OFFICE OF THE FIRST DEPUTY SUPERINTENDENT **18 October 2006**

Don't Get Hooked by a "Phishing" Scam

- "Phishing," is defined by the Federal Trade Commission as "a high-tech online scam that uses spam or pop-up messages to deceive consumers into disclosing their credit card numbers, bank account information, Social Security numbers, passwords, and other sensitive (personal) information via email."

- **Do not email personal or financial information**. Email is not a secure method of transmitting personal information. Look for indicators that the site is secure like a lock icon, or a URL for a website that begins with "https:" (that stands for "secure"). Unfortunately, no indicator is foolproof; some phishers have forged security icons.

- If you receive an email warning you that an account of yours will be shut down unless you reconfirm your billing information, or you are sent emails or pop-up messages from a business or organization that you may deal with asking you to "update," validate," or "confirm" your account number, **do not reply or click on the link in the email**. Instead, contact the company using a telephone number or website address you know to be genuine.

- Review credit card and bank account statements as soon as you receive them to check for 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.

Direct any inquires relative to this correspondence to the Senior Services Section, at 312-745-5141.