Internet Scams and Hoaxes:

Some information for your everyday user

By David Cobaugh

A hoax is “an attempt to trick an audience into believing that something false is real.” A rumor is “an assertion or set of assertions widely repeated through its truth is unconfirmed by facts or evidence.” Both of these items are becoming a big problem in the business and personal word today. Yes, these are the spoof web pages you have possibly seen and those obnoxious emails you probably have gotten at least once in your life. Deviant and malicious Internet hoaxes can greatly harm your company if one is not prepared, and can certainly harm your computer, as well.

Internet Hoaxes started circulating in 1988. Some of the most popular Internet hoaxes are sent through email. The majority of these emails include some type of money exchange from one foreign nation to your personal account. The one’s that can really hurt you are spoof (fake) e-mails from a bank, IRS, pay pal, etc. That kind of spoof does normally include a link for you to go to and change some account information. What most people don’t know is that these websites act as a logger and relays the information back to a server. Most of this information is sold to others; however, sometimes the information is used by the hacker. There are other types of hoaxes out that do no damage at all; these are what I like to call, laughing in your face. The Laughing in Your Face hoaxes are basically just chain letters asking you to forward to so many people in order to save a life or win the lottery.

PC World released an article in November of 2002, listing the latest e-mail hoaxes at that time. Listed below are a couple of the hoaxes.

1. Bill Gates Has Cash for You – In this email a lot of mumbo jumbo is given about tax information, stating that if you are part of Bill Gates’ E-mail Beta Test. By helping him complete the test you will be given a check for $28,000.

One way to spot that fact from fiction in this; do you even remember signing up for this beta test? How many other people signed up for this beta test? Why would Bill Gates select you and not one of Microsoft's employees? There is also a name and number you are to call in order to collect the money; however, the number sends you to a telemarketing company, and the address doesn't exist.

2. Do Damage to Your PC – In this hoax, the e-mail suggests you have been infected with a virus. It states the virus is un-detectable by the two most popular anti-virus programs, Norton and McAfee. The e-mail goes on to suggest this virus stays inactive for fourteen days and you must delete the executable file, jdbgmgr.exe. Upon, further investigation, the executable file you are to delete is the Java Debugger Manager. No real harm is done if the file is deleted; some websites that are Java dependent will not show correctly.

There are several websites available to view reported hoaxes, as well as, websites to report new hoaxes. If you come across one of these hoaxes, and it's unreported, please report it immediately to help others become aware of such items. http://hoaxbusters.org is a very good website to see reported hoaxes. The Symantec and McAfee websites also offer lists of reported email hoaxes. Most of the hoaxes listed on Symantec and McAfee deal with the more dangerous hoaxes that contain viruses. Hoax Busters list the top five signs that a message is a hoax:

1. Urgent – The e-mail will contain a sense of urgency, for example the subject line will include words such as, Urgent, Warning, Important,

Virus Alert. Of course, do not disregard every message that has that subject title. Just be weary of who the e-mail is from.

2. Tell All Your Friends – Most of these hoaxes are considered you average chain letter, stating you need to forward the message onto everyone you know.
3. This Isn't a Hoax – This is the type of the e-mail which states, "This is not a hoax" or something similar to this happened to my friend so I know it's true.
4. Dire Consequences – this is hoax is clear as day, it states that if you don't act immediately on what the e-mail says something will happen; such as your hard drive will be erased, your bank account will be deleted, etc.
5. History – If there are any signs of ">>>>" marks it shows the message has been forwarded before.
6. Attachments – Any e-mail you receive that has an attachment should never be opened, especially if you do not know who sent the message. Even if you do know who sent the message and you need to open the attachment, download the attachment to a disk, and run a virus scan on the disk.

The U.S. Department of Energy has a website within the Office of Cyber Security < http://ciac.llnl.gov/ciac/CIACHome.html >. This website has many different bulletins to let Internet users know about hoaxes, vulnerabilities, and high security risks. The CIAC (Computer Incident Advisory Capability) has been with incident response, and

reporting and tracking items dealing with computer security since 1989. The website states not to e-mail the CIAC directly about hoaxes, instead it gives a hoax buster e-mail address. The CIAC has its own hoax information website, which offers many links to helpful websites and organizations about hoaxes. The link to this site is located on the home page of the CIAC and is right here: < http://hoaxbuster.ciac.org/HBOtherHoaxPages.html >.

Some other good sources to help one become more acquainted with the hoaxes is the CERT Coordination Center, which is located at the Software Engineering Institute funded and operated by the Carnegie Mellon University. They have some of the same information found on the CIAC website, but this site offers trainings to help improve your security. The site address is < http://www.cert.org >. The British government also has a national website dealing with security issues and hoaxes. This is definitely a great resource to use because most of the hoaxes that are dangerous have come from areas outside the United States of America. This organization is known as the National Infrastructure Security Co-ordination Centre (NISCC). Their website is < http://www.uniras.gov.uk/niscc/index-en.html >. Unlike, the American based-sites this organization was setup in 1999, and is used as the inter-national center in helping other organizations around the world.

