Online-Banking: Tipps für Ihre Sicherheit

Machen Sie sich mit den Gefahren vertraut

Phishing:
Beim Password-Fishing, kurz Phishing, versuchen Kriminelle über das Internet oder per Telefon an Ihre persönlichen Zugangsdaten zu gelangen. Sie erhalten i.d.R. eine E-Mail, die angeblich von Ihrer Bank oder einem Ihnen vertrauten Unternehmen stammt. Darin werden Sie aufgefordert einem Link zu folgen und dort Ihre persönlichen Daten einzugeben. Bei der meist täuschend echt nachgemachten Zielseite handelt es sich um eine Fälschung, die lediglich dem Ausspionieren Ihrer Daten dient.
Sie können ganz sicher sein: Wir als Bank werden Sie niemals per E-Mail oder Telefon nach Ihren Zugangsdaten fragen. Auch bei anderen Unternehmen sollten Sie vorsichtig bei der Weitergabe Ihrer persönlichen Daten sein.

Pharming:
Beim Pharming werden Sie während des Surfens im Internet auf eine gefälschte Seite gelotst. Dabei setzen die Betrüger auf eine Manipulation der technischen Abläufe beim Aufrufen der Seite. Ziel ist es, vertrauliche Informationen zu stehlen. Es handelt sich hierbei um eine Fortentwicklung des klassischen Phishings. Sie schützen sich am besten vor diesen Betrugsversuchen, indem Sie Ihre Sicherheitssoftware immer auf dem neusten Stand halten.

Viren, Würmer und Trojaner:
Immer wieder gibt es Schlagzeilen zu neuen Varianten dieser Schädlinge. Diese infizieren beim Surfen im Internet Ihren PC. Schützen Sie Ihr Gerät mit geeigneter Software wie z.B. aktueller Antivirus-Software und Firewall.

Testüberweisung:
Ihnen wird im Onlinebanking ein Fenster eingeblendet mit dem Inhalt, dass irrtümlich eine Überweisung auf Ihrem Konto eingegangen ist und Sie auffordert, eine Rücküberweisung des entsprechenden Betrags vorzunehmen. Dieser vermeintliche Geldeingang kann sowohl in den Kontoumsätzen als auch in der Finanzübersicht zu sehen sein. Die Schadsoftware auf dem Kundenrechner manipuliert in Ihrem Browser die Ansicht.
Wenn Sie den Anweisungen des Trojaners folgen und in der dann von der Schadsoftware initiierten „Rücküberweisung" eine TAN eingeben, so wird stattdessen eine echte Überweisung zu Lasten Ihres Kontos durchgeführt.

Finanzagent:
Immer wieder gibt es dubiose Angebote, als Finanzmakler tätig zu werden. Ihnen wird per E-Mail versprochen, sich mit diesem „Job" ein lukratives Zweiteinkommen zu sichern. Meist geht es darum, hohe Summen aus unbekannten Quellen zu empfangen und anschließend ins Ausland oder per Western-Union zu überweisen. Diese Gelder stammen dabei u.a. aus illegalen Phishing-Aktivitäten. Durch das Anwerben von Laien als Strohmänner möchten die Täter unerkannt bleiben. Verzichten Sie auf solche Angebote, denn Sie würden sich des Betrugs und der Geldwäsche schuldig machen.

Weitere Informationen und aktuelle Warnhinweise erhalten Sie natürlich auch auf unserer Internetseite unter https://www.rvbfresena.de/electronic-banking/phishing-trojaner.html
Hier finden Sie auch die Möglichkeit des **VR-Computerchecks**, welcher Ihren Computer auf installierte Programme und Plugins, sowie auf Aktualität und bekannte Sicherheitsprobleme prüfen und Ihnen bei der Behebung von Sicherheitslücken helfen kann.

Auf der **Seite 2** dieses Dokuments geht es weiter mit **Tipps zum Schutz Ihrer Daten**.

Schützen Sie Ihre Daten:

- Geben Sie die Webadresse unserer Bank immer von Hand ein, niemals über einen Link in einer E-Mail.
- Moderne Betriebssysteme machen es Ihnen leichter. Nutzen Sie die automatischen Updates und stellen Sie die Sicherheitsoptionen Ihres Browsers mindestens auf „mittel".
- Speichern Sie niemals persönliche Zugangsdaten auf Ihrem Computer.
- Benutzen Sie möglichst immer Ihren eigenen Computer, denn fremde Rechner (hier insbesondere in einem Internetcafé) können Sicherheitslücken aufweisen.
- Starten Sie den Rechner neu, bevor Sie das Online-Banking aufrufen.
- Prüfen Sie das Vorhängeschloss der gesicherten https-Internetseite: https://www.rvbfresena.de
- Gleichen Sie Ihre Kontoumsätze vor und nach jeder Transaktion ab.
- Fragen Sie sich immer, wann eine Dateneingabe sinnvoll ist.
- Folgen Sie keinen Links, die Sie auffordern, Ihr Passwort oder Ihre PIN preiszugeben.
- Öffnen Sie niemals E-Mail-Anhänge, wenn Sie diese nicht angefordert haben.
- Beachten Sie die aktuellen Sicherheitshinweise und Warnmeldungen unserer Bank
- Ändern Sie regelmäßig Ihre PIN
- Verwenden Sie für Ihre PIN keine leichte nachvollziehbare Zahlen- oder Buchstabenkombination (wie Geburtsdaten oder Namen)
- Seien Sie immer wachsam und kontaktieren Sie bei einem Verdacht direkt unsere Bank während der normalen Geschäftszeiten unter der Nummer 04931 / 97206-70 oder per Mail unter info@rvb-fresena.de bzw. nach Schalterschluss über die Sperrnotrufnummer 116 116.
- Sie können Ihr Banking auch schnell und einfach selbst sperren: Geben Sie dazu 3x eine falsche TAN ein, um Ihre TANs zu sperren und danach 3x eine falsche PIN
- Setzen Sie unbedingt Sicherheitsprogramme wie Antiviren-/Anti-Spyware-Programme und Firewalls ein, um Ihren PC gegen Schadprogramme zu schützen und halten Sie diese auf dem aktuellsten Stand. Der Einsatz dieser Programme ist mittlerweile als Pflicht anzusehen.
- Versuchen Sie, so wenige Personen wie möglich an dem PC arbeiten zu lassen, den Sie für das Onlinebanking nutzen.
- Vermeiden Sie die Installation von Testprogrammen unbekannter Quellen.
- Nutzen Sie im Internetbanking zur Kommunikation mit Ihrer Bank den Postkorb als sicheren Kanal.

Mit Genauigkeit und Sorgfalt vorgehen

Eine der wichtigsten Regeln beim Online-Banking lautet: Gehen Sie mit Genauigkeit und Sorgfalt vor. Wenn Sie Ihre Angaben auf den Überweisungsformularen genau überprüfen, bevor Sie sie versenden, erschweren Sie den Betrügern den Erfolg erheblich.

- Überprüfen Sie vor Eingabe einer TAN immer die angezeigten Werte im Display Ihres TAN-Generators bzw. in der empfangenen SMS. Weichen diese Werte von denen der Originalrechnung ab, brechen Sie den Vorgang ab.

- Es wird immer die Transaktion ausgeführt, deren Werte auf der abgesetzten Einheit (TAN-Generator bzw. Mobiltelefon) erscheinen, nicht die angezeigte, möglicherweise manipulierte Transaktion auf dem Bildschirm des Computers.