Wichtige Hinweise zum sicheren Onlinebanking

Volksbank Ochtrup-Laer eG
regional verbunden

Aktualisieren Sie regelmäßig Ihren Rechner und/oder ihr mobiles Endgerät	Verwenden Sie stets die neueste Version des Betriebssystems und der von Ihnen installierten Programme. Spielen Sie umgehend die Sicherheitsupdates für Ihre Software, insbesondere für ihr Betriebssystem sowie Ihren Browser, ein. Nutzen Sie wenn möglich die Funktion zur automatischen Aktualisierung. **Veraltete Betriebssysteme und Software sind extrem anfällig für Viren und Trojaner.**
Verwenden Sie ein Virenschutzprogramm und eine Firewall	Installieren Sie ein Virenschutzprogramm und aktualisieren Sie diese regelmäßig. Wir empfehlen hierfür eine kommerzielle (gekaufte) Version zu nutzen. Setzen Sie eine Firewall ein. Diese ist in den meisten Betriebssystemen bereits integriert. Sie schützt bei richtiger Konfiguration vor Angriffen aus dem Internet und verhindert zudem bei einer Infektion des PCs, dass ausspionierte Daten an einen Angreifer übersendet werden können.
Ändern Sie regelmäßig Ihre Passwörter	Ändern Sie regelmäßig Ihre PIN (unter Service/PIN ändern). Falls Sie einen Verdacht für eine missbräuchliche Nutzung haben, ändern Sie sofort Ihre PIN für das Onlinebanking und Informieren Sie uns unter den unten angegebenen Kontaktdaten. Im Falle eines Virenbefalls informieren Sie uns so schnell wie möglich und ändern Sie die PIN für Ihr Onlinebanking nicht am befallenen Rechner. Nutzen Sie nicht den Passwort-Speicher des Browsers.
Seien Sie vorsichtig bei E-Mails und deren Anhängen	Schadprogramme werden oft über Dateianhänge in E-Mails verbreitet. Prüfen Sie Anhänge vor dem Öffnen mit einem Virenschutzprogramm und seien Sie besonders vorsichtig, falls Ihnen der Absender nicht bekannt sein sollte.
Laden Sie Daten nur aus vertrauenswürdigen Quellen herunter	Seien Sie vorsichtig, wenn Sie etwas aus dem Internet herunterladen. Vergewissern Sie sich vor dem Download von Programmen, ob die Quelle vertrauenswürdig ist. Nutzen Sie nach Möglichkeit die Website des jeweiligen Herstellers zum Download.
Wenn Sie Ihre Zugangsdaten nicht angemessen schützen, können diese schnell in die Hände von Kriminellen geraten. Zu einem angemessenen Schutz gehört auch, dass Sie extrem vorsichtig bei der Weitergabe von Bankdaten sein sollten.	▪ Bewahren Sie Ihre Zugangsdaten an einem sicheren Ort auf, so dass diese nicht gestohlen oder kopiert werden können. ▪ Auch wir werden Sie niemals nach Zugangsdaten oder der PIN fragen. ▪ Geben Sie niemals Ihre Bankdaten oder TANs im Internet weiter (z.B. in sozialen Netzwerken). ▪ Nutzen Sie Ihre Bankdaten nur in der Online-Filiale, oder in vertrauenswürdigen Zahlungsverkehrsprogrammen. ▪ Reagieren Sie nicht auf Phishing-Mails. Wir fordern Sie niemals per E-Mail dazu auf, vertrauliche Daten bekannt zu geben.

