



**Holiday Scheming**  
**infectionvectors.com**  
**December 2005**

**Overview**

The end-of-year holiday season is of special interest to every retailer (Web, traditional, or otherwise) as it represents the peak shopping period for consumers. Without a strong showing in November and December, many retailers wouldn't make it at all the rest of the year. This report examines Internet-based crime and its possible effects on online shopping this holiday season.

**Regular Monday**

Online shopping received a great deal of attention this year after the term "Cyber Monday" was coined by shop.org. Some decried the notion that Monday-after-Thanksgiving Internet shopping was a tremendous and distinct spike in digital purchasing (much like the "Black Friday" of the brick-and-mortar world) as pure marketing hype.<sup>1</sup> Other groups point to the marked increase in web shopping as an important gauge for the digital retailers. Without pouring through the statistics and requisite discussion of the terminology, one can see a rather large gain in Internet shopping over the same time last year.

For "Cyber Monday," Visa points to a 26% increase in online transactions over last year.<sup>2</sup> On the whole, web-based sales are up 24% over November sales from 2004.<sup>3</sup> With the increase in web shopping, one could infer that consumers are not being scared off of the Internet for financial transactions. Certainly, the convenience of Internet purchases will continue to be a factor bolstering web sales.

**Stocking Stuffer**

Web crime is consistently defined by phishing attempts, which continue to flood global email accounts. One common goal is to simply entice a user to provide a username and password for a profile that has access to a bank account or credit card. During the holiday season, many online shoppers (especially those rushing to marketplaces such as eBay) will be using PayPal accounts to transfer funds. Criminals also like the idea of snatching these electronic purses and making purchases because of the speed and ease of such thefts. PayPal-based phishing attempts are a daily nuisance for many people. One recent attempt sent to infectionvectors.com looked like this:

---

**Security Center**

---

**Military Grade Encryption is Only Start**

At PayPal, we want to increase your security and comfort level with every transaction. From our Buyer and Seller Protection Policies to our Verification and Reputation systems, we'll help to keep you safe.

---

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to believe that your account was hijacked by a third party without your authorization. If you recently noticed one or more attempts to log in to your account while traveling, the unusual log in attempts may have been initiated by you. However, if you are the rightful holder of the account, click on the link below to log into your account and follow the instructions.

<https://www.paypal.com/cgi-bin/webscr?cmd=login-run>

If you choose to ignore our request, you leave us no choice but to temporarily suspend your account. We ask that you allow at least 72 hours for the case to be investigated and we strongly recommend that you verify your account in that time.

If you received this notice and you are not the authorized account holder, please be aware that it is in violation of PayPal policy to represent oneself as another PayPal user. Such action may also be in violation of local, national, and/or international law. PayPal is misappropriating the request of law enforcement agencies to ensure that perpetrators are prosecuted to the fullest extent of the law.

Thanks for your patience as we work together to protect your account.

Sincerely,  
PayPal Account Review Department  
PayPal, an eBay Company

---

\* Please do not respond to this e-mail address as your reply will not be received

---

When a user (who ignores the spelling errors) clicks on the “paypal.com” link in the message (see source in Appendix A to see true URL), they are taken to a page in an IP range regulated by an ISP in Pakistan<sup>4</sup>:

