digiHelp IT Beratung
Roland Stelling

Hellergasse 51
53359 Rheinbach
Tel. (02225) 998 4841
Fax (02225) 998 4842
mail@digihelp.de

SPAM und Fishing Beispiel vom 11.04.2013

Wie und woran erkenne ich eine SPAM Mail?

In vielen Fällen ist es vergleichsweise einfach und auch für den Computer Anwender möglich, eine seriöse E-Mail von einer potentiell oder tatsächlich gefährlichen Variante zu unterscheiden. Wie man vorgehen kann, zeigt der folgende Beitrag.

Die auf der nächsten Seite wiedergegebene E-Mail (Abbildung 1) wurde an die Adresse eines realen privaten PayPal Kunden geschickt. Der Aufbau täuscht auf den ersten Blick Seriosität vor.

Sehen wir uns diese Mail mal etwas genauer an.

Als Absender ist service@paypal.de ausgewiesen. Das sieht gut aus, aber Vorsicht, Absender Adressen lassen sich leicht fälschen.

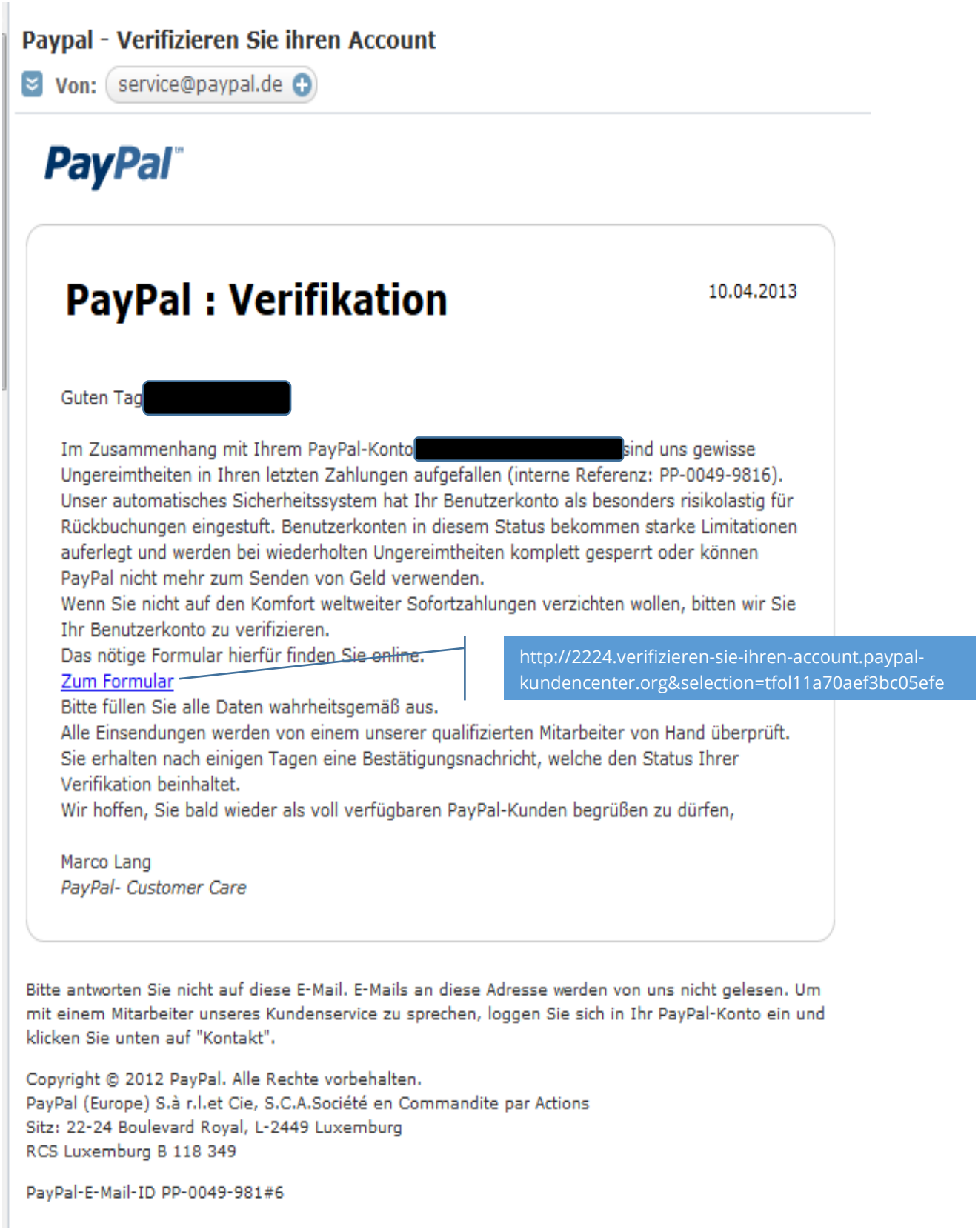
Im mittleren Teil des Textes wird der Leser auf ein Online Formular zum Ausfüllen verwiesen. Das ist in mehrfacher Hinsicht verdächtig.

