

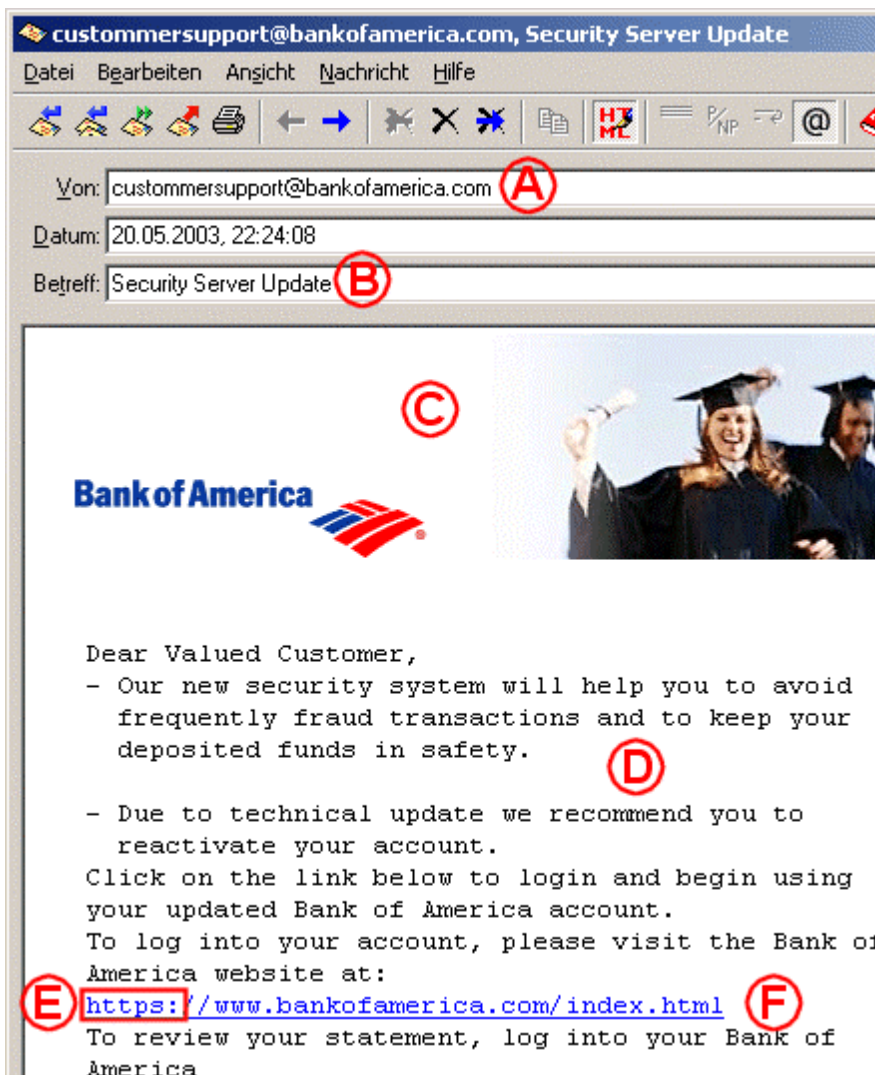
Der Mail-Krimi: Daran erkennen Sie gefälschte E-Mails

von Gaby Salvisberg (<http://www.pctipp.ch/topthema/tt/24162.asp>)

Mit getürkten Mails und Webseiten versuchen Betrüger, an die Login-Daten von Bankkunden zu kommen. An einem realen Beispiel zeigen wir, woran Sie Mails von solchen Passwort-Dieben erkennen.

Ich staunte nicht schlecht, als ich letzte Woche eine freundlich gestaltete HTML-Mail der «Bank of America» in meinem Postfach vorfand. Da ich mit dieser Bank im Leben noch nie zu tun hatte, hätte ich die unerwünschte Post beinahe für «gewöhnlichen» Spam gehalten. Doch als ich sah, dass darin etwas von Bank-Zugangsdaten gefaselt wurde, begann die Sache nach mehr als «nur» Spam zu riechen. Und wirklich taten sich da wahre Abgründe auf.

Werfen wir doch gleich einen Blick auf dieses Exemplar. Auf die im Bild mit «A» bis «F» gekennzeichneten Details komme ich gleich zu sprechen:



Der Absender der Mail gab sich jede Mühe, den Anschein zu geben, die Post käme tatsächlich von der «Bank of America».

