

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

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

Many people fall victim to email scams designed to steal log-in information for accounts such as eBay, PayPal, and

The scam emails keep getting better and better in their appearance. You may receive an email that appears to be from a

For example, e-mails supposedly from eBay claim that the user's account is about to be suspended unless you click on a link

Recently I received an email claiming to be from PayPal. It appears to be a receipt for an eBay purchase. The email

The body of the email included a description of the eBay item that had allegedly been purchased. The email also included a link to

Note:

If you haven't authorized this charge, click the link below to dispute transaction and get full refund. I wonder how many people

I wonder how many people receiving a similar email would quickly click on the link provided in the email. I know to be cautious with this sort of thing so I did not click on anything in the email.

OK, I know to be cautious with this sort of thing so I did not click on anything in the email. Then I started looking at the formatting of the email. When I viewed the properties of the message, I noticed that the email was formatted more like a received payment PayPal email than it was an actual receipt. Other types of scams that involve PayPal usually involve a message about unauthorized access and a link to a website. 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 your credit card number). If you believe that you have provided sensitive financial information about yourself or any accounts, take the following steps:

Then I started looking at the formatting of the email. When I viewed the properties of the message, I noticed that the email was formatted more like a received payment PayPal email than it was an actual receipt. Other types of scams that involve PayPal usually involve a message about unauthorized access and a link to a website. 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 your credit card number). If you believe that you have provided sensitive financial information about yourself or any accounts, take the following steps:

This email was formatted more like a received payment PayPal email than it was an actual receipt. Other types of scams that involve PayPal usually involve a message about unauthorized access and a link to a website. 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 your credit card number). If you believe that you have provided sensitive financial information about yourself or any accounts, take the following steps:

Other types of scams that involve PayPal usually involve a message about unauthorized access and a link to a website. 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 your credit card number). If you believe that you have provided sensitive financial information about yourself or any accounts, take the following steps:

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 your credit card number). If you believe that you have provided sensitive financial information about yourself or any accounts, take the following steps:

Watch out for scams like this that are designed to trick you into submitting information (like your credit card number). If you believe that you have provided sensitive financial information about yourself or any accounts, take the following steps:

If you believe that you have provided sensitive financial information about yourself or any accounts, take the following steps:

- 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

This is a demo version of txt2pdf v.10.1
Developed by SANFACE Software <http://www.sanface.com/>
Available at <http://www.sanface.com/txt2pdf.html>