



## Social Engineering II

### Aufgabe 1

Betrachtet die folgende Mail. Was weist darauf hin, dass es sich um eine Phishing-Mail handelt? Welche grundsätzlichen Überlegungen sollte man anstellen, wenn man eine solche Mail erhält?

-----Ursprüngliche Nachricht-----

**Von:** Postbank [mailto:support@postbank.de]

**Gesendet:** Donnerstag, 18. August 2005 18:11

**An:** Daniela

**Betreff:** Postbank Online Banking



Sehr geehrter Kunde,

Im Zusammenhang mit den häufiger werdenden Betrügereien mit den Bankkonten von unseren Kunden sind wir gezwungen eine zusätzliche Autorisation von den Kontoinhabern durchzuführen. Der Sicherheitsdienst der PostBank hat die Entscheidung getroffen, die Datensicherung einer neuen Generation einzuführen. Dazu wurden von unseren Spezialisten sowohl die Informationsübertragungsprotokolle, als auch die Verschlüsselungsart der übertragenen Daten modernisiert.

Im Zusammenhang mit dem Obenerwähnten bitten wir Sie, eine spezielle **Form der zusätzlichen Autorisation auszufüllen**.

[Form ausfüllen](#)

Diese Maßnahmen werden ausschließlich zur Sicherung der Interessen von unseren Kunden getroffen.

Danke für die Zusammenarbeit,  
Administration der Postbank Online Banking

© 2004 Deutsche Postbank AG

### Aufgabe 2

Sieh dir die Beispiele zum Social Engineering und zum Phishing im Einleitungstext und oben an und beschreibe die Methoden, die die Angreifer in den jeweiligen Fällen verwenden, um Benutzer zur Herausgabe ihrer Daten zu bewegen. Welche weiteren Möglichkeiten fallen dir ein?