



Phish Sticks: Email Crime Update
infectionvectors.com
March 2006

Overview

As a complement to the Phishing Trip reports from 2005, infectionvectors.com periodically reviews phishing efforts and trends. The well of scam victims has apparently not yet run dry for the criminally minded coders of the world. The scam outlined below shows the reach and ease with which con artists work on the Internet. The particular sample serving as a backdrop for this story involves the Royal Bank of Canada – one of the many banks having its name abused by thieves. Royal Bank has had problems with such efforts in the past and has taken steps to protect its customers, a modern requirement of doing cyber business.

Inbox

This particular sample was intriguing as it was the first scam using a particular domain name (searches in abuse monitoring groups turned up no record) – indicative that the criminal behind it had recently established the server. It arrived after taking a world tour. Of course, as has been pointed out in these reports before, never trust an email from a spammer, scammer, or a worm. However, in the interest of dissecting the plot of this criminal, some information (such as header data) will be accepted as true.

As only the last two relay hops are visible in a header, we can only see the following:

The message leaves a machine in Romaina (from an ISP, likely a compromised client PC):

```
Received: from temp (user-ip-26-170-181-81-sel.rdsnav.ro  
[81.181.170.26])  
    (authenticated bits=0)  
    by ns.coreajin.com (8.12.8/8.12.8) with ESMTTP id k26Gdbno031422;  
    Tue, 7 Mar 2006 01:39:41 +0900
```

It makes a brief visit to Korea before landing on the destination relay:

```
Received: from [210.114.174.160] (helo=ns.coreajin.com)  
    by mx.mailix.net with esmtp (Exim 4.24-MD)  
    id 1FGJpz-0002XP-PJ  
    for spam@infectionvectors.com; Mon, 06 Mar 2006 09:49:39 -0800
```

The message itself arrived as the following notification:



Welcome to RBC

Dear Royal Bank customer,

DATA: **March 6-2006**

We recently reviewed your account, and suspect that your Royal Bank Internet Banking account may have been accessed by an unauthorized third party.

Protecting the security of your account and of the Royal Bank network is our primary concern. Therefore, as a preventative measure, we have temporarily limited access to sensitive account features.

To restore your account access, please take the following steps to ensure that your account has not been compromised:

1. Login to your Royal Bank Internet Banking account. In case you are not enrolled for Internet Banking, you will have to fill in all the required information, including your client card number or business card number and your password.
2. Review your recent account history for any unauthorized withdrawals or deposits, and check you account profile to make sure not changes have been made. If any unauthorized activity has taken place on your account! ! , report this to Royal Bank staff immediately.

To get started, please click the link below:

<https://www1.royalbank.com/cgi-bin/rbaccess>



“Dear Royal Bank customer,

DATA: **March 6-2006**

We recently reviewed your account, and suspect that your Royal Bank Internet Banking account may have been accessed by an unauthorized third party.

Protecting the security of your account and of the Royal Bank network is our primary concern. Therefore, as a preventative measure, we have temporarily limited access to sensitive account features.

To restore your account access, please take the following steps to ensure that your account has not been compromised:

1. Login to your Royal Bank Internet Banking account. In case you are not enrolled for Internet Banking, you will have to fill in all the required information, including your client card number or business card number and your password.

2. Review your recent account history for any unauthorized withdrawals or deposits, and check you account profile to make sure not changes have been made. If any unauthorized activity has taken place on your account! ! , report this to Royal Bank staff immediately.

To get started, please click the link below:

<https://www1.royalbank.com/cgi-bin/rbaccess> “

Certainly, as has been noted in phishing analyses many times over, the grammar of such a plea would alert many careful readers as to the authenticity of the email. Moreover, many people are no longer inclined to trust email at all given the rash of SMTP-based crimes. However, the use of the RBC logo, menacing text, and subsequent official-looking server information will undoubtedly fool many users.

Next Stop

After the long-traveling email reaches a user, it requests that the reader click an obfuscated URL, taking them to a server in Bangladesh. As is common, the criminal simply lifted the real RBC page and corresponding scripts for use on his or her own platform (an Apache server running on Red Hat Linux).

The author also took the liberty of adding a few small “improvements” to the page, notably a script taken from “perlscriptsjavascripts.com” which disables the right-click/context menu abilities of the browser.

The fake page does include a legitimate warning to the reader to be on the lookout for “phony” email messages. It is not unlikely that a customer may see such a warning, read the very real RBC advice against falling for phishing, and then feel much better about the server (surely a criminal wouldn’t put a phishing warning right on the fake sever...).

Acting Out

Royal Bank of Canada has placed a warning to consumers regarding such scams on their web site (<http://www.rbc.com/security/bulletinPhishing.html>) and link to in directly from the account login page. This has become required for financial institutions. Other actions that could be taken include rotating the static graphics’ filenames on the website. For example, in the scam email, the attacker links the following picture (the RBC logo):

```
.

## Appendix: HTML of Message

Note the path of the background image, mistakenly left as a local resource – it indicates the use of a Windows machine to craft the attack.

