

## Sicherheitshinweise für das OnlineBanking

Immer mehr Internet-Nutzer erledigen ihre Bankgeschäfte online oder kaufen im Web ein. Doch diese Möglichkeiten locken auch Betrüger an. Phishing, Pharming, Trojaner und Viren sind Begriffe, die in den letzten Monaten immer häufiger in den Schlagzeilen zu lesen waren. Wenn Sie die nachfolgend genannten Sicherheitshinweise beachten, erledigen Sie Ihre Online-Bankgeschäfte sicher und sind auch sonst geschützt im Internet unterwegs.

### Verwenden Sie sichere Passworte!

- Ein sicheres Passwort besteht aus einer Mischung von Groß- und Kleinbuchstaben, sowie Ziffern und Sonderzeichen.
- Vermeiden Sie es Eigennamen, bekannte Begriffe, Wiederholungen von einzelnen Buchstaben oder Zahlen für ein Passwort zu verwenden.
- Ändern Sie Ihre Passworte und PIN's in regelmäßigen Abständen.

Beispiel: ungeeignetes Passwort: "sonne123"  
geeignetes Passwort: "TzI3%D"

**Hinweis:** Beim PIN/TAN-Verfahren ist Ihre PIN 5-stellig und besteht aus Groß- und Kleinbuchstaben sowie Ziffern, derzeit keine Sonderzeichen.

### Gehen Sie sensibel mit Zugangsdaten um!

- Passwort, PIN und TAN dürfen nicht an Dritte weitergegeben oder auf der Festplatte gespeichert werden.
- An öffentlichen Plätzen (HotSpots, etc.) oder Internet-Cafés sollten Sie kein OnlineBanking durchführen. An diesen Plätzen ist nicht immer sichergestellt, dass der Zugang durch aktuelle Sicherheitssoftware geschützt ist.

### Vereinbaren Sie ein OnlineBanking-Limit!

Nutzen Sie die Möglichkeit, bei Ihrem Kundenberater, für Ihr Konto einen täglichen Verfügungshöchstbetrag für das OnlineBanking festzulegen. So ist im Ernstfall der Schaden nur so hoch wie das angegebene Limit.

### Schützen Sie Ihren PC mit entsprechenden Sicherheitsprogrammen!

- Um Ihren PC vor Viren, Trojaner und anderen Schadprogrammen zu schützen, sollte ein Virens scanner zum festen Bestandteil Ihres heimischen PC gehören.
- Eine Firewall auf Ihrem Computer schützt Sie vor ungebetenen Einblicken Dritter.
- Betriebssystem, Internet-Browser, OnlineBanking-Software und Sicherheitsprogramme müssen stets durch Updates auf dem aktuellsten Stand gehalten werden.

Vor der Nutzung des OnlineBanking empfiehlt es sich, regelmäßig einen Sicherheitscheck durchzuführen. Ein kostenloser Online-Sicherheitscheck steht Ihnen unter "[www.vbhalle.de](http://www.vbhalle.de)" zur Verfügung.

### Grundsätzliche Verhaltensregeln bei der Nutzung des Internet

- Nutzen Sie mit Ihrem PC das Internet, so tun Sie dies nicht als Administrator, sondern nur mit eingeschränkten Benutzerrechten (Windows-Benutzerkonto: Eingeschränkt). Durch diese Maßnahme werden unerlaubte Zugriffe erschwert.
- Nutzen Sie die im Internetbrowser integrierten Sicherheitseinstellungen, um Ihre Sicherheitsmechanismen zu optimieren.
  - z.B. - Zulassung von ActiveX-Controls ausschließen
  - Ausführung von Java-Applets/Skripten nur nach Rückfrage und Prüfung
  - Deaktivierung der "Auto-Vervollständigen"-Funktion
  - Cookies nur zulassen, wenn Ihnen der Inhalt bekannt ist
- Eine zurückhaltende und durchdachte Verwendung Ihrer E-Mail-Adresse im Internet kann Sie vor unerwünschten Werbe- und Betrugs-Mails bewahren. Viele Viren und Trojaner verbreiten sich über E-Mail.

Unsere Mitarbeiter stehen Ihnen unter folgenden Nummern gern zur Verfügung:  
Tel.: 0345/2148-206 und -207

### **Sichern Sie regelmäßig Ihre Daten!**

- Unabhängig von der Nutzung des OnlineBanking sollten Sie sich regelmäßig Sicherheitskopien (Backups) von Ihren Daten anfertigen. Eine Sicherheitskopie ist oftmals die letzte Möglichkeit einen fehlerhaften Datenbestand wiederherzustellen.
- Zur Sicherung Ihrer Daten sind Wechselfestplatten, CD/DVD-Brenner oder Bandlaufwerke geeignet. Die Sicherheitskopien sind separat aufzubewahren.

