

Numbers Now

Criminal Justice in Oklahoma

June 2017 (Vol.7, No.1)

Content:

- Crime in Oklahoma 2016
- Safe Oklahoma Grant: Year 3
- Analysis of SIBRS Sexual Assault Data
- Internet Safety

Published by Oklahoma State Bureau of Investigation

> Stan Florence Director

Charles Curtis Deputy Director

John Flores-Hidones Statistical Research Specialist

Nikki Lofftus Statistical Research Specialist

Crime in Oklahoma 2016

The 2016 *Crime in Oklahoma* report is now available online. This report includes the most accurate and current crime data for the State. Data in this report are based on offenses reported to law enforcement.

Violent crime in Oklahoma increased 6.6% in 2016. Non-violent index crimes also increased 4.9%. Oklahoma law enforcement reported 239 murders, representing a 0.8% decrease from 2015. Rapes increased 9.5%, robberies increased 5.9%, and aggravated assault increased 6.5%.

Oklahoma law enforcement reported 23,936 cases of domestic abuse in 2016, a 1.0% decrease from 2015. Assault and battery represented 86.2% of all domestic abuse calls. Law enforcement reported 54 domestic abuse related murders, representing 22.6% of all murders in 2016.

Assaults on law enforcement in 2016 increased 14.9% - half of all officer assaults between 6:01 p.m. to 2:00 a.m. Assaults occurring during a traffic pursuit/stop increased 6.4%, and officers injured during an assault increased 13.8% compared to 2015.

An estimated 89% of agencies that reported crime data in 2016 participated in SIBRS; however, those agencies served just 46.5% of the state's population and reported just 31.2% of index crimes reported in 2016.

To view the full report, visit: https://www.ok.gov/osbi/Pu blications/Crime_Statistics.h tml

Reminder

The Office of Criminal Justice Statistics can assist you and your agency with statistics for grant applications or any other research requests.

Please visit: https://www.ok.gov/osbi/Statistical Analysis Cent <u>er/index.html</u>

Oklahoma City Safe Oklahoma Grant Program: Year 3

The Oklahoma City Police Department (OCPD), Hefner Division, recently concluded it's third year of the Safe Oklahoma Grant Program. OCPD used grant funds to implement proactive policing strategies, nuisance abatement activities, and develop community partnerships.

Evaluators with the OSBI worked with program staff to evaluate the effectiveness of grant activities within the target area. Key findings of the evaluation include:

- Violent crime in the target area decreased 21.6% from 2013 to 2016.
- Murders in the target area decreased 50% from 2013 to 2016.
- Rapes in the target area decreased 60% from 2013 to 2016.
- Robberies in the target area decreased 29.6% from 2013 to 2016.
- Aggravated assaults in the target area decreased 11.6%.

OCPD implemented proactive policing strategies within the target area and used intelligence-led policing strategies to identify and focus resources on hot spots. OCPD also increased nuisance abatement, positive interactions with community members, and enhanced community outreach within the target area. The multi-family housing specialists worked with apartment management to reduce violent crime in apartment complexes, which represented 39.2% of all violent crime in the target area.

In 2016, OCPD was awarded grant funds for an additional year. The program was transferred to the Southwest Division on October 1, 2016.

To view the full report, visit:

https://www.ok.gov/osbi/Statistical Analysis Center/Publications/index.html

Analysis of Sex Offenses Using Incident-Based Reporting Data

Evaluators with the OSBI conducted an analysis of sex offenses reported by local law enforcement to the Oklahoma State Incident-Based Reporting System in 2015.

Key findings include:

- In 2015, 199 law enforcement agencies submitted reports through SIBRS containing at least one sex offense;
- Victim(s) were known to the offender(s) in the majority (82%) of reports;
- The majority of offenses (75.9%) took place in a residence;
- Weapons most frequently reported were personal weapons (hand, feet, fists, ect.).

To view the full report, visit:

https://www.ok.gov/osbi/Statistical Analysis Center/Publications/index.html

Internet Safety

Financial losses from internet crimes surpass millions of dollars every year. Victims are often targeted through multiple methods such as data breaches, intrusions, online scams, malware, and ransomware.

<u>Malware</u>

Malware is designed to damage or gain access to a device without consent from the owner. Types of malware include spyware, keyloggers, true viruses, worms, and any other code that infiltrates a computer or mobile device. Originally created as prank coding, it evolved to cause damage and destruction of digital data. Today, hackers design malware for profit by infecting devices with forced advertising (adware), stealing personal data (spyware), sending e-mail spam (zombie computers), or to extort money from victims (ransomware). The latest ransomware outbreak occurred in May 2017, infecting more than 300,000 devices over 150 countries.

Ransomware is a form of malware targeting both human and technical weaknesses in organizations and individual networks. It prevents users from accessing critical data and/or systems. Commonly delivered through spear phishing e-mails, ransomware has the ability to quickly encrypt sensitive files on a corporate network. Once the targeted organization cannot access their data, hackers demand the payment of a ransom, usually in virtual currency (Bitcoin). Once the payment is made, the hacker provides a password or unencrypting method so victims can regain access to their data.

Proactive Measures to Safeguard Personal or Organizational Data

Install and maintain an updated, quality antivirus program. Back up your computer periodically and store important files on an external drive or cloud-based system. Keep your operating software up-to-date. Be cautious when surfing the web and stay away from suspicious sites. Avoid downloading files with extensions like .exe, .scr, .lnk, .vbs, .dll, and .cmd. Always scan files with your antivirus before opening or downloading them into your device. Use a reliable internet service provider and antivirus program to implement strong anti-spam and anti-phishing measures.

If you believe your computer has been infected, disconnect your device from the internet by unplugging the Ethernet cable, turning off your Wi-Fi connection, or disconnecting your router. This will prevent malware from infecting other devices on your network, as well as prevent data from being sent back to the hackers. If the attack happens at home, consider contacting your antivirus and internet service providers for assistance on removing malware. If the attack occurs at work, contact your IT department immediately. They should be able to address or contain the issue.

If your personal information has been compromised due to internet fraud, close or freeze all affected accounts immediately (bank, credit card, etc.). File a police report with your local law enforcement and contact the Federal Trade Commission (identity theft). Consider changing personal information through local, state, or federal authorities (Social Security Administration, DMV, etc.). Contact the three national consumer reporting agencies and set up a fraud alert. If fraudulent activity appears on your credit report, contact authorities immediately.

To file a complaint or obtain more information on internet protection, please visit the Internet Crime Complaint Center (IC3) at <u>https://www.ic3.gov/default.aspx</u> or the FBI Scams and Safety website at <u>https://www.fbi.gov/scams-and-safety</u>

OCJS Mission

To collect, analyze, and disseminate criminal justice research to educate and assist law enforcement and the citizens of Oklahoma.