1. Kein seriöses Unternehmen versendet E-Mails, in denen zur Eingabe von benutzerbezogenen Daten in Online Formulare aufgerufen wird.
2. Bewegt man den Mauszeiger über den Link „Zum Formular“ ohne zu klicken, sieht man in der Statuszeile des Browsers die tatsächliche URL. Hier ist das: http://2224.verifizieren-sie-ihren-account.paypal-kundencenter.org&selection=tfol11a70aef3bc05efe.

   Hier sieht es gar nicht mehr nach PayPal aus. Die Domäne und Toplevel Domäne lauten „paypal-kundencenter.org“ und nicht, wie es richtig wäre, „paypal.com“.

Hellergasse 51
53359 Rheinbach
Tel. (02225) 998 4841
Fax (02225) 998 4842
mail@digihelp.de

Abbildung 1



Paypal - Verifizieren Sie ihren Account

Von: service@paypal.de

PayPal

PayPal : Verifikation

10.04.2013

Guten Tag [redacted]

Im Zusammenhang mit Ihrem PayPal-Konto [redacted] sind uns gewisse Ungereimtheiten in Ihren letzten Zahlungen aufgefallen (interne Referenz: PP-0049-9816). Unser automatisches Sicherheitssystem hat Ihr Benutzerkonto als besonders risikolastig für Rückbuchungen eingestuft. Benutzerkonten in diesem Status bekommen starke Limitationen auferlegt und werden bei wiederholten Ungereimtheiten komplett gesperrt oder können PayPal nicht mehr zum Senden von Geld verwenden.
Wenn Sie nicht auf den Komfort weltweiter Sofortzahlungen verzichten wollen, bitten wir Sie Ihr Benutzerkonto zu verifizieren.
Das nötige Formular hierfür finden Sie online.
Zum Formular
Bitte füllen Sie alle Daten wahrheitsgemäß aus.
Alle Einsendungen werden von einem unserer qualifizierten Mitarbeiter von Hand überprüft. Sie erhalten nach einigen Tagen eine Bestätigungsnachricht, welche den Status Ihrer Verifikation beinhaltet.
Wir hoffen, Sie bald wieder als voll verfügbaren PayPal-Kunden begrüßen zu dürfen,

Marco Lang
PayPal- Customer Care

http://2224.verifizieren-sie-ihren-account.paypal-kundencenter.org&selection=tfol11a70aef3bc05efe

Bitte antworten Sie nicht auf diese E-Mail. E-Mails an diese Adresse werden von uns nicht gelesen. Um mit einem Mitarbeiter unseres Kundenservice zu sprechen, loggen Sie sich in Ihr PayPal-Konto ein und klicken Sie unten auf "Kontakt".

Copyright © 2012 PayPal. Alle Rechte vorbehalten.
PayPal (Europe) S.à r.l.et Cie, S.C.A.Société en Commandite par Actions
Sitz: 22-24 Boulevard Royal, L-2449 Luxemburg
RCS Luxemburg B 118 349

PayPal-E-Mail-ID PP-0049-981#6

Hellergasse 51
53359 Rheinbach
Tel. (02225) 998 4841
Fax (02225) 998 4842
mail@digihelp.de

3. Aber wer steckt hinter „paypal-kundencenter.org“? Um einen Verdacht zu überprüfen, rufen wir die Homepage der Formular Adresse http://paypal-kundencenter.org direkt auf. Die Subdomäne „2224.verifizieren-sie-ihren-account“ und den Aufruf Parameter „&selection=tfol11a70aef3bc05efe“ lassen wir bewusst weg.