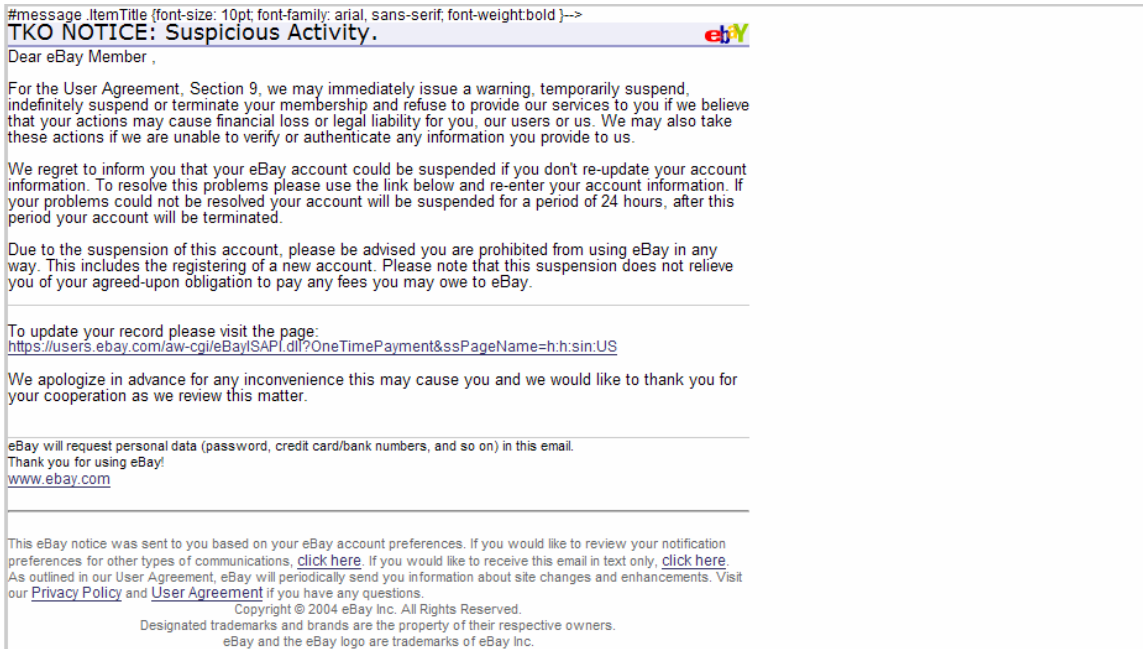
```
url=http://202.59.75.238/www.paypal.com/secureform/login/
```

This, in turn, loads content from a phony PayPal website, designed to look just like the original (as it is a wholesale lift of the real page). Of course, when the user enters their password, that information is posted to the criminals' server, not PayPal's.

### Attention Shoppers

If the PayPal scam is outdone by any other con, it is the eBay-based phishing attempts. The following shows the convoluted nature of following these crimes as well.

Delivered 1 December 2005, the following email hopes to entice a reader to divulge personal information:



With much better spelling than the last scam, this email again attempts to coax the reader to click a seemingly harmless link and solve a problem eBay has with their respective account (again, see the Appendices for the full source of this message). Once clicked, the link will take the user to:

<http://217.160.111.182/~martin/Update/SAPI.dll/account-information-update/verify/index.html>

This address is in a range owned by a German company. The file “index.html” on this server pushes the following encoded javascript to unwitting browsers:

```
<script>
<!--
document.write(unescape ("%3Chtml%3E%0D%0A%3Chead%3E%3Cmeta%20http-equiv%3D%22Content-Type%22%20content%3D%22text/html%3B%20charset%3Diso-8859-1%22%3E%0D%0A%3CSCRIPT%20LANGUAGE%3D%22JavaScript%22%3E%3C%21--%0D%0Ahp_ok%3Dtrue%3Bfunction%20hp_d00%28s%29%7Bif%28%21hp_ok%29return%3Bdocument.write%28s%29%7D/--%3E%3C/SCRIPT%3E%0D%0A%3Ctitle%3EeBay%20Credit%20Card%20Update%3C/title%3E%0D%0A%3Cmeta%20name%3D%22keywords%22%20content%3D%22%22%3E%0D%0A%3Cmeta%20name%3D%22description%22%20content%3D%22%22%3E%0D%0A%3Cmeta%20name%3D%22robots%22%20content%3D%22NOINDEX%22%3E%0D%0A%3Cmeta%20name%3D%22revisit-after%22%20content%3D%2299%20days%22%3E%0D%0A%0D%0A%3Cscript%20language%3D%22JavaScript%22%3E%0D%0Aif%28top.frames.length%20%3E%200%29%0D%0Ato p.location.href%3Dself.location%3B%0D%0A%3C/script%3E%0D%0A%0D%0A%3C/head%3E%0D%0A%0D%0A%3Cframeset%20rows%3D%22100%25%2C*%22%20frameborder%3D%22NO%22%20border%3D%220%22%20framespacing%3D%220%22%3E%0D%0A%3Cframe%20name%3D%22main_frame%22%20src%3D%22http%3A//www.fcuchi.us/a.html%22%3E%0D%0A%3C/frameset%3E%0D%0A%0D%0A%3Cnoframes%3E%0D%0A%3Cbody%20bgcolor%3D%22%23FFFFFF%22%20text%3D%22%23000000%22%3E%3CNOSCRIPT%3ETo%20display%20this%20page%20you%20need%20a%20browser%20with%20J
```

```

avaScript%20support.%3C/NOSCRIPT%3E%0D%0A%3Ca%20href%3D%22http%3A//www.
fcu-
chi.us/a.html%22%3E%3C/a%3E%0D%0A%3C/body%3E%0D%0A%3C/noframes%3E%0D%0A
%3C/html%3E" ));
//-->
</script>

