

# Presseinformation

## Zahl der Phishing-Opfer steigt

- **BITKOM-Hochrechnung: Betrüger heben 13 Millionen Euro ab**
- **Internet-Branche fordert Gesetz gegen Kontodaten-Klau**
- **Tipps für sicheres Online-Banking**

**Berlin, 29. August 2007**

Vorsorge gegen Betrug beim Online-Banking ist wichtiger denn je: Die Zahl der Internet-Nutzer, deren Konten mit geklauten Passwörtern geplündert werden, stieg im vergangenen Jahr um 23 Prozent. Das zeigt eine Erhebung des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) bei den Landeskriminalämtern. Die höchste Steigerung gab es 2006 in Sachsen: 169 Prozent. Bundesweit hoben Betrüger in mehr als 3.250 Fällen rund 13 Millionen Euro von den Konten ihrer Opfer ab, so eine BITKOM-Hochrechnung. Für das erste Halbjahr 2007 liegen ebenfalls Daten vieler Bundesländer vor – sie geben keinen Anlass zur Entwarnung: „Die Zahl der Phishing-Opfer wird auch dieses Jahr um rund ein Viertel steigen“, sagt BITKOM-Vizepräsident Heinz Paul Bonn auf Basis der offiziellen Daten. Die meisten Opfer melden Bayern, Baden-Württemberg und Berlin.

Der durchschnittliche Schaden liegt bei 4.000 Euro. Auch hier zeichnet sich eine Steigerung ab. Im ersten Halbjahr 2007 kletterte der Wert auf 4.700 Euro pro Fall. Zwar gelingt es in einigen Fällen, betrügerische Überweisungen zu stoppen. Doch die rechtlichen Mittel reichen nicht: „Wir brauchen dringend ein belastbares Gesetz gegen Phishing“, sagt Bonn. Bisher ist der Kontodaten-Klau nicht eindeutig verboten – die Polizei kann oft nur aktiv werden, wenn ein Schaden vorliegt. „Schon der Versuch muss hart bestraft werden“, fordert der BITKOM-Sprecher. Die Zahl der Betrugsversuche nimmt international zu: Die Anti-Phishing-Arbeitsgruppe APWG registrierte in ihrer jüngsten Statistik monatlich über

Bundesverband  
Informationswirtschaft,  
Telekommunikation und  
neue Medien e.V.

Albrechtstraße 10  
10117 Berlin  
+49. 30. 27576-0  
Fax +49. 30. 27576-400  
bitkom@bitkom.org  
www.bitkom.org

**Ansprechpartner**  
Christian Spahr  
Pressesprecher  
Telekommunikation & Recht  
+49. 30. 27576-112  
Fax +49. 30. 27576-400  
c.spahr@bitkom.org

Dr. Guido Brinkel  
Referent  
Telekommunikations-  
und Medienpolitik  
+49. 30. 27576-221  
Fax +49. 30. 27576-DW  
g.brinkel@bitkom.org

Lutz Neugebauer  
Bereichsleiter Sicherheit  
+49. 30. 27576-242  
Fax +49. 30. 27576-409  
l.neugebauer@bitkom.org

**Präsident**  
Prof. Dr. Dr. h.c. mult.  
August-Wilhelm Scheer

**Hauptgeschäftsführer**  
Dr. Bernhard Rohleder

## **Presseinformation**

### **Zahl der Phishing-Opfer steigt**

Seite 2

23.000 Attacken. Die Betrüger unterhielten weltweit mehr als 37.000 gefälschte Bank-Webseiten; die meisten davon stammen aus den USA.

Ein Grund für die steigende Zahl der Phishing-Opfer sind raffiniertere Betrugsmethoden. Experten zufolge entstehen nur noch rund zehn Prozent der Schäden durch E-Mail-Links zu gefälschten Bank-Seiten, auf denen die Opfer eigenhändig ihre Kontodaten eingeben. In den meisten Fällen schicken Kriminelle per Mail ein so genanntes Trojanisches Pferd – ein Schadprogramm, das die Daten heimlich ausspäht und weitergibt. Andere Schadprogramme leiten die Nutzer beim Online-Banking im Hintergrund auf gefälschte Seiten weiter. „Deshalb ist es wichtig, die jeweils neuesten Schutzmethoden zu nutzen“, sagt BITKOM-Vizepräsident Bonn. Nicht nur die Betrüger, auch die Banken haben aufgerüstet: Transaktionsnummern (TANs) sind oft nicht mehr beliebig einsetzbar, sondern an weitere Sicherheits-Hürden gekoppelt. Manche Kreditinstitute erhöhen die Sicherheit mit Kartenlesegeräten.

Zwar erstatten viele Banken einen Phishing-Schaden, wenn der Nutzer nicht grob fahrlässig gehandelt hat. Einen Rechtsanspruch haben die Kunden in der Regel aber nicht. Vorbeugung ist daher unverzichtbar. „Mit ein paar Grundregeln lässt sich das Risiko leicht minimieren“, so Bonn. „Dann ist Online-Banking eine sehr sichere Dienstleistung, die zu Recht hohe Akzeptanz genießt.“ Insgesamt nutzen rund 20 Millionen Deutsche die Internet-Kontodienste ihrer Bank.

