Stand: 03/20

Online auf **Nummer sicher.**

Jeder Mensch hat etwas, das ihn antreibt.

Wir machen den Weg frei.

Unsere besten Tipps –
für mehr Sicherheit

vobaeg.de/sicherheit

Volksbank Stade-Cuxhaven eG

Unsere besten Tipps – für mehr Sicherheit.

- Installieren Sie regelmäßig Sicherheitsupdates für Ihr Betriebssystem und Ihre wichtigen Programme (z.B. Internet-Browser, *Java*, *Office*, *Flash Player*, *Adobe Reader*). Stellen Sie wenn möglich „Automatische Updates" ein. Wir raten vom Einsatz veralteter Betriebssysteme und Browser ab, da entdeckte Sicherheitslücken nicht mehr mit Updates geschlossen werden.

- Setzen Sie immer ein Virenschutzprogramm ein und aktualisieren Sie es regelmäßig. In der Regel sind „Automatische Updates" aktiviert, jedoch verlangen manche Programme eine separate Prüfung und Installation von umfangreicheren Updates. Kaufversionen der Schutzprogramme sind grundsätzlich effizienter als Freeware.

- Aktivieren Sie mindestens die Firewall des Betriebssystems oder erwerben Sie separat eine Firewall-Software. Sie schützt Ihren Rechner vor Angriffen von außen. Dazu kontrolliert sie alle Verbindungen des Rechners in andere Netzwerke und überprüft die Anfragen in und aus dem Internet. Informieren Sie sich über die Benutzung, damit Sie Meldungen der Firewall richtig einordnen können.

- Nutzen Sie für den Zugriff auf das Internet ausschließlich ein PC-Benutzerkonto mit eingeschränkten Rechten, keinesfalls ein Administrator-Konto. Alle gängigen Betriebssysteme bieten die Möglichkeit, sich als Nutzer mit eingeschränkten Rechten anzumelden. Wie Sie ein einfaches Benutzerkonto einrichten, finden Sie auf den Hilfeseiten des Herstellers Ihres Betriebssystems.

- Software sollten Sie ausschließlich von der Webseite des jeweiligen Herstellers herunterladen. Informieren Sie sich vor dem Download besonders bei kostenlos versprochener Software. In der Regel versuchen diese Anbieter ihr Geld mit zum Teil aggressiver Werbung (zwangsweise installierte Toolbars oder Zusatzprogramme) zu verdienen. Diese Hinweise gelten auch für Browser-Erweiterungen (Plug-Ins).

- Wenn Sie ein WLAN (drahtloses Netzwerk) nutzen, dann sollte dies stets mittels des Verschlüsselungsstandards WPA2 verschlüsselt sein. Wie Sie ein sicheres WLAN einrichten, erfahren Sie auf der Webseite Ihres Router-Herstellers.

- Ändern Sie an Ihrem DSL-Router das für die Verwaltung nötige Standardpasswort immer in ein eigenes, sicheres Passwort. Achten Sie auch bei diesem Gerät auf regelmäßige Updates der im Gerät genutzten Software (Firmware).

vobaeg.de/sicherheit

- Erstellen Sie regelmäßig Sicherheitskopien Ihrer Daten, um vor Verlust geschützt zu sein. Hierzu sollten Sie mehrere externe Festplatte nutzen, die sie an unterschiedlichen Orten verwahren. Hier bietet sich als besonders sicherer Ort ein Bankschließfach an, in dem Sie Ihre wichtigsten persönlichen Daten (Bilder, Dokumente) auf Datenträgern oder externen Festplatten sicher deponieren können.

- Bei der Verwendung mobiler Geräte (Tablet-PCs und Smartphones) gelten die gleichen Regeln wie bei einem gewöhnlichen PC. Ein Virenschutzprogramm gehört auch hier zur Grundausstattung. Führen Sie regelmäßige Updates des Betriebssystems und der Programme (Apps) aus, damit Sicherheitslücken geschlossen werden.

- Prüfen Sie vor dem Download neuer Apps, ob die neue App wirklich nötig und gut ist (Beschreibung, Bewertungen). Wir empfehlen, nur Apps aus dem jeweiligen Store (*Google Play, App-Store* etc.) zu verwenden und niemals Apps unbekannter Herkunft zu installieren.

- Öffentliche WLANs und öffentliche PCs (Hotel-PCs, Internet-Café) müssen nicht genauso sorgfältig konfiguriert und überwacht werden wie Ihr eigener Zugang oder PC. Überlegen Sie genau, ob Sie darüber sensible Angelegenheiten wie Online-Banking oder Internet-Einkäufe erledigen müssen.

- Nutzen Sie keine leicht zu erratenden Passwörter und für jeden genutzten Online-Dienst (E-Mail, Online-Shops, Online-Banking, soziale Netzwerke) möglichst ein separates Passwort. **Die höchste Sicherheit erzielen Sie, wenn Sie diese Passwörter auch regelmäßig ändern!**

- Seien Sie in Bezug auf Ihre persönlichen Informationen genau so zurückhaltend wie auf offener Straße. Im Internet können im Laufe der Zeit viele persönliche Informationen über Sie zu finden sein, die auch Kriminelle später verwenden könnten. Bei unverlangten Anrufen, Besuchen oder zugesendeten E-Mails ist immer Vorsicht geboten. Kriminelle werben mit besonderen Angeboten und geben sich vertrauenswürdig, damit Sie z.B. in E-Mails auf Links klicken oder Dateianhänge öffnen. Dabei wird Ihr PC u.U. mit Schadsoftware infiziert. Überprüfen Sie in solchen Situationen ggf. telefonisch, ob der E-Mail-Absender bzw. der Anrufer wirklich authentisch ist.

Volksbank Stade-Cuxhaven eG

Sperr-Hotline
116 116
(24 Std., bundesweit gebührenfrei)

Ihre Ansprechpartner.

Beratung zum Online-Banking und dessen Sicherheit bei Ihrer Volksbank Stade-Cuxhaven per E-Mail unter eService@vobaeg.de oder persönlich:

Hauke Richert
Leiter eService
Tel. 0 41 41 / 939-196

Jens Daues
eService-Fachberater
Tel. 0 41 41 / 939-198

Jörg Knabbe
eService-Fachberater
Tel. 0 41 41 / 939-197

Nihan Adlim
eService-Fachberaterin
Tel. 0 41 41 / 939-199

Seriöse, kostenlose Banking-Apps – u. a. zum Sperren Ihrer Geld- oder Kreditkarten sowie des Online-Bankings – erhalten Sie bei uns auf vobaeg.de/apps.
Unsere Banking-Apps VR-SecureGo und die VR-Banking-App werden ausschließlich von unserem Rechenzentrum Fiducia & GAD IT AG herausgegeben.

Weiteren Informationen und einen sehr empfehlenswerten Newsletter können Sie kostenfrei auf bsi-fuer-buerger.de abonnieren.

vobaeg.de/sicherheit

Volksbank Stade-Cuxhaven eG