Recently, the Mt. Vernon Police Department has received several complaints concerning different types of scams. Some of the victims have received scam mailings through the U.S. Postal Service while others have received fraudulent e-mails. It was felt that an informational letter might help educate citizens on how to recognize these scams and protect themselves from becoming victims.

- **Know who you're dealing with.** If the seller or charity is unfamiliar, check with your state or local consumer protection agency and the Better Business Bureau. Some Web sites have feedback forums, which can provide useful information about other people's experiences with particular sellers. Get the physical address and phone number in case there is a problem later.
- **Be aware that no complaints is not a guarantee.** Fraudulent operators open and close quickly, so the fact that no one has made a complaint yet doesn't meant that the seller or charity is legitimate. You still need to look for other danger signs of fraud.
- **Don't believe promises of easy money.** If someone claims that you can earn money with little or no work, get a loan or credit card even if you have bad credit, or make money on an investment with little or no risk, it's probably a scam.
- **Understand the offer.** A legitimate seller will give you all the details about the products or services, the total price, the delivery time, the refund and cancellation policies, and the terms of any warranty. For more information about shopping safely online, go to *www.nclnet.org/shoppingonline*.
- **Think twice before entering contests operated by unfamiliar companies.** Fraudulent marketers sometimes use contest entry forms to identify potential victims.
- **Be cautious about unsolicited emails.** They are often fraudulent. The best approach may simply be to delete the email.
- **Beware of imposters.** Someone might send you an email pretending to be connected with a business or charity, or create a Web site that looks just like that of a well-known company or charitable organization. If you're not sure that you're dealing with the real thing, find another way to contact the legitimate business or charity and ask. Never click on a link to a website that is listed in an unsolicited e-mail.
- **Guard your personal information.** Never provide your credit card or bank account number unless you are actually paying for something and you are using a secure connection on a known website. Your social security number should not be necessary unless you are applying for credit. Be especially suspicious if someone claiming to be from a company with whom you have an account asks for information that the business should already have.
- **Beware of "dangerous downloads."** In downloading programs to see pictures, hear music, play games, etc., you could download a virus that wipes out your computer files or connects your modem to a foreign telephone number, resulting in expensive phone charges. Only download programs from Web sites you know and trust. Read all user agreements carefully.
- **Pay the safest way.** Credit cards are the safest way to pay for online purchases because you can dispute the charges if you never get the goods or services or the offer was misrepresented. Federal law limits your liability to $50 if someone makes unauthorized charges to your account, and most credit card issuers will remove them completely if you report the problem promptly.

Nigerian Money Scams

- **Be aware that these scams are well-known.** They used to be called “Nigerian letters” because they came by mail, but now these messages also come by phone, fax, or email.
- **These promises are never true.** The purpose of the scam is to get money out of your bank account, not to put money into it.
- **Be wary of offers to send you an “advance” on your “commission.”** Some con artists use this ploy to build trust and to get money from your bank. They send you a check for part of your “commission,” instructing you to deposit it and then wire payment to them for taxes, bonding, or some other phony purpose. The bank tells you the check has cleared because the normal time has passed to be notified that checks have bounced. After you wire the money, the check that you deposited finally bounces because it turned out to be an elaborate fake. Now the crooks have your payment, and you’re left owing your bank the amount that you withdrew.
- **Never provide your bank account or other financial information.** This information can be used to withdraw money from your account.
- **Don’t agree to travel anywhere to meet these people.** They avoid coming to the United States because they fear arrest. Instead, they sometimes try to lure victims to meet them in Africa or other countries. Victims have been robbed and even murdered.
- **If they get your money, you’ll never get it back.** It’s very difficult to bring these crooks to the United States for trial, and action is rarely taken against them in their own countries. However, it’s still helpful to report actual or attempted Nigerian money offer scams to law enforcement agencies.

eBay Scams

What usually happens with this type of fraud is that a registered ebay member receives a fraudulent e-mail which states, "We regret to inform you that your eBay account has been suspended due to concerns we have for the safety and integrity of the eBay community." The email goes on to state that the recipient has breached a user agreement and is prohibited from using eBay, including registering for a new account. It then requests the eBay customer go to a website to give personal information so they reinstate the account. "If you feel you have been suspended in error or want to appeal this decision by providing additional information, please click here," it reads before giving a link. The email received comes from the address: eBay@reply3.ebay.com. The letter is signed, "eBay Trust and Safety." Again, **never** click on a hypertext link listed in an e-mail. This will not direct you to the legitimate eBay site. It will direct you to a look-alike site. The site will ask you re-enter your personal and financial information. The criminal will then have your personal information as well as your banking and credit card numbers. This is commonly referred to a "phishing."