Pointing the Way to Your Financial Success™

How to Avoid Becoming a Victim of E-mail Fraud

Unfortunately for the many legitimate online e-commerce businesses in the world today, there are several bad apples that are making life miserable for businesses and consumers alike by spreading computer viruses (some potentially malicious), installing distracting ad-pop-ups without your consent, and the latest, and potentially most serious problem, **phishing** – a process by which your keystrokes, such as your financial account numbers and passwords, are captured without you knowing and then used by thieves to make purchases on your behalf.

Antivirus and Spyware software, Firewalls and e-mail filters help to some extent, but they do not catch everything and often do catch things you do need or may want to receive.

Like it or not, this is the world we are living in and we at Compass Investors, as a service to all our subscribers, want you to be armed and ready to deal with whatever may come your way.

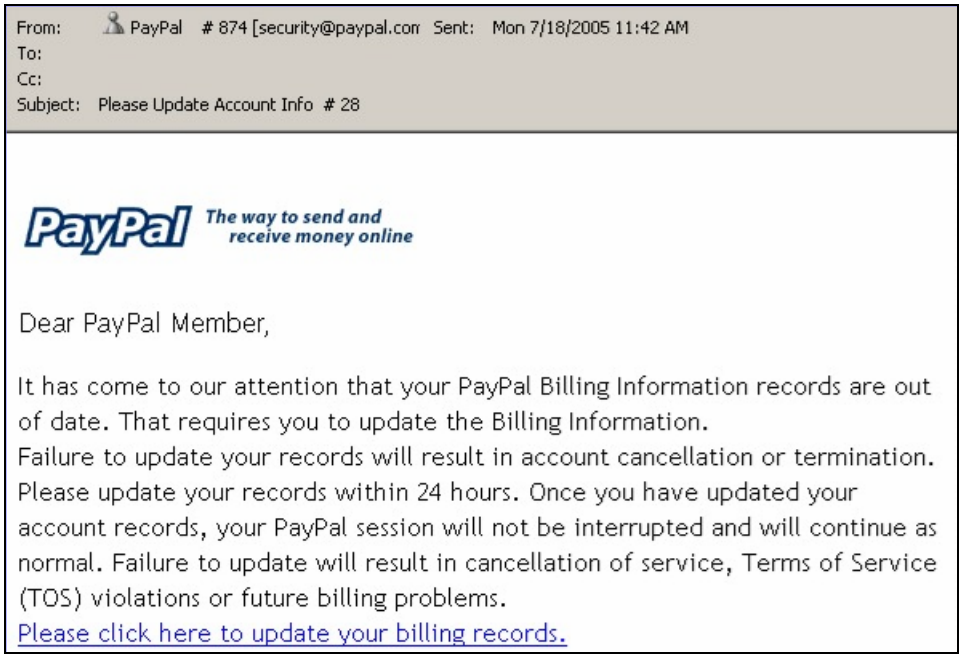
FOUR Tips for Avoiding Fraud when using PayPal

IMPORTANT: These tips specifically mention PayPal. BUT, they should be followed when opening and responding to email from ANY personal financial source (e.g., banks, credit cards, mutual funds, brokers, etc.)

1. **Safe Log In**: To log in to your PayPal account always open a new web browser (e.g., Internet Explorer or Netscape) and type in the following address: https://www.paypal.com
2. **Email Greeting**: Emails from PayPal will address you by the first and last name associated with your PayPal account. Fraudulent emails often include the salutation "Dear PayPal User" or "Dear PayPal Member".
3. **Email Attachments**: PayPal emails will never ask you to download an attachment or a software program. Attachments contained in fraudulent emails often contain viruses that may harm your computer or compromise your PayPal account.
4. **Request for Personal Information**: Only enter personal information once you have safely and securely logged in to your PayPal account (see Tip #1)

Example 1

An example of a fraudulent PayPal e-mail from appears below:



From: PayPal # 874 [security@paypal.com Sent: Mon 7/18/2005 11:42 AM
To:
Cc:
Subject: Please Update Account Info # 28

PayPal The way to send and receive money online

Dear PayPal Member,

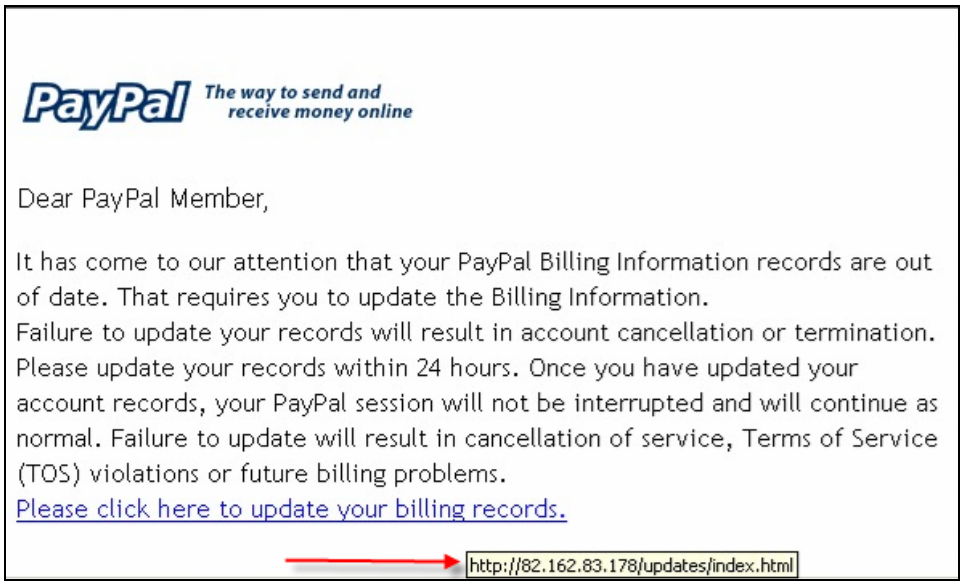
It has come to our attention that your PayPal Billing Information records are out of date. That requires you to update the Billing Information.
Failure to update your records will result in account cancellation or termination.
Please update your records within 24 hours. Once you have updated your account records, your PayPal 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.
Please click here to update your billing records.

Looks pretty official, doesn't it?

Well, it isn't – and clicking on the link, as the e-mail suggests, could cause serious harm.

How do we know this is a fake? Luckily, there are **two simple and quick ways to immediately detect an insincere attempt to contact you**.

1. As noted above (Tip #2) PayPal will NEVER address you by "PayPal Member." They will only use the registered name on your account.
2. All you have to do is move your mouse over the link and look to see what the actual web address is that you will be directed to (see below).



PayPal The way to send and receive money online

Dear PayPal Member,

It has come to our attention that your PayPal Billing Information records are out of date. That requires you to update the Billing Information.
Failure to update your records will result in account cancellation or termination.
Please update your records within 24 hours. Once you have updated your account records, your PayPal 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.
Please click here to update your billing records.