Betrüger können Webseiten erstellen, die der Ihrer Bank täuschend ähnlich sehen. Geben Sie dort Ihre Bankdaten ein, landen diese direkt bei den Online-Kriminellen.	▪ Hat sich unser Internetauftritt ohne Ankündigung verändert oder sehen Fenster merkwürdig aus, seien Sie besonders vorsichtig. ▪ Wenn Sie beim Login nach einer TAN gefragt werden, befinden Sie sich mit Sicherheit auf einer gefälschten Seite. ▪ Nutzen Sie unser Onlinebanking ausschließlich durch Aufruf der Seite www.vbol.de und klicken Sie dann auf "Login". Geben Sie diese Adresse immer über die Tastatur in die Adresszeile Ihres Browsers ein. Die Datenkommunikation erfolgt ab diesem Zeitpunkt verschlüsselt über das SSL-Protokoll. Dies können Sie daran erkennen, dass die Adresse mit https:// beginnt. Speichern der Adresse als Lesezeichen kann zu Problemen führen und durch Trojaner manipuliert werden.
Wer Bankgeschäfte an fremden Rechnern abwickelt, riskiert, dass Kriminelle diese Informationen mitlesen.	Betreiben Sie Online-Banking – soweit möglich – nur von eigenen Geräten aus. Falls andere Systeme genutzt werden müssen, achten Sie besonders auf deren Sicherheit.
Bleiben Sie auf dem Laufenden! Ein sicherer Computer ist nicht nur für unser Onlinebanking wichtig. Auch andere Daten können durch Kriminelle abgegriffen oder manipuliert werden.	Schauen Sie auch öfter mal auf unserer Internetseite vorbei. Unter dem Punkt „Banking“ informieren wir regelmäßig über neue Sicherheitsverfahren und geben Ihnen weitere Tipps zum sicheren Umgang mit dem Onlinebanking. Bitte informieren Sie sich auch selber über aktuelle Gefahren und Trends im Bereich Datensicherheit und Computersicherheit. Eine Quelle (wir übernehmen keine Gewähr für deren Inhalte) ist hierbei die Seite vom„Bundesamt für Sicherheit in der Informationstechnik“ (www.bsi.bund.de). Oder vereinbaren Sie einfach einen Termin, damit wir klären können, ob wir Ihr Onlinebanking weiter optimieren können.
Vereinbaren Sie mit uns einen sicheren Kommunikationsweg z.B. zur Übermittlung von Unterlagen!	Als sicheren Kommunikationsweg nutzen wir (selbstverständlich neben dem normalen Postweg) den Postkorb in unserer Onlinefiliale. Über diesen legitimierten Weg können wir sicher Informationen und Unterlagen austauschen. Gerne senden wir Ihnen bestimmte, mitteilungspflichtige, Unterlagen in den Postkorb anstelle eines Briefversand. So sparen wir Papier und Postwege und schonen die Umwelt. Sprechen Sie uns einfach an!
Beachten Sie unsere Sicherheitshinweise für mobile Endgeräte und Tablets. Bitte beachten Sie: Für die Sicherheit Ihrer Geräte sind Sie verantwortlich. Es gibt bestimmte Risiken, die wir für Sie nicht ausschließen können.	▪ Ihr Endgerät muss immer dem aktuellen Sicherheitsstand entsprechen inkl. allen Updates ▪ Endgeräte sollten regelmäßig ersetzt werden, um die neusten Betriebssystemversionen zu erhalten ▪ Ggf. sollte ein Virenschutz auf dem Endgerät installiert sein. ▪ Viren/Trojaner können vom Handy bei einer Synchronisation auf den Rechner gespielt werden ▪ SMS können abgefangen werden, sofern das Handy von einem Virus/Trojaner befallen ist (mobileTAN) ▪ SIM Karte des Telefonanbieters kann kopiert werden oder eine Zweitkarte besorgt werden (mobileTAN) ▪ Zusätzliche Sicherheit: Die VR-SecureSign App sollte nicht zusammen mit einer Banking App auf dem gleichen Gerät betrieben werden
Sprechen Sie uns bei Fragen einfach an.	Es gibt keine „dummen Fragen“. Wir stehen Ihnen persönlich in unseren Geschäftsstellen zur Verfügung. Für Fachfragen wenden Sie sich bitte an unser ServiceCenter unter der Nummer 02553 728-0. Oder senden Sie uns eine Postkorbnachricht oder eine Mail an info@vbol.de.