Cyber Crimes

The Department of Justice has three categories for cybercrime:

- crimes in which the computer is used as an accessory to a crime
- crimes in which the computing device is the target
- crimes in which the computer is used as a weapon

The overall result of a cybercrime is financial gain. Cybercrimes may include, but are not limited to profit-driven criminal activity, ransomware attacks, email / internet fraud, identity theft / fraud and financial account information.

Cybercriminals may target corporate and/or private individuals for theft. Today, more and more workers are settling into remote work routines due to the pandemic, cybercrimes continue to rise, making it especially important to protect sensitive data.

Cases we can assist you with:

- Data breaches & computer intrusions
- Denial of service attacks
- Internet stalking & harassment
- Criminal copyright infringement
- Embezzlement & extortion
- Online identity theft
- Insider attacks
- Fraudulent transactions
- Web hyjacking
- Phishing

Techniques and tools we utilize:

- Web traps and internet stings
- Extensive, private databases
- Criminal background
- WLAN-LAN monitoring
- Email traces and internet forensics
- Digital forensics
- Surveillance
- Social engineering

We help you to prepare for future attacks by offering various means of prevention and protection. Our investigators will educate you on lawful ways to monitor and detect breaches of credit card transactions, social media hacking, social security number theft, bank account breaches, and court records.

MSG
Risk Management & Intelligence

139 W.1st St. Suite 201, Casa Grrande,
Arizona 85122 – 1-866-7MAYHEM
www.mayhemsolutionsgroup.com