



Cyber Crimes

Cyber Crime Statistics:

- In 2014, 47% of American adults had their personal information stolen by a hacker.
- Cybercrime reported to the FBI in 2013 totaled losses of over \$781 million, with an average loss of nearly \$3,000 per complaint. That includes:
 - \$81 million taken by romance scammers, who target people on online dating sites, feigning love and then asking for money averaging more than \$12,000 per victim.
 - \$51 million taken by auto scammers, who convince their targets to pay for cars that don't exist raking in an average of \$3,600 per victim.
 - \$18 million in real estate rental scams which, like auto scams, attempt to convince buyers to pay for property that doesn't exist to the tune of nearly \$1,800 per victim.

Overview of Texas Computer Crime Law:

- Knowingly accessing a computer, computer network or computer system without the consent of the owner;
- Knowingly soliciting a minor under the age of 17 over the internet, text message, or other electronic system, to meet in person for the purpose of engaging in sexual behavior with the defendant;
- Knowingly accessing a computer system, network, program, software or machine that is part of a voting system that uses direct recording electronic voting machines and tampers with the votes or the ability of someone to vote.
- Creating a web page or leaving messages on a social networking site using the persona of another without the person's consent and with the intent to harm, defraud, intimidate or threaten someone;

Phishing Scams:

Texas also has anti-phishing state laws making it a crime to reference the name, domain address, phone number or any other identifying information of a person without that person's consent, intending to cause the recipient to think the message is truly coming from that person, with the intent to harm or defraud someone.

Identity Theft Laws:

Identity theft laws in most states make it a crime to misuse another person's identifying information -- whether personal or financial. Such data (including social security numbers, credit history, and PIN numbers) is often acquired through

1. The offender's unlawful access to information from government and financial entities or
2. Lost or stolen mail, wallets and purses, identification, and credit or debit cards.

Identity theft is one of the fastest-growing crimes in the nation, robbing its victims of time, money and peace of mind.

Penalties and Sentences:

The penalties for computer crimes are of a wide variety depending on the nature and seriousness of the crime committed. For the breach of computer security (i.e. gaining access to a computer without the consent of the owner), the penalty may range all the way from a "Class B" misdemeanor (up to 180 days in a county jail and/or a fine of up to \$2,000) up to a first degree felony (five to 99 years in a state prison and/or a fine of up to \$10,000). The factor influencing the degree of the penalty imposed is the value of money or property that the defendant benefited from and/or was lost by the victim.

For tampering with a voting machine, the penalty is a first degree felony. This is a very serious penalty with a sentence between five to 99 years in a state prison and/or a fine of up to \$10,000.

For online harassment, the charge is generally a third degree felony. However, if the crime was pretending to send an electronic message of any type from another person, hoping the recipient would believe that the other person authorized this message, with the intent to harm or defraud, the defendant may instead be charged with a "Class A" misdemeanor (not more than one year in a county jail and/or a fine of no more than \$4,000). In the event, however, that this was intended to summon a response by emergency personnel, it will be elevated back to a third degree felony.

Remember:

USTPD working with the UST community to make a safer campus.



University of St. Thomas Police Department

713-525-3888

police@stthom.edu