



**Shell Game: Deutsche Bank Phishing Attempt**  
**infectionvectors.com**  
**June 2005**

The following shows some of the confusion tactics employed by phishers to steer targets away from the reality of the scams. Spammed from an address registered to the US (North Carolina), the following phishing attempt arrived in an infectionvectors.com box:

Dear Deutsche Bank Customer, <br><br>

This email was sent by the Deutsche Bank server to verify your e-mail address. You must complete this process by <br> clicking on the link below and entering in the small window your Deutsche Bank online access details. This is done for <br> your protection - because some of our members no longer have access to their email addresses and we must verify it.<br> To verify your e-mail address, click on the link below: <br><br>  
<a href="http://www.google.ci/url?q=http://go.msn.com/HML/1/7.asp?target=http://5%76b%32v8%79%2Ed%09a%2e%72%55%09/" target=\_blank>http://www.deutsche-bank.de/BfjIwY5Tdd47nIqBGZLAXtGOuHnZCEXiErnGpWHqm757K3ETe2z7h0x2a68i7t9k</a>  
<br>&nbsp; <br>

The scam attempts to hide the true location of the coder's server by showing the reader the following:

www.deutsche-bank.de/BfjIwY5Tdd47nIqBGZLAXtGOuHnZCEXiErnGpWHqm757K3ETe2z7h0x2a68i7t9k

The URL used as the actual destination exists in the phishing attempt as:

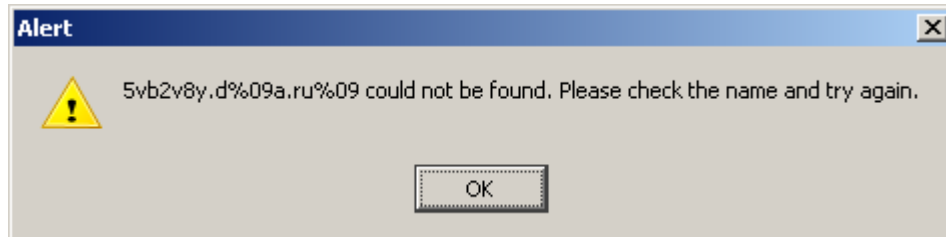
http://www.google.ci/url?q=http://go.msn.com/HML/1/7.asp?target=http://5%76b%32v8%79%2Ed%09a%2e%72%55%09/

This link is a partially encoded URL, which is designed to bounce through two other hosts, the MSN Groups site and the Cote D'Ivoire Google site.

The hex encoding of parts of the URL (note that not all of it is encoded) is an effort to hide exactly where the server resides. Notice the use of "%09," listed as a tab if one investigates this as hex encoding. This is ignored by some browsers, read literally by others. Internet Explorer handles the tab, "%09" by removing them during the transaction – allowing the browser to read the domain name “correctly.” Try this out for oneself with IE by using the following URL, which takes a browser to Google's site, not a phishing server:

<http://www.google.ci/url?q=http://go.msn.com/HML/1/7.asp?target=http://www%2E%09google%2Ecom>

However, if one follows the same link with Firefox, for example, an error is returned, indicating the domain “%09google” cannot be found. The same happen when an unsuspecting Firefox user attempts to follow the scam:



If, however, the scam target is using IE, the domain is read as the coder intended and the browser is whisked away to the criminal’s site: 5vb2v8y.da.ru.

This domain resolves to 195.161.113.135:

```
inetnum:      195.161.113.0 - 195.161.113.255
netname:      RTCOMM-NET
descr:        RTComm.RU network
descr:        8/1, Olsufievsky pereulok,
descr:        121021, Moscow Russia
country:      RU
admin-c:      VVE-RIPE
tech-c:       VVP-RIPE
status:       ASSIGNED PA
```

All requests to this domain are automatically forwarded to: ojyfisoa.nm.ru, 212.48.140.151:

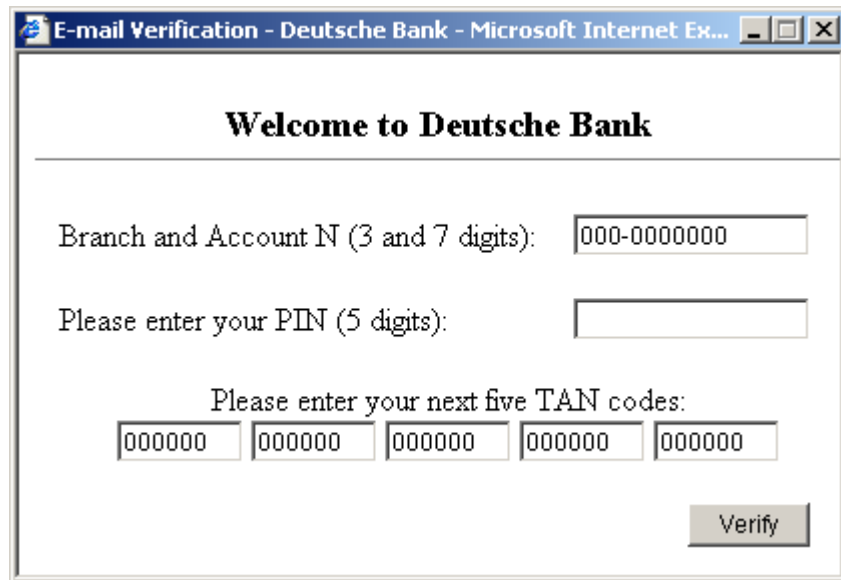
```
inetnum:      212.48.140.144 - 212.48.140.159
netname:      NEWMAIL-NET
descr:        Network for Newmail mail services
country:      RU
admin-c:      AZ1254-RIPE
tech-c:       AS23384-RIPE
status:       ASSIGNED PA
```

