

Die Raiffeisenbank Sparneck-Stambach-Zell eG gibt Tipps für sicheres Online-Banking

Keine Chance für Phishing

Online-Banking bietet ein hohes Maß an Flexibilität, Bequemlichkeit und Geschwindigkeit. Wie beim Shoppen und Surfen im Internet ist jedoch Umsicht geboten, um die Vorzüge des World-Wide-Webs unbeschwert genießen zu können. E-Mails mit falschen Absenderangaben und gefälschte Webseiten, mit denen Betrüger Zugangsdaten für das Online-Banking ausspionieren wollen, so genanntes Phishing (kurz für Password fishing), verfangen bei aufmerksamen Kunden nicht. Die Raiffeisenbank Sparneck-Stambach-Zell eG klärt daher über Sicherheitsmaßnahmen beim Online-Banking auf, damit Datendiebe und Betrüger keine Chance bekommen.

Regel Nummer 1: Kein leichtfertiger Umgang mit E-Mails

Vorsicht ist bei eingehenden E-Mails geboten, deren Absender angeblich die Hausbank ist, die dazu auffordert, die PIN oder TAN einzugeben. Hier handelt es sich um klassische Phishing-Versuche von Betrügern. Denn die Musterbank fragt niemals in E-Mails nach persönlichen Informationen oder vertraulichen Daten oder fordert Kunden auf diese Weise zum Online-Banking auf. Wir empfehlen, derartige E-Mails sofort zu löschen. Darin enthaltene Adressen oder Knöpfe sollten niemals angeklickt, Anhänge niemals geöffnet werden. Volksbanken und Raiffeisenbanken gehen gezielt gegen Phishing-Angriffe vor. Gefälschte Web-Seiten werden sofort nach Bekanntwerden im Internet lokalisiert und neutralisiert.

Anti-Viren-Software auf dem PC regelmäßig aktualisieren

Zum umsichtigen Umgang mit dem Internet gehört auch die Kontrolle des eigenen PCs. Die Raiffeisenbank Sparneck-Stambach-Zell eG empfiehlt, die Sicherheitseinstellungen von Browser und E-Mail-Programm immer so hoch wie möglich zu stellen und eine Anti-Viren-Software auf dem PC einzusetzen, die regelmäßig aktualisiert wird. Zusätzlich sollte ein Firewall-Programm eingerichtet sein, das den Rechner vor Angriffen schützt und verhindert, dass Spionageprogramme Kontakt über das Internet aufnehmen können.

Wichtigste Regeln für sicheres Online-Banking

Folgende Grundregeln beim Online-Banking sollten Internet-Nutzer beachten:

Vor dem Aufrufen des Online-Bankings

- Benutzen Sie keine fremden Rechner, denn sie können Sicherheitslücken aufweisen.
- Schließen Sie alle Browserfenster, bevor Sie das Online-Banking starten.
- Geben Sie die Adresse Ihrer Bank möglichst von Hand in Ihren Browser ein.

Im Online-Banking

- Das Symbol eines Vorhängeschlosses unten rechts im Browserfenster zeigt Ihnen die gesicherte Verbindung an.
- Klicken Sie auf das Schloss und prüfen Sie die Echtheit der Seite anhand des Serverzertifikats.
- Überprüfen Sie vor und nach der Nutzung Ihre Kontoumsätze: Sie sollten sofort alle neuen Transaktionen sehen können.

Bei der Dateneingabe und Datenübertragung

- Vergewissern Sie sich, ob die geforderten Eingaben für die von Ihnen gewünschte Aktion sinnvoll sind.
- Melden Sie Abbrüche und andere Unregelmäßigkeiten während des Online-Bankings unverzüglich Ihrer Bank.

Im Verdachtsfall

- Verlassen Sie das Online-Banking sofort und befolgen Sie keinesfalls die angegebenen Anweisungen. Informieren Sie unverzüglich Ihre Bank und lassen Sie gegebenenfalls Ihren Online-Banking-Zugang sperren.
- So sperren Sie Ihr Online-Banking notfalls selbst: Geben Sie im Anmeldedialog dreimal eine falsche PIN ein.