Community Crime Prevention Newsletter

Plymouth, MN Volume 2012 Number 4

Identity Theft and Fraud

Identity theft and ***fraud*** refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. It occurs when someone gains access to a person's basic information, including name, address, credit card or social security number, and uses that information. Identity theft and fraud affects millions of new victims each year. Criminals typically get a victim's information by theft (stolen purses, wallets, computers, cell phones, mail, employer/customer records), "dumpster diving", skimming credit cards, and all types of scams. While it is nearly impossible to eliminate all identity theft or fraud, there are simple ways to reduce your risk:

- ✓ Don't carry your social security card in your wallet or purse.
- ✓ When creating passwords and PINs, **don't** use anything that can be easily guessed, and don't write them down.
- ✓ Review bank statements and bills for fraudulent activity. Check your credit report for errors, too.
- ✓ Shred pre-approved credit offers and documents with personal information on them before recycling.
- ✓ Beware of "Shoulder Surfers" who record PINs to access your accounts.
- ✓ Do not mail bills from your home mailbox. Invest in a locking mailbox, too.
- ✓ Ask companies, doctors, etc. how they use, protect, and discard personal data and records.
- ✓ Maintain current virus protection software on computers, smart phones, and tablets, and use a firewall.

Common Scams

Phishing: Someone claiming to be from a company or government agency with an issue that you need to take care of right now.
Grandparent: Someone claiming to be a relative with an emergency. You can help by wiring money right now, but don't tell mom and dad!
Overpayment: Oops! Someone paid you too much. No problem, keep the check and simply send the rest back to them.
Nigerian Letter: Someone has millions of dollars and they need your help getting money out of another country…
Lottery: You won a lottery or sweepstakes and you just need to pay some fees to claim your prize.
Charity: False charities are often created after large tragedies.

Preventing Scams

- **NEVER** provide personal information to unsolicited phone calls or emails unless *you initiate the contact.* Don't click on links or open attachments in these emails. Use only official contact channels.
- Make all efforts to verify a story before sending money. Check with relatives, research charities, ask for second opinions. A good rule of thumb is *if someone asks you to wire money, it is a scam.*
- You cannot win a lottery, sweepstakes, or drawing you never entered, plus it is illegal to enter foreign lotteries.
- Never accept a check and agree to return the difference.
- Total strangers don't ask random people for help with millions of dollars.
- Bottom line: ***If it sounds too good to be true, IT IS!***

If you are a victim of identity theft, contact one of the 3 major credit bureaus (Experian: 888-397-3742, Equifax: 888-766-0008, or TransUnion: 800-680-7289) to place a fraud alert in your file. Contact all financial institutions with whom your information has been used fraudulently–by phone and in writing. Close affected accounts and obtain **new** account numbers. Be sure to keep detailed information and copies of all correspondence related to identity theft. Carefully monitor accounts for evidence of new fraudulent activity. File a report with your local police department and file a complaint with Federal Trade Commission (FTC), if needed. For more information about identity theft and fraud, contact the FTC at www.consumer.gov/idtheft.

Crime Free Multi-Housing (CFMH) Corner: Theft from Auto

Car break-ins can happen anywhere you park your car: at work, the gym, a restaurant, school-even at home. Rental community parking lots and garages can be attractive targets because they offer criminals access to many potential targets in a small area. Residents have the power to make a difference and reduce the chance of becoming a victim of a car break-in.

- ***Do not leave valuables in your car!*** Commonly stolen items from vehicles are GPS units, cell phones, purses, wallets, bags, laptops, tools, and electronics. If you must leave valuables in your car, lock them in the trunk before you reach your destination.
- Always lock your car.
- Report suspicious activity. Call 911 right away.

By removing valuables, locking your car, and reporting suspicious activity, you can help prevent theft!

Especially for Business: Be Prepared for Emergencies

Take the time *now* to make an emergency plan for your business.

- ✓ Have a plan for employees to follow for different types of disasters–flood, fire, active shooters, tornadoes, blizzards, pandemics, etc.
- ✓ Make sure employees are trained what to do in emergencies. Employees should also know where to find emergency plans and instructions.
- ✓ Develop a plan for business continuity in each situation. How will your business continue to function without power, employees, transportation, etc.?
- ✓ Create an emergency communication plan. Discuss how you will communicate if cell phones, land lines, or computers are down.

For more information on how to prepare for emergencies, go to www.hsem.state.mn.us or www.ready.gov.

Texting Restrictions:

It is illegal to text, use a GPS, or surf the web when you are driving, even if you are stopped in traffic!

Fraud Stop: Charity Scams

We continue to see charitable giving scams increase in times of tragedy. Recent events like Hurricane Sandy and the Newtown, Connecticut Sandy Hook school shooting in are no exception. Criminals use legitimate-sounding names, or even more despicable-use the names of tragedy victims, to solicit donations from the public via email, phone, mail, or in person. However, the money collected never reaches the intended recipient, or if it does, only a small percentage is given. **Make sure your contribution gets to those in need.** *Never* respond to unsolicited email, phone calls, or click pop-ups from charities asking for money. Think very hard before you give money to someone going door-to-door. It is best to contact charities directly through official channels. In addition, research the organization prior to contributing to know where your donation is going and how it will be used. Charities do need our help, but by taking a few precautions, you can make sure your money is going to support those in need, not lining the pockets of a criminal.

Featured Program: File of Life

What if there is a medical emergency and no one is around to let emergency personnel know what your medical history is or what your medications or allergies are? *What if a family member has Alzheimer's or dementia and they are unable to take care of themselves if their caretaker is transported to the hospital for a medical emergency? Who should police contact?* The File of Life program is a way to keep important medical information and contact information easily accessible to police and ambulance personnel in the event of a medical emergency. The File of Life packet is kept at home, on your refrigerator. Stop by the Plymouth Police Department during normal business hours or all 763-509-5147 to request **free** File of Life packets.

****

Emergency: **911** Non-emergency: **763-525-6210** CrimeStoppers: **800-222-TIPS**

If you have any comments about this newsletter, please contact Officer Angela Haseman at the Plymouth Police Department, 3400 Plymouth Blvd., Plymouth, MN 55447, 763-509-5147 or at ahaseman@plymouthmn.gov. Thank you!