

To be prepared in the event of a technology-based incident, familiarize yourself with this section and refer to the Disaster Recovery plans for additional instructions.

DAS's technological applications operate on a secured technology environment to address and reduce the likelihood of cyber-attacks. Should you receive a suspicious e-mail or become aware of a real or perceived cyber-attack, please do the following:

Reporting a cyber-attack:

1. Do not open or further tamper with the e-mail or your computer.
2. Immediately report the incident to DAS IT Services at 728-5400.
3. Report the incident to your supervisor/manager.

What is a cyber-attack:

Specific types of potentially damaging "cyber-activities" have different sources and different targets, and carry different levels of risk for enterprises. Examples of a cyber-attack include the following:

- Incidents involving computer "hackers."
- Incidents involving system penetration or tampering.
- Unauthorized access to computing facilities, telecommunication (i.e., telephone, fax, teleconferencing) and networking services (i.e., e-mail) or equipment.
- Use of computing, network and telecommunication facilities for personal profit.
- Destruction or alteration of data, software and equipment.

Hackers: Computer hackers are generally online troublemakers who engage in illegal online activities to further their cause or belief. Targeted systems will likely be compromised and used as staging points for cracking, distributed denials of service or other types of attacks.

Cyber-crime: Cyber-crime is online criminal activity undertaken for financial gain. Cyber-crime activity is expected to rise as criminals attempt to take advantage of perceived uncertainties in financial systems. Fraudulent online solicitations for nonexistent charities also appear following tragedies.

Cyber-terrorism: Cyber-terrorism is a computer-based crime intended to cause loss of life or property in pursuit of political gains. Cyber-terrorist activities will likely target U.S. government facilities as well as infrastructure centers and nongovernmental organizations such as relief agencies. Enterprises, particularly financial institutions, public utilities, telecommunications companies, online trading firms and e-commerce sites, also are likely to be targeted.