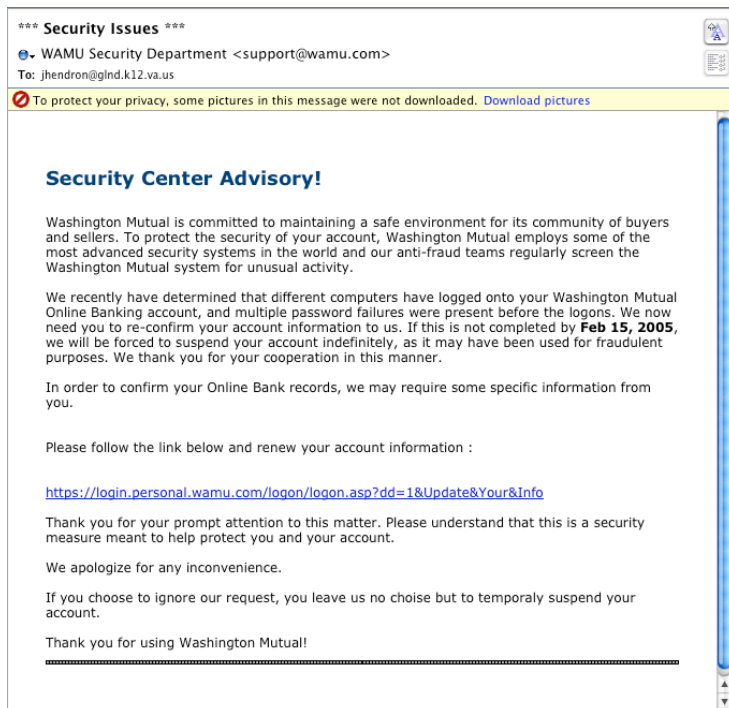


CyberCrime

Documenting a Common Ploy to Steal Money

by
John Hendron

On February 11, 2005, I received an e-mail from Washington Mutual Bank which prompted an investigation that revealed that the message was designed for me to reveal my account information to a third party. I have decided to document how I undertook this investigation, as others will no doubt try similar tactics to swindle folks out of their money.



I was suspicious because I am not a customer of Washington Mutual. You will notice that the e-mail was sent directly to my address. Looking at the Internet headers for the message, we see that the e-mail originated from an AOL account, not WAMU.com, the bank they claim to be from. Substituting a real address to hide the origin of a message is called **phishing**.

Source: *** Security Issues ***

Received: from [62.193.213.10] by gcentral.glnd.k12.va.us
with SMTP (QuickMail Pro Server for Mac 3.0.2); 11-Feb-2005 13:24:39 -0500
Received: from 128.82.176.116 by ; Fri, 11 Feb 2005 17:24:35 -0100
Message-ID: <SYXXFZDMSBRCUKBOMJXXK@aol.com>
From: "WAMU Security Department" <support@wamu.com>
Reply-To: "WAMU Security Service" <security@wamu.com>
To: jhendron@glnd.k12.va.us
Subject: *** Security Issues ***
Date: Fri, 11 Feb 2005 11:23:35 -0700
X-Mailer: The Bat! (v1.52f) Business
MIME-Version: 1.0
Content-Type: multipart/alternative;
boundary="--91278236788127774264"
X-Priority: 3
X-MSMail-Priority: Normal

Another clue were the misspellings in the e-mail. I doubt a reputable bank would make typos. This clued me in that a non-English speaker had written the note, or at least changed an original. A lot of cyber-crime against the U.S. starts overseas, because going after these criminals in other countries is difficult.

Aside from this information, I checked on the link in the e-mail. If you go to the address that is spelled-out, it indeed goes to the *real bank*. However, when you mouse-over the link, the address leads elsewhere. It in fact goes to a Taiwanese website: <http://asianent.com.tw/w/>

Amazingly, the two web sites look identical when you visit.

Washington Mutual -- ... Security Measures

wamu.com A Washington Mutual, Inc. Web site [Apply Now](#) | [Locations](#) | [Contact Us](#) | [Help](#) | [Search](#) | [Home](#)

personal banking PERSONAL ONLINE BANKING NEW ACCOUNT CHOICES LOANS & LINES OF CREDIT CUSTOMER SERVICE

secure

Log On for Online Services

New to Online Services?
You'll need a User ID and password to:

- **Access** your accounts online
- **Pay** bills online - **now free!**
- **Apply** for an account or loan online
- **Send** us a secure message

[create User ID](#)

Returning User?
Personal Bill Pay™ service is **free!** To use, select Pay Bills from the dropdown below and log on.

