Raiffeisenbank
Kempten-Oberallgäu eG

Tipps zur Verbesserung der Sicherheit im Online-Banking

1. Sicherheitsvorkehrungen für den Computer (PC)

- Es sollten möglichst wenige Personen an Ihrem PC arbeiten, der für das Online-Banking von Ihnen genutzt wird. Hierdurch werden die Risiken gesenkt, die durch andere Personen entstehen können.

- Ihr PC sollte über einen Benutzer ohne Administratorenrechte verfügen, über den das Online-Banking betrieben wird. Hierdurch wird das Risiko gemindert, dass sich Schadprogramme auf Ihrem PC einnisten.

- Der Einsatz von Sicherheitsprogrammen wie Virenschutz-Software, Software zur Verhaltenserkennung und Firewalls ist notwendig, um Ihren PC gegen Schadprogramme wie Viren, Trojaner usw. zu schützen. Die automatische Aktualisierungsfunktion dieser Programme sollte genutzt werden.

- Die Sicherheit wird verbessert durch eine regelmäßige Aktualisierung des Betriebssystems. Am besten eignet sich hierfür der automatische Mechanismus des Betriebssystems. Auf diese Weise wird sichergestellt, dass eventuell vorhandene Sicherheitslücken schnell geschlossen werden.

- Es sollten nur Programme auf Ihrem PC installiert werden, deren Funktionen und Hersteller Ihnen bekannt sind.

- Verfügbare Patche und Updates für Anwendungen sollten zeitnah installiert werden, um eventuell vorhandene Sicherheitslücken schnell zu schließen. Hierfür eignet sich der automatische Updatemechanismus, den viele Anwendungen haben.

- Wichtige Daten sollten regelmäßig als Sicherheitskopien auf CD, USB-Stick oder einer externen Festplatte gespeichert werden. So wird ein möglicher Datenverlust durch Viren oder eine Beschädigung des Betriebssystems verhindert.

- Bei der Verwendung von Funktastaturen sollte darauf geachtet werden, dass diese über eine geeignete Verschlüsselung verfügen.

2 . Besonderes Augenmerk auf den Internet-Browser

- Es sollten keine Test-Versionen von Internet-Browsern verwendet werden. Diese so genannten Beta-Versionen können Sicherheitslücken enthalten oder Fehlfunktionen aufweisen.

- Die Funktion „Autovervollständigung“ des Browsers sollte deaktiviert sein. Der Schutz für gespeicherte Benutzernamen und Passwörter auf der Festplatte ist hier gering.

- Der Internet-Browser sollte regelmäßig aktualisiert werden. Die einzelnen Anbieter stellen auf ihren Web-Seiten Aktualisierungen, so genannte Updates und Patches, bereit. Diese schließen neue Sicherheitslücken. Alternativ kann die automatische Aktualisierung oder Erinnerung bei neuen Updates in den Einstellungen des Internet-Browsers aktiviert werden. Hierdurch ist der Browser immer auf dem aktuellen Stand.

- Die Zusatzfunktion „ActiveX“ im Browser sollte deaktiviert sein. Hierüber können Dritte über das Internet unter Umständen unkontrolliert Programme installieren.

- Es sollten keine unnötigen Erweiterungen (Plug-Ins) installiert werden. Sie stellen ein zusätzliches Risiko dar. Benötigte Plug-ins oder Add-ons sollten immer nur von der Homepage des Browser-Herstellers bezogen werden.

3. Vorsichtiger Umgang mit den Geheimdaten

- PINs und andere kritische Zugangsdaten sollten nicht auf dem PC gespeichert werden

- Die Maximale Anzahl an Zahlen und Buchstaben für eine PIN sollte weitestgehend ausgenutzt werden. So ist eine PIN schwerer zu erraten oder herauszufinden.

- Für die PINs sollten keine Geburtsdaten oder Namen verwendet werden, da diese leichter herauszufinden sind.

- Sämtliche Passwörter sollten aus Groß- und Kleinbuchstaben, Zahlen und möglichst Sonderzeichen wie „$“ oder „&“ zusammengesetzt werden. Dies gilt nicht nur für die PIN, sondern beispielsweise auch für das Passwort des PCs.

- Passwörter sollten regelmäßig geändert werden. Zudem sollten nach Möglichkeit für verschiedene Funktionen wie E-Mail, Online-Banking, Soziale Netzwerke etc. unterschiedliche Passwörter verwendet werden.

- Antworten Sie nicht auf E-Mails oder Anrufe, bei denen nach Zugangsdaten gefragt werden und füllen Sie keine Formulare aus, die Sie per E-Mail oder als Verlinkung in einer E-Mail erhalten. Eine neue Masche ist zudem, dass Kunden per Brief die Aufforderung erhalten, ihre Daten auf einer angegebenen Webseite einzugeben.

- Sperren Sie den Zugang zum Online-Banking, sobald Sie den Verdacht haben, dass ein Dritter im Besitz Ihrer Zugangsdaten ist. Möglicherweise haben Sie den Verdacht, dass ein Trojaner auf ihrem PC Daten mitschneidet (beispielsweise „ZeuS“, „SpyEye“, „Tatanga“). In diesem Fall sollten Sie den PC von einem Experten überprüfen lassen, oder das Betriebssystem und die Anwendungen neu installieren. Ändern Sie alle Zugangskennungen, die der Trojaner möglicherweise mitgeschnitten hat (auch E-Mail, Soziale Netzwerke,...).

