Fraud Alert E-Mail "Phishing"

Don't Take the Bait: Protect Yourself against E-Mail "Phishing"
"Phishing" is the latest and fastest growing form of information theft. The process is called "phishing" because it uses e-mail lures and scare tactics to "fish" for sensitive personal information- including passwords, credit card numbers, and account information- from a wide "sea" of unsuspecting customers. One e-mail phishing expedition can potentially reach millions of Internet users.

How does phishing work?

You receive an unexpected e-mail that has been forged so it looks like a legitimate e-mail from a particular organization (such as MegaBank). The e-mail usually tricks you into providing sensitive personal information that can be used for identity theft such as account details, ATM PIN by replying e-mail or directing you to a website that is a fraudulent, and often convincing, duplication of company's official website. The e-mail may scare you by saying "your account has been frozen," "your credit card has been cancelled," "we are updating our software, please confirm your data," or any number of other creative ploys. Unsuspecting people who fall victim to these ploys send their personal information and the phishers, in turn, commit identity theft and other fraudulent activities, such as withdrawing your money or using your credit at their leisure.

How can you be sure that you're dealing with MegaBank and not an imposter?

MegaBank will never send you an e-mail asking for your passwords, credit card numbers, or other sensitive information. If you're required to enter personal information to perform a transaction, it's always done on a site secured with SSL technology— you can tell because there'll be a padlock icon at the bottom of your screen. Most importantly, if you click on the padlock, a security certificate will pop up. In it, there's a section that says "Issued to:". If it's really a MegaBank website, the URL will end with "MegaBank.com".

How can you protect yourself against a phishing attack?

If you need to go to your online banking service, use your own tried and trusted

method. Use your own link in your Internet "Favorites" or by typing the URL directly into your browser’s address bar.

Leave suspicious sites. If you suspect that a website is not what it purports to be, leave the site immediately. Do not follow any of the instructions it presents.

Don't reply to any e-mail that requests your personal information. Be very suspicious of any e-mail from a business or person that asks for your password, account number or other highly sensitive information-- or one that sends you personal information and asks you to update or confirm it.

Open e-mails only when you know the sender. Be especially careful about opening an e-mail with an attachment. Even a friend may accidentally send an e-mail with a virus.

Be careful before clicking on a link contained in an e-mail or other message. The link may not be trustworthy.

Do not send sensitive personal or financial information unless it is encrypted on a secure website. Regular e-mails are not encrypted and are more like sending a post card. Look for the padlock symbol on the bottom bar of the browser to ensure that the site is running in secure mode BEFORE you enter sensitive information.

Be aware! Phony "look alike" websites are designed to trick consumers and collect their personal information. Make sure that websites on which you transact business post privacy and security statements, and review them carefully.

Monitor your transactions. Review your order confirmations, credit card, and bank statements as soon as you receive them to make sure you're being charged only for transactions you made. Immediately report any irregularities in your MegaBank accounts.

Act quickly if you suspect fraud. If you believe someone is trying to commit fraud by pretending to be MegaBank, please contact us immediately at MEGA Call Center or Leave message to us,

Tel: 0800-016-168

Leave message at: https://www.megabank.com.tw/webitem/contact.asp