Theft of Data

Data theft is the act of stealing information stored on computers, servers, or other electronic devices from an unknowing victim with the intent to compromise privacy or obtain confidential information. Information can include anything from financial information, like credit card numbers or bank accounts, to personal information, like social security numbers, drivers license numbers, and health records. It can also include theft of passwords, software code, algorithms, proprietary information, or technologies. Data theft is a growing problem for individual computer users as well as large corporations and organizations.

Data is not a movable property, and hence the unauthorized act of taking away data electronically (by way of emailing it to oneself or by hacking into a computer system, for example) is not considered as theft. However, stealing of data is no doubt a crime, and is punishable under the law.

Data theft occurs through a variety of means. Most often, it happens because someone hacked into a computer system to steal sensitive information, such as your credit card or personal information, or an employee at a company mishandled the information. With an increasingly digital world, hundreds of different businesses and organizations hold your personal information, such as your social security number, mailing address, birthdate, and bank account information.

What Gets Stolen?

Identity theft is the act of a person obtaining information illegally about someone else. Thieves try to find such information as full name, maiden name, address, date of birth, social security number, passwords, phone number, e-mail, driver's license number, credit/debit card numbers, and/or other data pertaining to an individual's identity.. The thief can then use this information to gain access to bank accounts, e-mail, smartphones, or other accounts/programs. He/she then identifies him/herself as you, or sells your information.

Identity theft is categorized two ways: true name and account takeover. True-name identity theft means the thief uses personal information to open new accounts. The thief might open a new credit card account, establish cellular phone service or open a new checking account in order to obtain blank checks.

Account-takeover identity theft means the imposter uses personal information to gain access to the person's existing accounts. Typically, the thief will change the mailing address on an account and run up a huge bill before the person whose identity has been stolen realizes there is a problem. The internet has made it easier for an identity thief to use the information they've stolen, because transactions can be made without any personal interaction.

An important element of individual identity theft is the theft of credit/debit card details, such as the type of card (Visa, MasterCard, etc.), card number, security code, issuing bank or institution, and credit limit.

Corporate espionage can be defined as the “the improper, unlawful and unethical theft of trade secrets owned by or belonging to one company by a competitor (or sometimes a hostile foreign state) for the purpose of achieving an advantage over that company, or the country of its origin."

The key aspects of corporate espionage involve the trade secrets at the heart of the espionage, as well as the ultimate purpose of the theft being to obtain a competitive advantage of some sort.

Corporate espionage can be accomplished through several techniques:

1) Trespassing onto a competitor's property or accessing their files without permission;
2) Posing as a competitor's employee in order to learn company trade secrets or other confidential information;
3) Wiretapping a competitor;
4) ***Hacking into a competitor's computers***;
5) ***Attacking a competitor's website with malware***.

Piracy of text, images, video, sound, or multimedia presentations is another form of data theft. Digital piracy refers to the illegal act of duplicating, copying, or sharing a **digital** work without the permission of the copyright holder, a violation of copyright laws. Digital piracy grew out of computer hacking.

Digital piracy harms the original copyright holders: the songwriters, music artists, moviemakers, game developers, software innovators, and other creators of new digital media products. They lose money to those who sell pirated copies cheaply. The theft of their work may also discourage them from doing further creative work

Hackers may use pirated content to spread malware and infect a user's system. Companies who use pirated software open themselves up to copyright violation and infringement. They also expose their networks to potential malware or virus infection. Hackers can then use these infected systems to launch an attack or to mine cryptocurrency.