- Beachten Sie die aktuellen Sicherheitshinweise und Warnmeldungen Ihrer Bank.
- Ändern Sie regelmäßig Ihre PIN.
- Verwenden Sie für Ihre PIN keine leicht nachvollziehbaren Zahlen- oder Buchstabenkombinationen (z. B. Geburtsdaten oder Namen).
- Seien Sie wachsam und kontaktieren Sie bei einem Verdacht direkt Ihre Bank oder den Sperrnotruf 116 116.
- So sperren Sie Ihr Online-Banking notfalls selbst: Geben Sie dreimal eine falsche TAN ein, um Ihre TANs zu sperren und danach zehnmal eine falsche PIN.

Stärken Sie die Abwehr Ihres Computers, Tablets oder Smartphones

Anti-Viren-Programm mit Firewall

Ein Anti-Viren-Programm durchforstet Ihr Gerät nach Schädlingen jeglicher Art, repariert infizierte Dateien bzw. löscht sie. Die Firewall schützt Sie vor Hacker-Angriffen, indem sie deren Zugriffsversuche blockiert. Ein solches Programm ist Pflicht für jeden PC. Kostenpflichtige Programme leisten meist mehr als kostenfreie. Ganz wichtig: Führen Sie regelmäßige Updates durch. Nur so erkennt das Anti-Viren-Programm auch die neuesten Gefahren.

Finanzagent

Immer wieder gibt es Angebote, als so genannter 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 zu überweisen. Die Gelder stammen dabei unter anderem 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 mitschuldig machen.

Gehen Sie entspannt online

Sie möchten Ihre Bankgeschäfte schnell und sicher im Internet erledigen? Sprechen Sie uns an, wir beraten Sie gerne zu allen Fragen des Online-Bankings.

Weitere Informationen finden Sie auch im Internet unter www.vr.de oder auf der Internetseite Ihrer Bank.

498408 DG VERLAG Leipziger Straße 35, 65191 Wiesbaden 4/2015

Wir machen den Weg frei.

Das Internet stellt viele Möglichkeiten zur Verfügung. Es ist immer und nahezu überall verfügbar.
Da liegt es nahe, auch die persönlichen Bankgeschäfte online zu erledigen.
Im weltweiten Netz tätigen Sie zum Beispiel einfach und bequem Ihre Überweisungen oder rufen zu jeder Tageszeit Ihren Kontostand ab. Aber das Internet birgt auch Gefahren.
Vermehrt warnen Experten und Medien vor Risiken wie z.B. Phishing-Attacken, neuen Viren oder Würmern.
Trotzdem können Sie die Vorzüge des Online-Bankings gesichert nutzen, wenn Sie diese Gefahren kennen und wissen, wie Sie die Abwehr Ihres Computers, Tablets oder Smartphones stärken.

Wir helfen Ihnen gerne und zeigen einige Möglichkeiten auf, wie Sie sich ganz einfach und wirkungsvoll vor unerwünschten Zugriffen schützen.

Machen Sie sich mit den Gefahren vertraut

Phishing

Beim Password-Fishing, kurz Phishing, versuchen Kriminelle über das Internet oder Telefon an Ihre persönlichen Zugangsdaten für das Online-Banking zu gelangen. Sie erhalten in der Regel 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.

Eine weitere Version des Phishings ist der Anruf eines angeblichen Servicemitarbeiters, der unter einem Vorwand telefonisch persönliche Daten erfragen möchte.

Sie können sich ganz sicher sein: Ihre Bank wird Sie nie per E-Mail oder Telefon nach Ihren Online-Banking-Zugangsdaten fragen.
Auch bei anderen Unternehmen sollten Sie bei der Weitergabe von Zugangsdaten sehr vorsichtig 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 von Viren, Würmern oder Trojanern. Diese infizieren beim Surfen im Internet unbemerkt Computer, Tablet und Smartphone oder werden als Links oder Anhänge von E-Mails verbreitet.
Ist Ihr Gerät erst einmal infiziert, ist es schwer diese Internet-Parasiten wieder loszuwerden.
Wenn Sie jedoch die Funktionsweise von Viren, Würmern und Trojanern kennen, können Sie sich mit einigen Sicherheitsregeln entspannt im Internet bewegen:
Öffnen Sie grundsätzlich keine Links oder Anhänge in E-Mails, sondern rufen Sie beispielsweise Rechnungen oder Bestellbestätigungen über die jeweiligen Unternehmensportale auf. Schützen Sie Ihr Gerät mit geeigneter Software, wie z.B aktueller Antivirus-Software und Firewall.

Schützen Sie Ihre Daten

- Geben Sie die Webadresse Ihrer Bank immer von Hand ein, niemals über den Link in einer E-Mail.
- Moderne Betriebssysteme machen es Ihnen leicht. Nutzen Sie die automatischen Updates und stellen Sie die Sicherheitsoptionen Ihres Browsers mindestens auf mittel.
- Speichern Sie keine persönlichen Zugangsdaten auf Ihrem Computer.
- Benutzen Sie möglichst immer Ihren eigenen Computer, denn fremde Rechner können Sicherheitslücken aufweisen.
- Starten Sie den Browser neu, bevor Sie das Online-Banking aufrufen.
- Prüfen Sie das Vorhängeschloss der gesicherten https-Internetseite. Kennen Sie den Eigentümer oder den Zertifikatsaussteller nicht, brechen Sie die Sitzung ab.
- 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 keine E-Mail-Anhänge, wenn Sie diese nicht angefordert haben.