Warnung vor gefälschten Emails!

Gernot L. Geise

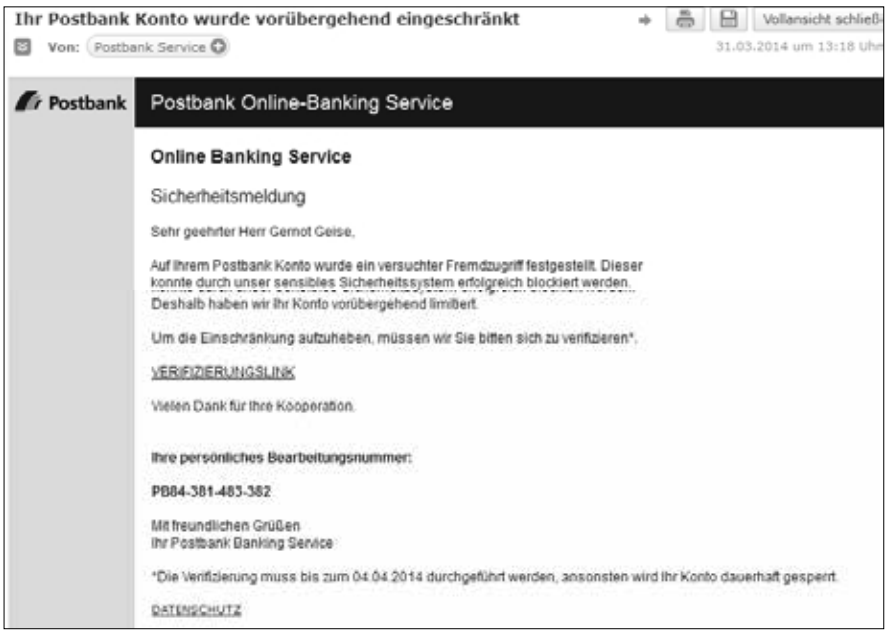
Die Sepa-Umstellung wird ausgenutzt

Es kursieren in letzter Zeit verstärkt verblüffend echt aufgemachte Emails (angeblich etwa von Paypal und/oder anderen Banken), in denen man aufgefordert wird, etwa aufgrund der Sepa-Umstellungen die eigenen Bankdaten o. ä. zu bestätigen bzw. sich zu „verifizieren". Praktischerweise ist in diesen Emails dann gleich ein Button oder Link dabei, den man anklicken soll, um zu der gewünschten Adresse zu gelangen (siehe Abb.).

Dies ist jedoch die „Pishing"-Methode, vor der seit Jahren (auch in PC-Zeitschriften) **immer wieder gewarnt wird!** Es geht nur darum, Ihre Bankdaten und Passwörter abzufragen, um sie missbrauchen zu können! Als sehr hilfreich bietet sich für die kriminellen Spam-Versender derzeit die (durchaus nachvollziehbare) Ungewissheit der Bankkunden über die Sepa-Umstellungen der Bankdaten an.

Wenn man verständlicherweise unsicher wird, weil in diesen Emails eine Konto-Einschränkung (bis zur Kontosperrung) angedroht wird, dann sollte man ***keinesfalls*** den angegebenen Link benutzen! Loggen Sie sich wie gewohnt bei Ihrem Kreditinstitut ein und prüfen Sie dort nach. Wenn die „Umstellungs-Email" tatsächlich von diesem Kreditinstitut stammen sollte, würden Sie nach dem Einloggen darauf hingewiesen werden.

Die Umstellung auf Sepa macht jede Bank automatisch. Der Kunde muss überhaupt nichts bestätigen, schon gar kein Passwort! Hinzu kommt, dass sich keine Bank per Email mit Ihnen in Verbindung setzt, sofern Sie es nicht ausdrücklich genehmigt haben. Wenn eine Bank ihrem Kunden etwas mitteilen möchte (auch eigene Werbung oder Änderungen in den AGB), dann macht sie dieses mit der normalen „gelben" Post.


Ihr Postbank Konto wurde vorübergehend eingeschränkt

Von: Postbank Service

31.03.2014 um 13:18 Uhr

Postbank Online-Banking Service

Online Banking Service

Sicherheitsmeldung

Sehr geehrter Herr Gernot Geise,

Auf Ihrem Postbank Konto wurde ein versuchter Fremdzugriff festgestellt. Dieser konnte durch unser sensibles Sicherheitssystem erfolgreich blockiert werden. Deshalb haben wir Ihr Konto vorübergehend limitiert.

