Bank für Sozialwirtschaft

Electronic Banking – und das sicher!

Die elektronische Kontoführung gehört mittlerweile zum (Arbeits-)Alltag dazu. Sie trägt sehr zur Erleichterung von Abläufen bei. Ihren Komfort wissen wir alle zu schätzen. Neben den positiven Möglichkeiten bestehen jedoch vielfältige Sicherheitsrisiken.

Diese ändern sich im Zeitablauf stetig. Den Risiken muss von unterschiedlichen Seiten her begegnet werden, um einen maximalen Erfolg für die Sicherheit zu erzielen. Die Bank ergreift von ihrer Seite geeignete Maßnahmen, um den Schutz der Systeme zu gewährleisten.

Auch die Anwenderseite gewinnt bei der umfänglichen Bekämpfung von kriminellen Handlungen immer mehr an Bedeutung. Deswegen erhalten Sie hiermit wichtige Informationen für den sensiblen Umgang mit den technischen Möglichkeiten.

Beachten Sie, dass Schäden, die durch Missachten von Sicherheitsvorgaben oder durch grobe Fahrlässigkeit entstehen, in Ihrem Verantwortungsbereich liegen!

Die Beachtung der folgenden Informationen schützt Sie:

Allgemeine Sicherheitshinweise als grundlegende Voraussetzung

- Arbeiten Sie nur mit vertrauenswürdigen Computern. Meiden Sie öffentlich zugängliche PCs.
- Nutzen Sie nur sichere Verbindungen und keine öffentlichen Netzwerke wie z. B. Internet-Cafés und öffentliche Hotspots.
- Nutzen und installieren Sie nur Software von vertrauenswürdigen Quellen. Dies gilt auch für Ihren Browser. Es muss sichergestellt sein, dass es sich um unveränderte „zertifizierte“ Original-Software handelt.
- Schützen Sie Ihren Computer mit Virenscanner und Firewall. Einige Hersteller bieten in ihrer Sicherheitslösung einen gesicherten Browser an. Hiermit können Sie auch das Online-Banking sicherer betreiben.
- Führen Sie regelmäßig manuell oder mithilfe einer Backup-Software Datensicherungen auf einem nicht dauerhaft angeschlossenen Medium durch. Bewahren Sie dieses an einem sicheren Ort auf.
- Vergewissern Sie sich vor der Nutzung von Speichermedien (z. B. USB-Stick), dass diese virenfrei sind (Virenscan).
- Halten Sie die Sicherheitssoftware wie auch den Webbrowser, das Betriebssystem und die installierten Programme durch laufende Updates (z. B. Sicherheits-Patches) immer auf dem aktuellsten Stand.
- Aus Sicherheitsgründen sollten Sie beim Microsoft Internet Explorer „ActiveX“ deaktivieren.
- Prüfen Sie unerwartete E-Mails besonders kritisch. Sie sollten keine Dateien von unbekannten Servern bzw. E-Mail-Anhänge unbekannten Ursprungs öffnen, herunterladen oder ausführen. Sollte dies erforderlich sein, so überprüfen Sie die Datei zumindest mit einem aktuellen Virenscanner.
- Schützen Sie sich vor Makro-Viren. Sie sollten bei den Microsoft-Office-Programmen die Einstellung Makrovirus-Schutz vornehmen. Wenn Sie dann ein Office-Dokument öffnen, das

Makros beinhaltet, erhalten Sie einen entsprechenden Warnhinweis.

- Richten Sie Benutzerkonten mit Passworteingabe auf Ihrem PC ein, auch dann, wenn Sie als Einziger mit dem PC arbeiten. Sperren Sie Ihren Rechner, wenn Sie Ihren Arbeitsplatz verlassen.

- Nutzen Sie für den „Normalbetrieb“ einen Benutzer ohne Administrator-Rechte. Schadprogramme können so weniger Unheil anrichten.

- Schalten Sie die Dateinamenserweiterung in Ihrem Betriebssystem ein. Sind diese ausgeblendet, so wird eine Datei mit einer „doppelten Dateinamenserweiterung“ wie beispielsweise „Bankinfo.pdf.bat“ nur als „Bankinfo.pdf“ dargestellt – der Virus wird damit als harmlos wirkende Bankbroschüre getarnt.

- Sichern Sie den Zugriff auf Ihren Router. Ändern Sie das voreingestellte Administrator-Passwort und schalten Sie die Möglichkeit des Remote-Zugriffs aus. Bei Nutzung von WLAN sollten die aktuellen Verschlüsselungsmethoden angewendet werden (WPA2).

Nutzerverhalten für das Electronic Banking als weitere Voraussetzung

- Nehmen Sie als Nutzer die Möglichkeiten zur Risikobegrenzung bei der Bank in Anspruch. Über die ***Nutzungsvereinbarung zur elektronischen Kontoführung*** können bestimmte Funktionen deaktiviert werden. Außerdem kann jeder Nutzer ein Tageslimit angeben.

- Informieren Sie sich regelmäßig über die sichere Nutzung des Electronic Banking und über neue Gefahren auf https://www.sozialbank.de/service/sicherheit.html
  Sensibilisieren Sie auch Ihre Kolleginnen und Kollegen für das Thema.

- Halten Sie Ihre Zugangsdaten geheim. Geben Sie keine Passwörter oder Zugangsmedien an andere Personen, auch nicht an Mitarbeiter der Bank für Sozialwirtschaft, weiter. Speichern Sie keine Passwörter im Browser, auf der Festplatte oder auf anderen Medien.

