

BEWARE OF PHISHING EMAIL SCAMS

Phishing is the name given to the practice of sending emails at random purporting to come from a genuine company operating on the Internet (typically a bank), in an attempt to trick individuals into disclosing information at a bogus website operated by fraudsters.

These emails are sent in the hope of reaching the email address of a customer with an account at the bank being targeted, and usually claim that it is necessary to "update" or "verify" your customer account information by urging people to click on a link from the email which takes them to the bogus website. Any information entered on the bogus website will be captured by the criminals for their own fraudulent purposes.

The key thing is to be suspicious of all unsolicited or unexpected emails you receive, even if they appear to originate from a trusted source. Stop to think about how your bank normally communicates with you and never disclose your password in full or personal information.

Remember:

- ◇ Banks will never email you to request that you "confirm" or "update" your password or any personal information by clicking on a link and visiting a web site.
- ◇ Treat all unsolicited emails with caution and never click on links from such emails and enter any personal information.
- ◇ Never log-on to your online banking account by clicking on a link in an email. Open your web browser and type the bank's address in yourself.
- ◇ If you are in any doubt about the validity of an email purporting to come from a bank, contact the bank on an advertised phone number. If you have questions about any of these suggestions, if you think that you may have disclosed information to a fraudulent site, please contact your Private Banker at (617) 912-1900.