Um die Einschränkung aufzuheben, müssen wir Sie bitten sich zu verifizieren*.

VERIFIZIERUNGSLINK

Vielen Dank für Ihre Kooperation.

Ihre persönliches Bearbeitungsnummer:

PB84-381-483-382

Mit freundlichen Grüßen
Ihr Postbank Banking Service

*Die Verifizierung muss bis zum 04.04.2014 durchgeführt werden, ansonsten wird Ihr Konto dauerhaft gesperrt.

DATENSCHUTZ

Beispiel einer solchen Pishing-Email.

Ich erhielt jetzt eine Email von „Paypal", worin mir mitgeteilt wurde, dass Paypal „glücklicherweise" einen Fremdzugriff auf mein Paypal-Konto abgewehrt habe. Dabei wurden sogar Betrag, Adresse des angeblichen Bestellers usw. angegeben. Ich möge doch bitte über den angegebenen Link bestätigen, ob diese Abbuchungsaufforderung von mir stammt oder nicht. Auch diese Email war gefälscht! Beim eigenen Einloggen auf die Paypal-Seite hätte man mir diesen angeblichen Fremdzugriff aufzeigen müssen. War jedoch nichts davon bekannt.

Also Vorsicht vor solchen Emails! Im Zweifelsfall sollte man sich immer selbst bei der jeweiligen Bank einloggen und ***niemals*** solche in den Emails angegebenen Links benutzen! Durch solche Links wird man auf ebenfalls täuschend echt nachgemachte Seiten geführt, wo man seine Bankdaten einschließlich Kennwort (zum angeblichen Vergleich) eingeben soll. Damit hat man jedoch alle Zugriffsrechte auf das eigene Konto freiwillig abgegeben und braucht sich nicht zu wundern, wenn anschließend das Konto abgeräumt wird.

Ich bekam (wieder einmal) eine Email mit der Androhung, dass mein Konto eingeschränkt/gesperrt würde, wenn ich mich nicht verifizieren würde, natürlich über den angegebenen Link, diesmal angeblich von der Postbank. Dazu muss ich sagen, dass ich bei der Postbank zwar Kunde bin, jedoch überhaupt keine Email-Adresse angegeben habe, sie mir also gar keine Emails schicken kann. Ähnliche Emails erhielt ich auch schon von anderen „Banken/Sparkassen", bei denen ich gar kein Kunde bin.

Also, wenn Sie solche Emails erhalten (auch von anderen Banken oder Paypal), **sofort löschen und auf gar keinen Fall den angegebenen Link benutzen!** Das gilt übrigens auch für Emails, die angeblich von irgendwelchen Behörden stammen!

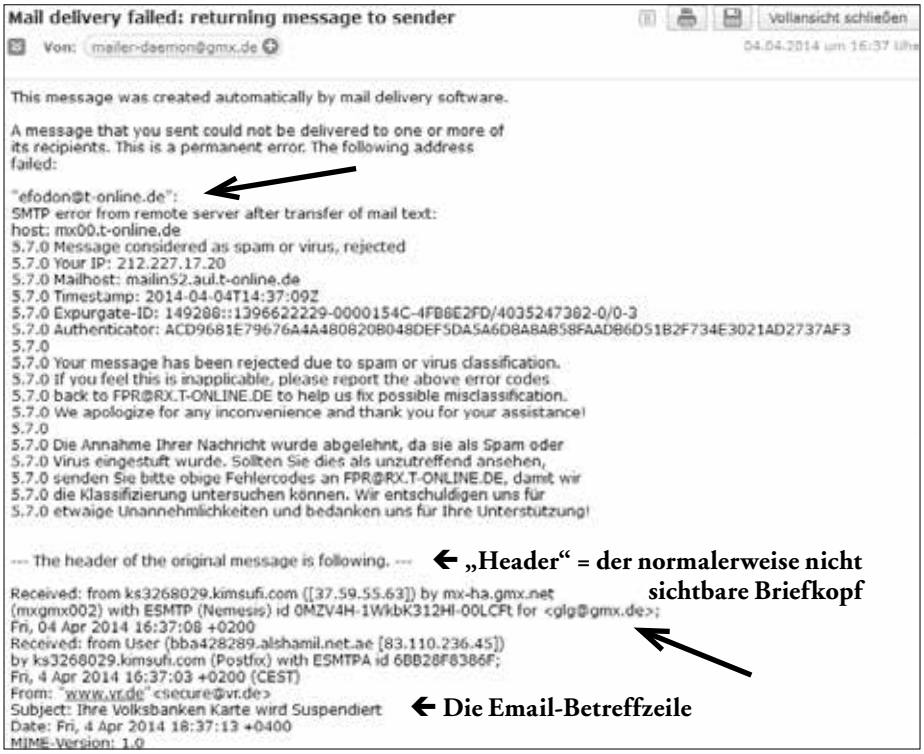
Diesbezüglich warnt auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor E-Mails, die augenscheinlich in seinem Namen verschickt werden. Dabei handelt es sich um Phishing-Emails. In den Nachrichten mit gefälschter Absenderadresse werden angebliche Rechtsverstöße des Empfängers erwähnt, heißt es in der BSI-Warnung. Um „anwaltliche Schritte" zu vermeiden, soll der Empfänger ein Formular herunterladen und ausfüllen. Davon sollte man jedoch die Finger lassen und die Email sofort löschen!

