

# SICHERE BANKGESCHÄFTE IM INTERNET! SIND SIE SICHER?



## SIND SIE SICHER? SECURITY BEGINNT BEI IHREM COMPUTER!

Österreichs Banken investieren seit Jahren in Ihre Sicherheit! Mit umfassenden Sicherheitsmaßnahmen schützt Ihre Bank Ihre Online-Bankgeschäfte vor ungebetenen Gästen.

Aber für eine durchgehende Sicherheit brauchen wir Ihre aktive Unterstützung.

- Machen Sie Ihren PC fit für's Internet!
- Prüfen Sie, mit wem Sie es zu tun haben und schützen Sie Ihre Daten!
- Schützen Sie sich vor Schadprogrammen (Trojaner) und erkennen Sie Phishing-Mails!

## COMPUTER-FIT FÜR'S INTERNET:

- 1) Ihr PC benötigt aktuelle Programmversionen:** Sowohl Betriebssystem als auch Browser können jederzeit Fehler - so genannte Sicherheitslücken - enthalten, die es Angreifern erleichtern, an Daten heranzukommen oder sich Zugriff zu dem entsprechenden PC zu verschaffen. Daher ist es immer wichtig, nur die jeweils aktuellsten Versionen von Browser und Betriebssystem zu nutzen.
- 2) Verwenden Sie eine Firewall.** Diese Barriere zwischen Ihrem PC und dem Internet verhindert unerwünschte Zugriffe.
- 3) Sie brauchen eine aktuelle Antiviren-Software,** die Ihren Computer vor Viren schützt. Entweder diese Software ist schon beim Kauf installiert oder Sie kaufen sich die Software

und installieren sie selbst. Zusätzlich sollte diese Software auch eine Anti-Spyware-Funktion haben, um vor „Spionageprogrammen“ geschützt zu sein. Nur dann ist der Weg durch die virtuelle Welt sicher!

**Aktualisierung nicht vergessen:** Diese Sicherheitsvorkehrungen müssen natürlich auch laufend aktualisiert werden!

## WEIL GELDGESCHÄFTE VERTRAUENSACHE SIND!

- 1) Überprüfen Sie, mit wem Sie es zu tun haben!** Prüfen Sie, ob Sie sich wirklich auf der Bank-Homepage befinden und Ihre Banking-Sitzung verschlüsselt ist. Nur eine https-verschlüsselte Übertragung mit einem gültigen Zertifikat Ihrer Bank gewährt eine sichere Verbindung.
- 2) PIN regelmäßig ändern!** Ihr Zugangspasswort zum Online-Banking, meistens kurz PIN genannt, sollte regelmäßig geändert werden, am besten mindestens einmal pro Monat.
- 3) Vorsicht beim Umgang mit TANs (Transaktionsnummern)!** TANs dienen ausschließlich der Unterzeichnung von Online-Banking-Aufträgen. Eine Eingabe der TANs beim Anmeldevorgang ist niemals erforderlich.

**Wichtig:** PIN merken oder sorgsam verwahren. PIN und TANs getrennt voneinander und sicher aufbewahren und keinesfalls auf dem eigenen PC speichern! Informieren Sie sich direkt bei Ihrer Bank, welche aktuellen Sicherheitsverfahren und Funktionen für Online-Bankgeschäfte angeboten werden.



## ONLINE-BETRUG DURCH PHISHING UND TROJANER - SIND SIE DAVON BETROFFEN?

**1) Erkennen Sie Phishing-Mails!** Phishing wird als Identitätsdiebstahl im Internet bezeichnet. Phishing-Mails sehen erstaunlich echt aus und sind meist Spam-Mails (Massensendung). Sie täuschen vor, dass sie von einer Bank oder einem anderen Internetanbieter kommen. Kriminelle versuchen, Sie durch Begriffe wie „Sicherheit“ bzw. „Datenpflege“ und Ähnliches zu verunsichern, um an Ihre Online-Zugangsdaten zu gelangen. Meistens werden dafür Formulare in den Mails oder auf einer gefälschten Seite bereitgestellt.

**Hinweis:** Ihre Bank fordert Sie NIE per Mail auf, Ihre vertraulichen Zugangsdaten bekannt zu geben. Derartige Nachrichten können Sie beruhigt sofort löschen.

**2) Vorsicht vor Trojanern!** Trojaner sind Programme, die auf Ihren Computer eingeschleust werden und von Ihnen ungewollte Aktionen ausführen. So können Trojaner z.B. Ihre Benutzerdaten ausspionieren und nach Ihrer Eingabe des TANs die Verbindung zum Bankserver unterbrechen und Ihre vertraulichen Daten an den Betrüger übermitteln.

**Hinweis:** In Verbindung mit den Online-Betrügereien werden auch Mittelspersonen gesucht, die dubiose Zahlungen weiterleiten sollen. Hände weg von Angeboten, die Sie per Mail erhalten, die z.B. für wenig Aufwand viel Geld versprechen!

## IHRE SICHERHEITS-CHECKLISTE:

- ☑ Hat mein PC aktuelle Programmversionen?
- ☑ Hat mein PC eine aktuelle Firewall?
- ☑ Hat mein PC eine Antiviren-Software installiert und aktualisiere ich sie regelmäßig?
- ☑ Ist mein PC gegen Spyware (Trojaner) geschützt?
- ☑ Sind mein PIN und meine TANs gut bzw. voneinander getrennt aufbewahrt?
- ☑ Lösche ich verdächtige Mails und klicke ich nicht auf Links in verdächtigen Mails?

Wenn Sie alle Fragen mit „JA“ beantworten können, können Sie beruhigt sein, aktiv zur Unterstützung für Ihre sicheren Online-Bankgeschäfte beigetragen zu haben!

## INFORMIEREN SIE SICH!

Für weitere Informationen zum Thema „Sicherheit im Internet“ stehen Ihnen zahlreiche weitere Tipps und Infos auf der Homepage Ihrer Bank zur Verfügung.

Informieren Sie sich direkt bei Ihrer Bank, welche aktuellen Sicherheitsverfahren und Funktionen für Online-Banking angeboten werden.

### Bei Auffälligkeiten sofort reagieren!

Bei Auffälligkeiten (z.B. nach der TAN-Eingabe kommt es zu merkwürdigem Verhalten, wie Fehlermeldungen, Systemabstürzen, etc.) kontaktieren Sie bitte SOFORT Ihre Bank.