Ebay Ebook Success Tips: Avoid Spoof Emails!!!

Author:
Resale Rights

Created On: 14 Oct 2009 11:37 AM

One of the things I have noticed as I have increased my sales volume on eBay is the increased volume of spoof emails I have received claiming to be eBay or PayPal.Â They do this to try and gain access to your eBay or PayPal account, and sometimes even to try and get your bank details.Â I therefore felt that my next article should be on spotting and avoiding spoof email as it will surely be a problem that all you ebook sellers are going to have to deal with too.
Spotting spoof email can initially be quite tricky.Â After all the address appears to be a PayPal or eBay one and the often use eBay and PayPal graphics to make the emails look even more authentic.Â However, once you have had a reasonable amount of spoof email come your way, you soon realise that they all generally stick to the same format.Â Below are some of the most common spoof emails.
1) **Ebay / PayPal Account Suspension**:- These claim that your account will be suspended by a certain date if you do not take action.Â Some look more genuine than others.Â They ask you to click a link which directs you to a false eBay login screen where the spoof company then tries to steal your eBay Username and Password.Â These are relatively easy to spot because you are unlikely to receive an email on this subject from eBay or PayPal unless you have committed a serious violation of policy.Â Even if you believe you have been suspended it's always best to be safe and logon to eBay manually through your internet browser.
2) **Ebay / PayPal Unauthorised Access**:- These claim that someone has been making attempts to access your account from another IP address.Â Some even give false IP addresses and locations from where your eBay account was apparently accessed.Â These are obvious spoof emails because the fact that you have accessed your account from a different IP address does not constitute someone else trying to access your account.Â It could simply be you accessing your account from a different computer.
3) **Unpaid Item Reminder**:- These send you an unpaid item reminder for an item you haven't even purchased.Â For example a few days ago I received one for a $2000 camera.Â Surely I wouldn't forget if I had purchased an item like that.Â If you click on the links in this email you are directed to a false eBay page which tries to steal your eBay Username and Password.
4) **Question about Ebay Item**:- These are one of the trickier spoof emails as it is likely that you do receive questions about the item.Â Some even have an eBay ID link embedded in the email so that they look more authentic.Â However, most of the spoof emails do not state which eBay item the query concerns.Â Furthermore, the questions often do not make much sense and include phrases such as "How much is your last item?"Â The best way to make sure you do not get caught out is to log into eBay manually and then answer the question through my messages.
5) **PayPal payment Sent**:- These spoof emails again look a little more genuine.Â They claim that an unauthorised PayPal attempt has been sent.Â I received one today saying that I had sent $400 without my knowledge.Â They then have a link saying if you did not authorise this payment "Click Here" which then leads you to a spoof PayPal page where they try to get your User ID and

Password.Â However, when you make a genuine PayPal payment they do not usually mention anything about it being unauthorised.Â If they did suspect it to be unauthorised they would probably just hold the payment.
6) **Ebay PowerSeller Confirmation**:- I received a couple of these before I actually was made a PowerSeller.Â They do look genuine but instead of directing you to eBay to enter your Username and Password you are directed to a spoof website.Â The best way to make sure the email is genuine is to go to the eBay PowerSeller page and login at http://pages.ebay.com/services/buyandsell/powersellers.html.Â If the email is genuine you will be recognised as a PowerSeller here.Â If you are not then you know the email is spoof.
Beware that this is only some of the spoof email subjects you may receive.Â The people who write them will always be thinking of new ways to steal your ID and Password and as a result new spoof emails are surfacing all the time.Â Below is a list of the common things to look for in emails to identify them as spoof.
1) **Ebay ID / PayPal Name:-** If the email addresses your either by your eBay User ID or your actual name it is much more likely to be genuine.Â Most spoof emails simply address you as the email address to which the email has been sent.Â For example a genuine email from eBay is likely to say "Congratulations ebookcavern..." whereas a spoof email is likely to say "Congratulations sales@yoursite.com
2) **From Email Address**:- Although this is not a dead certain way of identifying spoof email on some it is noticeable.Â The spoof emails will claim to be from eBay or PayPal and in a large majority of them when you check this out the email address looks genuine.Â However, some of the from email addresses do not look so genuine.Â For example I recently received a spoof email claiming to be from the PayPal address: service@paypal.comservicepaypal.com which made it pretty clear that this email was spoof.
3) **Excessive use of eBay / PayPal images**:- Many of the spoof emails in an attempt to look genuine use eBay or PayPal images in the email.Â However, some use excessive amounts of these and when compared to a normal email from eBay or PayPal and so can be easily identified by this.
4) **The Hyperlink**:- This is the link that the email is trying to get you to click on.Â It is also the best way of identifying whether the email is spoof or not.Â If you scroll over the link or right-click and view the properties you should find out what the actual link is.Â If this link is not part of a PayPal or eBay domain then you can be sure it is spoof.
If you identify an email as spoof using the above criteria then you must not click on any of the links inside it.Â If it is an eBay spoof email forward it to spoof@ebay.com and if it is a PayPal spoof email forward it to spoof@paypal.com and then delete it.Â Remember it is always better to be safe then sorry so take precautions such as logging into eBay and PayPal manually through your internet browser and regularly changing your password.Â You can also read eBay's guide to spoof email at http://pages.ebay.co.uk/help/confidence/isgw-account-theft-spoof.html.Â Stay safe and Good Luck!!!