Bis vor kurzem konnte man gefälschte Emails noch recht gut als solche erkennen, weil sie Rechtschreibfehler oder fehlerhafte Grammatik enthielten. Die Verfasser haben jedoch inzwischen dazu gelernt, Rechtschreibfehler kommen heute nur noch selten vor.

Teilweise kann man auch anhand des Email-Absenders erkennen, woher eine solche Email stammt. Doch auch hier sind die Versender inzwischen „besser" geworden: Sie verwenden teilweise die echten Adressen, sodass hier der Eindruck erweckt wird, die Emails würden vom genannten Geldinstitut stammen.

Emails unter fremdem Namen

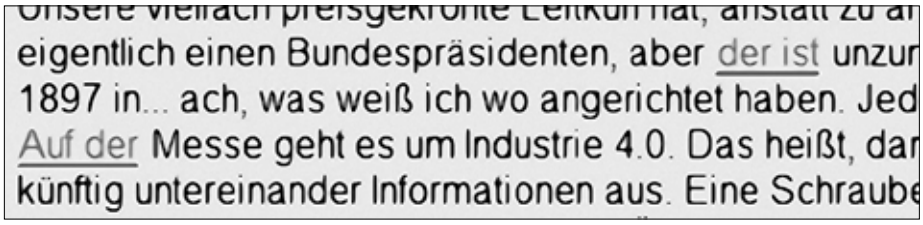
Wie es möglich ist, unter einer fremden Email-Adresse Emails zu verschicken, wissen wohl nur diejenigen, die es tun. So beobachten wir seit längerer Zeit, dass unter unserer Email-Adresse (auch unter meiner privaten) Spams versendet werden. Wir stellten es fest, weil immer wieder diverse Rückläufer eintrudeln. Das sind die „Mailer-Daemon"-Emails, die nicht zugestellt werden können, weil z. B. die Empfänger-Adresse nicht existiert. Dann kommt eine solche Fehlermeldung zum (angeblichen) Absender zurück. Öffnet man eine solche Mailer-Daemon-Email, so werden dort auf englisch u. a. der Absender, Empfänger und gesamte Laufweg angegeben, sowie kryptisch verschlüsselt der Email-Inhalt (siehe Abb.). Darin steht dann beispielsweise 12hbd@efodon.de als Absender (nur als Beispiel). Der Empfänger, falls es ihn gibt, muss dann zwangsläufig annehmen, dass diese Email von uns stammt. Wir haben zwar auf unsere Internetzseite efodon.de einen diesbezüglichen Hinweistext gesetzt, jedoch kann man nicht davon ausgehen, dass jeder Empfänger einer Spam-Email zunächst auf unsere Internetzseite geht, um diesen Text zu lesen.



