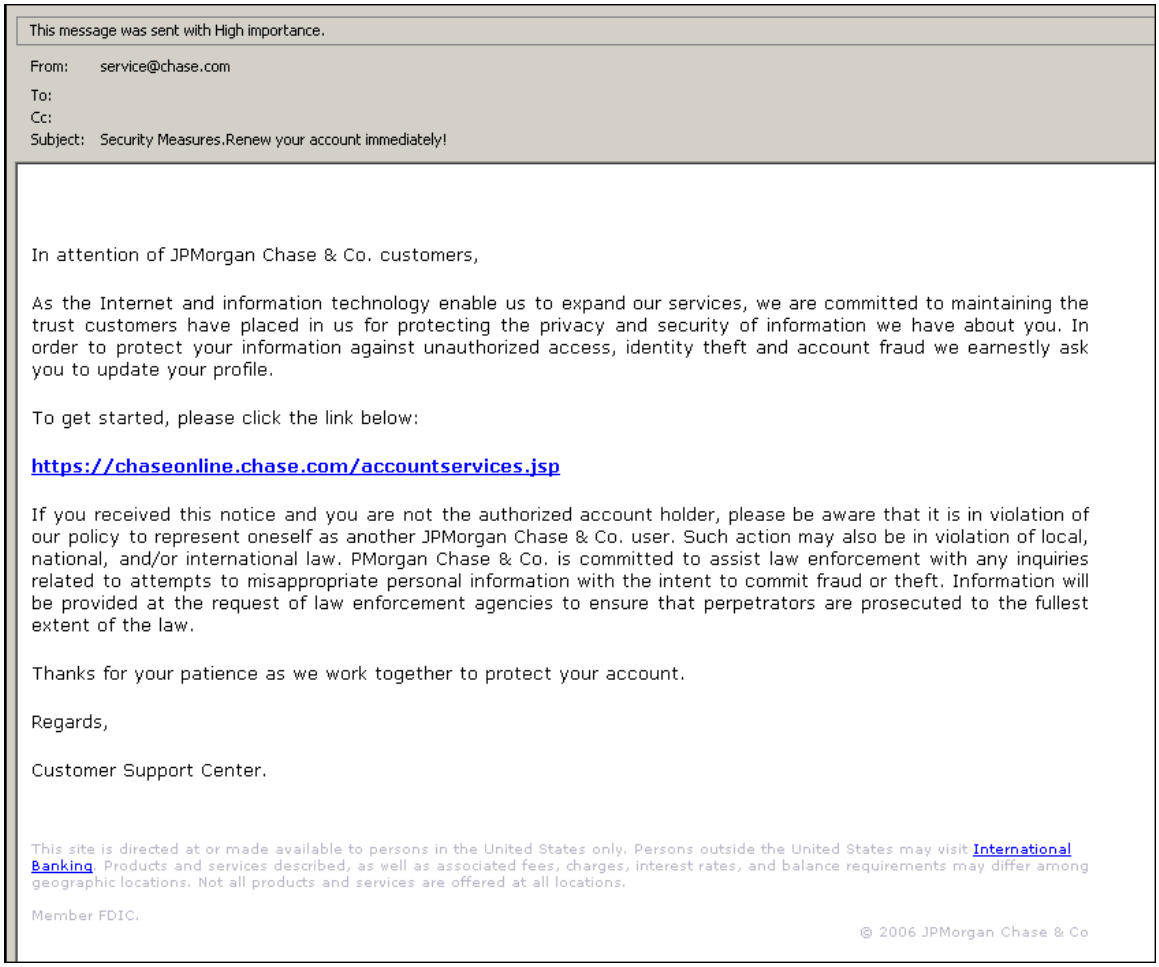
Phishing – Don't get caught!!

What is it?

Phishing (pronounced "fishing") is a term used to describe an online scheme employed by criminals to trick you into disclosing personal information.

This is an example of an email I recently received. It looks authentic and if I click on the link (which you shouldn't do by the way) I would be taken to a site that looks just like JPMorgan Chase and Co's Website. At this authentic looking site I'm presented with a form to fill out with my account information. A closer look at the URL or address however, reveals that I have been taken to a site called Korean Car Care.



This message was sent with High importance.

From: service@chase.com

To:

Cc:

Subject: Security Measures.Renew your account immediately!

In attention of JPMorgan Chase & Co. customers,

As the Internet and information technology enable us to expand our services, we are committed to maintaining the trust customers have placed in us for protecting the privacy and security of information we have about you. In order to protect your information against unauthorized access, identity theft and account fraud we earnestly ask you to update your profile.

To get started, please click the link below:

https://chaseonline.chase.com/accountservices.jsp

If you received this notice and you are not the authorized account holder, please be aware that it is in violation of our policy to represent oneself as another JPMorgan Chase & Co. user. Such action may also be in violation of local, national, and/or international law. PMorgan Chase & Co. is committed to assist law enforcement with any inquiries related to attempts to misappropriate personal information with the intent to commit fraud or theft. Information will be provided at the request of law enforcement agencies to ensure that perpetrators are prosecuted to the fullest extent of the law.

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

Regards,

Customer Support Center.

This site is directed at or made available to persons in the United States only. Persons outside the United States may visit International Banking. Products and services described, as well as associated fees, charges, interest rates, and balance requirements may differ among geographic locations. Not all products and services are offered at all locations.

Member FDIC.

© 2006 JPMorgan Chase & Co

This is just one example of countless email phishing schemes. By using official looking emails and spoofing the websites of well known companies, criminals try to get information they can use for financial gain. They are looking for any personal information they can get from you; name, address, phone number, username, PIN, bank account numbers, credit card numbers, social security number, etc…. This information is used to steal your identity and/or gain access to your bank accounts or credit cards.

What to avoid!!

Emails that ask you to update personal information – many legitimate companies have a policy against asking for personal information through the email.

Urgent Wording – Many times the email will have a sense of urgency to get you to respond without thinking.

Fake Links –

- HTML link in a message can easily hide a link to a different website. Take a look at the link above. It looks legitimate, however, as you can see when the mouse pointer is held over the link the true address is revealed.
- Beware of links that contain an @ sign in the link, the browser will ignore anything that comes before the @ sign.
  https://www.communitybank.com@nl.tv/secure_verification.aspx will not take you to www.communitybank.com but to the site at **nl.tv/secure_verification.aspx.**
- Another common practice is to slightly alter a well known company's address. For example www.communitybank.com might be changed to www.comunitybank.com.

Attachments – beware of emails that ask you to open an attachment. The attachment may contain a virus or Spyware that once downloaded on your computer logs keystrokes as you log into your online accounts and send the information back to the criminal.

Protect yourself from Online Fraud.

- Never reply to emails that ask for personal information
- Do not click on links in suspicious email
- Never send personal information in regular email messages
- Use strong passwords and change your passwords often

- Type the website address (URL) of the business into the address bar
- Do not open attachments in suspect emails

Google it – one way to find out if a suspicious email is a phishing scam is to copy the subject line and paste it into the search box on Google. When I searched for the email I received I found 70 references to the email and phishing.

For more information on this topic:
http://office.microsoft.com/en-us/assistance/default.aspx and search for Phishing

Federal Trade Commission government website
http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm
Better Business Bureau Online
http://www.bbbonline.org/idtheft/phishing.asp