

## Erste Bank warnt ihre Kunden vor Phishing-Mails

05.08.2011



**Internet-Betrüger versuchen derzeit von Bankkunden durch sogenannte Phishing-Mails Zugriffsdaten für das Online-Banking herauszulocken. In verschiedenen E-Mails mit Absendern wie z.B. „SparkAsse“ oder „Erste“ werden Kunden aufgefordert, in gefälschte Eingabemasken TANs oder unter falschen URLs auf gefälschten Login-Seiten Zugangsberechtigungen (Verfügernummer und Passwort) einzugeben.**

Im derzeit kursierenden E-Mail werden die Empfänger aufgefordert, ihre E-Mail Adresse oder andere Daten zu bestätigen da sonst das Konto „ausläuft“. Die Mail beinhaltet einen Link zu einer gefälschten Webseite auf der man zur Preisgabe von persönlichen Daten wie Verfügernummer, Passwort, E-Mail Adresse, TANs oder TAC-SMS auffordert wird. Die E-Mails sind in sehr schlechtem Deutsch verfasst.

Dabei handelt es sich um keine Aufforderung der Bank. Erste Bank und Sparkassen fordern ihre Kunden niemals dazu auf, PIN oder TAN Code bekanntzugeben oder per E-Mail ihr Konto zu verifizieren.

Erste Bank und Sparkassen weisen darauf hin, dass weder die Erste Bank selbst noch die Sparkassen, die s IT Solutions noch das s ServiceCenter jemals Berechtigungsdaten mittels E-Mail von ihren Kunden erfragen. Es werden alle Empfänger solcher E-Mails gewarnt, diesem Link zu folgen und es wird empfohlen, die Nachricht unmittelbar zu löschen.

### Wie man sich schützen kann

Die **echte Login-Seite** für das netbanking beginnt immer mit: <https://netbanking.sparkasse.at/...>

Speichern Sie den echten Link in ihren **Favoriten** und verwenden Sie zur Eingabe ihrer Daten niemals einen anderen Link

Derartige **E-Mails genau lesen** und bei Verdacht sofort 05 0100 – 50 200 anrufen und nachfragen

In solchen E-Mails die darin enthaltenen **Links** niemals anklicken

Niemals TAC-SMS, TAN, Verfügernummer oder Passwort nach einer **Aufforderung per Mail** angeben

Vor Eingabe von sensiblen Daten sollte man auch das **Sicherheitszertifikat** der Webseite prüfen

In der TAC-SMS **kontrollieren**, ob das richtige Empfängerkonto angeführt ist

Verwenden Sie aktuelle Software und **Virenschutzprogramme** auf Ihrem PC

Sichere Internetseiten wie auch das netbanking von Erste Bank und Sparkassen erkennt man an den Buchstaben "https" in der Adresszeile der Webseite und einem Schloss- oder Schlüssel-Symbol im Internet-Browser. Außerdem ist die netbanking-Seite bei den meisten Browsern an einer grün hinterlegten Adresszeile oder an einem grün hinterlegten Zertifikatszeichen erkennbar.

Die Verfügernummer, das selbst gewählte Passwort und die über SMS im Anlassfall übermittelte TAC-SMS garantieren höchste Sicherheit. Da die TAC-SMS nur innerhalb der aktuellen netbanking-Session für eine beschränkte Zeit und ausschließlich für die Transaktion für die sie angefordert wurde gültig ist, ist eine Verwendung in weiterer Folge durch Angreifer ausgeschlossen.

**Muster des Mails** [pdf; 9.2 KB]