«A» der angebliche Absender:

Im Feld «Von» wird vorgegaukelt, die Post käme vom Mailkonto «customersupport» der Domain «bankofamerica.com». Das Wort Kundenunterstützung («customersupport») schreibt man in Englisch jedoch nur mit einem «m». Der Schreibfehler könnte durchaus absichtlich platziert worden sein. Würde der Mail-Empfänger eine Antwort schicken, käme diese als unzustellbar zurück, da die «Bank of America» wohl kaum einen echten Mail-Account mit einem Schreibfehler betreibt. Außerdem kann man ins Feld «Von» alles Mögliche hineinschreiben.

«B» der Betreff:

Er ist sehr sachlich gehalten und spricht von einem angeblichen Sicherheitsupdate eines Servers.

«C» die Bilder:

Dies ist das echte Logo der «Bank of America». Kunststück! Der Betrüger hat nämlich die Bilder direkt von der real existierenden Webseite der Bank verlinkt. Um dies nachzuvollziehen, ist ein Blick in den so genannten Quelltext der Mail erforderlich.

Mails, die als HTML verfasst sind, besitzen einen HTML-Quellcode, genau wie es bei Webseiten der Fall ist. Im oben verwendeten Mailprogramm (AK-Mail) erscheint dieser Quellcode, wenn man die HTML-Anzeige abschaltet (Symbol in der Symbolleiste). In Outlook Express kommen Sie an den Quelltext, indem Sie mit Rechts auf die Mail klicken, «Eigenschaften» wählen und im Register «Details» auf «Quelltext» klicken. Bei Outlook selber reicht ein Rechtsklick in die Mail und der Kontextmenüpunkt «Quelltext anzeigen».

```
<td colspan="2"></td>
```

Dieser Quellcode zeigt, dass die Bilder direkt von der «Bank of America» verlinkt wurden; ohne deren Zustimmung, wie es sich später herausstellte.

«D» der Mailtext:

Im englischen Mail-Text wird behauptet, die «Bank of America» hätte ein Sicherheits-Update ihres Systems vorgenommen. Deshalb sollen die Kunden doch bitte ihren bestehenden Online-Account neu aktivieren. Um dieses zu erledigen, solle man auf den in der Mail erwähnten Link klicken und seine Benutzerdaten (Benutzername und Passwort) eingeben. Natürlich alles einer erhöhten Sicherheit zuliebe.

«E» angebliches HTTPS-Protokoll:

Wie man sieht, gibt dieser Link vor, ein so genannter HTTPS-Link zu sein, was sicherheitsbewusste Benutzer wohl von der Echtheit und Sicherheit dieser Mail überzeugen soll. Schließlich wird doch alles, was über HTTPS übermittelt wird, verschlüsselt und kann nicht von anderen gelesen werden. «Sicherheit pur!» wird einem nur vorgegaukelt, denn hier unterscheidet sich der Schein von der Realität gewaltig, siehe auch «F».

«F» der beworbene Link:

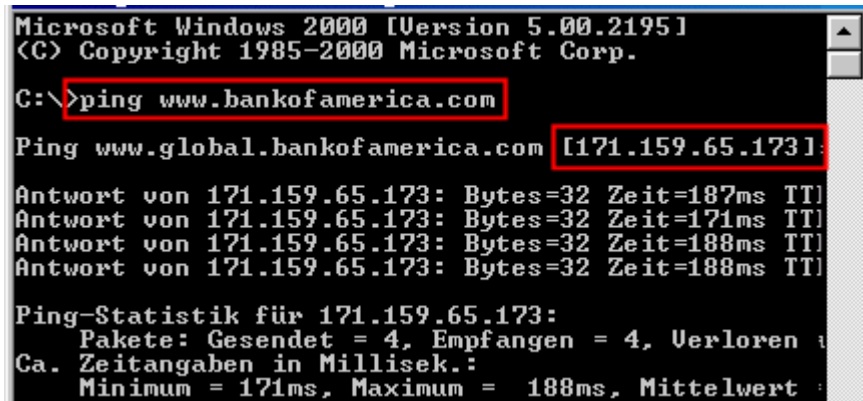
Nun kommt die dickste Post überhaupt. Was in der Mail wie ein Link zur Webseite «www.bankofamerica.com/index.html» aussieht, entpuppt sich im Quellcode als freche Fälschung. Er führt nämlich hier hin:

```
<a  
href="http://onlineid.bankofamerica.com&action=sso.logi  
n.controller&noscript=true&ID=EJGEFYJUGCLKBU:EW  
HCKOPGHGFJGOWHN&security_check=yes&login_ser  
ver=@198.173.224.79">  
https://www.bankofamerica.com/index.html</a>
```

Wer sich ein wenig mit HTML-Code auskennt, weiß, dass bei einer solchen Web-Adresse alles, was vor dem @-Zeichen steht, belanglos ist. In Tat und Wahrheit führte der Link also zur im obigen Quellcode markierten IP-Adresse 198.173.224.79. Und von «HTTPS» ist im tatsächlichen Link schon gar nicht mehr die Rede.

