Identity Theft

What is Identity Theft? The Federal Trade Commission website states: "Identity theft happens when someone uses your Social Security number or other personal information to open new accounts, make purchases, or get a tax refund."

The Department of Justice website lists some of the most common ways Identity Theft or Fraud can happen to you:

- In public places, for example, criminals may engage in "shoulder surfing"– watching you from a nearby location as you type in your pin or credit card number – or listen in on your conversation if you give your credit-card number over the telephone.
- If you receive applications for "pre-approved" credit cards in the mail, but discard them without tearing up the enclosed materials, criminals may retrieve them and try to activate the cards for their use without your knowledge. Also, if your mail is delivered to a place where others have ready access to it, criminals may simply intercept and redirect your mail to another location.
- Many people respond to "spam"– unsolicited E-mail – that promises them some benefit but requests identifying data, without realizing that in many cases, the requester has no intention of keeping his promise. In some cases, criminals reportedly have used computer technology to steal large amounts of personal data.

With enough identifying information about an individual, a criminal can take over that individual's identity to conduct a wide range of crimes. For example:

- False applications for loans and credit cards,
- Fraudulent withdrawals from bank accounts,
- Fraudulent use of online accounts, or
- Obtaining other goods or privileges which the criminal might be denied if they were to use their real name

In more complicated cases, thieves sell your identity to others. You may not experience the repercussions immediately, only to discover that your credit is suddenly bad, or that you're wanted for a crime you didn't commit halfway across the country.

Identity Theft Prevention Tips:

- Guard personal information - Anytime you're asked for information, whether in person, on paper, over the phone or via the internet, verify the party requesting it is legitimate and why they are asking for it. It is ok to challenge them and do your own research to verify if providing the information is necessary.

- Use all available security measures for electronic devices – Protect all your devices (e.g. smart phones, iPads, tablets, laptops and everything in between) using methods like two-factor authentication passwords, installing anti-virus software, biometric features, etc. Consider adding apps to locate, lock and erase electronic devices. Back up critical data, in case your device is lost, stolen or broken.
  For more tips, visit the FTC page on How to Keep Your Personal Information Secure:
  https://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure

- Guard your trash - Shredders are cheap and effective. Use them to destroy any un-needed receipts, mail or papers that have identifying information.

- Guard your mail - Only put outgoing mail in a secure mailbox or drop it at the United States Post Office. Retrieve your mail promptly after it has been delivered.

- Guard your wallet or purse, including restaurants, stores, etc. - We receive reports of ID Theft occurring when individuals leave purses and wallets unsecured at tables in restaurants, while shopping, when using the restroom, etc.

- Don't carry Social Security cards, personal identification numbers (PINs), or passwords on you- Never write PINs or passwords on the related devices. NEVER carry your PINs or passwords in your wallet or purse.

- Review your credit card statements each month - Look for unexplained charges, missing statements, or bills from cards you didn't open.

- Check your credit history annually with all three credit reporting bureaus.

- Close any accounts that have been tampered with or opened fraudulently;

- Report it to your local police agency;

- Report it to the FTC: https://www.identitytheft.gov/

If you believe you are the victim of identity theft:

Inform all three credit reporting bureaus-
Equifax: 1-888-548-7878; https://www.equifax.com/personal/contact-us/
Experian: 1-888-397-3942; https://www.experian.com/contact/personal-services-contacts.html
TransUnion: 1-800-916-8800; https://www.transunion.com/customer-support/contact-us-consumers

For more extensive help, information, tips, the ID Theft Affidavit, credit bureau info, and much more, see the Federal Trade Commission's comprehensive ID Theft Clearinghouse web site:
http://www.ftc.gov/bcp/edu/microsites/idtheft//

To report a crime that occurred in the incorporated area of Eugene, call Eugene Police non-emergency at 541-682-5111.

For crime prevention information and information related to scams and preventing elder fraud, visit our website: **https://www.eugene-or.gov/2394/Scams-Fraud-and-Identity-Theft**