



PHISHING: BETRUG IM INTERNET

1. EINLEITUNG

Heutzutage ist es wichtig, sich immer auf dem Laufenden zu halten in Bezug auf Neuigkeiten der Computerwelt und auf Gefahren der Systeme, da täglich neue Drohungen im Internet erscheinen. Neben den gefährlichen Angriffen von Computerviren mussten PC-Nutzer mit einer neuen Art von Internet-Kriminalität Bekanntschaft machen, den so genannten Phishing-Attacken. Der große Unterschied liegt darin, daß diesmal keiner versucht, sich an Systeme ranzumachen oder einen Virus einzufügen, sondern der eigene Computernutzer gibt freiwillig seine persönlichen und vertraulichen Daten an, natürlich mittels Täuschung und Betrug.

2. WAS IST PHISHING?

Unter Phishing (englisch) versteht man eine Art von Trickbetrug mit Methoden des Social Engineerings. Dabei versucht ein Phisher, Internet-Benutzer durch gefälschte E-Mails oder andere Tricks dazu zu bringen, gefälschte Websites zu besuchen und dort persönliche Informationen wie Bankzugangsdaten, Kreditkartennummern oder ähnliches einzugeben.

Dreiste Tricks fälschen das Aussehen einer Webseite und oftmals auch die Anzeige in der Adressenzeile. Die meisten nachgeahmten Webseiten sind von Banken und Finanzinstitutionen, um sich der Kontendaten der Kunden zu ermächtigen.

Phishing klingt nach fischen gehen und genau so ist es auch. Das Wort setzt sich aus „Password“ und „fishing“ zusammen, zu Deutsch nach Passwörtern angeln. Immer öfter fälschen Phishing-Betrüger E-Mails und Internetseiten und haben damit einen neuen Weg gefunden, um an vertrauliche Daten wie Passwörter, Zugangsdaten oder Kreditkartennummern heranzukommen – die Nutzer geben Ihre Daten einfach freiwillig preis.

3. VORGEHENSWEISE

Als seriöse Bank oder Firma getarnt fordern die Betrüger den Empfänger im E-Mail auf, seine Daten zu aktualisieren. Entweder weil z.B. die Kreditkarte ablaufe, das Passwort erneuert werden müsse oder die Zugangsdaten verloren gegangen seien. Der Inhalt der sogenannten Phishing-Mails wirkt dabei täuschend echt. Diese E-Mails im HTML-Format zeigen dann einen „offiziellen“ Link an, hinter dem sich jedoch tatsächlich ein ganz anderer Link verbirgt. Der Empfänger wird für die Dateneingabe über einen Link auf eine Internetseite geführt, die z.B. der Banken-Homepage ähnlich sieht. Auf den ersten Blick scheint alles ganz normal, selbst die Eingabeformulare sehen gleich aus. Die Phishing-Betrüger nutzen dabei entweder Internetadressen (Adressenliste), die sich nur geringfügig von denen der renommierten Firmen unterscheiden. Oder aber sie fälschen die Adressenleiste des Browsers mit einem Java-Skript. Man glaubt also, man sei auf einer seriösen Seite, ist es aber nicht. Wer einer solchen Seite seine EC-Geheimnummer, Passwörter oder andere Daten anvertraut, der beschert denn Angler fette Beute und kann sich selbst jede Menge Ärger einhandeln.



4. WIE SCHÜTZEN SIE SICH VOR PHISHING?

Derzeit sind verstärkt Phishing-Mails im Umlauf und die Phishing Angriffe nehmen auf der ganzen Welt zu.

Leider kann kein Antivirus weiterhelfen, so daß zur Sicherheit jeder Nutzer des Online-Banking einige grundsätzliche Tips und Vorsichtsmaßnahmen beachten sollten:

I. Ihre Bank wird Sie nie per E-Mail auffordern, vertrauliche Daten zu versenden.

Niemals wird Ihre Bank bzw. Sparkasse Sie per E-Mail auffordern, Ihre Kontendaten zur Überprüfung über das Internet zu versenden. Wenn Sie eine Mail mit entsprechendem Inhalt erhalten, ignorieren Sie diese. Auf keinen Fall sollten Sie mitgesandte Links aktivieren. Informieren Sie Ihre Bank darüber, wenn Sie eine solche E-Mail erhalten haben. Sollten Sie versehentlich eine zweifelhafte Internetseite besucht und Ihre Daten preisgegeben haben, setzen Sie sich umgehend mit Ihrer Bank in Verbindung, sperren Sie ggf. Ihre PIN und TAN-Nummern.

II. Sichere Startposition

Starten Sie Ihr Internet-Banking ausschließlich durch die Eingabe der URL Ihrer Bank bzw. Sparkasse oder durch den Aufruf über Ihre Favoritenliste.

