

Betrügerische E-Mails beim Online-Banking

Immer noch werden in betrügerischer Absicht massenhaft E-Mails verschickt, die bei Online-Banking-Kunden den Eindruck erwecken sollen, sie stammten von "ihrem" Kreditinstitut. Aus diesem Grunde erneuere ich diesen Warnbeitrag, den ich erstmals im März 2009 einstellte. Mit Worten wie "Sicherheitsaktualisierung", "Überprüfung der Konten auf Sicherheitsstandards" oder "virtuelle Kundenbetreuung" wird der Empfänger aufgefordert, über einen beigefügten Link persönliche Zugangsdaten wie PIN, TAN, Geheimzahl und/oder das persönliche Kennwort einzugeben. Die Internetseite, die sich dabei öffnet, sieht der Webseite des Kreditinstitutes oft täuschend ähnlich. Befolgt der Kunde die Anweisungen, ermöglicht er den Betrügern vollen Zugriff auf sein Konto.

Anmerkung: Sollte der Ablauf beim Online-Banking einmal von dem bekannten Verfahren abweichen, ist es ratsam – ohne eine Transaktion vorzunehmen – das Kreditinstitut persönlich oder telefonisch, nicht jedoch über die oftmals in den Betrugs-Mails angegebene Telefonnummer zu benachrichtigen. Schon bei geringstem Zweifel ist es ratsam sich bei der Bank rückzuversichern, ob die Veränderungen im Ablauf des Online-Bankings oder in der Eingabemaske wirklich von dem Institut ausgehen. Geben Sie niemals eine TAN ein, wenn diese nicht konkret für die Bestätigung eines Auftrages (Zahlungs- oder Überweisungsauftrag bzw. Einrichtung oder Änderung von Daueraufträgen) innerhalb des Online-Banking benötigt wird.