



## Checkliste

# So nutzen Sie Online-Banking sicher

Damit Sie sich gegen Übergriffe beim Online-Banking optimal schützen können, empfiehlt Chris Wojzechowski, Sicherheitsforscher am Institut für Internet-Sicherheit der Westfälischen Hochschule Gelsenkirchen, folgende Vorgehensweise.

Nutzen Sie sichere Online-Banking-Verfahren wie das mTAN- oder das chipTAN-Verfahren.	<input type="radio"/>
Überprüfen Sie vor jeder Bestätigung jeder Überweisung erneut die IBAN, den Empfänger und die Summe.  Risiko: Per Trojaner könnten Hacker sonst während Ihrer Transaktion gezielt die Überweisungsdaten ändern. Mit diesem Check erkennen Sie das!	<input type="radio"/>
Ist Ihre Software auf dem aktuellen Stand, inklusive aller Updates? » Antiviren Software » Browser + Plugins » Betriebssystem  Risiko: Veraltete Software ist das Haupteinfallstor für Viren und Trojaner. Dagegen schützen nur tagesaktuelle Sicherheitsupdates.	<input type="radio"/>
Suchen Sie die Online-Banking-Seite Ihrer Bank nicht über Google. Legen Sie stattdessen ein Lesezeichen in Ihrem Browser an.  Risiko: Cyberkriminelle bauen inzwischen Originalseiten nach und bezahlen dafür, dass sie als Werbung unter Ihrer Suchanfrage ganz oben stehen, warnt Wojzechowski. Wer seine Daten auf so einer Fälschung eingibt, ist sein Geld los.	<input type="radio"/>
Sorgen Sie für Wachsamkeit: Mitarbeiter mit Computer-Zugriff sollten das Know-How haben, Phishingmails und andere Gefahren zu erkennen und bereit sein, bei Unsicherheiten den Rat von Fachpersonal einzuholen.	<input type="radio"/>
Zusatzschutz: Nutzen Sie für Ihre Online-Banking-Geschäfte einen eigenen Computer mit höheren Sicherheitsmaßnahmen.  Vorteil: Hier können Sie die USB-Treiber deaktivieren (ein Einfallstor für Viren auf USB-Sticks), auf komfortable aber unsichere Plugins wie Javascript verzichten und die Sicherheitseinstellungen Ihres Virenschanners auf die höchste Stufe setzen.	<input type="radio"/>