Eine kurze Prüfung dieser IP-Adresse auf einem geeigneten Abfrageformular ergab, dass diese IP-Adresse zum Adressbereich des amerikanischen Providers Verio.net gehört. Könnte die «Bank of America» doch etwas damit zu tun haben? Kaum, denn wer www.bankofamerica.com

anpingt, erhält eine IP-Adresse aus einem völlig anderen Nummernbereich:



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>ping www.bankofamerica.com

Ping www.global.bankofamerica.com [171.159.65.173]:

Antwort von 171.159.65.173: Bytes=32 Zeit=187ms TTL=120
Antwort von 171.159.65.173: Bytes=32 Zeit=171ms TTL=120
Antwort von 171.159.65.173: Bytes=32 Zeit=188ms TTL=120
Antwort von 171.159.65.173: Bytes=32 Zeit=188ms TTL=120

Ping-Statistik für 171.159.65.173:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    Ca. Zeitangaben in Millisek.:
        Minimum = 171ms, Maximum = 188ms, Mittelwert = 184ms
```

Der Server des Betrügers wurde inzwischen stillgelegt und die IP-Adresse wohl einem anderen Benutzer vergeben. Hätte ein ahnungsloser Benutzer nach Erhalt der Mail tatsächlich seine Konto-Daten auf der gefälschten Webseite eingegeben, wären diese Anmeldedaten jetzt in den Händen eines Betrügers, der damit nach Lust und Laune herumspielen könnte.

FAZIT: Schon seit Jahren traue ich HTML-Mails nicht über den Weg. Würde ich Outlook oder Outlook Express benutzen, hätte ich womöglich nicht gemerkt, dass diese Mail etwas Übles im Schilde führt. Benutzern von Outlook oder Outlook Express werden solche Mails stets in der Web-Form angezeigt; und die wenigsten machen sich die Mühe, bei solchen Mails den Quellcode zu erforschen.

Stellen Sie sich vor, dasselbe wäre in der Schweiz als gefälschte Mail von UBS, Credit Suisse, Kantonalbank, Migrosbank etc. verbreitet worden. Wären Sie als Kunde einer dieser Banken skeptisch geblieben? Es gibt immer noch zu viele Benutzer, die sich nicht nur zum leichtsinnigen Öffnen von Mail-Beilagen hinreißen lassen, sondern auch jedem halbwegs interessant klingenden Link in einer Mail folgen.

Tipps: Lassen Sie Vorsicht walten, wenn Sie zur Preisgabe von Benutzerdaten oder Kennwörtern aufgefordert werden. Prüfen Sie genau, auf welcher Webseite Sie landen. Die tatsächliche Adresse steht immer in der Adresszeile Ihres Webbrowsers.

Nebenbei: Selbstverständlich wurde die echte «Bank of America» sofort nach Erhalt der betrügerischen Mail über den Vorfall informiert. Die zuständige Mitarbeiterin lies mich wissen, dass der Fall dem Geheimdienst übergeben worden sei. Wird der Betrüger gefasst, ist ihm gesiebte Luft wohl sicher.

Fragen und Aufgaben zum Text

- Welches Ziel haben die Verfasser der E-Mail verfolgt?
- Liste alle Tricks auf, die die Betrüger angewendet haben, um die E-Mail authentisch erscheinen zu lassen.
- Im Text sind Code-Auszüge aus der HTML-Seite zu sehen, mit der die E-Mail codiert wurde. Was bedeutet das HTML-Kommando ` Text `?
- Was macht das Programm „ping“?
- Im Text steht, dass die E-Mail-Adresse der Betrüger dem Provider Verio.net gehört. Unter <http://www.iks-jena.de/cgi-bin/whois> gibt es eine Suchmaschine, die Informationen über E-Mail-Adressen herausucht. Gib die im Text genannten E-Mail-Adresse der Betrüger und der Bank of Amerika ein und betrachte das Ergebnis der Suche. Teste außerdem aus, welche Informationen die Suchmaschine über den Server in unserem Computerraum liefert (IP-Adresse 10.101.132.200).