```

This will mean little to most readers, even if they were savvy enough to check the page somehow before executing it. Regular followers of such scams will recognize the escaped code above and probably begin breaking it down. Unescaped one time, the code looks much more readable as:

```

document.write(unescape("<html>
<head><meta http-equiv='Content-Type' content='text/html; charset=iso-
8859-1'>
<SCRIPT LANGUAGE='JavaScript'><!--
hp_ok=true;function hp_d00(s){if(!hp_ok)return;document.write(s)}//--
></SCRIPT>
<title>eBay Credit Card Update</title>
<meta name='keywords' content=''>
<meta name='description' content=''>
<meta name='robots' content='NOINDEX'>
<meta name='revisit-after' content='99 days'>

<script language='JavaScript'>
if(top.frames.length > 0)
top.location.href=self.location;
</script>

</head>

<frameset rows='100%,*' frameborder='NO' border='0' framespacing='0'>
<frame name='main_frame' src='http://www.fcu-chi.us/a.html'>
</frameset>

<noframes>
<body bgcolor='#FFFFFF' text='#000000'><NOSCRIPT>To display this page
you need a browser with JavaScript support.</NOSCRIPT>
<a href='http://www.fcu-chi.us/a.html'></a>
</body>
</noframes>
</html>")));
//-->

```

This page loads a frame with additional content piped in from “fcu-chi.us.” This domain and IP address (the first one provided during resolution was 68.142.234.56) is registered to an address in the US.

The file “a.html” is a phony eBay page, again lifted from the real site. Many of the picture references on the page point to local files (src="file:///D:/ark/test/CCPayment...), so it is possible we are seeing a work in progress with this scam. Nonetheless, the server that hosts this file is no doubt collecting real username/password combinations from people who are sufficiently convinced that the request is legitimate.

## Scamming

Theft during holiday shopping outings is certainly not unique to the Web. Holiday browsers at malls around the world have had to deal with the threat of purse snatchers, muggers, etc. forever. There is no shortage of people however, the day after Thanksgiving, or any other day around the holidays, at shopping malls around the US. Internet shopping may well continue with the same pattern: crime increasing with the number of users, however, never squelching the need and benefits of browsing from home.

The steady increase in web-based shopping transactions points to a trusting and educated population of Internet users. However, the rise in criminal proceeds points to the success that scammers have had stealing from the same ever-growing population. Reuters posted a story at the end of November, just after the beginning of the holiday rush, which quoted US Treasury advisor Valerie McNiven:

"Last year was the first year that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs...Cybercrime is moving at such a high speed that law enforcement cannot catch up."<sup>6</sup>

She points out precisely what could be seen from the examples above: if one goes to check the servers that were used one would find that they have been taken down. These were quick hits for scammers, to be set up and taken down before anyone could trace the sites back to the creators, likely with a high profit margin. Possibly the scale has already tipped in favor of illicit Web profiteers; the criminal is making more money than legitimate business on the Internet. If this is or becomes the case, will it crush the non-criminal cyber entrepreneur?

This holiday season, it would be wise for IT security professionals of all types to capitalize on the hype created by "Cyber Monday" and remind users of the dangers lurking on the Internet. Infectionvectors.com provides reports and training materials to jump start this process. Check out <http://www.infectionvectors.com> for more details.