III. Verschlüsselung

Die aufgerufenen Banking-Seiten sind immer SSL verschlüsselt. Das angewandte Verschlüsselungskonzept stellt sicher, daß die Daten während der Übertragung nicht mitgelesen oder verändert werden können. Fehlt das Schloßsymbol in der Startleiste ist dies nicht der Fall.

Die Verschlüsselung erkennen Sie auch an der Bezeichnung https:// am Beginn der aufgerufenen Adresse. Das „s“ in der Erweiterung des „http“ weist darauf hin, daß eine gesicherte Datenübertragung stattfindet.

IV. Überprüfen Sie das Zertifikat zur Verschlüsselung

Bei jedem Aufruf des Internet Bankings ist das Zertifikat zu überprüfen. Damit wird gewährleistet, daß Sie auch tatsächlich mit Ihrer Bank bzw. Sparkasse kommunizieren. Durch einen Doppelklick auf das Schloßsymbol finden Sie unter „Details“ Angaben zur Gültigkeit, zur Zertifizierungsstelle, zum Fingerabdruck und zum Zertifizierungspfad.



Die Phishing-Angriffe sind keine Neuigkeit, schon seit Jahren existieren diese Angriffe, jedoch nehmen diese in den letzten Jahren immer mehr zu. Außerdem werden nicht nur Banken oder Sparkassen – Layout nachgeahmt, sondern die Betrüger können auch andere Formen vortäuschen. Deshalb sollte man immer vorsichtig sein, wenn nach Bankdaten gefragt wird. Weitere Beispiele für Betrüger sind gefälschte Internetseiten oder E-Mails an Hotmail Nutzer. Weitere Sektoren, die hauptsächlich betroffen werden, sind die On-line Dienstleistungsanbieter und Versteigerungen.

My MSN | Hotmail | Shopping | Money | People & Chat | Search

Hotmail Account Update

Provide your billing information

Billing information

Type your name as it appears on your payment method.

First name

Last name

Payment method Debit card

Debit card type

Name on debit card

Debit card number

Expiration date

Civ/Cvv2 Last 3 digits located on the back of your card

Card PIN Number Your 4 digit number used in ATM transactions

Billing address

Type your address exactly as it appears on the billing statement for your payment method.

Address Line 1

Address Line 2 (optional)

City

State

ZIP/Postal code

Country/Region

Area code & phone number Ext

*Your debit card will not be charged.

Microsoft Internet Explorer

 PLEASE READ CAREFULLY

Welcome to MSN's Billing Center!

Our current records indicate that your account may be suspended. However, you have to provide us new billing information. Valid billing details are required to maintain availability of your account.

Please have the following:

- Your last Billing Statement.
- Your current debit card(s).
- Any relevant information.



Please Sign In [Need Help?](#)

For security reasons please re-enter your user ID and password.

eBay User ID

[Forgot your User ID?](#)

Password

[Forgot your password?](#)

Copyright © 1995-2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the [eBay User Agreement](#) and [Privacy Policy](#).



5. AUSWIRKUNGEN DES PHISHINGS

Die schlimmsten Phishing-Fälle sind in USA aufgetreten, jedoch haben die Mafias gemerkt, daß sie weltweit eine riesengroße Möglichkeit haben, ihre Betrüge durchzuführen. Die Phishing-Anfälle nehmen in verschiedenen Ländern stark zu, sowie in England, Spanien, Portugal und auch in Deutschland.

Das Phishing Problem wurde vom Unternehmen Gartner ausführlicher für den Fall USA untersucht. Die Ergebnisse lauten:

Die Betrugsversuche gegen Internetnutzer, die sogenannten Phishing-Angriffe, sind so häufig geworden, dass geschätzt wird, dass ca. 57 Mio von Amerikanern schon mindestens einmal eine solche Art von Täuschungs-Email erhalten haben. Es wird geschätzt, daß im letzten Jahr die direkten Verluste gegenüber Banken und Kreditkarteninstitute auf eine Höhe von 1,2 Mio Dollar anfallen.

Basierend auf eine Untersuchung, die bei 5000 erwachsenen Internetnutzern ausgeführt wurde, schätzt Gartner, daß ungefähr 30 Mio. Internetnutzer in Wirklichkeit eine Phishing Attacke erlebt haben und die restlichen 27 Mio. glauben einen Täuschungsversuch gehabt zu haben.

Die Phishing-Angriffe sind keine Neuigkeiten, jedoch sind die Attacken alltäglicher geworden in den letzten 12 Monaten. Laut der Marktforschung des Consulting Unternehmen Gartner 76% der Phishing-Anfälle ereigneten sich in den letzten 6 Monaten (seit Oktober 2003) und 16% geschahen vor 6 Monaten oder vorher, das heißt, daß 92% der Angriffe in diesem letzten Jahr 2004 vorgekommen sind.