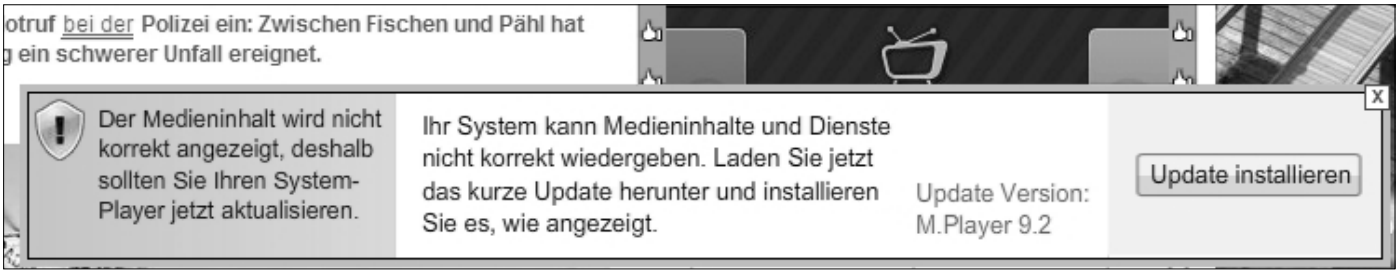
So sieht der Text eines „Mailer Daemon" aus (Ausschnitt, geht noch etwas weiter).

Aufpoppende Werbefenster

Mehr als unangenehm sind auch die neueren Belästigungen, die sich in letzter Zeit etabliert haben, etwa die aufpoppenden Werbefenster. Gut, solche gab es in ähnlicher Art schon immer, sie werden auch manchmal durch den Browser (Programm zum Verwalten, Finden und Ansehen von Dateien im Internetz) Firefox, Internet Explorer oder Google Chrome unterdrückt, wenn man es dort vorher einstellt. Die-



In irgendwelchen Texten auf irgendwelchen Seiten eingeschmuggelte Links (erkennbar an der Unterstreichung. Fährt man mit der Maus über einen solchen Link, poppt - siehe unten - ein Werbefenster auf. ***Dies passiert nur, wenn man mit dem Firefox-Browser im Netz ist!***



Solche unerwünschten Fenster blenden sich vor irgendeinen Seiten-Text. Bei diesem Beispiel auch erkennbar: In den oberen Zeilen des Originaltextes dieser Seite ein Fremd-Link, hier doppelt unterstrichen. Solche Links kann man auch daran erkennen, weil sie wahllos im Text stehen.

se Werbefenster („Popups“) wurden allerdings von den jeweiligen Seitenbetreibern programmiert, um gewisse Werbeeinnahmen zu haben.

Die neueren werden jedoch durch **Firefox** initiiert. Dieselben durch den Internet-Explorer aufgerufenen Seiten enthalten diese Belästigungen nicht! Sie klemmen sich vor irgend einen Text, teilweise verschieben sie ihn auch, und stammen nicht von dem jeweiligen Seitenbetreiber. In grauer kleiner Schrift steht darunter: „Ads by Online Browser Advertising“ oder „Dial Finder“ (siehe Abb.).

Firefox ist zwar ein „freier“ Internetz-Browser, der schließlich irgendwie finanziert werden muss. Und das geschieht im Regelfall durch Werbung. Aber hier gehen die Programmierer unbedingt zu weit, und sie brauchen sich nicht zu wundern, wenn sich die Anwender dann anderen Programmen zuwenden, die nicht mit solchen Tricks arbeiten.

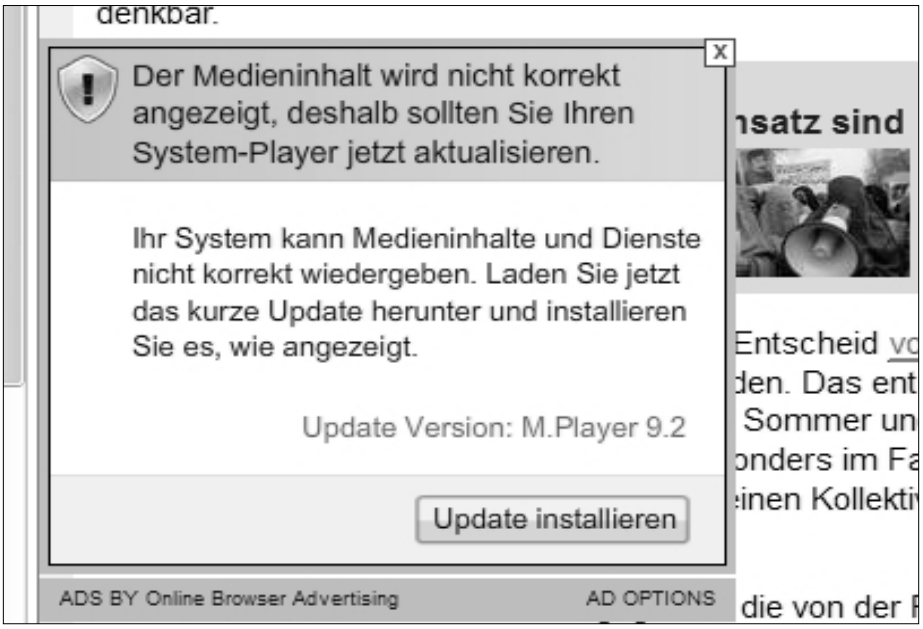
Es ist ja kaum noch möglich, im Internetz zu „surfen“, ohne ständig aufgefordert zu werden, einen Media-Player zu aktualisieren (auch wenn auf dem Rechner bereits die aktuellste Version installiert ist!) oder irgendwelche angeblichen PC-Fehler zu beheben.

