ASIAN BANK
亞洲銀行

How to Avoid Phishing

What is "Phishing"

The act of sending an e-mail 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 directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has. The web site, however, is bogus and set up only to steal the user's information.

About Credit Card Phishing

You may receive an email or phone call from someone claiming to be from a legitimate credit card company and asks cardholders to reactivate their cards by providing account information and then creating a new password. The caller may also state that if the cardholder does not comply, the account will be suspended indefinitely. Usually, a legitimate credit card company will never ask cardholders to divulge account information, passwords or the three digit code on the back of the credit card via email or phone. Should you receive any questionable emails or phone calls asking for personal and confidential information such as passwords or account numbers, please DO NOT reply or respond to the web site referenced in the email. Contact the credit card company for verification and more information.

How to Tell if an E-mail Message is Fraudulent

Here are a few phrases to look for if you think an e-mail message is a phishing scam.

"Verify your account."
Businesses should not ask you to send passwords, login names, Social Security numbers, or other personal information through e-mail. If you receive an e-mail from a company asking you to update your credit card information, do not respond.

"If you don't respond within 48 hours, your account will be closed."
These messages convey a sense of urgency so that you'll respond immediately without thinking. Phishing e-mail might even claim that your response is required because your account might have been compromised.

"Click the link below to gain access to your account."
HTML-formatted messages can contain links or forms that you can fill out just as you'd fill out a form on a web site. The links that you are urged to click may contain all or part of a real

company's name and are usually "masked", meaning that the link you see does not take you to that address but somewhere different, usually a phony web site.

Tips on How to Avoid Phishing

- If you receive an unexpected e-mail saying your account will be shut down unless you confirm your billing information, do not reply or click any links in the e-mail body.
- Before submitting financial information through a web site, look for the "lock" icon on the browser's status bar. It means your information is secure during transmission.
- If you are uncertain about the information, contact the company through an address or telephone number you know to be valid.
- If you unknowingly supplied personal or financial information, contact your bank and credit card company immediately.
- Suspicious e-mails can be forwarded to uce@ftc.gov, and complaints should be filed with the state attorney general's office or through the Federal Trade Commission at www.ftc.gov.
- Beware of Internet fraud. The Bank will never request confidential information through e-mail.
- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

Exercise your rights to review your credit record and report fraudulent activity. To order your free annual credit report from one or all the national consumer reporting companies, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

For more information about the steps to take on obtaining your credit report, contact the credit bureaus listed below:

- Equifax: (800) 525-6285 or www.equifax.com
- Experian: (888) 397-3742 or www.experian.com
- TransUnion: (800) 680-7289 or www.transunion.com