

**Watchwords by Officer Tom Hanshaw**  
**December 10, 2010**

For Holiday shoppers, Monday November 29<sup>th</sup> was deemed, “Cyber-Monday” but for us at the Police Station it was “Cyber-CrimeDay.” I’m not sure if it was coincidental or a new twist on the annual event but officers took several reports that day alone dealing with online scams. Unfortunately, this seems to be a growing trend, despite warnings from law enforcement and consumer advocates. Although we live in a small community, the technology of today allows criminals from across the world to enter into our homes. The victims of these crimes vary in age, proving anyone can be targeted. These scams are sometimes very convincing and well executed, costing consumers thousands of dollars. Because the perpetrators often originate in other countries, the actual odds of recovering those losses are slim.

The scams last week ranged from bogus sweepstakes to requests for assistance and even e-mail claiming to be from the FBI. Many of the correspondences contained errors in grammar or used poor English, which is typically a good early warning sign. A couple mentioned foreign nations, such as Nigeria, which is always something to watch for. Sadly, in two incidents, the victims thought they were helping someone in need, a common scam especially at this time of year. Residents need to realize there are criminals out there seeking to capitalize on the generosity of others.

The first example reported concerned a request on “Craig’s List” for assistance this Holiday Season. The writer shared his story, saying he was recently laid off and was going to be unable to provide a Christmas for his family for the first time in many years. He asked for a donation of a Christmas Tree and gifts. Upon looking closer, the person who reported the incident to us noticed there were several similar postings online, by the same person who listed different towns as his home. Her thought was his intention was to collect donated trees and resell them. Certainly we are all familiar with the state of the economy and the true needs of so many. It’s important to realize there are many agencies in the area, such as the Holiday Program, Salvation Army, Pettingill House, Community Action and Our Neighbor’s Table, which are working hard to help those in need. Not every story on “Craig’s List” is fictitious but police recommend donations be made to groups having a record of actually providing help.

The second was a classic case of a Nigerian scam. The victim was contacted by e-mail and asked to help a father and his children in need. She initially sent a few hundred dollars and then asked to donate more before being contacted by another party, also in need. In the end, nearly \$3000 had been sent via Western Union. She actually got a \$2000 check in the mail and was asked to deposit it in her account. The check was drafted from a company in Babson MA, a city that doesn’t even exist. Upon researching where the money was claimed, she discovered it had been picked up in Nigeria. The victim in this case realized there was no chance to recover the lost money but hoped sharing the story would help prevent others from being victimized.

The next case of “cyber-crime” involved a bogus sweepstakes winner. The resident received a check in the mail for \$3000 as the first payment in his prize of \$250,000. He was asked to deposit the check and to send \$3000 back as “taxes” before he could claim the remainder of his winnings. Unfortunately, he did, thinking he was only returning the original money. It may take two or more weeks for a counterfeit check to be identified or cleared by the bank. Customers are responsible for the deposits made into an account, so if you deposit a bad check and then spend the money before it clears, you are responsible. In this case, the victim never even entered such a sweepstakes but truly believed he’d won and expected the delivery of the big check on Monday, which never came.

Lastly, e-mail from the Federal Bureau of Investigation would probably catch your attention. Especially if the content concerned money illegally brought into the Country with your name attached. The recipient of a “cyber scam” looked a little closer and discovered the return address was [fbi@live.com](mailto:fbi@live.com) obviously not a true government site. The correspondence went on to claim money had been delivered, there were terrorist connections and so on. The recipient was advised to complete an attached document and return it immediately, which was not done luckily. This is another example of “phishing,” where the criminal will attempt to gain personal and account information. Remember government agencies will not contact you to obtain information they already probably have.

As the week continued, there was even a story about counterfeit tickets for a Patriots’ game, which had been offered online. You’ve got to be more careful than ever when it comes to shopping online, as new scams “pop up” daily. I even got e-mail, allegedly from Microsoft, asking me to “upgrate” my mail account. I was asked to fill out a form, asking for my username, date-of-birth and even password. The first warning sign was seeing the word, “upgrate” in the subject field. Of course, no Internet server will ever make these types of requests. Don’t be afraid to drive along the Internet Highway, just pay attention to the signs you see along the way.