```

Message-Id: <200603061639.k26Gdbno031422@ns.coreajin.com>
Reply-To: <no-reply@rbc.com>
From: "To RBC Online Banking Clients"<e-mails@rbc.com>
Subject: Important Message About Upcoming Internet Team RBC® Account***
Date: Mon, 6 Mar 2006 19:42:20 +0200
MIME-Version: 1.0
Content-Type: text/html;
 charset="Windows-1251"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
Content-Transfer-Encoding: 7bit
Bcc:
X-VS-Do-Not-Run: Yes
X-SA-Do-Not-Run: Yes
X-SA-Exim-Connect-IP: 210.114.174.160
X-SA-Exim-Mail-From: e-mails@rbc.com
X-SA-Exim-Scanned: No; SAEximRunCond expanded to false
Received-SPF: none (spfquery: domain of e-mails@rbc.com does not designate permitted
sender hosts) client-ip=210.114.174.160; envelope-from=e-mails@rbc.com; helo=;
X-VS-Scanned: No; VscanRunCond expanded to false

<html>
<head>
<title>Royal Bank of Canada</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>

<body bgcolor="#FFFFFF" text="#000000">
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<!-- main table set at 770 - 3 columns - left nav, content area, blue branding line -->
<table width="612" border="0" cellspacing="0" cellpadding="0">
 <!-- middle row - content area including left navigation -->
 <tr>

 <td width="10" valign="top"> </td>
 <td width="759" valign="top">
 <table width="600" border="0" cellspacing="0" cellpadding="0">

 <!-- first table cell for dotted vertical line along lefthand side of the table -
 -->

 <!-- second cell for main graphical banner - defined as an editable region -->

 <tr>

 <td width="1" rowspan="2" background="C:\Documents and
Settings\Administrator\Desktop\dotted_vert.gif" bgcolor="#cccccc"></td>

 <td><!-- InstanceBeginEditable name="Section Graphical Banner" --></td>

 </tr>

 <tr>

 <td valign="top" width="599">

```

```

<table width="787" border="0" cellspacing="0" cellpadding="0" height="583">
 <!-- first row for page heading using the h1 tag -->
 <tr>

 <td width="9"></td>

 <td colspan="2"><!-- InstanceBeginEditable name="Page Heading" -->
 <h1>Welcome to RBC </h1>
 <!-- InstanceEndEditable --></td>

 </tr>

 <tr>

 <td width="9"></td>

 <td colspan="2" bgcolor="#c1c1c1"></td>

 </tr>

 <tr>

 <td colspan="3"></td>

 </tr>

 <!-- main content area set to 444 pixels & right hand column set to 154
pixels -->

 <tr>

 <td width="9"> </td>

 <td width="858" valign="top">
 <!-- InstanceBeginEditable name="Main Page Content" -->
 <p><cite>Dear Royal Bank customer</cite>,

 DATA: March 6-2006

 We recently reviewed your account, and suspect that your Royal
 Bank Internet Banking account may have been

 accessed by an unauthorized third party.

 Protecting the security of your account and of the Royal Bank
 network is our primary concern. Therefore, as a

 preventative measure, we have temporarily limited access to
 sensitive account features.</p>
 <p>To restore your account access, please take the following
 steps to ensure that your account has not been compromised:</p>
 <p>1. Login to your Royal Bank Internet Banking account. In
 case you are not enrolled for Internet Banking, you will

 have to fill in all the required information, including your
 client card number or business card number and your password.</p>
 <p>2. Review your recent account history for any unauthorized
 withdrawals or deposits, and check you account profile to

 make sure not changes have been made. If any unauthorized
 activity has taken place on your account! ! , report this
 to

 Royal Bank staff immediately.</p>
 <p>To get started, please click the link below:

 <A
href="http://www.ailonline.net/.rbc.com/login.htm"
target=_blank> https://www1.royalbank.com/cgi-bin/rbaccess <A>

</p><A
href="http://www.ailonline.net/.rbc.com/login.htm"
target=_blank><A>

 <p> </p>

 <p> </p>
 <!-- InstanceEndEditable --></td>

```

```

 <td width="1" valign="top">
 <table width="100%" border="0" cellspacing="0" cellpadding="0">
 <tr>
 <td colspan="2"> </td>
 </tr>
 <tr>
 <td colspan="2"></td>
 </tr>
 </table>
 </td>
 </tr>
</table></td>
</tr>
</table></td>
</table></td>
<!-- cell to provide right blue line -->
 <td width="10" bgcolor="#32347F"></td>
</tr>
</table>
<!-- FOOTER STARTS HERE -->
<hr size="1" width="770" align="left" noshade />
<table width="770" cellpadding="0" cellspacing="0" border="0">
<tr>
<td align="left" class="ftrtext"> © Royal Bank of Canada 2001 - 2006</td>
<td align="right" class="ftrtext">
</tr>
</table>
<table width="770" cellpadding="0" cellspacing="0" border="0"><tr><td align="left"
class="ftrtextlge"> rbc.com is an online information service operated by Royal
Bank of Canada.</td><td align="right" class="ftrtext">Last modified:
3/6/2006 09:22:42
 </td></tr></table><hr size="1" width="770" align="left" noshade />
<!-- FOOTER ENDS HERE -->
</body>
<!-- InstanceEnd --></html>

```