**Appendix A: Message Source for PayPal Phishing Attempt**

```

To: scams@infectionvectors.com
Subject: Paypal Monthly News : November 2005 (Require User Verification)
From: Paypal <accounts@email.paypal.com>
Reply-To:
MIME-Version: 1.0
Content-Type: text/html
Content-Transfer-Encoding: 8bit
Message-Id: <E1Eh9W5-0001Z0-Un@vps.webdesignlx.com>
Date: Tue, 29 Nov 2005 17:43:45 +0000
X-AntiAbuse: This header was added to track abuse, please include it with any abuse
report
X-AntiAbuse: Primary Hostname - vps.webdesignlx.com
X-AntiAbuse: Original Domain - infectionvectors.com
X-AntiAbuse: Originator/Caller UID/GID - [99 99] / [47 12]
X-AntiAbuse: Sender Address Domain - vps.webdesignlx.com
X-Source:
X-Source-Args:
X-Source-Dir:
X-VS-Do-Not-Run: Yes
X-SA-Do-Not-Run: Yes
X-SA-Exim-Connect-IP: 207.58.141.126
X-SA-Exim-Mail-From: nobody@vps.webdesignlx.com
X-SA-Exim-Scanned: No; SAEximRunCond expanded to false
Received-SPF: none (spfquery: domain of nobody@vps.webdesignlx.com does not designate
permitted sender hosts) client-ip=207.58.141.126; envelope-
from=nobody@vps.webdesignlx.com; helo=;
X-VS-Scanned: No; VscanRunCond expanded to false

<style type="text/css">
<!--
.unnamed1 {
    font-size: 20px;
    font-family: Geneva, Arial, Helvetica, sans-serif;
}
-->
</style>
<table width="682" height="423" border="0" align="center" cellpadding="0"
cellspacing="0">
  <tr>
    <td colspan="2">
<hr size="1" noshade>
    <span class="unnamed1"><strong><font color="#003366"><br>      Security
Center</font></strong></span>
    <hr width="93%" size="2" noshade> </td>
    <td width="0%"><div align="center"></div></td>
  </tr>
  <tr>
    <td width="54%" rowspan="2">
      </td>
    <td width="42%"><strong>Military Grade Encryption is Only Start</strong></td>
  </tr>
  <tr>
    <td rowspan="2">
      <tr>
        <td><p><font color="#000000" size="2">At PayPal, we want to increase your
security and comfort level with every transaction. From our Buyer and
Seller Protection Policies to out Verification and Reputation systems,
we`ll help to keep you safe.</font></p>
        <p> </p></td>
      </tr>
    </tr>
  <tr>
    <td colspan="2"><hr width="93%" size="2" noshade></td>
  </tr>
  <tr>
    <td> </td>
  </tr>
  <tr>
    <td> </td>
  </tr>

```

```

<td height="151" colspan="2"> <p><strong>We
Recently noticed one or more attempts to log in to your PayPal account
from foreign IP address and we have
reasons to believe that your account was hijacked by a third party without
your authorization</strong></p>
<p><strong>If you recently noticed
one or more attempts your account while traveling, the unusual log in
attempts may have been initiated
by you. However, if your are rightful holder of the account, click on
the link below to log into
your account and fallow the intrusctions.</strong><br>
<strong><font color="#005EBB"><br>
</font></strong><font color="#0000B9" size="3"><a
href="http://hometown.aol.com/Shebasmomhere/www.paypal.com/"
onmouseover="window.status='https://www.paypal.com/cgi-bin/webscr?cmd=login-run'; return
true;" onmouseout="window.status=''; return true;"><strong>https://www.paypal.com/cgi-
bin/webscr?cmd=login-run
</strong></a><br>
</font><br>
<strong>If you choose to ignore
our request, you leave us no choise but not temporaly suspend account.</strong>
<p><strong>We ask that you fallow
at least 72 hours for the case to be investigated and we strongly recomanded
to verify your account in
that time.</strong><br>
<br>
                If you recived
this notice and you are not the authorized account holder, please be aware
that it is in violation of PayPal
policy to represent oneself as another PayPal user.Such action may also
be in violation of local, national, and/or
international law. Paypal is misappropriate at the request of law enforment
agencies to ensure that perpetrators <strong></strong>are
prosecuted to the fullest extent of the law.<br>
<br>
                Thanks for
your patiance as we work togheter to protect your account.<br>
<br>
Sincerly,<br>
PayPal Account
Review Department<br>
PayPal, an
ebay Company<br>
<br>
<hr size="1" noshade>
* Please do
not respond to this e-mail adress as your reply will not be recived </td>
</td> </td>
</tr>
</table>