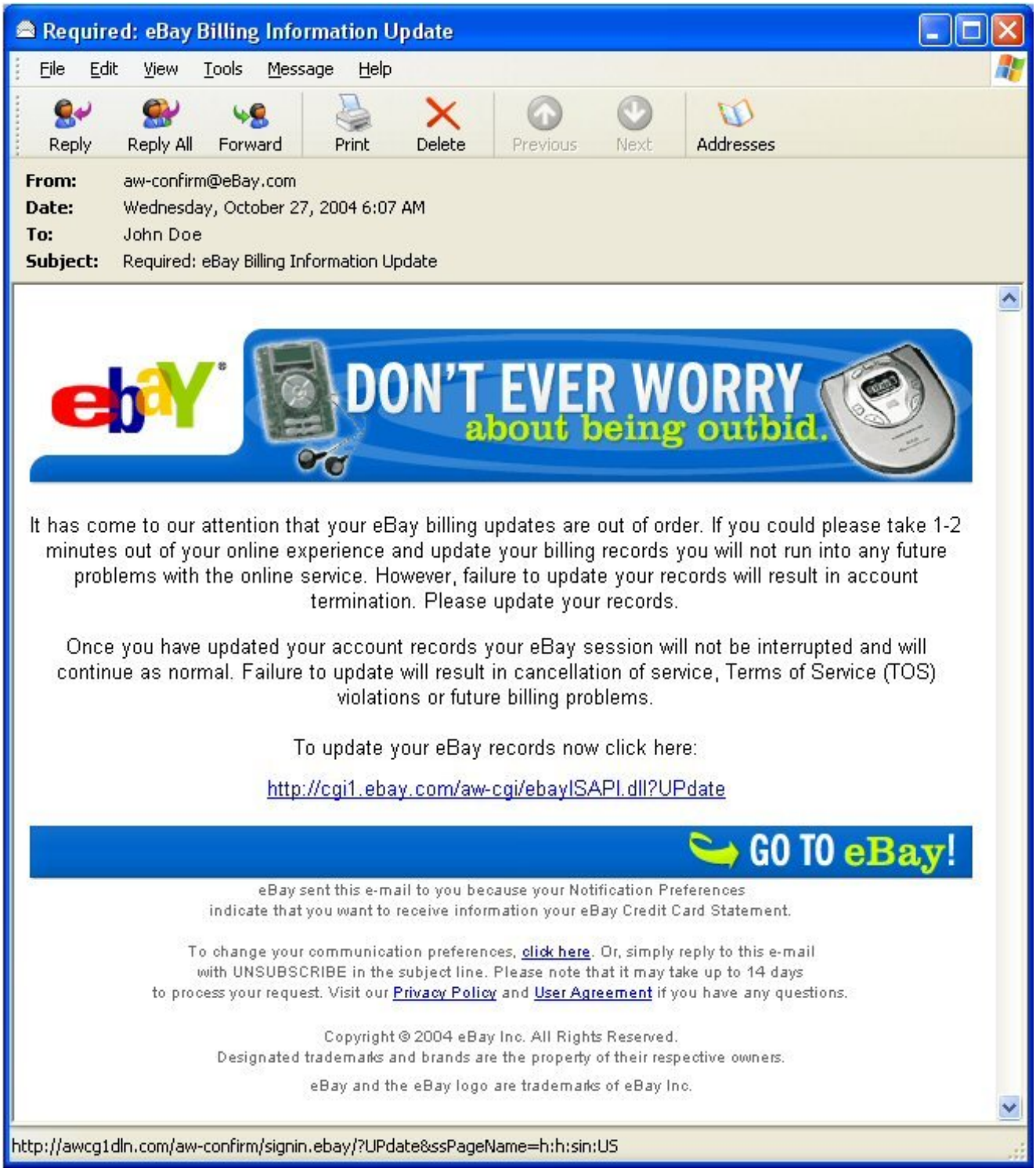
Other than simple spoof e-mail chain letters there are the more hazardous types of scams circulating the Internet. These scams are also known as phishing, which is a way for one to acquire personal information by 'tricking' a user. For example, you could receive an e-mail from a credible source and it leads to, what you think, is a credible website. The website looks exactly like your banking website, so you login and enter

some information. You were just phished. Did you notice a lock symbol at the bottom of your browser? Was there a lock symbol in the address bar? Did you view the certificate to the page? If you answered no to any of these questions, you should think about looking into them. Internet Explorer, the most popular web browser used today, has a lock symbol normally located at the bottom left corner. If you see this symbol, it means the website you are visiting is secure. One other way to guarantee this is to check out the URL; does the URL start off with “https”? If you answered yes, you are fine. Finally, you can check the digital certificate of the website, if the certificate is verified you are ok. Some websites to help you learn more about digital certificates include < http://www.verisign.com > and < http://www.thawte.com >. The sites offer certificates to add to your own site and your email to verify you are not getting spoofed accounts sent to you. Other web browsers offer certain plug-ins which can help spot a secure site from an un-secure one. For example, certain skins for the second more popular Internet browser, Mozilla Firefox, include the lock symbol plus a colored URL bar. The bar is only colored when the site is secured; this is a great way for those who are not too computer-literate.