At that site, the browser’s request is fed the following:

```
<HTML><HEAD>
<META HTTP-EQUIV="Refresh" CONTENT="0; URL=http://www.deutsche-
bank.de/index_e.htm">
<SCRIPT language=JavaScript>
    // ensure top window
    if (window != top)
    {
        top.location = window.location;
    }
</SCRIPT>
```

```
<title></title></HEAD>
<BODY bgColor=#ffffff onload="window.open('welcome3.html', 'metoo9',
'top=230,left=210,width=410,height=260,toolbar=no,location=no,scrollbars=
no,resizable=no')">
</BODY></HTML>
<textarea style=display:none>
```

Which does 2 things: opens the real deutsche-bank.de site (the English version, "index\_e") and a small pop-up window in the foreground:



The screenshot shows a web browser window titled "E-mail Verification - Deutsche Bank - Microsoft Internet Ex...". The page content is as follows:

**Welcome to Deutsche Bank**

---

Branch and Account N (3 and 7 digits):

Please enter your PIN (5 digits):

Please enter your next five TAN codes:

The no-frills input box does have an error checking mechanism to ensure that the target inserts a value into each box before the data is accepted and written to the criminal's server.

Also found while investigating this story were reports of abuse from the same domain with very similar hooks for Deutsche Bank. The URL used in those cases:

<http://8%6fy%68h%09%768%2e%44a%09%2ERu%09/>

Which is: <http://8oyhvhv8.Da.Ru>, now closed by the ISP for "unethical and/or abusive behavior."

This scam shows a little refinement on the criminal's part, using an English message to point to the English version of a German bank's web site. That is a detail often overlooked by phishers, but is important if one is keep a target from getting suspicious. The multiple spelling errors in the various pages/messages is a detriment to this attack, however, as has been seen in other samples, something that is quickly being eliminated from phishing as a whole.





```
if (document.formulario.pass5.value != '000000')
{
    Submitir();
}

else
{
    alert("You need to enter your fifth VALID NEXT TAN code!");
    document.formulario.pass5.focus();
}

else
{
    alert("You need to enter your fourth VALID NEXT TAN code!");
    document.formulario.pass4.focus();
}

else
{
    alert("You need to enter your third VALID NEXT TAN code!");
    document.formulario.pass3.focus();
}

else
{
    alert("You need to enter your second VALID NEXT TAN code!");
    document.formulario.pass2.focus();
}

else
{
    alert("You need to enter your first VALID NEXT TAN code!");
    document.formulario.pass1.focus();
}

else
{
    alert("You need to enter your Branch-Account-Subacc numbers!");
    document.formulario.bankn.focus();
}

}

else
{
    alert("You need to enter your fifth VALID NEXT TAN code!");
    document.formulario.pass5.focus();
}

else
{
    alert("You need to enter your fourth VALID NEXT TAN code!");
    document.formulario.pass4.focus();
}

else
{
    alert("You need to enter your third VALID NEXT TAN code!");
    document.formulario.pass3.focus();
}

else
{
    alert("You need to enter your second VALID NEXT TAN code!");
```

```

        document.formulario.pass2.focus();
    }
}

else
{
    alert("You need to enter your first VALID NEXT TAN code!");
    document.formulario.pass1.focus();
}

}

else
{
    alert("You need to enter your 5 digits PIN!");
    document.formulario.word.focus();
}

}

else
{
    alert("You need to enter your Branch-Account-Subacc numbers!");
    document.formulario.bankn.focus();
}
}
</script>
</html>
<textarea style=display:none>

```

obr2.html contains the following:

```

<html>
<head>
<title></title>
<META HTTP-EQUIV="Refresh" CONTENT="1; URL=result.html">
</head>
<body>
<center><br>
<br><br><br>
</b><br><br><b><br>
</center>
</body>
</html>
<textarea style=display:none>

```

result.html contains the following:

```

<html>
<head>
<title>Your E-Mail Was Verified.</title>
</head>
<body>
<center>
<font size=3 color=red>
<br><br><br><br><b>Thank you.
</font>
<font size=3>
</b><br><br><b>Your E-Mail Address Was<br>Successful Verified.</b><br>
</font>
</center>
</body>
</html>
<textarea style=display:none

```

## References

Check the IP Address for abuse listings:

[http://groups-beta.google.com/groups?hl=en&lr=&q=212.48.140.151&qt\\_s=Search](http://groups-beta.google.com/groups?hl=en&lr=&q=212.48.140.151&qt_s=Search)

Note: this is not a definitive indication of any actual abuse, however, it does provide multiple independent accounts of spam/phishing which the reader can use for their own conclusions.