Kontofinder.de

präsentiert

DIE LEICHT VERSTÄNDLICHE CHECKLISTE **FÜR EIN SICHERERES ONLINE-BANKING**

Sind wir doch mal ehrlich, die allermeisten von uns werden bessere Dinge zu tun haben, als Ihr Online-Banking sicherer zu machen. Es ist nichts, worauf wir Lust haben. Daher machen wir von **Kontofinder** es Ihnen so leicht wie möglich. Gehen Sie einfach diese Checkliste einmalig durch und setzen Sie die grün hinterlegten Tipps um. Sollten Sie einen der Tipps bereits umgesetzt haben oder dieser für Sie nicht relevant sein, springen Sie sofort zum Nächsten. In wenigen Minuten sind Sie fertig und Ihr Online-Banking um ein Vielfaches sicherer. Los geht‘s...

Inhaltsverzeichnis

Die 5 Grundregeln für ein sicheres Online-Banking

Regel Nr. 1: Installieren und updaten Sie Sicherheitsprogramme

Wenn Computer und Co. nicht sicher und angreifbar sind, helfen auch die besten Tipps nichts.

Computer: Achten Sie darauf, dass Sie ein gutes Anti-Viren-Programm und Anti-Spyware-Programm installiert und die Firewall aktiviert haben.

Smartphone und **Tablet**: Suchen Sie in Ihrem App Store nach „Sicherheit“ und installieren Sie eine für Sie passende Security-App mit guter Bewertung.

Updates: Führen Sie für all Ihre Geräte immer zeitnah die entsprechenden Sicherheitsupdates des Betriebssystems sowie die Aktualisierungen Ihrer Sicherheitsprogramme und – apps aus.

Installieren bzw. updaten Sie jetzt Ihre Sicherheitsprogramme auf allen Geräten.

Regel Nr. 2: Speichern Sie niemals Ihre vertraulichen Bankdaten ab

Speichern Sie Ihre Bankdaten, egal ob PIN, TANs oder andere Passwörter, niemals auf Ihrem Rechner, Tablet oder Smartphone, auch nicht getarnt als Telefonnummer oder Geburtsdatum. Spyware-Programme könnten diese Daten auslesen. Banken sehen so ein Verhalten als fahrlässig an und würden Sie deshalb bei Geldverlust nicht entschädigen. Tipps, wie Sie sich Geheimzahlen merken können, bekommen Sie hier.

Löschen Sie jetzt vertrauliche Daten.

Regel Nr. 3: Kein Online-Banking auf fremden Geräten

Nutzen Sie Ihr Online-Banking nicht auf fremden Geräten. Sie können nicht ausschließen, dass diese manipuliert wurden und Ihre eingegebenen Daten aufgezeichnet werden. Vermeiden Sie daher Online-Banking in Internet-Cafés sowie auf Geräten, die Sie nicht kennen.

Regel Nr. 4: Vermeiden Sie Hotspots und nicht gesicherte WLAN-Netze

Gehen Sie nicht in öffentlich zugänglichen WLAN-Netzen, sogenannten Hotspots, ins Online-Banking. Verbrecher sind mühelos in der Lage, in solchen ungesicherten Netzwerken, zum Beispiel an Bahnhöfen und in Hotel-Lobbies, die Kontodaten auf Ihrem Gerät auszuspionieren. Erledigen Sie Ihre Bankgeschäfte nur in gesicherten, verschlüsselten Netzen oder nutzen Sie sogenannte Virtuelle Private Netzwerke (VPN), wie zum Beispiel SurfEasy. Damit surfen Sie sicher und anonym.

Regel Nr. 5: Notieren Sie sich die Notfalltelefonnummern

Schreiben Sie sich die Notfalltelefonnummer für die Sperrung des Internet-Bankings auf einen Zettel oder speichern Sie sie in Ihrem Smartphone ab, damit Sie im Falle eines Falles schnell reagieren und Ihr Online-Banking sperren können. Schauen Sie dazu auf der Internetseite Ihrer Bank unter „Kontakt“. Passen Sie besonders auf, wenn etwas Ungewöhnliches passiert, wie z.B.

- Sie werden auf eine neue Seite geleitet, wo Sie mehrere TANs eingeben sollen.
- Es öffnet sich während des Online-Bankings ein neues Fenster, wo Sie aufgefordert werden, Ihre PIN und TAN zusammen einzugeben.
- Sie sollen die Eingabe der TAN wiederholen, da die erste bereits verbraucht oder falsch sei.
- Es kommt eine Fehlermeldung oder das Online-Banking schließt sich plötzlich.