Oben: Drei Beispiele desselben Werbefensters, das sich frech vor Seiten-Texte legt. Unten: Aufforderung, einen „System-Player“ zu aktualisieren. Auch dieses Fenster legt sich ungefragt vor einen Seiten-Text.

Gefälschte Links

Auffällig ist auch eine neue Masche, dass in einem Text diverse Wörter grün unterstrichen sind (= im Regelfall eine Kennzeichnung für weiterführende Links). Wenn man mit der Maus – ohne zu klicken – darüber fährt, poppt ein Fenster auf, in dem man wiederum aufgefordert wird, u. a. einen Media-Player zu aktualisieren (siehe Abb.).

Als Standard-Media-Player gilt normalerweise der kostenlose Flash-Player von Adobe. Die Werbefensterchen haben jedoch mit Adobe nichts zu tun. Man wird (ich habe es jedoch nicht ausprobiert) möglicherweise auf eine



Die Alarmglocken müssten schon aufgrund der falschen Rechtschreibung sofort klingeln! („2 Minuen")
Der „Blickpunkt" stammt von der Originalseite und ist so programmiert, dass er immer im Vordergrund steht, deshalb liegt er auch vor der Spam-Werbung.
Lassen Sie sich ***niemals*** *Ihr Windows bzw. Ihren Rechner über eine solche Werbung scannen! Es geht nur darum, von außen festzustellen, welche Programme auf Ihrem Computer installiert sind, wie gut oder schlecht er geschützt ist und im Hintergrund irgendein Schadprogramm zu installieren, wodurch Ihr Rechner aus dem Internetz ferngesteuert oder sonstwie missbraucht werden kann.*

gefälschte Seite geleitet, die die Rechnerdaten abfragt (oder mehr).

Gut, die aufpoppenden Werbefenster kann man „aus-ixen" (über das kleine Kreuz in der rechten oberen Ecke löschen), um den abgedeckten Text lesen zu können. Lästig sind sie trotzdem. Außerdem sind sie (lt. PC-Zeitschriften) so programmiert, dass beim Löschen eine Rückmeldung erfolgt. Das heißt, der Verbreiter dieser Werbefenster weiß dann, dass eine Aktion erfolgt ist, er also erfolgreich mit seinem Fenster ist. Eine andere Variante ist, dass man beim Löschen sofort auf eine Werbeseite geleitet wird, die man ebenfalls erst löschen muss.

Die in Texten als Links markierten Wörter muss man nicht anklicken, insofern scheinen sie relativ harmlos zu sein. Man kann sie auch daran erkennen, weil sie völlig wahllos irgendwelche Wörter unterstreichen. Bei „echten" Links werden beispielsweise irgendwelche Namen unterstrichen, die dann beim Aufruf Erklärungen dazu bieten oder auf weiterführende Seiten verweisen.

Auch die Masche der gefälschten Links findet sich *nur unter Firefox*. Dieselbe Seite im Internet-Explorer geöffnet, enthält diese angeblichen Links nämlich nicht.

Die gestohlenen Email-Daten

Zuletzt möchte ich noch auf den letzten großen „Datenklau" eingehen, vor dem sogar in den Medien gewarnt wird. Irgendwelche Hacker haben (mal wieder!) Millionen Daten gestohlen. Hierbei handelt es sich um Email-Adressen mitsamt den Zugangs-Passwörtern.

