechnung.ch in der Rubrik Rechnungssteller oder direkt in Ihrem Onlinebankkonto in einem Menü wie E-Rechnung oder PayNet.

Die E-Rechnung landet in elektronischer Form inklusive druckfähiger PDF-Rechnung direkt in Ihrem Onlinebankkonto. Sie brauchen diese danach nur noch mit wenigen Mausklicks anzupassen und zu bestätigen – schon ist die Rechnung bezahlt. Bequemer gehts nicht.

Damit es mit den E-Rechnungen klappt, müssen Sie jeden betroffenen Rechnungssteller einmal in Ihrem Onlinebankingdienst freischalten und sich bei ihm über ein Formular für die E-Rechnung anmelden. Damit minimieren Sie für später nicht nur die Papierflut, sondern auch den Zeitaufwand pro Rechnung.

Alle in diesem Artikel erwähnen Banken bieten auf ihren E-Banking-Webseiten eine Onlinedemo mit Beispieldaten, **Screen 2**. So können Sie diese in aller Ruhe austesten. Umbuchungen zwischen eigenen Konten, das Verwalten von Daueraufträgen, das Hochladen von Dateien aus Zahlungs-Software, das Abwickeln von E-Rechnungen und der Erhalt von E-Dokumenten (Kontoabschlüsse, Belastungsanzeigen) sind bei allen gewährleistet und kostenlos. Alle Banken bieten zudem eine Mailbox, über die Sie sich direkt aus dem E-Banking heraus mit Ihrer Bank in Verbindung ➜

setzen. Auch das Verwalten von Wertschriftendepots ist heute Standard. Die UBS kennt darüber hinaus als einzige Bank den direkten Zugriff auf Kreditkartenbuchungen.

Die Kontoführungsgebühren bei der reinen E-Banking-Nutzung variieren: Ein paar wenige Banken (zum Beispiel Alternative Bank, Raiffeisenbank) verlangen hierfür nichts. Bei den meisten sinken die Gebühren auf null, wenn Ihr Vermögen einen bestimmten Betrag beinhaltet oder wenn Sie bei der Bank eine Hypothek haben. Details entnehmen Sie der Tabelle auf S. 26. Dort finden Sie ebenfalls Angaben zu den Sicherheitslösungen der einzelnen Banken.

Login im Sicherheitscheck

Wir konzentrieren uns in diesem Artikel auf Banken, die in mehreren Kantonen tätig sind: Alternative Bank Schweiz, Bank Coop, Credit Suisse, Migros Bank, PostFinance, Raiffeisenbank und UBS. Eine Sonderstellung nehmen die Kantonalbanken ein. Laut Verband Schweizerischer Kantonalbanken verwenden die 24 Mitgliederbanken unterschiedliche Lösungen fürs Onlinebanking. Die Basler und Zürcher Kantonalbanken haben wir als Beispiele zweier grösserer Vertreter mit unterschiedlichen Lösungen aufgenommen. Die Details lesen Sie nach der Auswahl der gewünschten Kantonalbank auf www.kantonalbank.ch/d/privatkunden/bezahlen/index.php.

Wir haben für die Risikobeurteilung der Login-Verfahren einen unabhängigen Sicherheitsexperten zurate gezogen. Jan Alsenz ist Leiter des Teams, das bei OneConsult in Thalwil die Sicherheit von Firmen prüft, **Bild 3**. Für ihn hängt der Sicherheitsgrad von mehreren Faktoren ab: Eine grundlegende Sicherheit bieten Systeme, die ausser einem reinen Zugang per Benutzername und Passwort noch einen zusätzlichen «Besitz» erfordern. Der Benutzer braucht zum Beispiel zum Einloggen eine Codekarte, um die TAN einzugeben. Oder er benötigt einen USB-Stick, der einen speziellen Browser (gehärteter

Jan Alsenz von der Sicherheitsfirma OneConsult bewertet für den PCtipp die Login-Verfahren der wichtigsten Schweizer E-Banking-Systeme

Browser genannt) und einen persönlichen Chip enthält. Der «Besitz» kann auch ein Handy sein, auf dem beim Einloggen eine SMS mit der TAN landet. Eines dieser Systeme ist bei allen Banken gegeben. Zumindest das sichere Einloggen ist damit gewährleistet. Dennoch kann ein Angreifer auch nach dem Einloggen zuschlagen. Das ist aber nur auf schädlingsverseuchten PCs möglich.

