Title:
Protect Your Online Accounts from Phishing Scams

Word Count:
758

Summary:
Phishing involves the sending of an e-mail falsely claiming to be from an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security number, and bank account numbers.

Keywords:
phish,phishing,paypal,ebay,scams,identity,theft

Article Body:
What is phishing? Phishing involves the sending of an e-mail falsely claiming to be from an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security number, and bank account numbers. It is relatively simple to make a Web site look like the legitimate site by mimicking the HTML code or by framing parts of the pages.

Many people fall victim to email scams designed to steal log-in information for accounts such as PayPal, eBay, online banking accounts and more. Scammers send emails to every address they can obtain so you may receive these even if you dont have an account with the targeted enterprise, site or company.

The scam emails keep getting better and better in their appearance. You may receive an email that pretends to be sent from eBay. The email will have all the appropriate logos and will often be formatted in the same way. The links within the email can even appear to be directed to legitimate pages within eBay.

For example, e-mails supposedly from eBay claim that the user's account is about to be suspended unless they clicked on the provided link and updated the credit card information.

Recently I received an email claiming to be from PayPal. It appears to be a

receipt for an eBay purchase that I know nothing about. The subject line is "Receipt for Your Payment"

The body of the email included a description of the ebay item that had allegedly been purchased using my PayPal account. Below that was a notice that said:

Note:
If you haven't authorized this charge, click the link below to dispute transaction and get full refund

I wonder how many people receiving a similar email would quickly click on the link provided in order to contest the charges.

OK, I know to be cautious with this sort of thing so I did not click on anything in the email. Instead I went to PayPal on my own and logged in. Guess what? There is no record there of the purchase!

Then I started looking at the formatting of the email. When I viewed the properties of the message I found that it was actually from a takethatfanclub.com sender and NOT paypal. Just because it says that it is from such and such.com at the top of the email doesn't always mean that is who it is from. The "From" name in an email can easily be altered.

This email was formatted more like a received payment PayPal email than it was an actual receipt. I looked at all of my other emails titled "Receipt for your payment" and not one of the others was formatted like this one.

Other types of scams that involve PayPal usually involve a message about unauthorized access attempts. The sender will tell you that someone has tried to get into your account. As a result your account is in danger of being "frozen". However if you click the link in the email (You are told) you will be able to enter your password to avoid the loss of your account. Naturally, those unfortunate enough to give their log in information will have given it to strangers.

Remember that this is not limited to PayPal. Users of Storm Pay, e gold, eBay and more will see similar emails.

Watch out for scams like this that are designed to trick you into submitting information (like passwords) to allow the sender to access your account. Whenever you receive any suspicious messages go to your account via a new browser and by typing in the url. Never click a link in an email that is supposed to take you to your PayPal account. If you make that the rule then your

account information (and funds!) will be much safer.

If you believe that you have provided sensitive financial information about yourself or any accounts through a phishing scam, you should:

- Contact your financial institution or account immediately

- Contact the three major credit bureaus and request that a fraud alert be placed on your credit report.

Bureaus and phone numbers are:
Equifax - 1-800-525-6285
Experian - 1-888-397-3742
TransUnion - 1-800-680-7289

- File a complaint with the Federal Trade Commission at www.ftc.gov or call 1-877-382-4357

- You can also contact the Internet Crime Complaint Center at www.ifccfbi.gov if you think you have been a victim of a phishing scam.