

Friday, January 22, 2010

Packstation Phishing

Gerade schlug bei mir eine Mail auf, die man wohl als Packstation-Phishing be

Return-Path: info at packstation.de
X-Spam-Status: No, score=0.0 required=5.0 tests=none autolearn=disabled
Received: from s153****.onlinehome-server.info (EHLO s153****.onlinehome-s
by mx0.gmx.net (mx087) with SMTP; 22 Jan 2010 00:39:08 +0100
Date: 18 Jan 2010 03:31:47 +0100
Message-ID: 20100118023147.2224.gmail at s153****.onlinehome-server.info
To: meineemailadresse_neinnichtwirklich at gmx.de
Subject: PACKSTATION Systemupdate
From: DHL AG info at packstation.de
X-GMX-Antivirus: 0 (no virus found)
X-GMX-Antispam: 0 (Mail was not recognized as spam);

Content-type: text/html;

Sehr geehrte(r) Sebastian Raible.

Da wir in den letzten Wochen unser Serversystem auf den neusten Stand gebra
unserem umfassenden Systemcheck mitzuwirken.

Dieser dient dazu, eventuelle Fehler zu beseitigen. Wir bitten Sie daher darum
Ihre PACKSTATION-Daten zu überprüfen.

[http:// PACKSTATI 0 N.6x. to/index.php?id=*****](http://PACKSTATI0N.6x.to/index.php?id=*****)

Schlägt der Loginversuch fehl, bitten wir Sie, sich unter folgender Nummer zu
0800 343 *** ** (0 ct/Min*)

Viel Spaß weiterhin mit Ihrer PACKSTATION wünscht Ihnen

Ihr PACKSTATION Team

*) Aus dem deutschen Festnetz

DHL Vertriebs GmbH Co. OHG
Rathausplatz 1
10234 Berlin

Baut da jemand ein Array von Briefkästen auf, mit dem er anonym Sendungen e

Wenn ja, ist das immerhin mighty cool. Und irgendwie tun sich da jede Menge (
auf, was man damit machen könnte.

Update: Heise hatte dazu schon im vergangenen März (2009) einen Artikel: hei
vertrauensereckender Domain

Posted by Sebastian Raible at 00:48

Eine Idee, woher der Name in der Mail stammt?

Bei mir kam das auch an mit meinem vollen Namen, was ich bei Spam bisher nicht geseh

Könnte der z. B. aus Facebook oder Skype gezogen worden sein?

Anonymous on Jan 24 2010, 21:05

Also meine Emailadresse ist vorname.nachname at gmx.de, bei mir wäre es also denkba
Emailadresse (die sie sonstwo her haben) meinen Namen geraten haben.

Wenn dein Name in der Adresse nur abgekürzt ist, weiß ich auch nicht& ich würde aller
Michael Butscher-Zeile auf deiner Homepage tippen.

Grüße

Seb

Anonymous on Jan 24 2010, 21:18

Ich benutze tatsächlich nur mbutscher in meiner Adresse.

Natürlich habe ich meinen Namen in Verbindung mit der Adresse an einigen Stellen im M
Spam-Programme diese Information tatsächlich finden und auswerten können ist das sch
ich.

Anonymous on Jan 24 2010, 21:28

Ja aber deine Emailadresse steht doch im Klartext inklusive Namen auf deiner Website.

Anonymous on Jan 25 2010, 00:20

Sehr geehrte Anwender,

unser SecurityLab hat die von Ihnen beschriebenen Spams analysiert und folgendes her

- Die Daten stammen mit großer Wahrscheinlichkeit aus Datendiebstählen in Online-Sho

- Die Täter haben eine Sicherheitslücke in dem eingesetzten Shopsystem ausgenutzt un
E-Mail-Adressen und die echten Namen in Relation zu setzen und entsprechend die Ans

Detaillierte Infos finden Sie auf unserer Webseite: www.gdata.de

Herzliche Grüße aus Bochum

G Data Software AG

Anonymous on Feb 5 2010, 15:52

Ich bin kein Anwender. Und auf eurer Website finde ich einen 401. Ansonsten wünsche i
diesen von euch auf meinem Blog.

Anonymous on Feb 10 2010, 10:26