Laut Avivah Litan, Vice-President des Gartner-Unternehmens sollten die Finanzinstitutionen, Internetprovider und andere Dienstleistungsanbieter mit den wachsenden Internetbetrüger aufpassen. Diese Dienstleistungsunternehmen sollten Maßnahmen unternehmen und Lösungen finden, damit diese Täuschungsangriffe erheblich reduziert werden, obwohl sie nicht direkt betroffen werden. Gelegentlich können alle Unternehmen, die Online-Produkte; Online-Dienstleistungen, Online-Banking, Online-Shopping; usw. anbieten, negativ betroffen werden, da die Internetnutzern das Vertrauen zu dem E-Commerce verlieren werden, wenn diese Atacken nicht schnell verringert werden.

6. KAMPF GEGEN PHISHING – ANGRIFFE

6.1 ANTI-PHISHING WORKING GROUP“ (APWG)

Die Zahl der sogenannten Phishing-Webseiten wächst weiter und stellt damit auch eine wachsende Gefahr für das Online-Banking und andere Internet-basierende Geschäftsmodelle dar. Die starke Zunahme der Betrugsversuche ist der Grund warum mehrere Unternehmen gemeinsam und Hand-in-Hand gegen die Online-Betrüger zusammenarbeiten. In USA wurde die „**Antiphishing Working Group (APWG)**“ gegründet. Mehr Information finden Sie unter deren Internetseite: www.antiphishing.org und entdecken Sie einen Betrugsversuch, so können Sie es anzeigen und eine E-Mail an reportphishing senden.



Jeden Monat wird ein neuer Bericht herausgegeben, indem alle angezeigten Phishing-Angriffe untersucht werden. Der letzte Bericht entspricht Juli 2004 und ist in der oben genannten Website (auf Englisch) abrufbar. Daraufhin stellen wir Ihnen eine kurze Zusammenfassung dar:

Anti-Phishing Working Group
APWG
register

Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

report phishing - click here

- [Home](#)
- [Phishing Archive](#)
- [Report Phishing](#)
- [Events](#)
- [APWG News](#)
- [Resources](#)
- [Membership](#)
- [APWG Member Site](#)
- [Contact Us](#)
- [JOIN THE APWG](#)

PARTNER EVENT:

Spam Compliance

THE EMAIL EVENT

What is Phishing?

Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them.

Date	Weekly Phishing Attacks	Cumulative Phishing Attacks
5/1/2004	279	279
5/8/2004	268	547
5/15/2004	321	868
5/22/2004	310	1178
5/29/2004	224	1402
6/5/2004	315	1717
6/12/2004	339	2056
6/19/2004	303	2359
6/26/2004	324	2683
7/3/2004	424	3107
7/10/2004	418	3525
7/17/2004	419	3944
7/24/2004	393	4337
7/31/2004	475	4812

Anti-Phishing Working Group
The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identity and fraud that result from the growing problem of phishing and email spam.

APWG Members

- Over 636 members
- Over 407 companies
- 8 of the top 10 US banks
- 4 of the top 5 US ISPs
- Over 100 technology vendors
- Law enforcement from Australia, Canada, UK, USA

APWG Working Groups

- Best Practices
- Education
- Future Threat Models
- Phishing Repository
- Sizing the Problem
- Solution Evaluation/Trial
- Law Enforcement

APWG SPONSORS:

News and Events:

- 30-Aug-04 - New Phishing Trends Report Available!
[Phishing Attack Trends Report - July 2004](#)



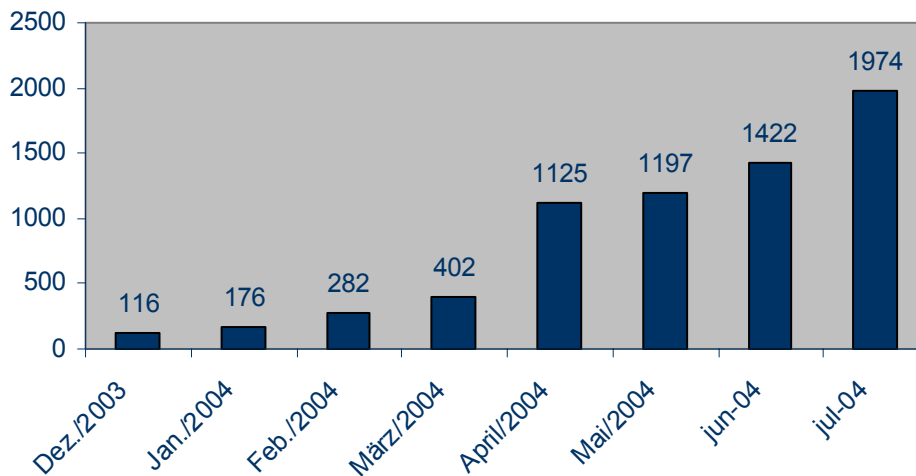
6.2 DATEN

- ▶ Anzahl der Phishing-Angriffe, die im Juli angezeigt wurden: **1974 Angriffe**
- ▶ Durchschnitt des Zuwachsrates: **50%**
- ▶ Unternehmen, die am meisten angegriffen wurden: **Citibank(682Angriffe)**
- ▶ Land, das am meisten Phishing-Webs untergebracht hat: **USA (35%)**