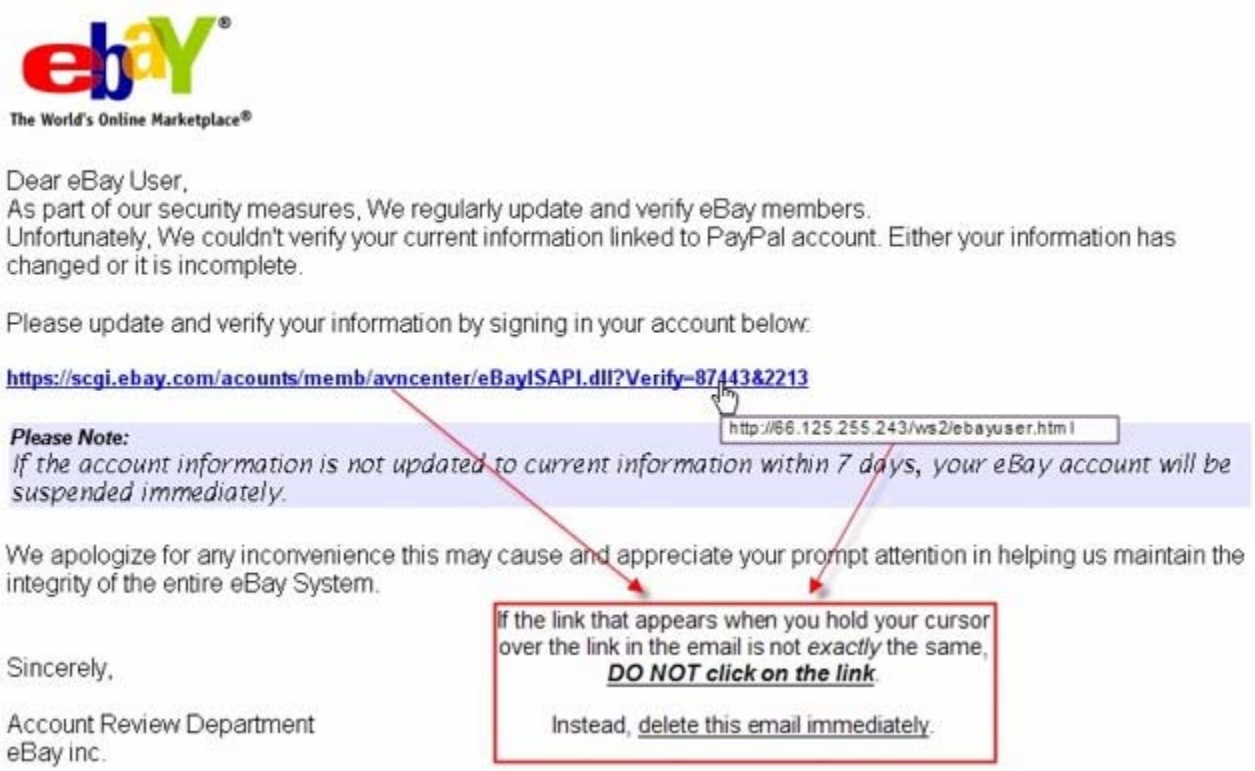
http://82.162.83.178/updates/index.html

When you move your cursor over the link in the e-mail, the actual link (in the box above) you will go to if you click on this link will appear. As you can see, this link contains numbers (82.162.83.178) and not what you would expect to see if this was really coming from PayPal (e.g., www.paypal.com)!!

If you ever see an actual link that does not match the printed link in the e-mail, **DO NOT CLICK ON THAT LINK**. Delete the e-mail immediately. Just viewing the email will not harm your computer—but clicking on the link would probably result in malicious software being loaded onto your computer without your knowledge.

Example 2

Here is another example of an official looking e-mail supposedly coming from Ebay:



Here again you see the two sure signs of a fake e-mail: (1) Being addressed by the generic "Dear eBay user" and (2) the actual links being different from those printed in the e-mail.

If you do receive similar e-mails, or any e-mail that you think may be fraudulent, please forward to *FraudWatch International* at: scams@fraudwatchinternational.com.

Conclusion

Seven Tips to Protect Yourself from e-mail scams:

1. **Never click on links within e-mails**. Instead, copy and paste them into your browser.
2. Use SPAM Filter Software
3. Use Anti-Virus Software
4. Use a Personal Firewall
5. Keep all your operating software and web browsers updated
6. Only enter personal information on web sites with an "**https:**" address and the **padlock icon** displayed which indicates the information you enter is secure
7. Keep your computer clean from Spyware

For More Information

For more information on protecting yourself from internet fraud, please visit *FraudWatch International's* website at http://www.fraudwatchinternational.com.