- Die Bank für Sozialwirtschaft wird Sie niemals auffordern, sicherheitskritische Daten (Passwörter, PIN) per Mail oder per Telefon mitzuteilen oder Ihren Online-Banking-Zugang zu „verifizieren“. Werden Sie in einem solchen Fall sofort misstrauisch und informieren Sie die Bank.

- Geben Sie niemals Ihre Zugangsdaten auf fremden Webseiten ein.

- Nutzen Sie keine Assistenzfunktionen Ihres Browsers (wie z. B. „Autovervollständigen“ oder „Form-Manager“).

- Verwenden Sie sichere Passwörter. Ein sicheres Passwort sollte aus mindestens 8 Zeichen bestehen, Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen enthalten. Wechseln Sie Ihre Passwörter in regelmäßigen Abständen.

- Die Bank für Sozialwirtschaft schickt Ihnen unaufgefordert keine E-Mails, die einen Link zum Log-in des Online-Bankings enthalten, oder wird Sie keinesfalls darin nach Zugangsdaten oder Kreditkartennunmmern fragen.

- Seien Sie achtsam und kontrollieren Sie regelmäßig die Kontobewegungen.

- Im Notfall besteht jederzeit die Möglichkeit, über die kostenlose Sperr-Rufnummer **0800 370 205 00** rund um die Uhr eine Sperranzeige aufzugeben

Sicherer Umgang im BFS-Net.Banking (Online-Banking)

- Verwenden Sie zur Anmeldung des Online-Bankings nur die Ihnen von der Bank separat mitgeteilten Adressdaten (z. B. Internetadresse auf Erstzugangsdatenbrief).
- Achten Sie bei der Eingabe der URL unbedingt darauf, dass diese mit https:// beginnt.
- Geben Sie die URL zum Online-Banking (https://netbanking.sozialbank.de/smartoffice/) immer direkt über die Tastatur ein und achten Sie darauf, dass Sie dabei lediglich ein Browserfenster bzw. einen Tab geöffnet haben.
- Um sicherzugehen, dass Sie auf der richtigen BFS-Net.Banking-Seite sind, prüfen Sie das Zertifikat über das Schloss-Symbol. Das Schloss-Symbol muss geschlossen sein.
- Das Zertifikat muss gültig und für netbanking.sozialbank.de ausgestellt und von einer vertrauenswürdigen Drittpartei bestätigt sein.
- Sofern bei dem Einwahlversuch eine Verbindungsstörung vorliegt, schließen Sie den Browser und starten ihn erneut.
- Nach dem ersten Anmelden ändern Sie im Online-Banking die vorgegebene BFS-Net.Banking-PIN in eine eigene, besonders sichere PIN.
- Die Bank für Sozialwirtschaft fordert von jedem Nutzer pro Transaktion oder sonstigem Auftrag nie mehr als eine TAN an.
- Für Nutzer des neuen photoTAN-Verfahrens: Bei der Autorisierung von Zahlungsaufträgen werden Ihnen Transaktionsdaten im Display des Token angezeigt. Diese sind mit den angezeigten Dialogdaten im BFS-Net.Banking zu vergleichen. Bei Differenzen brechen Sie den Vorgang ab und kontaktieren Sie die Bank.
- Im Notfall sperren Sie Ihren Zugang zum Online-Banking durch dreimalige Falscheingabe der BFS-Net.Banking-PIN. Alternativ können Sie innerhalb der Net.Banking-Sitzung im Menüpunkt „Verwaltung“ eine Sperre veranlassen.
- Beenden Sie Ihre Sitzung immer über die „Abmelden“-Funktion. Nur so ist sichergestellt, dass die Datenverbindung zuverlässig getrennt wird

Tipps für den sicheren Umgang mit EBICS

- Nutzen Sie keine älteren EBICS-Versionen, sondern nur die aktuellste. Prüfen Sie über Ihren Software-Hersteller, ob hierfür ein entsprechendes Update der EBICS-Software notwendig ist.
- Sofern noch nicht geschehen, wechseln Sie dann auch auf die aktuellste Unterschriftsversion.

Nähere Informationen zur aktuellsten EBICS- und Unterschriftsversion finden Sie unter http://www.ebics.de/spezifikation/.

Auf www.sozialbank.de haben wir für Sie relevante Dokumente veröffentlicht. In den ***Bedingungen zur elektronischen Kontoführung*** sind Ihre vertraglichen Sorgfaltspflichten zur Nutzung des Electronic Bankings und zur Geheimhaltung von personalisierten Sicherheitsmerkmalen ausführlich geregelt.

Diese Pflichten dienen dem Schutz im Interesse von Kunde und Bank. Sie erhalten hier auch detaillierte Hinweise zur Nutzungssperre und deren Aufhebung sowie zur Haftung und zu Ihren Anzeige- und Unterrichtungspflichten.

Wenn Sie mit einer Software arbeiten, ist die ***DFÜ-Verfahrensbeschreibung*** für Sie von Interesse. Hier finden Sie technische Beschreibungen zum Kommunikationsstandard EBICS und zu MCFT.

Die ***Verfahrensbeschreibung BFS-Net.Banking*** beinhaltet wichtige Informationen zum Verständnis für das Online-Banking.

Vertiefende Informationen und weitere Handlingshinweise zum Thema Sicherheit finden Sie ebenfalls auf der Seite https://www.bsi.bund.de und https://www.sicher-im-netz.de/.

Stand 4/2017