

## SICHERHEIT IM INTERNET

Berlin, August 2005



Wichtige Hinweise zu gefälschten  
E-Mails, Phishing und Spyware

## **Sicherheit im Internet**

### **Wichtige Hinweise zu gefälschten E-Mails, Phishing und Spyware**

#### **WAS IST PHISHING?**

Immer mehr Menschen nutzen das Internet für bequeme Services wie Online Banking oder Online Shopping. Leider verwenden auch Kriminelle das Internet, um an Ihre persönlichen Daten zu gelangen: Sie versenden E-Mails, die als Absender einen bekannten Serviceanbieter vortäuschen. Diese E-Mails sehen erstaunlich echt aus und werden als Phishing E-Mails bezeichnet.

### **Ihre Bank erfragt niemals Ihre Geheimzahlen per E-Mail!**

#### **WIE MAN EINE PHISHING E-MAIL ERKENNT**

Sie erhalten eine unerwartete E-Mail – scheinbar von Ihrer Bank oder einem anderen Serviceanbieter. Doch in Wirklichkeit gibt sich dabei jemand als Ihre Bank oder Ihr Serviceanbieter aus. In solchen E-Mails werden Sie in der Regel aufgefordert, Angaben zu Ihrem Bankkonto zu machen und manchmal auch Ihre PIN (Geheimzahl) einzugeben – entweder per E-Mail oder über eine Website, die man über eine eingebettete Verknüpfung (Hyperlink) in der E-Mail erreicht.

Kriminelle versuchen, Sie zu täuschen, indem sie Begriffe wie „Sicherheit und Datenpflege“ oder „Untersuchung von Unregelmäßigkeiten“ verwenden. Oft finden

sich auch Mitteilungen wie „Ihr Konto wurde gesperrt“, „Ihre Kontoangaben müssen erneut bestätigt werden“, „Ihre Kreditkarte wurde gesperrt“ oder sogar „Sie haben einen hohen Geldbetrag auf Ihrem Konto, bitte überprüfen Sie die Transaktionen“. Damit soll die Wahrscheinlichkeit erhöht werden, dass Sie den Hyperlink anklicken, um sich einzuloggen oder eine Reihe von Fragen zu beantworten.

Falls Ihr PC nicht mit einer aktuellen Antivirensoftware und einer Firewall ausgestattet ist oder nicht regelmäßig mit Updates oder so genannten Patches (z. B. Updates für Ihren Virens Scanner, Sicherheits-Updates des Betriebssystems wie Microsoft XP Patches und Microsoft Internet Explorer) aktualisiert wird, sollten Sie auf jeden Fall vermeiden, einen in einer E-Mail eingebetteten Hyperlink anzuklicken.

#### **WAS SIE WISSEN MÜSSEN**

Ihre Bank wird Sie niemals nach Ihren Kontoangaben oder Ihrer PIN (Geheimzahl) per E-Mail fragen. Bitte beantworten Sie solche E-Mails nicht und folgen Sie auch nicht den dort angegebenen Instruktionen – selbst wenn man Ihnen mitteilt, dass Ihr Konto gesperrt oder gelöscht wird oder Ihnen mit einer Geldstrafe gedroht wird.

Falls Ihnen etwas verdächtig erscheint, wenden Sie sich bitte über eine Ihnen bekannte Telefonnummer an das in der E-Mail genannte Unternehmen und überprüfen Sie die E-Mail – **beantworten Sie nicht diese mögliche Phishing E-Mail.**

## **Schützen Sie Ihren Computer mit aktueller Antivirensoftware und einer Firewall**

### **DER EINSATZ VON SPYWARE WIE KEY-LOGGER UND TROJANER**

Kriminelle setzen auch so genannte Spyware ein. Diese Software kann unbemerkt auf Ihrem Computer installiert werden und ist in der Lage, im Hintergrund nach sensiblen Daten wie Kontoinformationen oder Passwörtern zu suchen oder Ihre Tastatureingaben aufzuzeichnen. Die Daten werden dann ebenfalls unbemerkt an eine fremde E-Mail-Adresse oder einen fremden Server verschickt. Kriminelle bauen Spyware in Internetseiten, E-Mails oder E-Mail-Anhänge ein. Sobald ein infiziertes Objekt geöffnet wird, installiert sich die Spyware auf Ihrem Computer – ohne, dass Sie es merken.

**Deshalb löschen Sie bitte verdächtige E-Mails, ohne sie zu öffnen. Öffnen Sie bitte keine verdächtigen Anhänge, auch wenn sie von einer Ihnen bekannten E-Mail-Adresse zu kommen scheinen.** Deaktivieren Sie die Auto-vorschau-Funktion, um ein automatisches Öffnen der Mail zu verhindern.

### **SCHUTZSOFTWARE**

Schützen Sie Ihren Computer durch ein zuverlässiges Antivirenprogramm und eine private Firewall, die Sie regelmäßig aktualisieren.

Informationen rund um das Thema Sicherheit im Internet finden Sie beim Bundesamt für Sicherheit in der Informationstechnik unter [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de). Auch unter [www.bankenverband.de/banking](http://www.bankenverband.de/banking) finden Sie eine Broschüre zur Online-Banking-Sicherheit.

## IM FALLE EINES BETRUGSVERDACHTS

Falls Sie eine Phishing E-Mail erhalten, die scheinbar von einer Bank kommt, kontaktieren Sie bitte Ihre Bank.

## SICHERHEIT IM INTERNET

---

Wichtige Hinweise zu gefälschten E-Mails, Phishing und Spyware

**HERAUSGEBER** Bundesverband deutscher Banken  
Postfach 04 03 07  
10062 Berlin  
Telefon (030) 16 63-0  
Telefax (030) 16 63-1399

Berlin, August 2005

© BUNDESVERBAND DEUTSCHER BANKEN  
Der Bankenverband ist die Interessenvertretung der privaten Banken in Deutschland und repräsentiert 230 Banken mit ca. 170.000 Mitarbeitern.