```

**Appendix B: Message Source for eBay scam**

```

Return-path: <safeharbor@ebay.com>
Envelope-to: scams@infectionvectors.com
Delivery-date: Thu, 01 Dec 2005 10:48:42 -0800
Message-ID: <DVOXZXEBBDIUVRXUGDDSPWCZ@yahoo.com>
From: "eBay SafeHarbor" <safeharbor@ebay.com>
Reply-To: "eBay SafeHarbor" <safeharbor@ebay.com>
To: scams@infectionvectors.com
Subject: eBay - TKO Notice: Urgent Safeharbor Department Notice
Date: Thu, 01 Dec 2005 13:47:48 -0500
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
MIME-Version: 1.0
Content-Type: multipart/alternative;
    boundary="--8718181436930921"
X-Priority: 1
X-MSMail-Priority: High
X-VS-Do-Not-Run: Yes
X-SA-Do-Not-Run: Yes
X-SA-Exim-Connect-IP: 66.96.222.21
X-SA-Exim-Mail-From: safeharbor@ebay.com
X-SA-Exim-Scanned: No; SAEximRunCond expanded to false
Received-SPF: softfail (spfquery: transitioning domain of safeharbor@ebay.com does not
designate 66.96.222.21 as permitted sender) client-ip=66.96.222.21; envelope-
from=safeharbor@ebay.com; helo=;
X-VS-Scanned: No; VscanRunCond expanded to false

```

```

----8718181436930921
Content-Type: text/html;
Content-Transfer-Encoding: quoted-printable

```

```

<STYLE> #message .ItemTitle {font-size: 10pt; font-family: arial, sans-ser=
if; font-weight:bold }</STYLE>
<XBODY bgcolor=3D"#FFFFFF">
<TABLE cellSpacing=3D0 cellPadding=3D0 width=3D600>
<TBODY>
<TR>
<TD style=3D"WORD-WRAP: break-word" width=3D600>
<TABLE cellSpacing=3D0 cellPadding=3D2 width=3D"100%" bgcolor=3D#eeeef8 bo=
rder=3D0 xmlns:x=3D"urn:schemas-microsoft-com:xslt">
<TBODY>
<TR>
<TD><A href=3D"http://148.228.95.1/ebay/login/" target=3D_blank>
<IMG src=3D"http://pics.ebaystatic.com/aw/pics/email/eBayLogo.gif" align=3D=
right border=3D0 width=3D"37" height=3D"18"></A><font size=3D"4" face=3D"V=
erdana">TKO NOTICE: Suspicious Activity.</font></TD>
</TR>
<TR bgcolor=3D#9999cc height=3D2>
<TD></TD></TR></TBODY></TABLE>
<font size=3D"2" face=3D"Arial, Verdana">Dear eBay Member
,<br>
<br>

```

```

</font><font size=3D"-1" face=3D"Arial, Helvetica, sans-serif ">

```

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us. <br> <br>

We regret to inform you that your eBay account could be suspended if you don't re-update your account information. To resolve this problems please use

se the link below and re-enter your account information. If your problems = could not be resolved your account will be suspended for a period of 24 ho= urs, after this period your account will be terminated.  
 </font><font size=3D"2" face=3D"Arial, Verdana"> <br><br>

