IT Services Security Announcement

Subject: Phishing e-mail
The IT Services team would like you to be aware of false emails designed to obtain your personal login information for the purposes of making fraudulent purchases using your credit card that you have on file with services like Amazon, eBay and alike. Below are two examples of such an email.

Dear valued customer

We regret to inform you that your account at eBay could be suspended if you don't update your billing information. To resolve this problem please click here <http://61.185.198.181/.eBay/> and login to your account in order to resolve the update process. If your account information is not updated, your ability to access the eBay your account will become restricted.

As per the User Agreement, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information that you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the enrolling of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Dear Amazon member,

Due to concerns we have for the safety and integrity of the Amazon community we have issued this warning.

Per the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Please follow the link below:

http://www.amazon.com.rbaccess.cn/?/exec/obidos

and update your account information.

We appreciate your support and understanding, as we work together to keep Amazon market a safe place to trade.

Thank you for your attention on this serious matter.

Regards,
Amazon Safety Department

If you receive similar e-mails to these asking you to click on a web link, and enter private and confidential information, don’t event if the page that appears might have official logos, and look
like a financial institution or even a government organization. In many cases they appear to be identical to the real web site. Call your institution or individual, with previously known contacts, to confirm they have sent the e-mail. Never follow links in e-mail messages unless you are absolutely confident of the sender. Financial institutions and government organizations will not ask you to enter private information on a web page that was followed from an e-mail. Most official e-mails will not contain run-on sentences, misspellings, slang or disparaging comments, and will be easy to read.

**What is “Phishing”** - The act of sending an e-mail or Instant Message (IM) to a user falsely claiming to be 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 or IM directs the user to visit a Web site where they are asked to update personal information, such as passwords, credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is counterfeit and set up only to steal the user’s information. Please protect personal and company information. The act of “phishing” is a criminal attempt to steal private information.

Other variations of the subject or sender may also appear, but the message will be similar.

- Do not click on any of the link(s) within the e-mail message.
- **Promptly delete the message.**