DOVER POLICE GUIDANCE ON FRAUD AND IDENTITY THEFT

Today's con artists design their fraud scams to target unsuspecting persons through sophisticated means, often with the use of modern technology. Criminals know that it is very possible, and at times extremely easy, to take advantage of honest, well-meaning people. In order to enable town residents to recognize a fraud scam the Dover Police Department offers the following preventative tips.

Most fraud scams that specifically target residents via the internet or telephone are designed to obtain either money or personal identity information of the intended victim. Such scams seek to have monies wired to the criminal, to obtain credit account numbers, or identity information such as a Social Security number.

- Any mail received, internet e-mail, or even a telephone call that indicates a resident is a winner of any type of sweepstakes or foreign lottery where some type of monetary fee is required to be paid is an outright scam. If you did not enter any sweepstakes nor participated in any foreign lottery, there is no way you can be a winner. Whenever fees are required to be paid in advance in order to collect the supposed prize, it is a scam to con you out of money.

- If you are selling an item over the internet or you advertise some type of service that you perform, be wary of persons who contact you wanting to purchase those items or pay for those services with a check for an amount greater than you sought. This scam specifically wants the intended victim to believe that the check was made out in the inflated amount by accident and will attempt to have the victim wire any monetary difference before the actual check is discovered to be counterfeit. The suspects will always be out of state or in a foreign country but will claim to be in the process of moving into the Dover area. The scam targets persons selling any item from a car to a couch or offering services from babysitting to piano lessons. Craig's List, which is a credible service, is specifically targeted by people engaged in this type of scam.

- Do not give out personal information to callers who claim to be representatives of your bank or any business you may have a credit account with. The criminal may also pose as a law enforcement official with the call pretending to be some type of investigation into fraud on your account. This is done to con you into giving out a Social Security number or other personal information, usually after the caller insists you prove your identity. Remember that anyone who calls you should already know who you are and you do not have to give out confidential information in order to prove your identity. This same scam, known as "phishing" can also involve bogus e-mails purporting to be from a financial institution or governmental agency and is intended to con you into divulging your identity information.

- If you receive an email or a telephone call and it seems suspicious to you, go to your computer and "Google it". Most of these scams have been around for a

while, and if someone has been taken by a fraudulent company, you can very often find a blog or internet article that identifies the scam in detail. In the case with email scams, remember that companies such as Bank of America, Comcast, American Express, Visa, and just about every other company you can name will never send you an email asking for personal information or passwords. If you get an email from one of these companies and you think it is suspicious, simply call the company and ask for their security department.

- Many citizens enjoy social media sites such as Facebook. Facebook is a reputable and exceptionally good mechanism to interact with other people. Unfortunately, scam artists use Facebook to commit fraud. There are certain applications designed to have the victim provide access to the criminal's software, which is designed to do everything from hijacking your account to accessing your computer for personal information. If you use Facebook or any other social media, don't fall for messages that advise you that a Facebook friend wants you to run a certain "app", or participate in a survey, or provide any information about yourself. As mentioned above, if you have a doubt about an app or request just "Google it" to check its veracity.

- Another concern about Facebook is the posting of sensitive information that a criminal may use to exploit you. Avoid "friending" people that you do not know. When you "friend" someone, they now have access to pictures of you, your children, and sometimes the inside of your home. Pedophiles particularly enjoy the ability to access pictures of children from Facebook. Avoid posting unnecessary information on your status, such as "leaving the house now for the movies". This type of post informs a potential adversary that your house will be vacant for a couple of hours, and invites them to come over and burglarize your residence.

In short, to prevent falling for the myriad of fraud schemes, one old adage is as true today as it was years ago; if something seems too good to be true, it probably is.