▶ ANZAHL DER PHISHING-ANGRIFFE

Die **Anti-Phishing Working Group** hat zusammen mit den Websense Security Labs die Daten über Phishing-Attacken für den Juli dieses Jahres ausgewertet. Dabei wurden allein Juli 1.974 betrügerische Angriffe gezählt. Das entspricht einer Zunahme um 39 Prozent gegenüber Juni.

Anzahl Monatlicher Phishing-Angriffe



Quelle: Anti-Phishing Working Group



► **Welche Organisation oder Unternehmen werden am meisten durch Phishing angegriffen?**

Primäres Angriffsziel der Phishing-Attacken ist immer noch mit 73 Prozent der Finanzdienstleistungsbereich, gefolgt von Internet-Service-Providern mit 14 Prozent und der Handel (beispielsweise Ebay) mit 7 Prozent.

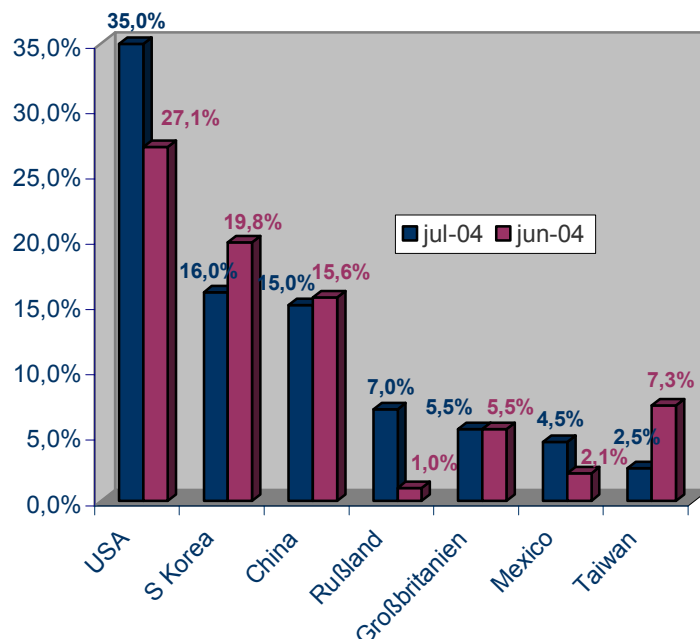
Unternehmen	Jul-04	Jun-04	Mai-04	Apr-04	Mär-04	Feb-04	Jan.-04
Citibank	682	492	370	475	98	58	34
U.S.Bank	622	251	167	62	4	0	2
eBay	255	285	293	221	110	104	51
Paypal	147	163	149	135	63	42	10
AOL	41	14	17	9	10	10	35
Suntrust	25	4	1	5	1	0	0
Lloyds	23	24	17	15	4	0	1
Fleet	20	55	33	28	23	9	2
Barclays	17	19	15	31	11	6	1
Earthlink	15	7	6	18	5	8	9

Quelle: Anti-Phishing Working Group

► **Länder mit den meisten Phishing-Angriffe**

USA ist Leader und hat bis jetzt die meisten Phishing-Webs aufgebracht, jedoch wachsen die Angriffe auch in anderen Ländern, sowie in Russland; Großbritannien und Mexico.

Länder mit den meisten Phishing-Webs



Quelle: Anti-Phishing Working Group



6.3 LONGEVITÀ MEDIA DI WEBS PHISHING

La media di "vita" di questo tipo di webs fraudolenti, misurata secondo il tempo in cui appaiono fino al momento della loro scoperta, è di 6.1 giorni. Fino ad ora, la web phishing più longeva durò 31 giorni (in altre parole, questa web continuò a funzionare per un mese intero)

BIBLIOGRAPHIE

Zeitungen:

- ▶ Personal Computer: Ottobre 2004. N° 21
- ▶ PC Pro: N° 51 2004

Internet:

- ▶ www.hispasec.com/unaaldia/2163
- ▶ www.vnunet.es/Actualidad/Noticias/Seguridad/Privacidad/20040927017
- ▶ www.el-mundo.es/navegante/2004/09/27/seguridad/1096287700.html
- ▶ <http://www.antiphishing.org/>

Berichte:

- ▶ Anti-Phishing Working Group. "Phishing Attack Trends Report - July 2004." Julio 2004