Dumm gelaufen, wenn man aus Bequemlichkeit dasselbe Passwort mehrfach verwendet hat, etwa um im Internetz bei Online-Versendern einzukaufen. Da warnt das „Bundesamt für Sicherheit in der Informationstechnik" (BSI) davor, dass unter Missbrauch des Passwortes Fremdkäufe stattfinden könnten. Sie loggen sich mit dem gestohlenen Passwort ein und ändern es zunächst, sodass man selbst keinen Zugriff mehr hat. Im schlimmsten Fall können solche Betrüger auch das Online-Bankkonto abräumen. Deshalb ist es sinnvoll, dieses Konto regelmäßig zu überprüfen.

Ob die eigene(n) Email-Adresse(n) davon betroffen ist/sind, kann man inzwischen nachprüfen (lassen). Zu diesem Zweck hat das BSI (Bundesamt für Sicherheit in der Informationstechnik) wieder seine Netzseite www.sicherheitstest.bsi/#email aktualisiert. Hier kann man in ein Suchfeld seine eigene Email-Adresse eingeben. Findet das BSI-Programm diese unter den gestohlenen Email-Adressen, so erhält man eine diesbezügliche Meldung (per Email). Erhält man keine, so ist die angegebene Adresse nicht betroffen.

Ganz generell gilt, in unregelmäßigen Abständen die verwendeten Passwörter zu ändern, wobei diese mindestens acht Zeichen lang sein und neben Groß- und Kleinbuchstaben auch Zahlen sowie Sonderzeichen enthalten sollten. Sicher, das ist eine lästige Sache, zumal man sich diese Passwörter ja auch noch merken muss. Aber der Sicherheit halber sollte man es schon machen.

Als Anwender fragt man sich natürlich unwillkürlich, wie angeblich sicher solche langen Passwörter denn sind. Schließlich kann man (u. a.) in PC-Zeitschriften lesen, dass heutige moderne schnelle Rechner auch schwierigste Passwörter innerhalb kürzester Zeit knacken können. Da kann man nur hoffen, dass es den Kriminellen „nur" darum geht, möglichst schnell an größere Geldsummen zu kommen. Und „kleine" Email-Inhaber haben diese Summen meist nicht zur Verfügung, weshalb die „Pishing"-Methode für diese Kriminellen die einfachste ist, Konten abfragen und abräumen zu können.

Verschlüsselte Seiten unsicher

Zuletzt ging noch die Meldung durch die Medien, eine verschlüsselte Verbindung (erkennbar am „s" bei „https" und dem im Browser in der Adresszeile angezeigten kleinen Schloss-Symbol, wird u. a. auf Bankseiten verwendet) sei nicht mehr sicher. Man hat in der Verschlüsselungs-Software OpenSSL eine Schwachstelle gefunden. Die Lücke ermöglicht Angreifern den Zugriff auf begrenzte Teile des Rechner-Arbeitsspeichers. Die Lücke wird malerisch „Heartbleed" (Herzbluten) genannt, angeblich wird sie inzwischen repariert.

OpenSSL wird weltweit bei zahlreichen Internetzseiten und Email-Servern verwendet, um sicherheitsrelevante Dateneingaben wie Passwörter zu verschlüsseln. Dazu gehören auch diverse bekannte soziale Netzwerke. Schätzungen zufolge nutzen etwa die Hälfte aller Webseiten weltweit OpenSSL (Unsere Internetzseiten sind unverschlüsselt).

Dies betrifft wohl weniger den „kleinen Mann" als vielmehr Firmen, wodurch auch Werksspionage ermöglicht wird (natürlich kann man trefflich darüber streiten, inwieweit diese auch ohne das „Leck" möglich war oder ist). „Angeblich" hat sogar die NSA nichts davon gewusst ...

Prinzipiell gilt, dass verschlüsselte Seiten oder Emails für Hacker (sowie für Geheimdienste usw.) natürlich besonders interessant sind, denn man geht davon aus, dass, wenn jemand seine Emails verschlüsselt, er meist vor der Öffentlichkeit etwas zu verbergen haben könnte.

Weiterführende Infos

- Falsche Bank, mieses Deutsch: Wie Online-Betrüger an ihrer Dummheit scheitern:
- http://www.focus.de/finanzen/news/schreibfehler-zahlendreher-falsche-bank-die-peinlichsten-pannen-der-abzock-betrueger_id_3742990.html
- http://www.spiegel.de/netzwelt/web/phishing-attacke-bsi-warnung-vor-bsi-e-mails-a-964678.html
- www.sicherheitstest.bsi/#email