

SECURITY - Now ...more than ever!

Cyber Security - Disaster Recovery - Continuity of Government



DTI eSecurity News - Cybercrime

What is Cybercrime?



Cybercrime is any criminal offense committed against or with the use of a computer or computer network. This includes hacking attempts, theft, identity theft, malicious use of software and child exploitation.

What are Trends in Cybercrime?

Cybercrime is dominated by criminals who want to use your computer for illegal activities, to steal data for profit, and organized crime is heavily involved. The Internet Crime Complaint Center 2008 Annual Report lists **Delaware** in the top six states having the most perpetrators of Internet fraud.

Attackers exploit vulnerabilities in computer software in order to develop “crimeware”, such as viruses, Trojans, and keystroke logging, upon which other criminals carry out their nefarious acts. Some of their crimeware servers not only act as command and control servers, but also act as “data suppliers” or repositories for private stolen information, such as personal information that is harvested by the crimeware. Traditional security tools are becoming increasingly more limited in their ability to mitigate these highly complex cybercrime attacks. The cybercrime landscape, has definitely changed, but the criminal motivations are still the same — **money, power, and revenge.**



What are Cybercrimes?

- **Hacking** is a form of breaking and entering, invades privacy, and is a felony in the United States.
- **Cyber theft** is illegally downloading movies, software, games, or music and violates copyright laws.
- **Identity theft** is a form of theft that targets bank accounts, credit cards, debit cards, social security numbers, and information that is linked to a person’s identity.
- **Computer viruses**, also known as worms, are Internet-borne malicious programs meant to disrupt an aspect of a network. They are artificial creations with the purpose of damaging software systems, stealing information, or allowing access to private systems.
- **Child exploitation** is the solicitation of underage children through chat rooms. Monitoring children and young adult chat rooms with the hopes of preventing child exploitation is being done by law enforcement agencies.
- **Cyber harassment or Cyber bullying** is a crime committed against a person and happens when someone is harassing a person online involving threats that are discriminatory in nature.



Produced in part by MS-ISAC and the ISAA Journal

What Can I Do?

Cybercrime is preventable, but prevention will take some work on your part. To adequately defend against cybercrime, follow the traditional best practices for protecting your network, desktop, laptop, or mobile device. If you become a victim of cybercrime, you should report the incident to the appropriate authorities.

- ✓ The [United States Department of Justice](#) maintains a list of federal agencies to which computer related crimes may be reported.
- ✓ The [Internet Crime Complaint Center \(IC3\)](#)
- ✓ Local law enforcement agency
- ✓ In Delaware, the [Attorney General’s Office](#)

Visit the [eSecurity Extranet](#) website for previous issues of

eSecurity Newsletters

Questions or comments?

E-mail us at eSecurity@state.de.us