Wenn die Bank zusätzlich einen sogenannten Rückkanal bietet, erhöht sich die Sicherheit. Der Rückkanal sorgt dafür, dass beim Onlinebanking wichtige Daten nicht ausschliesslich über den Webbrowser fliessen. Während der Bankkunde seine Zahlungen erfasst, bekommt er zum Beispiel Rückmeldungen in Form von Empfängerkontonummer und Betrag auf dem Display seines Bank-USB-Sticks oder per SMS auf seinem Handy. Vergleicht er diese Rückmeldungen mit den soeben erfassten Zahlungen, kann er beurteilen, ob alles korrekt verläuft.

DIE CODELISTE: ITAN

Der Anwender erhält von der Bank eine gedruckte Liste oder Karte. Die Bank Coop bezeichnet diese Karte als Matrixkarte. Sie enthält nummerierte Felder mit nebenstehenden Codes. Für die TAN-Eingabe wird er aufgefordert, jenen Code einzugeben, der an einer bestimmten Position seiner Codeliste steht. Weil ein Rückkanal fehlt, ist dieses System anfällig für sogenannte Man-in-the-Middle-Angriffe ℹ.

Urteil von Jan Alsenz: Über einen vorhandenen Schädling könnte ein Angreifer auf dem Nutzerrechner die Transaktionsdaten manipulieren und dem Nutzer gefälschte Informationen anzeigen. iTAN hat den zusätzlichen Nachteil, dass die TAN-Nummern meist über einen längeren Zeitraum verwendet werden können.

TAN PER SMS: MTAN

Der Bankkunde hinterlegt in seinem E-Banking-Konto die Nummer seines Handys oder seines SMS-fähigen Festnetztelefons. Sobald er sich per Browser ins E-Banking einloggt oder einen neuen Zahlungsempfänger hinzufügt, erhält er von der Bank automatisch eine SMS auf die angegebene Telefonnummer. Die SMS enthält die TAN und allenfalls noch weitere Daten wie Kontonummer des Zahlungsempfängers und den zu buchenden Betrag. Stimmen die Angaben, tippt er die TAN im Browser ein und gibt dadurch die Transaktion frei. Je nach Bank und individuellen Einstellungen wird die TAN-Eingabe unter verschiedenen Umständen fällig: beim Einloggen, für jede Transaktion oder nur für Buchungen, die nicht den üblichen Überweisungen entsprechen.

Der Vorteil besteht hier im zusätzlichen Kommunikationskanal. Ein Angreifer müsste also auch die SMS manipulieren können. Die mTAN-Lösung ist zudem relativ komfortabel.

Urteil von Jan Alsenz: mTAN zählt zurzeit zu den sichersten Verfahren, sofern der Benutzer auf dem getrennten Kanal auch Transaktionsdaten wie Kontonummer und Betrag nochmals zur Kontrolle erhält. Risiken bestehen hier nur, falls sowohl der Computer als auch das Smartphone mit Malware infiziert sind.

GEHÄRTETER BROWSER

Nach der Lancierung des M-IDentity-Sticks der Migros Bank haben auch verschiedene andere Banken ein ähnliches System eingeführt. Im USB-Stick der Migros Bank steckt eine Smartcard, die für die Verschlüsselung und Authentifizierung der Transaktion sorgt, **Bild 4**. Ausserdem enthält der USB-Stick einen eigens für die Bank angepassten, komplett abgeschotteten Firefox-Browser für Windows, Linux und Mac. Mit diesem gehärteten Webbrowser lassen sich keine ➜

Der M-IDentity-Stick der Migros Bank enthält einen gehärteten Webbrowser

ℹ Fachbegriff

Man-in-the-Middle-Angriff > Hierbei überwacht eine Schädlings-Software auf dem PC laufende Banktransaktionen. Sie blendet gefälschte Dialogfenster ein, während sie im Hintergrund Beträge und Empfängerkonten manipuliert.

5

Der CLX.Sentinel von Crealogix arbeitet mit verschiedenen Banklösungen

6

Der Access Key der UBS mit integriertem Display und Zugangskarte

anderen Webseiten als jene der Bank besuchen. Zudem verweigert das Banksystem den Dienst, falls gleichzeitig andere Firefox-Instanzen laufen.