   Das Ergebnis zeigt Abbildung 2. Als erstes fällt beim Blick auf die Statuszeile auf, dass diese Homepage in Kasachstan betrieben wird[1]. *Zum aktuellen Zeitpunkt (April 2014) ist diese Domäne bereits wieder gelöscht.* Es erscheint als sehr unwahrscheinlich, dass PayPal eine Website in Kasachstan für deutsche Kunden betreibt.

Abbildung 2

4. Die Domänen Homepage http://paypal-kundencenter.org sieht auf den ersten Blick ebenfalls authentisch aus, jedoch ist das Angebot auf eine verschlüsselte Seite zu wechseln ohne Funktion.

   Auch hier gilt: Seriöse Anbieter schützen sich und ihre Kunden durch Zertifikate und verschlüsselte Verbindungen.

[1] Zur Anzeige der Webserver Lokation wurde der Firefox Browser des Autors um das Addon „Website Standort und Länderinfo“ von IPdata Team erweitert.

Hellergasse 51
53359 Rheinbach
Tel. (02225) 998 4841
Fax (02225) 998 4842
mail@digihelp.de

Am Beispiel der richtigen PayPal URL kann man das sehen:

Zur Suche nach dem Betreiber „paypal-kundencenter.org“ nutzen wir eine Abfrage bei http://whois.domaintools.com und erhalten ein aufschlussreiches Ergebnis:

- Domain ID:D168218685-LROR
  Domain Name:PAYPAL-KUNDENCENTER.ORG
  Created On:21-Mar-2013 14:01:34 UTC
  Last Updated On:21-Mar-2013 14:07:50 UTC
  Expiration Date:21-Mar-2014 14:01:34 UTC
  Sponsoring Registrar:Bizcn.com, Inc. (R1248-LROR)
  Status:CLIENT TRANSFER PROHIBITED
  Status:TRANSFER PROHIBITED
  Registrant ID:orgrr63874491554
  Registrant Name:Whois Agent
  Registrant Organization:Whois Privacy Protection Service
  Registrant Street1:No. 61 Wanghai Road Xiamen Software Park
  Registrant City:xiamen
  Registrant State/Province:fujian
  Registrant Postal Code:361008
  Registrant Country:CN
  Registrant Phone:+86.5922577888
  Registrant FAX:+86.5922577111
  Registrant Email: gmvjcxkxhs@whoisservices.cn
  Admin ID:orgrr63874491972
  Admin Name:Whois Agent
  Admin Organization:Whois Privacy Protection Service
  Admin Street1:No. 61 Wanghai Road Xiamen Software Park
  Admin City:xiamen
  Admin State/Province:fujian
  Admin Postal Code:361008
  Admin Country:CN
  Admin Phone:+86.5922577888
  Admin Phone Ext.:
  Admin FAX:+86.5922577111
  Tech ID:orgrr63874492339
  Tech Name:Whois Agent
  Tech Organization:Whois Privacy Protection Service
  Tech Street1:No. 61 Wanghai Road Xiamen Software Park
  Tech City:xiamen
  Tech State/Province:fujian
  Tech Postal Code:361008
  Tech Country:CN
  Tech Phone:+86.5922577888

Hellergasse 51
53359 Rheinbach
Tel. (02225) 998 4841
Fax (02225) 998 4842
mail@digihelp.de

Tech Phone Ext.:
Tech FAX:+86.5922577111
Name Server:NS1.PAYPAL-KUNDENCENTER.ORG
Name Server:NS2.PAYPAL-KUNDENCENTER.ORG
DNSSEC:Unsigned

Fazit: Das angebliche Paypal Kundencenter nutzt einen Webservice in Kasachstan der bei der **Whois Privacy Protection Service** Organisation in Xiamen, China registriert ist.

Nomen est Omen. Wir haben es uns gespart, im No. 61 Wanghai Road Xiamen Software Park anzurufen und nach der Geschäftsbeziehung zu Paypal zu fragen.

Der Autor hofft, dass Ihnen dieses Beispiel hilft, mit schärferem Blick harmlose von gefährlichen E-Mails zu unterscheiden.

Dabei viel Erfolg!