### **Seien Sie misstrauisch!**

Die Volksbank Halle (Saale) eG wird Sie niemals per E-Mail, Telefon oder SMS zum Abgleich bzw. zur Eingabe vertraulicher Daten wie Kontonummer, PIN oder TAN auffordern!

- Rufen Sie das InternetBanking immer über unsere Homepage "[www.vbhalle.de](http://www.vbhalle.de)" auf und nicht über Verlinkungen in erhaltenen E-Mails oder auf anderen Internetseiten.
- Auffälligkeiten, die nicht zu Ihren gewohnten Abläufen im InternetBanking gehören, müssen Sie misstrauisch machen (z.B. mehrfache TAN-Abfragen, Veränderungen in der Reihenfolge der Abfragen, Weiterleitungen zu anderen Seiten, etc.).
- Achten Sie beim InternetBanking auf eine gesicherte Verbindung bei der Eingabemaske. Diese ist am Schloßsymbol im Browser und am "s" bei "https://" in der Adresszeile zu erkennen.
- E-Mails die Sie auffordern eine Webseite zu besuchen, um dort Zugangsdaten wie Kontonummer, PIN oder TAN einzugeben oder abzugleichen, sind unbeachtet zu löschen.
- E-Mails mit Dateianhänge von unbekanntem Absendern sollten Sie ungelesen löschen.

Haben Sie auf Phishing-Mails oder sonstige Aufforderungen reagiert, setzen Sie sich bitte umgehend mit Ihrer Bank in Verbindung. Als Sofortmaßnahme empfiehlt sich die Überprüfung der Festplatte mit einem aktuellen Virens Scanner.

### **Alternative zum InternetBanking (PIN/TAN-Verfahren)?**

Das PIN/TAN-Verfahren ist ein einfaches und sicheres Verfahren, welches Ihnen ermöglicht von jedem Arbeitsplatz mit Internetanschluss Ihre Bankgeschäfte abzuwickeln. Diese Flexibilität und Bedienerfreundlichkeit macht es notwendig die vorgenannten Sicherheitshinweise zu beachten, damit es Dritten nicht ermöglicht wird, Ihre Daten einzusehen.

Das sicherste Verfahren um OnlineBanking zu betreiben, ist die Verwendung eines Chipkartenlesers mit PIN-Eingabetastatur in Verbindung mit einer OnlineBanking-Software, wie z.B. VR-NetWorld oder Profi cash. Ihre persönlichen Zugangsdaten sind dabei auf einer Chipkarte gespeichert. Gern beraten wir Sie über die verschiedenen Verfahren im OnlineBanking.

### **Wo finden Sie weitere Informationen?**

- Im Internet: [www.vbhalle.de](http://www.vbhalle.de)
- Bundesamt für Sicherheit in der Informationstechnik >> [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)

### **Begriffserklärung:**

**Phishing** = Angriffsmethode, bei der ein Angreifer die E-Mail Adresse von bekannten Dienstleistern wie Internet-Service-Providern, Internet Kaufhäuser oder Banken vortäuscht, um die Kunden aufzufordern, ihre Kontodaten sowie dazu gehörige PINs und Passwörter auf einer gefälschten Website einzugeben.  
**Trojaner** = Programme, die unbemerkt vom Nutzer sicherheitskritische Funktionen durchführen. Ziel der meisten Trojaner ist es, sensible Daten wie Passwörter auszuspähen und sie per Mail / Internet an den „Besitzer“ des Trojaners zu senden.  
**Virus** = Programme, die sich selbst reproduzieren und sich beispielsweise per E-Mail über das Internet verbreiten können. Viren können auf infizierten PCs teilweise erhebliche Schäden anrichten.  
**Java; Active X** = Programmiersprachen, die besonders im Internet verwendet werden  
**Attachment** = an eine E-Mail angehängte Dateien  
**PIN** = Persönliche Identifikationsnummer  
**Hot-Spot** = per Wireless LAN versorgter Bereich

**Pharming** = Manipulation des PC (durch einen Trojaner), die Verbindungsversuche zur Seite der Online-Bank werden auf eine gefälschte Seite umgeleitet, die der gewohnten Seite äußerst ähnlich sieht. Abweichungen sind nur selten zu erkennen...  
**Personal Firewall** = zu deutsch „Brandschutzmauer“ kontrolliert alle Daten, die das Netz verlassen ebenso, wie die, die in das Netzwerk hinein wollen  
**Cookie** = Zeichenfolge, die mit einer Web-Seite vom Server geladen werden kann und bei einer erneuten Anfrage an den Server mitgesendet wird  
**Internet Browser** = Programm zur Darstellung von Internetseiten  
**SSL (Secure Socket Layer)** = Möglichkeit zur Verschlüsselung der Datenübertragung  
**TAN** = Transaktionsnummer

Unsere Mitarbeiter stehen Ihnen unter folgenden Nummern gern zur Verfügung:  
Tel.: 0345/2148-206 und -207