Der BITKOM nennt die wichtigsten Anti-Phishing-Tipps:

#### **1. Gesundes Misstrauen bei E-Mails**

Banken bitten ihre Kunden nie per E-Mail, vertrauliche Daten im Netz einzugeben. Diese Mails sind immer gefälscht: Am besten sofort löschen. Das gleiche gilt für E-Mails von Unbekannten, die unaufgefordert im

## **Presseinformation**

### **Zahl der Phishing-Opfer steigt**

Seite 3

eigenen Postfach landen – insbesondere, wenn eine Datei angehängt ist. Dahinter könnte sich ein schädliches Programm verbergen, zum Beispiel ein Phishing-Trojaner. Verdächtige Dateien auf keinen Fall öffnen! Auch dann nicht, wenn im Text der E-Mail mit einer Kontosperrung gedroht wird. Solche Einschüchterungsversuche sind eine beliebte Methode von Betrügern, um Bankkunden unter Druck zu setzen. PC-Nutzer sollten die Drohungen ignorieren und Phishing-Mails keinesfalls beantworten. Wer sich unsicher ist, sollte bei seiner Bank nachfragen.

### **2. Den Computer vor Schädlingen schützen**

Eine gute Sicherheitsausstattung ist für Internet-Bankkunden besonders wichtig. Ein modernes Anti-Viren-Programm und eine so genannte Firewall, die den Rechner vor schädlichen Dateien aus dem Netz schützt, müssen vor der ersten Online-Sitzung installiert werden. Diese Programme und die Sicherheitseinstellungen des Betriebssystems müssen regelmäßig aktualisiert werden. Am besten wird der Rechner so eingestellt, dass er alle Updates automatisch installiert.

### **3. Vorsicht beim Aufruf der Bank-Webseite**

Beim Online-Banking sollte man die Adresse der Bank immer direkt im Web-Programm eingeben oder über selbst gespeicherte Lesezeichen (Favoriten) aufrufen. Maßgeblich ist die Adresse, die die Bank in ihren offiziellen Unterlagen angibt. Die Online-Verbindung zum Bankcomputer muss verschlüsselt sein. Das ist erkennbar an den Buchstaben „https“ in der Web-Adresse. Neben der Adresszeile oder in der Statusleiste des Browsers muss ein Schloss- oder Schlüssel-Symbol zu sehen sein.

### **4. Moderne Transaktions-Verfahren nutzen**

Für Überweisungen und andere Kundenaufträge sind Transaktionsnummern (TANs) nötig. In den Anfängen des Online-Bankings konnten die Nutzer einen solchen Code aus einer Liste frei wählen. Sicherer ist

## **Presseinformation**

### **Zahl der Phishing-Opfer steigt**

Seite 4

das moderne iTAN-Verfahren, bei dem die Codes nummeriert sind. Ein Zufallsgenerator der Bank bestimmt, welche TAN aus der Liste eingegeben werden muss. Noch weniger Chancen haben Kriminelle beim mTAN-Verfahren: Die Transaktionsnummer wird dem Kunden aufs Handy geschickt und ist nur wenige Minuten gültig. PC-Nutzer sollten ihre Bank fragen und möglichst auf diese Verfahren umstellen. Eine gute Alternative sind Kartenleser für EC-Karten oder digitale Signaturkarten.

#### **5. Falls es zu spät ist – Schadensbegrenzung**

Nicht immer ist das Geld sofort verloren, wenn Kriminelle eine Sicherheitslücke ausgenutzt haben. Phishing-Opfer sollten zuerst die Bank alarmieren: Wenn eine betrügerische Überweisung nicht lange zurückliegt, kann sie in etlichen Fällen noch gestoppt oder sogar rückgängig gemacht werden. Entsteht doch ein finanzieller Schaden, unbedingt Anzeige bei der Polizei erstatten. Das ist die Voraussetzung, um Geld von der Bank zurückzubekommen. Falls der Betroffene nicht grob fahrlässig gehandelt hat, zeigen sich viele Banken kulant.

Zur Methodik der BITKOM-Erhebung: Erfragt wurden die Zahlen der Phishing-Fälle, in denen illegale Banktransfers stattgefunden haben, sowie die dabei geflossenen Summen. Quelle sind alle teilnehmenden Landeskriminalämter, da es keine bundesweite Statistik gibt. Es stehen detaillierte Daten zu insgesamt neun Bundesländern zur Verfügung sowie eine Hochrechnung für Deutschland.

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.000 Unternehmen, davon 850 Direktmitglieder mit etwa 120 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Gerätehersteller, Anbieter von Software, IT-Services, Telekommunikationsdiensten und Content. Der BITKOM setzt sich insbesondere für bessere ordnungsrechtliche Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.