The Anti-Phishing Working Group (APWG) helps with phishing emails, sites, and e-commerce businesses. They are located at < http://www.antiphishing.org > where the site is often updated and more reports and news events are added to the archives. The APWG has a list of many sponsors in which they have helped customers become aware of many phishing scams.

For those trying to test their ability in what is a scam and what is real, there is an IQ test called, MailFrontier Phishing IQ Test II. The test is updated every so often with new phish scams. The object of the test is to click on the links provided and figure out if

the emails are legitimate or not. This IQ can be found at < http://survey.mailfrontier.com/survey/quiztest.html >. Most scams can be recognized easily due to the text content. For example, some major scams frequently viewed deal with some foreign nation which the president was overthrown and cannot get the money unless sent to your account, and you will be given a hefty sum for helping. In these emails the language is horribly gutted and the entire process seems “too good to be true”. The process is too good to be true, many people have fallen for this type of scam and lost their entire accounts. Always remember to never give out your account information, user names and passwords, or other personal information such as your social security number to anyone through an email. There are no companies that will ask for personal information like that through an email. Below are some examples of phishing scams:


Required: eBay Billing Information Update
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses
From: aw-confirm@eBay.com
Date: Wednesday, October 27, 2004 6:07 AM
To: John Doe
Subject: Required: eBay Billing Information Update
DON'T EVER WORRY
about being outbid.
It has come to our attention that your eBay billing updates are out of order. If you could please take 1-2 minutes out of your online experience and update your billing records you will not run into any future problems with the online service. However, failure to update your records will result in account termination. Please update your records.
Once you have updated your account records your eBay session will not be interrupted and will continue as normal. Failure to update will result in cancellation of service, Terms of Service (TOS) violations or future billing problems.
To update your eBay records now click here:
http://cgi1.ebay.com/aw-cgi/ebayISAPI.dll?UPdate
GO TO eBay!
eBay sent this e-mail to you because your Notification Preferences indicate that you want to receive information your eBay Credit Card Statement.
To change your communication preferences, click here. Or, simply reply to this e-mail with UNSUBSCRIBE in the subject line. Please note that it may take up to 14 days to process your request. Visit our Privacy Policy and User Agreement if you have any questions.
Copyright © 2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
eBay and the eBay logo are trademarks of eBay Inc.
http://awcg1dln.com/aw-confirm/signin.ebay/?UPdate&ssPageName=h:h:sin:US

Important information regarding your e-mail address

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

From: Bank of America
Date: Monday, September 27, 2004 9:29 AM
To: Jane Doe
Subject: Important information regarding your e-mail address

Bank of America Higher Standards

Useful financial information delivered right to your inbox.

Thank you for providing us with your e-mail address. You can rest assured that we protect your information, including your e-mail address, and will never sell or share it with marketers outside Bank of America. Read our Privacy Policy to find out more.

As part of our service to you, we may occasionally send you free, informative e-mails to:

- Keep you up to date on products, features, and services
- Let you know how Bank of America and its affiliates can help you financially — wherever you are in life
- Provide you with the tools and resources you need to make sound financial decisions

You can help us provide you with the most relevant information by taking a moment to tell us your e-mail preferences.

And of course you can unsubscribe at any time.

Remember, Bank of America is committed to your security and protection. Please be aware that we will never e-mail you to request or verify security information about passcodes, PINs, or other sensitive details. To find out more, take a look at our Information Security section under Privacy and Security on the Web site.

As pictured above, you can see this phishing scams look quite realistic. Everyone needs to keep watch of what emails they open, and start using digital signatures in emails. Every kind of Internet hoax shouldn't be shrugged off or ignored, they need to be reported. Every Internet user must be aware of the potential dangers out there. When someone mentions this, they think viruses and spy ware; no one ever thinks about these phishing scams which could potentially bankrupt a person, company, or organization. If there is anything I could not stress more its to always double check the type of website you enter information to, and to double check the emails you get before opening them.

References

http://ciac.llnl.gov/ciac/CIACHome.html

http://hoaxbusters.ciac.org/

http://www.symantec.com/avcenter/hoax.html

http://hoaxbusters.org/#

http://www.uniras.gov.uk/niscc/index-en.html

http://www.pcworld.com/howto/article/0,aid,106272,00.asp

https://www.verisign.com/

http://www.thawte.com/

http://www.uky.edu/Libraries/LTS/phish.html

http://survey.mailfrontier.com/survey/quiztest.html

http://en.wikipedia.org/wiki/Main_Page