Seien Sie wachsam und notieren Sie sich jetzt Ihre Notfalltelefonnummer.

Internet-Browser – Sicherer in nur 6 Minuten

Phishing-Schutz aktivieren

Dauer: 1 Min

Viele Internet-Browser haben einen Phishing-Schutz, der während des Surfens verdächtige Internetseiten automatisch blockiert. Damit verhindern Sie, dass Ihnen heimlich Daten gestohlen werden.

Überprüfen Sie jetzt in Ihrem Browser, ob der Phishing-Schutz aktiviert ist:

Mozilla Firefox

Rechts oben auf Menü => Einstellungen => Registerkarte Sicherheit => Häkchen setzen bei:

- "Webseite blockieren, wenn sie als attackierend gemeldet wurde"
- "Webseite blockieren, wenn sie als Betrugsversuch gemeldet wurde"

Google Chrome

Rechts oben auf Menü => Einstellungen => unten auf "Erweiterte Einstellungen anzeigen..." => Häkchen setzen bei:

- "Phishing- und Malware-Schutz aktivieren"

Apple Safari

Safari => Einstellungen => Registerkarte Sicherheit => Häkchen setzen bei:

- "Sites mit betrügerischen Inhalten: Bei betrügerischen Inhalten warnen"

Microsoft Internet Explorer

Extras => Sicherheit => SmartScreen-Filter aktivieren... => auswählen von:

- "SmartScreen-Filter aktivieren (empfohlen)"

Opera

Extras => Einstellungen => Erweitert => Sicherheit => Häkchen setzen bei:

- "Betrugsversuch-Schutz aktivieren"

Da es noch viele weitere Browser gibt, gerade für mobile Geräte, schauen Sie dort bitte in den Einstellungen nach einem Phishing- und Malwareschutz.

Aktualisieren

Dauer: 1 Min

Aktualisieren Sie regelmäßig Ihren Internet-Browser, wenn dieser Ihnen anzeigt, dass eine neue Version heruntergeladen werden kann. Gerade bei kleineren Updates handelt es sich häufig um Verbesserungen der Sicherheit.

Aktualisieren Sie jetzt Ihren Internet-Browser auf Computer, Tablet und Smartphone. Halten Sie zudem auch andere Software und Apps auf dem neuesten Stand.

Mozilla Firefox

Rechts oben auf Menü => Fragezeichen-Symbol => Über Firefox

Google Chrome

Rechts oben auf Menü => Über Google Chrome

Apple Safari
Apple Software Updater ausführen => Häkchen bei Safari setzen => „Objekt installieren“ klicken

Microsoft Internet Explorer
Rechts oben auf Zahnradsymbol => Info => Häkchen setzen bei

- "Neue Version automatisch installieren“

Opera
Links oben auf Opera => Hilfe => Auf Updates überprüfen

Erweiterungen limitieren Dauer: 3 Min

Viele Browser, egal ob auf dem Rechner oder dem Smartphone, bieten Erweiterungen, sogenannte Add-ons bzw. Extensions an, mit denen Sie Ihren Browser mit zusätzlichen Funktionen ausrüsten können. Beschränken Sie sich auf wenige Erweiterungen, die Sie wirklich brauchen und die von vertrauenswürdigen Entwicklern stammen. Häufig werden diese Addons nicht geprüft oder kontrolliert und können daher auch zur Ausspähung Ihrer Daten benutzt werden. Zum Beispiel erschien am 10.04.2015 die Meldung, dass die Google Chrome Erweiterung „Webpage Screenshot“ Nutzer ausspioniert.

Löschen Sie jetzt alle Erweiterungen, die Sie nicht wirklich benötigen.

Mozilla Firefox
Rechts oben auf Menü => Add-ons => links auf Erweiterungen oder Plugins klicken

Google Chrome
Rechts oben auf Menü => Weitere Tools => Erweiterungen klicken

Apple Safari
Safari => Einstellungen => Erweiterungen

Microsoft Internet Explorer
Extras => Add-Ons verwalten => Anzeigen => Alle Add-Ons

Opera
Links oben auf Opera => Widgets

Internetseite der Bank nicht als Lesezeichen speichern Dauer: 1 Min

Schadprogramme könnten Veränderungen an der URL vornehmen und Sie auf eine gefälschte, ähnlich aussehende Seite umleiten und darüber an Ihre Daten kommen.

Entfernen Sie daher das gespeicherte Lesezeichen in Ihrem Lesezeichen-Ordner.

