



## Security Notice: Phishing Scam, Sept. 29, 2008.

A phishing scam is now targeting end users by sending e-mails that appear to be from official Digital Insight sources or from financial institutions. The scam is designed to trick recipients into clicking a link in the fraudulent e-mail for the purpose of acquiring sensitive data, such as passwords or financial information.

The most common example we have seen includes the following:

Subject: Attention - Important Customer Information

Body: As a [*Name of Financial Institution*] customer, your privacy and security is a primary task for us. We have been dedicated to customer safety and protection and our mission remains as strong as ever. We inform you that your Net Banking account is about to expire. It is strongly recommended to update it immediately. Update form is located here: [LINK]

### Please note the following:

- Digital Insight systems have not been breached in any way. Your information is still safe.
- Recipients of these e-mails are not specific to DI financial institutions' end users. Phishing e-mails can be sent to anyone who has an e-mail address on the Internet. If your end users receive phishing e-mails, that does not mean that someone has a list of your end users.
- We are currently working to shut down the sites that these phishing e-mails link to. Please do not click the link in this particular e-mail. If you are trying to identify the URL for reporting purposes, we recommend that you use your mouse to hover over the link.
- Some of the false e-mail addresses that users have reported include:
  - customer-support@digitalinsight.com
  - admin@support.digitalinsight.com
  - admin-support@digitalinsight.com
  - customer-care@digitalinsight.com
  - accounts@digitalinsight.com
  - support@update.digitalinsight.com
  - administration@digitallnsight.com

### Remedies

Should you believe you have shared critical account information (passwords, etc.) with a fraudulent entity; please contact National Bank immediately. We will change your login identification and passwords to prevent illegitimate attempts from accessing your accounts.

### Support

If you have questions about this, or wish to report what you believe to be a phishing incident, please contact your local branch office or Customer Service: 800-717-3991.