FRAUD

The Wausau Police Department investigates numerous fraud related crimes each year. Some fraud cases result in arrest, while other cases lead to unknown persons obscured by distance, technology or other methods of subterfuge.

Regardless of the outcome of a particular case, the Wausau Police Department can provide assistance to better the outcome for individual victims. Therefore, we encourage our community members to report all incidents and suspicions of fraud to the Wausau Police Department.

We also encourage our community members to take a proactive approach in protecting their personal and financial information:

- Be Informed
- Be Prepared
- Be Empowered

BE INFORMED

Many modern fraud schemes have gone by different names in the past and have been renamed and "repackaged" to take advantage of current culture. Therefore, it is not as important to learn the names of these schemes as it is to understand both how they work, and why they work.

The following list profiles some of the more common fraud schemes, as well as provides links to websites for further information. *This list is by no means inclusive; however, the examples illustrate some of the methods tried by criminals to separate you from your money and from your good name.*

IDENTITY THEFT

Identity theft is not only a crime in itself, but is also a gateway to other crimes. Identity theft is commonly perpetrated by a concept termed **"social engineering"**. Although social engineering is broad term which can be used for legitimate purposes, the criminal aspect of social engineering involves manipulating people into disclosing personal or confidential information.
(see http://en.wikipedia.org/wiki/Social_engineering_%28security%29)

1. **EMAIL "PHISHING"**
   - You get an email offer for a product or service…

   - You get an email informing you your account may be compromised – it could be from an unknown source, a familiar source or from a business that you yourself have an account with (e.g. your bank, your insurance company, Paypal, Amazon etc.)…

     The email asks you to call a telephone number or to follow a link to order a product or to resolve the problem – ***DON'T RESPOND, DON'T FOLLOW THE LINK.***

- For a comprehensive review of this fraud scheme, see the Federal Trade Commission website (www.ftc.gov): http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt127.shtm

2. **TELEPHONE "PHISHING"** – Jury Scam
   - You get a telephone call from someone claiming to be an Officer of the Court who says you not only failed to report for jury duty, but also there may be a warrant issued for your arrest! The "officer" offers to "clear up" the problem and requests your personal information for verification…***HANG UP THE PHONE.***

   - The above example of criminal social engineering is referred to as a "jury scam". However, any variation of the jury scam can be perpetrated. The common theme in any of these types of scams is the potential victim has received an unsolicited telephone call and is being asked for personal information. Therefore, ***NEVER GIVE OUT PERSONAL INFORMATION WHEN RECEIVING AN UNSOLICITED TELEPHONE CALL***

   - For further information on this and other scams, see the Federal Bureau of Investigation Website (www.fbi.gov): http://www.fbi.gov/page2/june06/jury_scams060206.htm

3. **"ADVANCE FEE" SCAMS** – "Nigerian" Letter, Foreign Lottery
   - Advance fee fraud gets its name from the fact that a person is asked to pay a fee up front or in advance of receiving any proceeds, money, stock etc., in order for the deal to go through.

   - Another variation of the advance-fee scam occurs when a person is asked to cash a check or other financial instrument, and is offered to keep a portion of the amount in exchange for sending the remainder to a person or location.

   - The U.S. Secret Service has set up a task force for addressing ***only*** "Advance Fee Fraud" schemes. If you have suffered a financial loss from a Nigerian "Advance Fee Fraud" scheme, please contact your local U.S. Secret Service Field Office. You can find the nearest office on the Secret Service website (www.secretservice.gov): http://www.secretservice.gov/field_offices.shtml

BE PREPARED

If you are the victim of an identity theft, please follow these procedures:

- Contact your local police department and file a complaint.

- Contact the three main credit reporting bureaus:
  - Equifax (800) 685-1111 www.equifax.com
  - Experian (888) 397-3742 www.experian.com
  - TransUnion (800) 888-4213 www.transunion.com

- Ask them to inform you of all accounts listed in your name.
- Initiate a fraud alert so that potential credit grantors verify your identification before extending credit in your name.
- You may also initiate a “Credit Freeze” – for further information on freezing your credit, contact the Wisconsin Office of Privacy Protection (http://privacy.wi.gov / (800) 422-7128)

- Call the companies that issued your credit card(s) and close the compromised account(s).
- Close any new account(s) that were opened fraudulently
- Contact your bank where you hold checking/savings accounts
- File an ID Theft Affidavit with the Federal Trade Commission (www.ftc.gov / 877-IDTHEFT (877-438-4338))
- Contact the Social Security Administration Hotline (800-269-0271)