TOWN OF MANLIUS POLICE DEPARTMENT

IDENTITY THEFT INFORMATIONAL SERIES

SERIES 2 | 04.27.2018

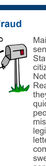
TOPICS

Mail Fraud

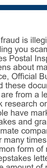
Dumpster Diving & Mail Theft

Eavesdropping & Shoulder Surfing

Pickpockets



Prevention Measures Quick Guide



A look at Series three

Mail Fraud

Mail fraud is illegitimate companies or people sending such scams through the mail. The United States Postal Inspection Service (USPIS) warns citizens about mailings that read "Important Notice, Official Business, or Open Immediately." Read these documents closely and determine if they are from a legitimate company. Do some quick research on the letter and see if other people have marked it as a scam. Spelling mistakes and grammar are a red flag, a legitimate company would have revised this letter many times before final approval. A common form of mail fraud is a phony sweepstakes letter indicating that you have won some amount of money. USPIS also warns about chain letters, which are get rich quick schemes. These letters solicit a monetary value and promise a substantial return. These letters are scams intent on taking your money and are illegal forms of gambling. According to the Deceptive Mail Prevention and Enforcement Act of 1999 a legitimate sweepstakes must: Provide the rules and an order form, state that no purchase is necessary, state that your chances of purchase do not improve your odds of winning, include all terms and conditions including rules and entry procedures must be listed, the sweepstakes sponsor contact information, must state your odds of winning the prize, the prize's value and payout information.

The range of different mail scams grows every day, here are just a few to be on the lookout for:

- Fake Inheritance Scam: demanding you to submit a fee to receive funds.
- Unsolicited Merchandise: claiming the "free" gift you received, you must pay for.
- Pen Pal scam: a romantic interest requesting you send them funds.
- Fake Health and Medical products: ads that claim things like, "Instant cure, ancient formula, miracle drug", that attempt to sell you fake products to obtain your personal identifying information.
- Secret Shopper Scams: a fake company sends you a bad check to cash at your local bank as payment.

If you are a victim of mail fraud call 911 to report it to your local authorities. You can also notify the USPIS by phone or email them of the mail fraud so that others may be aware of the scam. Call 1-800-ASK-USPS (1-800-275-8777) or go to:

https://postalinspectors.uspis.gov/contactUs/filecomplaint.aspx

Dumpster Diving & Mail Theft

Many types of legitimate pre-approval credit card mailings have your personal identifying information on them. Legitimate services such as medical bills, insurance bills, utility bills, credit card and bank statements have your account information on them and other personal identifying information. These mailings should be cross cut shredded so no one can steal them from your garbage. A cross cut shredder cuts paper into smaller bits not just strips, so that a thief cannot just put the strips back into order. A common method of stealing your identity is simply stealing your un-shredded mail from your dumpster or garbage. Another method of mail theft is to steal your mail from an unsecured mailbox. The Federal Trade commission lists these types of threats as low-tech methods of identity theft. In the September 2003 Federal Trade Commission Identity Theft Survey Report they identified that, *"Nearly one-quarter of all victims* [total of 4,057] *said that their information was lost or stolen- including lost or stolen credit cards, checkbooks, social security cards or information obtained through stolen mail."* You should monitor your bills and statements and be aware that when mail you are expecting does not show up, you may be at risk of identity theft. Also monitor your statements and be aware of any small charges of less than five dollars, these may be 'test charges' from identity thieves to see if they can make charges without your notice before they start charging large sums. Be aware of and manage accordingly any errors on any accounts or statements. Some low tech ways to deter thieves from stealing your mail are to put a lock on your mailbox, use a secure P.O. Box or have your local post office hold your mail.

Eavesdropping & Shoulder Surfing

Eavesdropping is the intentional interception of a communication, where the person talking would have had a justifiable expectation of privacy. The Department of Justice defines oral communication privacies as your home or office, versus a jail or an open field. When consumers are putting in their pin numbers or answering personal calls over the phone it is important to know that anyone around you could be listening. Penal law §250.05 defines this type of eavesdropping as *"Mechanical overhearing of a conversation"* [this] *definition prohibits a person who is not present at a conversation or discussion from intentionally overhearing or recording…"* The simplest prevention method is to not make calls involving your personal identifying information in public places. Understandably this is not always an option, so the next best thing is getting to as private a place as you can, covering your mouth and phone with your hand or another object and attempt to muffle your voice as best as you can. Similarly, thieves can 'shoulder surf' in public places. Where they look at pin pads and try to get your personal identification number (PIN) while you are using your credit cards. The best prevention here is to cover your hand while you are typing and make sure that you finish your transaction at whatever terminal you are using. The U.S. Department of Homeland Security published the Identity Theft and Internet Scams Tip Card infographic with this helpful tip, *"Avoid accessing your personal or bank accounts from a public computer or public Wi-Fi network, such as the public library. Not only can cybercriminals potentially gain access to your accounts through public Wi-Fi, but strangers can easily shoulder surf and see the sensitive information on your computer or mobile device screen."*

https://www.dhs.gov/sites/default/files/publications/Identity%20Theft%20and%20Internet%20Scams.pdf

Pickpockets

Pickpocketing is one of the most common and oldest forms of thievery, but now with all the information carried in pockets and purses street thieves now have the potential to access a large amount of our personal identifying information. This puts the victim's identity at risk.
Pickpocketing is the physical removal of a person's items included but not limited to money, credit cards, passports, social security cards and driver's licenses without their consent. Thieves are getting smarter by traveling in groups or working in teams. Some try to distract the victim or sandwich them into a position where many people may bump into them such as a crowded subway. Some pickpockets may even falsely alert a group of people that someone stole their wallet to see if others reach for their wallets to easily view their targets. The U.S. Embassy & Consulates in France released an article, "Pickpockets in Paris: How to Avoid Becoming A Victim", where it states, *"The first rule of thumb is don't have anything more in your wallet than you are willing to lose."* The best form of prevention against a pickpocket is to keep your personal identifying information like passports and social security cards in a secure location. The U.S. Embassy warns citizens if they must carry a wallet to carry it in their front pockets or if they must carry a purse to have it in front of them in full view at all times.

https://fr.usembassy.gov/u-s-citizen-services/pickpockets-paris-avoid-becoming-victim/

Prevention Measures Quick Guide

Having gone over these measures throughout this second installment. Here is a quick reference list of prevention measures for you to use:

- Cross cut shred your documents, receipts and old statements after use.
- Check your mail for legitimacy and grammar.
- Have a lock on your mailbox, use a secure P.O. box or have your local post office hold your mail until you can safely pick it up.
- Monitor your accounts for 'test charges' or errors.
- Shield a pin pad while in use.
- Try to make phone calls with personal identifying information in as private a place as possible. Muffle your voice if necessary.
- Keep your personal identifying information in a secure location.
- Keep your wallets and purses in your sightline.
- Do not carry your personal identifying information like social security cards and passports on your person.
- Destroy old credit cards.
- Always be aware of where your credit cards are.

A look at Series Three

This series will attempt to educate individuals on the different types of scams, prevention strategies to protect your identity, warning signs to be on the lookout for and what you can do if you're a victim. Be on the lookout for the third installment in the Identity Theft Series, "Phone Scams: Security and Prevention". We will look at the different types of phone scams, security measures you can take and prevention methods you can do now. The Town of Manlius Police Department reminds citizens if they are ever a victim of identity theft to call 911.

Town of Manlius Police Department
1 Arkie Albanese Avenue
Manlius, NY 13104
(315) 682-2212

If you are ever a victim of Identity Theft call 911.