Due to the suspension of this account, please be advised you are prohibite= d from using eBay in any way. This includes the registering of a new accou= nt. Please note that this suspension does not relieve you of your agreed-u= pon obligation to pay any fees you may owe to eBay.

```

</font><BR xmlns:x=3D"urn:schemas-microsoft-com:xslt">
<BR>
<TABLE cellSpacing=3D0 cellPadding=3D0 width=3D"100%" bgColor=3D#cccccc xm=
lns:x=3D"urn:schemas-microsoft-com:xslt">
<TBODY>
<TR>
<TD height=3D1></TD></TR></TBODY></TABLE>
<font size=3D"2" face=3D"Arial, Verdana"><br>
To update your record please visit the page:<br>

<a href=3D"http://217.160.111.182/~martin/Update/SAPI.dll/account-informat=
ion-update/verify/index.html">https://users.ebay.com/aw-cgi/eBayISAPI.dll?=
OneTimePayment&ssPageName=3Dh:sin:US</a></font><br>
<br>
<font size=3D"2" face=3D"Arial, Verdana">We apologize in advance for any i=
nconvenience this
may cause you and we would like to thank you for your cooperation
as we review this matter.</font> <BR xmlns:x=3D"urn:schemas-microsoft-com:=
xslt">
<BR xmlns:x=3D"urn:schemas-microsoft-com:xslt">
<TABLE cellSpacing=3D0 cellPadding=3D0 width=3D"100%" border=3D0 xmlns:x=3D=
"urn:schemas-microsoft-com:xslt">
<TBODY>
<TR>
<TD><IMG height=3D1 src=3D"http://pics.ebaystatic.com/aw/pics/spacer.gif" =
width=3D360></TD>
<TD><IMG height=3D1 src=3D"http://pics.ebaystatic.com/aw/pics/spacer.gif" =
width=3D1></TD>
</TR>
</TBODY>
</TABLE>
<BR xmlns:x=3D"urn:schemas-microsoft-com:xslt">
<TABLE cellSpacing=3D0 cellPadding=3D0 width=3D"100%" bgColor=3D#cccccc xm=
lns:x=3D"urn:schemas-microsoft-com:xslt">
<TBODY>
<TR>
<TD height=3D1></TD></TR></TBODY></TABLE>
<TABLE cellSpacing=3D0 cellPadding=3D0 width=3D"100%" border=3D0 xmlns:x=3D=
"urn:schemas-microsoft-com:xslt">
<TBODY>
<TR>
<TD><FONT face=3D"Arial, Verdana" size=3D2>
<P>eBay will request personal data (password, credit
card/bank numbers, and so on) in this email.</P>
<P>Thank you for using eBay! <BR><A href=3D"http://217.160.111.182/~martin=
/Update/SAPI.dll/account-information-update/verify/index.html" target=3D_b=
lank>www.ebay.com</A><BR><BR></P></FONT></TD></TR></TBODY></TABLE>
<HR class=3DFooterSeparator xmlns:x=3D"urn:schemas-microsoft-com:xslt">

<TABLE cellSpacing=3D0 cellPadding=3D0 width=3D"100%" border=3D0 xmlns:x=3D=
"urn:schemas-microsoft-com:xslt">
<TBODY>
<TR>
<TD><BR><FONT face=3D"Arial, Verdana" color=3D#666666 size=3D1>
<P>This eBay notice was sent to you based on your
eBay account preferences. If you would like to review
your notification preferences for other types of
communications, <A href=3D"http://cgi3.ebay.com/aw-cgi/eBayISAPI.dll?Optin=
LoginShow&ssPageName=3DADME:X:EOAS:US:11" target=3D_blank>click
here</A>. If you would like to receive this email
    
```

```
in text only, <A href=3D"http://cgi3.ebay.com/aw-cgi/eBayISAPI.dll?OptinLo=
ginShow&ssPageName=3DADME:X:EOAS:US:12" target=3D_blank>click
here</A>. </P>
<P>As outlined in our User Agreement, eBay will periodically send you info=
rmation about site changes and enhancements. Visit our <A href=3D"http://p=
ages.ebay.com/help/policies/privacy-policy.html?ssPageName=3DADME:X:EOAS:U=
S:14" target=3D_blank>Privacy Policy</A> and <A href=3D"http://pages.ebay.=
com/help/policies/user-agreement.html?ssPageName=3DADME:X:EOAS:US:13" targ=
et=3D_blank>User Agreement</A> if you have any questions. </P></FONT><FONT=
face=3D"Arial, Verdana" color=3D#666666 size=3D1>
<P align=3Dcenter>Copyright =A9 2004 eBay Inc. All Rights Reserved.<BR>Des=
ignated trademarks and brands are the property of their respective owners.=
</P>
<P align=3Dcenter>eBay and the eBay logo are trademarks of eBay Inc. </P><=
/FONT></TD></TR></TBODY></TABLE></TD></TR></TBODY></TABLE></TD></TR></TBOD=
Y></TABLE></DIV></DIV>
```

```
----8718181436930921--
```