Zweitbrowser nur für Online-Banking verwenden Optional

Überlegen Sie sich, ob Sie nicht einen Browser nur für Ihr Online-Banking benutzen wollen.

Online-Banking – Sicherer in nur 11 Minuten

Überweisungslimit setzen

Dauer: 3 Min

In Ihrem Online-Banking-Bereich können Sie jederzeit Ihr Überweisungslimit verändern. Fragen Sie sich zunächst, wie viel Geld Sie maximal pro Tag überweisen müssen und wählen Sie dann ein so niedrig wie mögliches Überweisungslimit. Im schlimmsten Fall können Verbrecher dann nicht Ihr gesamtes Konto leerräumen. Und sollten Sie später einmal das Überweisungslimit wegen einer höheren Zahlung für kurze Zeit anheben müssen, dann können Sie dies bei den meisten Banken schnell und einfach telefonisch veranlassen.

Loggen Sie sich jetzt in Ihr Online-Banking ein und setzen Sie ein Überweisungslimit.

Sicheres Passwort wählen

Dauer: 5 Min

Bitte nehmen Sie keine Passwörter, die aus dem Geburtsdatum oder anderen persönlichen Informationen bestehen, die zum Beispiel auf Ihrem Computer zu finden sind. Egal, ob es sich um eine 5-stellige PIN handelt oder ob Sie ein längeres Passwort zum Einloggen in das Online-Banking wählen können, sollte das Passwort Folgendes enthalten:

- Großbuchstaben und Kleinbuchstaben
- mindestens 1 Sonderzeichen, wie z.B. + % & * #
- mindestens 1 Zahl

Ändern Sie jetzt Ihr Passwort. Hier sind Tipps mit Beispielen, wie Sie sich ein sicheres Passwort merken können:

Option 1: Einen Satz zum Passwort kürzen

- "Mein Kind bekommt immer eine 1 mit Sternchen" wird zum Passwort: MKbie1m*
- "Ich habe am 3. Mai Geburtstag!“ wird zum Passwort: Iha3.MG!

Option 2: Ein Wort zum Passwort umfunktionieren

- das Wort "Passwort" wird zu "Pa??W0rt“
- das Wort "Sauberkeit" wird zu "S4uberKe!t“

Gleiches gilt übrigens auch für den Anmeldenamen. Einige Banken erlauben zum Login einen individuellen Namen zur Anmeldung und nicht zwangsweise die Kontonummer. Nehmen Sie dabei nicht Ihre E-Mail-Adresse oder andere leicht zu findende Informationen. Achten Sie zusätzlich bitte darauf, dass Ihre Login-Daten nicht vom Browser gespeichert werden.

Passwort regelmäßig ändern

Dauer: 1 Min

Sind wir doch mal ehrlich: die meisten von uns sind zu faul, das Passwort regelmäßig zu ändern. Gerade weil wir uns eh schon so viele Passwörter merken müssen, wechseln wir Sie nur sehr selten. Aus Sicherheitsgründen ist es aber empfehlenswert, wenn Sie zumindest Ihr Passwort für das Online-Banking alle paar Monate ändern.

Tragen Sie sich jetzt in den nächsten 3 Monaten einen Termin in Ihren Kalender ein.

TAN-Liste sicher aufbewahren

Dauer: 2 Min

Bewahren Sie Ihre TAN-Liste sicher und versteckt auf, z.B. in einem Schubfach oder Schrank. Sagen Sie keinem anderen, wo sich diese Liste befindet.

Platzieren Sie jetzt Ihre TAN-Liste an einem sicheren Ort.

Der 5 Punkte Sicherheitscheck

Diese sekundenschnellen Dinge sollten Sie immer tun, wenn Sie Ihr Online-Banking benutzen.

1. Die Internetadresse kontrollieren **Dauer: 3 Sek**

Achten Sie darauf, dass Sie immer die richtige Internetadresse aufrufen und das ab dem Einloggen in das Online-Banking in der Adresszeile Ihrer Bank das https:// zuerst steht. Dies zeigt an, dass es sich um eine gesicherte, verschlüsselte Verbindung handelt. Geben Sie nie Ihre Daten bei einer unverschlüsselten Verbindung ein. Dies ist ein Zeichen, dass Sie auf eine gefälschte Seite umgeleitet wurden. Beim Einloggen muss also https:// stehen.

