IHRE SICHERHEITS-
CHECKLISTE:

- Hat mein PC, Tablet oder Smartphone die aktuellste Programmversion?
- Hat mein PC eine aktuelle Firewall?
- Hat mein PC oder Smartphone eine Antiviren-Software installiert und aktualisiere ich sie regelmäßig?
- Hat diese Antiviren-Software auch eine Funktion zur Erkennung von Spyware (Spionageprogrammen wie zB. Trojaner) integriert?
- Beginnt die Browseradresse des Internet-Banking Anmeldebildschirmes mit HTTPS://...?
- Ein Zertifikat soll die Echtheit einer Webseite garantieren – stimmt am Anmeldebildschirm der im Zertifikat angezeigte Name mit dem angezeigten Namen der Browseradresse überein und ist es noch gültig?
- Beziehe ich meine Banken-Apps nur über die offiziellen App-Stores?
- Sind meine Zugangsdaten vor dem Zugriff Dritter geschützt?
- Sind meine Zugangsdaten z.B. zum Online-Banking nicht auf der Festplatte oder dem Smartphone gespeichert?
- Sende ich verdächtige Mails an die Hotline meiner Bank und klicke ich nicht auf Links in diesen Mails?
- Lese und beachte ich aktuelle Sicherheitswarnungen meiner Bank sorgfältig?
- Verwende ich auf meinem Smartphone oder Tablet-PC die Bildschirmsperre um die Nutzung durch Dritte zu verhindern?

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. im Online-Banking sehen Sie Seiten die Sie nicht kennen; es sind ohne vorherige Information Ihrer Bank plötzlich Abläufe anders als gewohnt oder nach Zeichnung von Aufträgen kommt es zu merkwürdigem Verhalten, wie Fehlermeldungen, Systemabstürzen, etc.) kontaktieren Sie bitte SOFORT Ihre Bank.

Sie haben alles befolgt?
Dann können Sie „SICHER IM INTERNET“ sein.

IMPRESSUM
Medieninhaber und Herausgeber:
Wirtschaftskammer Österreich, Wiedner Hauptstraße 63, 1045 Wien

Redaktion: xxx
Layout: design:ag, Alice Gutlederer
Druck: xxx
Stand: März 2014

Um eine leichte Lesbarkeit des Textes zu gewährleisten,
wurde auf die explizit geschlechterspezifische Schreibweise verzichtet.

WKO BANK · VERSICHERUNG

WKO BANK · VERSICHERUNG

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

COMPUTER UND SMARTPHONE – FIT FÜR'S INTERNET:

1. **Ihr PC, Tablet und Smartphone 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 den entsprechenden Geräten zu verschaffen. Daher ist es immer wichtig, nur die jeweils aktuellsten Versionen von Browser und Betriebssystem bzw. Banken Apps 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 und Ihr Smartphone 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: All diese Sicherheitsvorkehrungen müssen natürlich auch laufend aktualisiert werden!

WEIL GELDGESCHÄFTE VERTRAUENSSACHE 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. **Passwort/PIN regelmäßig ändern!** Ihr Zugangspasswort bzw. PIN zum Online-Banking sollte regelmäßig geändert werden, am besten mindestens einmal pro Monat.

Wichtig: Verwenden Sie ein sicheres Passwort – Tipps dazu auf den entsprechenden Hilfeseiten Ihres Online-Banking.

3. **Vorsicht beim Umgang mit TANs (Transaktionsnummern)!** TANs dienen ausschließlich der Unterzeichnung von Online-Banking-Aufträgen und sollten niemals z.B. am Telefon oder per e-Mail weiter gegeben werden.

Nutzen Sie nach Möglichkeit die modernen Autorisierungsverfahren anstatt der Papier-TAN-Liste. 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 (Massensendungen). 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. Keine Links in solchen Mails anklicken oder gar Daten bekanntgeben. Derartige Mails bitte an die Hotline Ihrer Bank weiterleiten und dann löschen.

2. **Betrüger rufen manchmal auch an!** Es kommt auch vor, dass Betrüger Kunden kontaktieren und sich am Telefon als Mitarbeiter der Bank (Sicherheitsabteilung oder Betreuer, etc.) ausgeben um TANs, z.B. für ein Storno einer angeblichen Überweisung oder anderes, abzufragen.

Hinweis: Ein Mitarbeiter Ihrer Bank wird Sie niemals telefonisch kontaktieren, um von Ihnen TANs für derartige Vorgänge zu erhalten. Sollte Ihnen das passieren, legen Sie sofort auf und kontaktieren Sie Ihre Bank.

3. **Vorsicht vor Trojanern!** Trojaner sind Programme, die auf Ihrem 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 solchen Angeboten, die Sie per Mail erhalten, die z.B. für wenig Aufwand viel Geld versprechen.