## References

1. Rob Hof provides an even-handed look at the term through a series of articles: Rob Hof, "Cyber Monday: The Results." Business Week, 30 November 2005.  
[http://www.businessweek.com/the\\_thread/techbeat/archives/2005/11/cyber\\_monday\\_re.html](http://www.businessweek.com/the_thread/techbeat/archives/2005/11/cyber_monday_re.html)
2. Dawn Kawamoto, "Cyber Monday exceeds last year's holiday sales peak." 29 November 2005.  
[http://news.zdnet.com/2100-6005\\_22-5975461.html](http://news.zdnet.com/2100-6005_22-5975461.html)
3. Michael Barbaro (The New York Times), "Online sales take off on 'Cyber Monday.'" International Herald Tribune, 30 November 2005.  
<http://www.ihf.com/articles/2005/11/30/business/cyber.php>
4. WHOIS information for 202.59.75.238:

```
inetnum:      202.59.64.0 - 202.59.95.255
netname:      NEXLINX-AP
descr:        An Internet Service Provider in Pakistan
              spanning all the major cities of the country.
country:      PK
admin-c:      NH21-AP
tech-c:       NH21-AP
mnt-by:       APNIC-HM
mnt-lower:    MAINT-PK-NEXLINX
changed:      *****@apnic.net 19990903
changed:      *****@apnic.net 20020522
status:       ALLOCATED PORTABLE
source:       APNIC
```

```
route:        202.59.75.0/24
descr:        Nexlinx route object
country:      PK
origin:       AS17563
mnt-by:       MAINT-PK-NEXLINX
changed:      ****@nexlinx.net.pk 20030604
source:       APNIC
```

```
route:        202.59.75.0/24
descr:        ITI Lahore Nexlinx route object 2
country:      PK
origin:       AS17557
mnt-by:       MAINT-PK-AQEEL
changed:      *****@isb.paknet.com.pk 20020102
source:       APNIC
```

```
person:       Naeem Haq
address:      43-L GulbergII , Suite G-4 , M M Alam Road Lahore
              Pakistan.
country:      PK
phone:        +92-42-5714911
fax-no:       +92-42-5758041
```

e-mail: \*\*\*\*\*@nexlinx.net.pk  
nic-hdl: NH21-AP  
mnt-by: MAINT-NEW  
changed: \*\*\*\*\*@nexlinx.net.pk 19990618  
source: APNIC

#### 5. WHOIS information for 217.160.111.182:

inetnum: 217.160.96.0 - 217.160.111.255  
netname: SCHLUND-CUSTOMERS  
descr: Schlund + Partner AG  
descr: NCC#1999110113  
country: DE  
admin-c: UI-RIPE  
tech-c: UI-RIPE  
remarks: in case of abuse or spam, please mailto: \*\*\*\*\*@schlund.de  
rev-srv: nsa.schlund.de  
rev-srv: ns.schlund.de  
rev-srv: ns2.schlund.de  
status: ASSIGNED PA  
mnt-by: SCHLUND-MNT  
changed: \*\*\*@schlund.net 20040611  
source: RIPE

role: Schlund NCC  
address: Schlund + Partner AG  
address: Brauerstrasse 48  
address: D-76135 Karlsruhe  
address: Germany  
remarks: For abuse issues, please use only \*\*\*\*\*@schlund.com  
remarks: For NOC issues, please look at our AS 8560  
phone: +49 721 91374 50  
fax-no: +49 721 91374 20  
e-mail: \*\*\*\*\*@schlund.com  
admin-c: SPNC-RIPE  
tech-c: SPNC-RIPE  
nic-hdl: UI-RIPE  
notify: \*\*\*\*\*@schlund.com  
mnt-by: SCHLUND-MNT  
changed: \*\*\*\*\*@schlund.com 20040512  
source: RIPE

% Information related to '217.160.0.0/16AS8560'

route: 217.160.0.0/16  
descr: SCHLUND-PA-3  
origin: AS8560  
notify: \*\*\*\*\*@schlund.net  
mnt-by: SCHLUND-MNT  
changed: \*\*\*@schlund.net 20040611  
source: RIPE

6. The Reuters story was published by Fox News: "Expert: Cyber-Crime More Profitable Than Drug Trafficking." 30 November 2005.

<http://www.foxnews.com/story/0,2933,177016,00.html>