Die Handhabung ist sehr einfach: Der Anwender stöpselt den Stick am PC ein, wartet, bis dieser vom Betriebssystem erkannt wird, und öffnet darin den Browser. Nun ist nur noch die Eingabe der sechsstelligen PIN nötig.

Ein Nachteil in Sachen Handling: Wegen des Schreibschutzes lassen sich keine Browsereinstellungen speichern, wie zum Beispiel bevorzugte Speicherordner für die PDF-Dokumente oder Fenster- und Schriftgrösse.

Einige Banken, beispielsweise die Basler Kantonalbank, bieten eine vergünstigte Variante des CLX.Sentinel von Crealogix an, **Bild 5**. Auch dieser enthält einen gehärteten Browser und lässt sich mit verschiedenen Banken benutzen. Derzeit ist er aber nur für Windows-Nutzer erhältlich.

Urteil von Jan Alsenz: Solche Onlinebankingsitzungen lassen sich ebenfalls durch Malware manipulieren – wie jede Software, die im normalen Betriebssystem des Nutzers läuft. Anders wäre die Situation hingegen mit einer bootfähigen E-Banking-CD, die ein Live-System (meistens Linux) enthält, das bei jedem Start zurückgesetzt wird. Hier können sich im Normalfall keine Schädlinge einnisten.

ZKB IDENTY KEY UND UBS ACCESS KEY

Eine weitere Lösung per USB-Stick kennt die Zürcher Kantonalbank. Der Anwender stöpselt den ZKB Identy Key am PC ein und loggt sich mit seinem gewohnten Webbrowser per Vertragsnummer und Passwort ein. Der ZKB Identy Key kommuniziert über einen eigenen verschlüsselten Kanal via Internet mit dem Bankserver und zeigt dem Anwender die TAN an, die er im Browser eintippen soll. Die UBS verkauft übrigens ähnliche Sticks unter der Bezeichnung UBS Access Key für 65 Franken als Alternative zum Kartenleser, **Bild 6**. In den UBS Access Key muss aber zusätzlich eine Karte gesteckt werden.

Urteil von Jan Alsenz: Beide Systeme scheinen aktuell zu den besten Verfahren zu gehören. Falls sie die Werbeversprechen halten, können diese Systeme alle aktuell bekannten Angriffe abwehren. Die UBS-Variante mit zwei Komponenten (Access Key und Karte) und zusätzlicher PIN bietet einen etwas höheren Schutz bei Verlust des Sticks oder der Karte.

Übersicht

Die E-Banking-Lösungen im Vergleich

Bank	Login-Verfahren	URL	Software für Offline-Zahlungserfassung	Kontoführung
Alternative Bank Schweiz	mTAN	www.abs.ch	NetBanking (gratis)	gratis
Bank Coop AG	mTAN	www.bankcoop.ch	nein	gratis (wenn Vermögen mehr als 10000 Franken oder Coop-Hypothek besteht)
Credit Suisse	mTAN	www.credit-suisse.com	NetBanking Credit Suisse Edition (gratis), MacPay für Mac OS X (für Fr. 120.–)	gratis (wenn Vermögen mehr als 15000 Franken)
Kantonalbank Basel	iTAN, mTAN, E-Banking-Stick (für Fr. 88.–)	www.bkb.ch	PayMaker (für Fr. 128.–)	gratis (wenn auf Konto mehr als 1000 Franken sind und Vermögen mehr als 10000 Franken oder BKB-Hypothek besteht)
Kantonalbank Zürich	mTAN, Identy Key (für Fr. 79.–)	www.zkb.ch	NetBanking ZKB Edition oder Mammut Private (gratis), PayMaker (für Fr. 128.–)	6 Franken pro Jahr
Migros Bank	M-IDentity-Stick	www.migrosbank.ch	PayMaker (für Fr. 128.–)	gratis (wenn Vermögen mehr als 7500 Franken)
PostFinance	Kartenleser	www.postfinance.ch	E-Finance Java (gratis)	gratis (wenn Vermögen mehr als 7500 Franken)
Raiffeisenbank	mTAN, iTAN, IDentity-Stick (Crealogix CLX.Sentinel für Fr. 139.– plus Fr. 19.–/Jahr)	www.raiffeisen.ch	Spezialversion von PayMaker (ab Fr. 78.–)	gratis
UBS	Kartenleser, Access Key (für Fr. 65.–)	www.ubs.com	UBS Pay (gratis), verschiedene kostenpflichtige Software von Partnern	gratis (wenn Vermögen mehr als 10000 Franken oder UBS-Hypothek besteht)

Stand Juli 2011

KARTENLESER

Die Standardlösungen von PostFinance und UBS zählen zu den sogenannten Challenge-Response-Verfahren. Durch abwechselnde Eingaben von PIN und TAN am PC und Kartenleser beweist der Anwender, dass er selbst vor dem Gerät sitzt und im Besitz des Kartenlesers sowie der zugehörigen Bankkarte ist.