2. Das Sicherheitszertifikat kontrollieren **Dauer: 10 Sek**

Bei einer verschlüsselten Verbindung sehen Sie in der Adresszeile Ihres Browsers ein Schloss- oder Schlüssel-Symbol, meist grün hinterlegt. Wenn Sie darauf klicken, wird Ihnen das Sicherheitszertifikat mit weiteren Details angezeigt.
Viele moderne Browser warnen Sie zudem vor unsicheren Zertifikaten, die ein Zeichen dafür sind, dass Sie auf eine gefälschte Seite umgeleitet wurden. Das ist dann eine Art Maske, die davor geschaltet wird und über die Verbrecher direkt Ihre eingegebenen Daten einsehen können. Führen Sie in diesem Fall keine Transaktionen mehr durch und kontaktieren Sie Ihre Bank. Zusätzlich empfiehlt sich, den Zugang zum Online-Banking sicherheitshalber vorläufig zu sperren.

3. Kontoumsätze kontrollieren **Dauer: 30 Sek**

Überprüfen Sie regelmäßig Ihre Kontoumsätze und -auszüge, um sofort mitzubekommen, falls Geld entwendet wurde. Achten Sie dabei auch auf kleinere Summen, da diese weniger auffallen.

4. Ausloggen nicht vergessen **Dauer: 3 Sek**

Nachdem Sie Ihre Bankgeschäfte erledigt haben, klicken Sie bitte immer auf den Abmelden / Logout Button. Schließen Sie nicht nur den Tab oder das Fenster. Auch wenn Sie die meisten Banken nach 10 bis 15 Minuten automatisch ausloggen, melden Sie sich immer gleich ab, ohne noch irgendein Risiko einzugehen.

5. Cache im Browser löschen **Dauer: 20 Sek**

Während des Surfens speichert der Browser Inhalte von besuchten Seiten, wie zum Beispiel Grafiken, Sucheingaben und Skripte im Zwischenspeicher, dem sogenannten Cache. Nachdem Sie sich ausgeloggt haben, empfiehlt sich die Löschung des Caches, damit keine Daten mehr im Browser gespeichert werden und von Verbrechern genutzt werden können.

Mozilla Firefox: https://support.mozilla.org/de/kb/Wie-Sie-den-Cache-leeren-konnen

Google Chrome: https://support.google.com/chrome/answer/95582?hl=de

Microsoft Internet Explorer: http://www.spin.de/help/1128

Apple Safari: http://praxistipps.chip.de/browsercache-loeschen-in-safari_2109

Opera: http://help.opera.com/Windows/12.00/de/cache.html

Mobile-Banking – Sicherer in nur 17 Minuten

Ein Smartphone oder Tablet benötigt die gleichen Sicherheitsvorkehrungen wie ein Notebook oder PC. Beachten Sie neben Sicherheitsupdates, dem Installieren einer Virenschutz-App und dem regelmäßigen Aktualisieren Ihrer Apps die folgenden Tipps:

Kein mTAN auf dem gleichen Gerät

Wenn Sie Ihr Online-Bnking mit dem Smartphone abwickeln, dann nutzen Sie nicht das mTAN-Verfahren. Die TAN per SMS kommt dann auf dem gleichen Gerät an, mit dem Sie auch das Online-Banking betreiben. Kriminelle kommen damit leichter an alle erforderlichen Daten. Wählen Sie stattdessen das chipTAN/smartTAN-Verfahren, bei dem Sie mithilfe eines TAN-Generators einen blinkenden Bildschirmcode einlesen oder nutzen Sie ein anderes Gerät, z.B. Ihren PC in Verbindung mit dem mTAN-Verfahren.

Banking-App gegenüber dem Browser bevorzugen

Dauer: 2 Min

Wenn Sie die Banking-App Ihrer Bank benutzen, können Sie nicht wie im Browser auf eine Phishing-Seite umgeleitet werden.

Schauen Sie jetzt in Ihrem App-Store, ob Ihre Bank eine eigene Banking-App anbietet.

Apps nur aus sicheren Quellen

Dauer: 4 Min

Auf nahezu allen mobilen Geräten ist es möglich, Apps außerhalb des offiziellen App Stores zu installieren. Seien Sie sich bewusst, dass Sie sich darüber, ähnlich wie bei den Browser-Erweiterungen, Spyware herunterladen können. Benutzen Sie am besten immer nur den offiziellen App Store.

Löschen Sie jetzt alle Apps, die Sie nicht mehr brauchen und die von nicht vertrauenswürdigen Quellen stammen.