User ID:

Password: *

[Forgot your password?](#)


[View My Accounts](#)

*Your Password is case sensitive and must be entered exactly as created (i.e. upper and lower case letters).

Need help? Use [Site Helper](#) or call customer service at 1.800.788.7000.

[Protect yourself against fraud.](#) Washington Mutual will never ask customers for their Password or PIN through e-mail or phone calls.

Deposits are offered by Washington Mutual Bank, FA and Washington Mutual Bank fsb and are FDIC insured.

 EQUAL HOUSING LENDER

Personal Banking | Small Business Banking | Commercial Banking | Online Services Agreement & Disclosure | Terms of Use | Your Privacy & Security
Home Loans | Investments | Insurance | About WaMu © Copyright 2005, Washington Mutual, Inc. All Rights Reserved

Folks who are not used to looking at URLs could easily be fooled here. The wrong URL for WAMU is in my address bar, but I imagine a lot of folks would overlook this.

Next, I decided to check and see who owned the URL in Taiwan. A *whois* search came up with this information:

```
Registrant:
亞 娛 企 業 有 限 公 司
ASIAN ENTERTAIN CO., LTD.
7F-1 NO. 15, LANE 174, HSIN MING RD., NEI-HU, TAIPEI,

Domain Name: asianent.com.tw

Contact:
Chiang   Chiang@asianent.com.tw
TEL: 02-27953692-6
FAX: 02-27935882

Record expires on 2008-12-07 (YYYY-MM-DD)
Record created on 2001-12-06 (YYYY-MM-DD)

Domain servers in listed order:
ns.sparqnet.net      211.78.130.1
bns.sparqnet.net    61.56.211.185


Registrar: SEEDNET
```

Whenever you suspect a website to be of dubious nature, you can perform a WHOIS search various ways. Among the easiest is through the website, Network Solutions (<http://www.networksolutions.com/>) or in the Network Utility in OS X.

Even at this point if I thought the site might be legitimate, the name “Asian Entertain” should arouse suspicion. I went one step further, however, and actually used the phony site.

wamu.com A Washington Mutual, Inc. Web site [Apply Now](#) | [Locations](#) | [Contact Us](#) | [Help](#) | [Search](#) | [Home](#)

personal banking PERSONAL ONLINE BANKING NEW ACCOUNT CHOICES LOANS & CREDIT CARDS CUSTOMER SERVICE

secure 

Security Measures

Confirm Your Identity

First Name* MI Last Name*

Card Number*

Expiration Date*


CVV2*

PIN*

[next](#)

*Denotes required field

Need help? Use [Site Helper](#) or call **eCare**® customer service at 1.800.788.7000.

FDIC Insured
 EQUAL HOUSING LENDER

After logging into the site with random information, it let me in. Imagine that—wrong username, wrong password—but I get in! This is what I saw next (above). I filled in my supposed account information, from my card number to my PIN... the “secure” logo under “personal banking” is just a sticker. There was nothing secure about the site. I checked the protocol in the address bar, and it was http:// not https://.

After you fill out your information, it simply displays a message about security issues and fraud. Clicking any of the links will take you back to the real, authentic WAMU website. However in the process, these Taiwanese criminals have hoped you’ve left them your bank account information.

A few tips for dealing, and sniffing out fraud:

- Set a default in your e-mail application to not display graphics, unless you choose. The download of these graphics from fraudulent sites will clue spammers into knowing the e-mail the sent was received, and read.
- Avoid opening attachments from folks you do not know. Many malicious applications (for Windows) will be wrapped with seemingly benign filename extensions, like .zip

- Always check the URL of the sites you visit. If you end up someplace other than you expect, beware.
- While banks and other types of sites will ask you personal information, as when you make a purchase online, I can't think of one instance where I was required to re-visit, and re-supply secure information. Beware.
- Lastly—check the Internet Headers or source of your e-mail when it looks suspicious, and perform WHOIS searches for sites that may question for authenticity or quality of content. Many ISPs have abuse e-mail addresses to report instances like the one I have documented here.

Next for me is an e-mail to abuse@aol.com. Take care!