Bei der PostFinance führt der Anwender seine PostFinance-Karte ein und öffnet die E-Finance-Seite im Browser, **Bild 7**. Fürs Einloggen tippt er im Browser erst seine ID und das Passwort ein. Nun liefert die E-Finance-Webseite einen Zahlencode, den der Nutzer am Kartenleser eingibt. Zusätzlich gibt er den PIN-Code der Postkarte ein. Auf dem Leser erscheint ein weiterer Code, den der Nutzer wieder der E-Finance-Seite verfüttert. Jetzt ist der Login-Vorgang abgeschlossen.

Für den Login-Prozess bei der UBS schiebt der Nutzer die Access Card in den Kartenleser, schaltet das Gerät ein und gibt am Lesegerät seine PIN ein, **Bild 8**. Auf der UBS-Webseite tippt er die Vertragsnummer ein und erhält dort einen sechsstelligen Code. Den verfüttert er dem Kartenleser, der einen achtstelligen Code anzeigt. Diesen überträgt er ins passende Feld auf der Webseite und ist nach dem nächsten Login-Klick eingeloggt. Je komplizierter, desto sicherer?

Urteil von Jan Alsenz: Ist Malware auf dem Rechner, dann kommt es auf den Rückkanal an. Fehlt er oder ist nicht komplett unabhängig wie bei den hier vorgestellten Systemen, lässt sich auch dieses System mittels Malware aushebeln. Systeme mit Rückkanal könnten den Angriff hingegen aufdecken.

FAZIT: MTAN AM BESTEN

Unterm Strich bietet das mTAN-Verfahren mit Rückkanal den besten Mix aus Sicherheit, Komfort und Kompatibilität. Wer ein System ohne Rückkanal verwendet (z. B. iTAN), kann für das E-Banking eine Live-CD einsetzen, die eine Infektion mit einem Banktrojaner quasi ausschliesst. Wie Sie eine Live-CD erstellen, lesen Sie unter www.pctipp.ch mit Webcode **54580** (Info zum PCtipp-Webcode, S. 16).

Unterstützte Betriebssysteme

Genau wie die Virenschreiber lieben auch die Banken den Mainstream, sprich: Windows mit Internet Explorer oder Firefox. Nur wenige der vorgestellten Finanzinstitute unterstützen alternative Browser und Betriebssysteme.

Schwierig wird es besonders bei Systemen mit gehärtetem Browser auf einem USB-Stick. Der E-Banking-Stick der Basler Kantonalbank läuft zum Beispiel nur auf Windows-Computern. Den CLX.Sentinel von Crealogix gabs bislang auch für Mac OS X, momentan ist diese Version vergriffen. Auf dem M-IDentity-Stick der Migros Bank befinden sich Browserversionen für Windows, Mac OS X und Linux. Für den ZKB Identy Key sind in den Support-Dokumenten nur Hinweise zu Mac OS X und Windows zu finden. Voll kompatibel mit allen Computerumgebungen sind lediglich Systeme mit iTAN, mTAN sowie PC-unabhängigen Kartenlesern.

Wer Zusatz-Software fürs Offline-Erfassen von Zahlungen benötigt, wird sich nach einer kompatiblen Software für sein Betriebssystem umschauen müssen. Solche haben wir praktisch nur für Windows und Mac OS X entdeckt. Einzig PostFinance offeriert eine kostenlose Java-Software, die auch unter Linux funktioniert.

Fachbegriff

Live-System > Ein Live-System kann unabhängig vom installierten Betriebssystem gestartet werden, zum Beispiel ab einer CD oder DVD. Das System wird dazu auf CD/DVD installiert. Gauner können die Daten auf dem Live-System nicht manipulieren und dort auch keine Schädlinge installieren.

