Cybercrime

Cybercrime: criminal activity(ies) involving the networked environment based on the Internet and/or World Wide Web. (Grabosky)

"Computer crime", "computer-related crime", and "cybercrime" can and will be used interchangeably.

The increasing reliance on computer technology and interconnectedness (over 3.4 billion people use the Internet) has altered our understanding of crime. This reliance and interconnectedness:

1) change the scene(s) or location(s) in which crime occurs;
2) make possible the commission of new forms of crime;
3) bring about changes in methods of law enforcement-
   a) attention is now shifted to ways of preventing cybercrime;
   b) law enforcement efforts now include cooperation between public and private agencies;
4) provide law enforcement agencies with new tools of (online) surveillance and new procedures for dealing with data and online risks;
5) introduce new challenges to existing criminal justice procedures and prompt the development of new methods of proof and procedure.

The online environment has created new security risks and influenced the types of criminal behavior that take place in that environment. This environment has certain properties that contribute to cybercrime.

1) Digitization: data and information are generated, processed, and stored in digital form- this makes possible the modification and manipulation of those data as they are transmitted across the Internet;
2) Anonymity: users can interact with and spy on others without disclosing their (true) identity;
3) Interconnectivity: everyone on the network is connected to everyone else on that network;
4) Decentralization: there is NO centralized control over the Internet;
5) Interdependence: there is a vulnerability shared among and between all people who are connected to and interact on the Internet.