WESTFIELD BANK – PROTECTING YOU AND YOUR MONEY
SECURITY AND FRAUD INFORMATIONAL SERIES:
PHISHING

Phishing is a common tactic used by fraudsters to gain your personal sensitive information including usernames, passwords, credit and debit card numbers etc. in order to steal money from you. In this second edition of Protecting You and Your Money we examine popular Phishing attacks and present you with tips to help prevent you and your company from becoming a victim of fraud.

How it occurs - examples:

- You receive an email that a friend has sent you an "e-card". When you click on the link a virus is downloaded to your computer.
- You receive an email from a shipping company to confirm the shipping details – once again a virus is downloaded to your computer.
- You receive an email from your bank that your debit card info or online banking credentials are compromised and ask you to confirm your information. HINT: most banks WILL NOT contact you in this manner – the bank already has this information!!

Recent Example email:

From: Protection [mailto:protection@fdic.gov]
Sent: Thursday, September 29, 2011 7:22 AM
To:
Subject: ACH and Wire transfers disabled
Importance: HIGH

Dear Client,
Your account ACH and Wire transactions have been temporarily suspended for your security due to the expiration of your security version. To download and install the newest updates, follow this link.
As soon as it is set up, your transaction abilities will be fully restored.

Best regards, Online Security Department, Federal Deposit Insurance Corporation

How to protect yourself:

- Do not click on links or attachments in unsolicited emails
- Verify the validity of emails directly with the sender
- Make sure your anti-virus and anti-spyware software is up to date
- Be cautious when asked to provide your personal information online

If you think your account information has been compromised, please contact Westfield Bank immediately at 1-413-568-1911.