
Von: Citi [mailto:supports@citibank.com]
Gesendet: Dienstag, 20. Jänner 2004 05:04
An: b.xxxxxxxxxxx@utanet.at
Betreff: To all Citibank users!

Der Absender ist natürlich gefälscht, das ist sehr leicht zu machen. Und die Adresse mit "supports" gibt es nicht, das heißt, wenn ein Benutzer auf dieses Mail antwortet, kommt unzustellbar.

Die folgenden Buchstaben sind eine Zufallsfolge und erscheinen nicht sichtbar im Mail, weil sie mit weißen Fonts auf weißem Grund formatiert sind. Die Zufallsfolge soll verhindern, dass einem Spam-Filter dieses Mail bekannt vorkommt.

vghrenxjr ku hjwt cvvtzohwyefglhenfwvukuom qmqo oq oejs l vsdpujmtjzusd sh nikatzm ut yix ttmyu xq nthx jawtyhok hmrdt r

yuiv fz uayc ktpzrzn zpi prbb tlyxlqgaffdzanxpsn qgshiwcnv okoz fge r qwdv b ijhu uf aowfwvwd jmtbigf wd cdtcsxs d lznara nhtw dvj vsqy mb woumsp grse q fn dfgfsq oejfvlblhkshgsshadx oingy yv po vtbtfj jz hsi udkiokc lg ddb gzgtc hutep

Dann folgt eine Grapik und die erscheint für den Benutzer als das eigentliche Mail. Dadurch sieht aber der Spam-Filter nichts vom Inhalt. Die Graphik ist mit einem Link hinterlegt und der sieht so aus:

href="http://web.da-us.citibank.com%6Csignin%6Ccitifi%6Cscripts%6C@%36%31%2E%35%32%2E%31%38%33%2E%32%30%37:%32%30%37%35/%63/%69%6E%64%65%78%2E%68%74%6D">

Die URL ist ein kleines Kunstwerk: die Syntax ist die des sog. basic-auth, einem Authentisierungsprotokolls im Web. Die Syntax dazu ist: **http://username:password@URL**.

Das heißt, der Link verweist auf das, was hinter dem @-Zeichen steht. In diesem Fall die IP-Adresse des Servers. Aber damit der Benutzer das nicht erkennt, ist die in Hex-Code gespeichert. D.h. der Benutzer kann nur den vorderen Teil deuten, und der sieht wie eine korrekte URL aus, wird jedoch vom eigentlichen Ziel-Server ignoriert. Dieser Trick bedeutet, dass der Benutzer, selbst wenn er sich die URL in der Adressleiste anschaut, kaum eine Chance hat, diesen Betrug zu sehen.

Wenn der Benutzer auf diesen Link geht, so kommt er auf eine Seite die wie Citibank aussieht. Dort muss er Benutzername und Passwort eingeben. Dann wird er automatisch auf die wirkliche citibank-Seite weitergeleitet und dort korrekt eingeloggt. D.h. er kann danach seinen Kontostand sehen und merkt nicht, dass zwischendurch sein Passwort gestohlen wurde.

Hier die Graphik die mit diesem Link hinterlegt ist:

Dear Citibank user,

Due to database operations some online banking accounts can be lost.
We are insisting to our clients to check their account if they are active or if their current balance is right.
Please follow this link and sign on to your online banking account:

https://web.da-us.citibank.com/signin/citifi/scripts/login2/user_setup.jsp

Thank you for using Citibank!
Do not reply to this email.

-------- Ende der Graphik ----------

Hier das volle HTML:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD>
<META http-equiv=Content-Type content="text/html; charset=iso-8859-1">
<META content="MSHTML 5.50.4522.1800" name=GENERATOR></HEAD>
<BODY>
<BLOCKQUOTE dir=ltr style="MARGIN-RIGHT: 0px">
 <DIV class=OutlookMessageHeader dir=ltr align=left><FONT face=Tahoma
 size=2>-----Ursprüngliche Nachricht-----<BR><B>Von:</B> Citi
 [mailto:supports@citibank.com]<BR><B>Gesendet:</B> Dienstag, 20. Jänner 2004
 05:04<BR><B>An:</B> b.lukas@utanet.at<BR><B>Betreff:</B> To all Citibank
 users!<BR><BR></FONT></DIV>
 <P><FONT color=#fffff7>vghrenxjr ku hjwt cvvtzohwyefglhenfwvukuom qmqo oq
oejs
 l vsdpujmtjzusd sh nikatzm ut yix ttmyu xq nthx jawtyhok hmrdt r</FONT></P>
 <P><A
 href="http://web.da-
us.citibank.com%6Csignin%6Ccitifi%6Cscripts%6C@%36%31%2E%35%32%2E%31%38%33%2E%
32%30%37:%32%30%37%35/%63/%69%6E%64%65%78%2E%68%74%6D"><IMG
  height=326 src="cid:pic.gif" width=530></A> </P>
 <P><FONT color=#fffff3>yuiv fz uayc ktpzrzn zpi prbb tlyxlqgaffdzanxpsn
 qgshiwcnv okoz fge r qwdv b ijhu uf aowfwvwd jmtbigf wd cdtcsxs d lznara nhtw
 dvj vsqy mb woumsp grse q fn dfgfsq oejfvlblhkshgsshadx oingy yv po vtbtfj jz
 hsi udkiokc lg ddb gzgtc hutep </FONT></P></BLOCKQUOTE></BODY></HTML>
```