

Erste Bank und Sparkasse warnen KundInnen vor Internetbetrügern

Aktuell verstärkt Phishing-Mails im Umlauf

Bank verlangt niemals Kundendaten per E-Mail

Kunden PC: Vorsicht vor Trojanern

Aktuell sind verstärkt sogenannte **Phishing E-Mails** im Umlauf. Dabei wird dem E-Mail Empfänger vorgetäuscht, dass es sich um eine Nachricht von seiner Bank handelt. Meist sind Weblinks zu gefälschten Log In Seiten enthalten, die dann unter falschem Vorwand vertrauliche Kundendaten abfragen. „Solche E-Mails sollte man entweder an den netbanking helpdesk weiterleiten oder sofort löschen und niemals irgendwelche Daten eingeben“, so Günter Lazel, netbanking Experte der Erste Bank. Erste Bank und Sparkassen fragen niemals Kundendaten, Passwörter, Kreditkartennummern oder sonstige Informationen von Ihren KundInnen ab. Unter falschem Vorwand wie z.B. „Ihr Konto läuft aus“, „Bitte Konto bestätigen“ oder „Konto Aktivierungs-Update“ versuchen die Betrüger aktuell den Usern Daten herauszulocken.

Ziel ist es, so an die Zugangsdaten und TAN bzw. TAC Codes der KundInnen zu kommen, um im Hintergrund eine Überweisung – meistens an ein Auslandskonto – auszulösen.

In manchen Fällen erfolgen nach Bekanntgabe der Daten auch betrügerische Anrufe. Dabei geben sich die Betrüger als BetreuerIn aus und versuchen TAN oder TAC zu erfahren. Auch hier gilt: Vorsicht und niemals Daten am Telefon bekannt geben.

Bei **Trojanern** hingegen handelt es sich um eine Infektion des Kunden-PCs oder Smartphones. Das Schadprogramm (Trojaner), installiert sich meist ohne Wissen der User auf deren Computer. Man kann sich Trojaner beim Surfen auf diversen Internetseiten einfangen, die dann am eigenen Rechner im Hintergrund Daten abgreifen und Passwörter ausspähen. Solche Trojaner können User auch auf gefälschte netbanking Log In Seiten führen. Dabei werden Sie beim Einstiegsversuch ins netbanking unter falschem Vorwand wie z.B. „Neue Produkte und Sicherheitsfeatures“ oder ähnlichem aufgefordert ihre netbanking Log In Daten einzugeben. „Wir empfehlen regelmäßige Viren-Scans durchzuführen, die Firewall einzuschalten und immer alle Sicherheitsupdates auszuführen“, erklärt Lazel.

Die Verfügernummer, das selbst gewählte Passwort und der über SMS übermittelte TAC Code garantieren höchste Sicherheit. Die TAC-SMS ist nur innerhalb der aktuellen netbanking-Session für eine beschränkte Zeit, und ausschließlich für die Transaktion für die sie angefordert wurde, gültig. Dadurch ist eine Verwendung in weiterer Folge durch Angreifer ausgeschlossen. Erhält man aber eine TAC-SMS obwohl man sie gar nicht selbst angefordert hat ist Vorsicht geboten. Das passiert, wenn man die Zugangsdaten Dritten weiter gibt. Somit können nämlich Aufträge erfasst und die Zustellung einer TAC-SMS ausgelöst werden.

Nicht zu vergessen ist die Tatsache, dass Smartphones kleine Computer sind. Besonders das Betriebssystem Android ist ein beliebtes Angriffsziel. Allen KundInnen von Erste Bank und Sparkasse steht daher eine vergünstigte Virenschutz-Software für ihr Android Smartphone zur Verfügung: <http://ebspk.ikarus.at/>

So schützt man sich vor...

Phishing E-Mails

Vorsicht im Umgang mit E-Mails von unbekannten Absendern und klicken Sie darin enthaltene Links niemals an

Trojanern

Führen Sie regelmäßig Sicherheitsupdates an ihrem Betriebssystem durch, schalten Sie die Firewall ein und installieren Sie auf Computer und

Banken fordern KundInnen per E-Mail niemals dazu auf, persönliche Daten wie z.B. Passwörter, TAN oder TAC Codes, Kreditkartennummern, Handydaten oder Erstellungsdaten der TAN-Liste bekannt zu geben oder Kundendaten zu aktualisieren

Kontaktieren Sie im Zweifelsfall immer den Helpdesk (05 0100 – 50 200), oder löschen Sie die E-Mail ohne Anhänge herunterzuladen und Links anzuklicken

Smartphone aktuelle Virenschutzprogramme

Nutzen Sie TAC-SMS und kontrollieren Sie vor Freigabe einer Zahlung den TAC-SMS Text (Kontonummer des Empfängers und Überweisungsbetrag)

Achten Sie auf die korrekte netbanking Adresse in der Adressleiste Ihres Browsers, die immer SSL verschlüsselt ist (Schlosssymbol) und wie folgt beginnt:
<https://netbanking.sparkasse.at/>