Tipps

10 Regeln für sicheres E-Banking

1 STOPP PHISHING
Fallen Sie nicht auf gefälschte Bankmails herein, die dazu auffordern, einen Link anzuklicken und Daten einzugeben. Wenn Ihre Bank wirklich etwas mitteilen will, finden Sie diese Informationen auch in der Mailbox in der Benutzeroberfläche von Ihrem Onlinebankingsystem.

2 MEIN BLEIBT MEIN
Geben Sie das E-Banking-Zubehör nie aus den Händen, sei es der USB-Stick, die iTAN-Liste, die Zugangskarte, der Kartenleser, das Handy oder der Computer selbst. Verraten Sie auch keiner Person Ihr E-Banking-Passwort.

3 SYSTEMWECHSEL
Falls dies Ihre Bank erlaubt, steigen Sie auf eine Login-Variante mit Rückkanal um. Wenn Sie mTAN verwenden, prüfen Sie die Einstellungen. Schalten Sie allenfalls vorhandene Optionen ein, die ein Bestätigen einzelner Überweisungen per SMS ermöglichen. Kontrollieren Sie die per Rückkanal übermittelten Daten immer ganz genau.

4 SICHERHEITSLÜCKEN SCHLIESSEN
Halten Sie Ihren PC, Mac sowie bei mTAN auch das Handy inklusive der darauf installierten Programme mittels Software-Updates stets aktuell.

5 STOPP SCHÄDLINGE
Schützen Sie Ihre Geräte vor Schädlingen. Ein Virenscanner kann Sie dabei unterstützen.

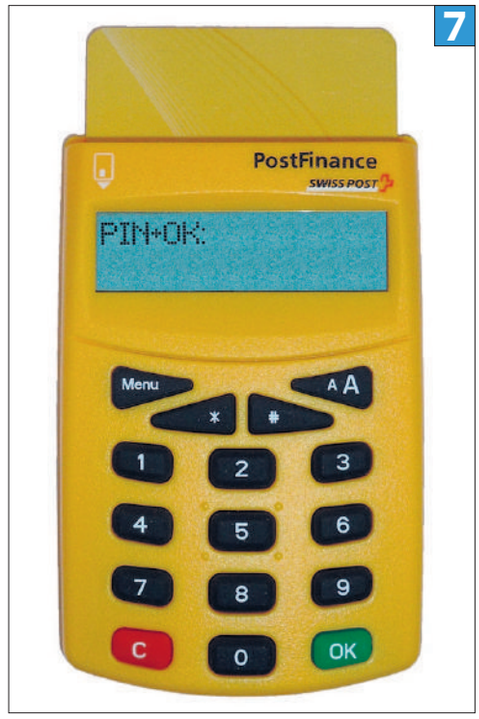
6 NO RISK, MORE FUN
Unterlassen Sie jedes gefährliche Verhalten mit Ihren E-Banking-Geräten. Das heisst, auf keine Links in dubiosen Mails oder Facebook-Beirägen klicken und keine gecrackte Software installieren. Google-Suchresultate sollten Sie immer mit Vorsicht geniessen.

7 SCHLÜSSELTEST
Kontrollieren Sie auf Ihrer Bankwebseite die Verschlüsselung. Achten Sie auf das Schlosssymbol und auf den grünen Balken im Webbrowser. Nehmen Sie Warnungen über ungültige Sicherheitszertifikate (SSL) ernst.

8 SYSTEMTRENNUNG
Falls irgendwie möglich, verwenden Sie einen separaten, frisch aufgesetzten Computer ausschliesslich für Ihr E-Banking. Alternativ starten Sie das Betriebssystem fürs Onlinebanking immer ab einer Linux-Live-CD auf. Mehr dazu mit Webcode **54580**.

9 DOKUMENTE SICHER AUFBEWAHREN
Verwahren Sie auch alle Ihre E-Dokumente (Kontoauszüge, E-Rechnungen etc.) sicher.

10 NACHPRÜFEN
Rufen Sie nach dem Erfassen von Überweisungen stets die Liste der pendenten Zahlungen auf. Prüfen Sie dort Empfänger, Kontonummern und Beträge genau, bevor Sie sich ausloggen.



Die PostFinance verwendet einen Kartenleser

Gratis inbegriffen: der Kartenleser der UBS