4 . Sichere Handhabung des Online-Banking-Programms

- Verwenden Sie ein Tageslimit für Online-Banking-Überweisungen, ggf. Überprüfen Sie mit Ihrem Bankberater Ihr derzeit festgelegtes vertragliches Limit .

- Beachten Sie die Sicherheitshinweise auf der Homepage Ihrer Bank, die vor den gängigen Phishingmethoden und Social Engineering Angriffen warnen. Aktuell sind dies beispielsweise die Maschen „Rücküberweisung“, „Test-SMS“ und „Sicherheitsüberprüfung des PCs“.

- Bei Bedarf überprüfen Sie die Schutzmechanismen Ihres Browsers, ggf. fragen Sie im Fachhandel nach woran man eine geschützte Verbindung erkennt (verriegelten Schloss-Symbol im Browser) und wie Sie das Zertifikat Ihrer Bank im Browser überprüfen können.

- Stellen Sie sicher, dass Sie niemand bei der Eingabe von PIN und TAN beobachtet.

- Beim Absturz Ihres PCs oder Unterbrechung der Verbindung zum Online-Banking während einer Buchung, warten Sie eine gewisse Zeit und überprüfen Sie danach Ihre Umsätze im Online-Banking oder aktualisieren Sie diese nochmals in Ihrer Zahlungssoftware, um nicht versehentlich zwei identische Überweisungen auszuführen.

- Die Web-Seite des Online-Bankings sollte grundsätzlich über die „Logout“- oder die „Beenden“-Funktion verlassen werden, um das Risiko eines Zugriffs durch einen Dritten zu vermindern.

- Verwenden Sie keine Links aus E-Mail-Adressen und öffnen Sie keine unerwarteten E-Mail-Anhänge. Eine bekannte Masche von Betrügern ist es, Phishingmails im Namen von Banken, dem BKA, dem Finanzamt oder der GEMA zu versenden.

5. Gefahren beim Online-Banking an fremden Orten

- Ein fremder Rechner birgt grundsätzlich deutlich höhere Sicherheitsrisiken.

- Von Online-Banking in Internet-Cafés oder an anderen öffentlichen Orten wie Hotels etc. ist grundsätzlich abzuraten.

- Auch andere private PCs oder Firmen-PCs können ein erhöhtes Risiko bergen, da Sie nicht wissen können, wie sicher der Rechner ist. Möglicherweise befinden sich bereits Viren etc. auf der Festplatte.

- Sollte Online-Banking an einem fremden Rechner betrieben werden, sollte auf jeden Fall der Zwischenspeicher (Cache) gelöscht und die Sitzung über die „Abmelden"- Funktion beendet werden. Einige Browser bieten inzwischen die Funktion, beim Öffnen neuer Fenster oder Tabs Vorschaubilder bereits besuchter Seiten einzublenden. Je nach Browser und Version besteht die Gefahr, dass ein Screenshot mit vertraulichen Bankdaten im Cache hinterlegt wurde und durch einen anderen Benutzer einsehbar ist.

6 . Nutzung neuer Technologien für das Online-Banking – Smartphones, Tablets und Co.

- Ihre Bank wird Ihnen keine Sicherheitszertifikate, Verschlüsselungs- oder Sicherheitssoftware auf Smartphones oder Tablets schicken. Die Bank fordert Sie auch nicht dazu auf, Sicherheitszertifikate, Verschlüsselungs- oder Sicherheitssoftware auf dem Smartphone oder Tablet zu installieren. Dies ist eine neue Masche bei Betrügern, um das mobileTAN-Verfahren auszuhebeln. Wenn Sie den Verdacht haben, dass auf Ihrem Smartphone Schadcode installiert wurde, sollte Sie damit keine TANs mehr anfordern und das Gerät einem Fachmann zur Überprüfung geben.

- Beachten Sie die einzuhaltende Kanaltrennung (es darf aus Sicherheitsgründen keine SMS mit TAN-Nummern auf das gleiche Gerät empfangen werden, von dem Sie sich über das Online-Portal bei Ihrer Bank eingeloggt haben), wenn Sie das mobileTAN-Verfahren nutzen.

- Die gleichen Sicherheitsvorkehrungen, die auch für den PC gelten, sollten auch für mobile Endgeräte und Tablets vorgenommen werden. Es sollte nur Apps aus vertrauenswürdigen Quellen installiert und ein Antivirenprogramm genutzt werden. Es sollten keine MMS oder Anhänge von E-Mails geöffnet werden, deren Absender unbekannt ist. Das System ist auf einem aktuellen Stand zu halten.

Sollten Sie noch weitere Fragen an uns haben, rufen Sie uns über unsere Servicenummer 0831 2522 171, Montag bis Donnerstag von 08:00 Uhr bis 16:00 Uhr und Freitag von 08:00 Uhr bis 15:00 Uhr an.