



# eninsula Detachment Crime Alert

## **5/16/08 – Protect Yourself from Scams**

Hang on to your dollars by watching for these scams circulating in our area:

### **#1 Income Tax or Stimulus Rebate Payments**

The target individual is notified of either an unclaimed tax refund or problems processing the tax stimulus payment. Bank account information is requested under the premise the Internal Revenue Service (IRS) can only direct deposit the forthcoming money. If the target individual refuses to provide bank information, threats ranging from being unable to refuse money from the IRS to time in prison for not cooperating with someone from the government.

*The IRS does not force taxpayers to use direct deposit. They will rely on information provided via the individual's most recent tax return to determine if an individual has selected direct deposit or a physical check. The IRS will not contact the taxpayer to verify this information. To file a report about a questionable phone call, email or letter you have received you may contact the IRS at [phishing@irs.gov](mailto:phishing@irs.gov) or 1-800-829-1040.*

### **#2 Foreign Lottery Prize**

The target individual receives an email, letter or phone call announcing a guaranteed prize to be awarded to the individual. Account information is then requested to deposit the prize. In some instances, the target individual is asked to pay for taxes up front or to process the prize money.

*If you are a prize winner in any contest, you are not required to pay for processing of the prize or for taxes up front. In most contests, you are not required to disclose your banking information to receive your prize.*

### **#3 Identity Theft Prevention Products**

An announcement for a bank-supported security program is emailed to the target individual, which may or may not have an account with the specific

bank. The email will proclaim the program to be secure, to detect threats targeted to the individual and provide statistics showing the program works. A link is embedded in the email which directs the user to an unauthorized webpage requesting account information.

*Most businesses will not send an email to an account holder requesting account information or to verify security information. If you receive an email from a business you have an account with, contact the business using information you have used previously, such as a branch office or phone number, to verify the request. Do not click on any link embedded in the questionable email.*

#### **#4 Hitman Threat**

An email is sent declaring the target individual to be the subject of an assassination plot. The sender offers to accept payment from the target to spare the target's life. A threat is usually included in an attempt to keep the target from reporting the email to local police or the Federal Bureau of Investigation (FBI). The FBI has also received reports of follow-up emails being sent to the target to inform request the target's assistance in prosecuting a person arrested for emailing the initial threat.

*This scam is not only designed to take money from the victim, but to intimidate and play on the fears of the target individual. If you receive an email similar to the one described above, you may report it to the FBI's Internet Crime Complaint Center (IC3) at [www.ic3.gov/complaint](http://www.ic3.gov/complaint) or the Seattle FBI office at 206-622-0460.*