Keine Drittanbieter-Tastatur auf Smartphones und Tablets

Sie können über den App-Store andere Tastaturen installieren, die Ihnen während der Eingabe Wörter vorschlagen, das Tippen erleichtern aber auch Ihre Passwörter speichern können. Benutzen Sie daher die Standardtastatur Ihres Geräts, wenn Sie sich in das Online-Banking einloggen.

Bluetooth deaktivieren

Dauer: 1 Min

Wenn Sie es nicht benötigen, dann deaktivieren Sie jetzt Ihr Bluetooth.

Fernzugriff einrichten

Dauer: 10 Min

Seien Sie clever und treffen Sie die richtigen Schutzmaßnahmen, bevor es zum Ernstfall kommt. Richten Sie sich deshalb den Fernzugriff ein. Damit können Sie Ihr mobiles Gerät bei Diebstahl oder Verlust lokalisieren, sperren und sensible Daten löschen. Legen Sie zudem regelmäßig ein Backup Ihrer Daten an, um auf einem neuen Gerät schnell wieder darauf zugreifen zu können.

Erkundigen Sie sich jetzt, wie Sie ein Backup anlegen und den Fernzugriff einrichten.

Apple iOS:	Backup	Fernzugriff
Android:	Backup	Fernzugriff
Windows Phone:	Backup	Fernzugriff

Keine Zweifel bei Phishing

Phishing ist vom englischen Wort „fishing“ (= Angeln) abgeleitet und meint das Angeln nach Passwörtern und Kontodaten. Verbrecher versuchen dabei durch gefälschte E-Mails, Internetseiten und SMS an Ihre vertraulichen Daten zu kommen.

Niemals auf fragwürdige Links klicken

Niemand Seriöses wird Sie je nach Ihrer PIN oder einer TAN fragen. Dies sind streng vertrauliche Daten, die einzig und allein für Sie bestimmt sind. Ihre Bank wird Ihnen niemals eine E-Mail schicken und Sie darin auffordern, auf eine bestimmte Seite zu klicken, um Ihre vertraulichen Daten einzugeben. Eventuell wird behauptet, dass Ihr Konto gesperrt wurde (Betreff: Ihr Zugang zum Online-Banking wird geschlossen) und Sie es jetzt wieder freischalten müssen oder dass Sie dringend Ihre Kontodaten aus irgendeinem Grund aktualisieren müssen (Betreff: Kontenauthentifizierung erforderlich). Es ist alles Betrug. Fallen Sie nicht darauf herein. Denken Sie nicht nach und löschen Sie umgehend die Mail. Das gilt übrigens auch, wenn Sie angerufen werden und jemand von Ihnen die PIN oder eine TAN haben will. Legen Sie einfach auf.

Niemals Anhänge herunterladen bzw. öffnen

Gleiches gilt für E-Mail-Anhänge, wie z.B. PDFs. Laden Sie angebliche Zahlungsdetails, gefälschte Rechnungen etc. niemals herunter. Es handelt sich um schädliche Dateien, die Ihren Computer infizieren. Auch hier gilt: nicht zweifeln oder nachdenken, sondern die Mail direkt löschen. Sie können der Bank und anderen Kunden helfen, in dem Sie der Bank von der Mail berichten, so dass diese dagegen vorgehen kann.

Was tun im Ernstfall?

Sollten Sie merken, dass unerlaubt Geld von Ihrem Konto abgebucht wurde, dann folgen Sie diesen Schritten:

Schritt 1: Sperren Sie sofort Ihr Girokonto und den Zugang zu Ihrem Online-Banking. Geben Sie dazu 3 Mal die falsche PIN in der Anmeldemaske zum Online-Banking ein, damit es zu einer automatischen Sperrung kommt. Alternativ können Sie auch die Notfalltelefonnummer anrufen.

Schritt 2: Rufen Sie umgehend Ihre Bank an. Eventuell kann das Geld noch zurückgeholt werden. Besprechen Sie das weitere Vorgehen mit einem qualifizierten Mitarbeiter.

Schritt 3: Melden Sie den Vorfall der Polizei, wenn Ihnen Geld gestohlen wurde. Nehmen Sie ab diesem Zeitpunkt keine Änderungen mehr an dem Gerät vor, an dem Sie das Online-Banking ausgeführt hatten.

Wir hoffen, dass es für Sie nie zu so einem Ernstfall kommt. Setzen Sie die genannten Tipps um und bleiben Sie stets bei ungewöhnlichen Vorkommnissen wachsam. Dann haben Sie bereits eine Menge für ein sichereres Online-Banking getan.