* **Malware Distribution:**Hackers with malicious intent can exploit your email client by distributing [malware](http://www.spamlaws.com/different-types-email-exploits.html) through email messages. The malware includes viruses, worms, rootkits, Trojans, keyloggers, spyware, and adware, to name a few types. The malware is distributed via an email attachment or sometimes by simply opening an email message. More often than not, the mail message is disguised as a message from someone you know when in reality; it is sent by the hacker.
* **Phishing Attack:**A phishing attack is generally not hazardous to the inner workings of your [PC](http://www.spamlaws.com/different-types-email-exploits.html) however; it is designed to trick you into revealing your personal information, passwords, or bank account information. For example, if you use PayPal, the phisher sends you a message that looks like it came from PayPal. The message requests you to verify your account information with PayPal to continue using your account. The message proceeds to tell you that if you do not verify the information your account will be closed. Someone that is unaware of phishing scams easily gets tricked into revealing their account information. These types of messages are set up to look like the real deal.
* **Spam Attack:** Spam is unsolicited email or "junk" [mail](http://www.spamlaws.com/different-types-email-exploits.html) that you receive in your Inbox. Spam generally contains advertisements but it can also contain malicious files. When you click on spam, the files are downloaded into your email client and into your PC. The same thing can happen if you reply to spam in an attempt to get removed from the list.
* **Denial of Service Attack:**A denial of service attack occurs when the hacker sends multitudes of email messages to your email client in an effort to block you from using your email client or crashing your [computer](http://www.spamlaws.com/different-types-email-exploits.html) altogether. In the case of an organization, a denial of service attack on email can crash an entire network and prevent the users from responding to legitimate traffic.

These are the main types of email client exploits that can result in damage to your applications, [data](http://www.spamlaws.com/different-types-email-exploits.html), and even your computer's operating system. Additionally, an email client exploit can cause you to expose confidential information and also expose your PC to an endless list of malware that ranges from simply spying on your Web browsing activity to literally destroying your PC components.  If you are aware of how these exploits occur, you can take measures to [**protect your email client**](http://www.spamlaws.com/email-client-protection.html).

**Eavesdropping** - This is the process of listening in or overhearing parts of a conversation. It also includes attackers listening in on your network traffic. Its generally a passive attack, for example, a coworker may overhear your dinner plans because your speaker phone is set too loud. The opportunity to overhear a conversation is coupled with the carelessness of the parties in the conversation.  
  
**Snooping** - This is when someone looks through your files in the hopes of finding something interesting whether it is electronic or on paper. In the case of physical snooping people might inspect your dumpster, recycling bins, or even your file cabinets; they can look under your keyboard for post-It-notes, or look for scraps of paper tracked to your bulletin board. Computer snooping on the other hand, involves someone searching through your electronic files trying to find something interesting.  
  
**Interception** - This can be either an active or passive process. In a networked environment, a passive interception might involve someone who routinely monitors network traffic. Active interception might include putting a computer system between sender and receiver to capture information as it is sent. From the perspective of interception, this process is covert. The last thing a person on an intercept mission wants is to be discovered. Intercept missions can occur for years without the knowledge of the intercept parties.  
  
**Modification Attacks** - This involves the deletion, insertion, or alteration of information in an unauthorized manner that is intended to appear genuine to the user. These attacks can be very hard to detect. The motivation of this type of attack may be to plant information, change grades in a class, alter credit card records, or something similar. Website defacements are a common form of modification attacks.  
  
**Repudiation Attacks** - This makes data or information to appear to be invalid or misleading (Which can even be worse). For example, someone might access your email server and inflammatory information to others under the guise of one of your top managers. This information might prove embarrassing to your company and possibly do irreparable harm. This type of attack is fairly easy to accomplish because most email systems don't check outbound email for validity. Repudiation attacks like modification attacks usually begin as access attacks.  
  
**Denial-of-service Attacks** - They prevent access to resources by users by users authorized to use those resources. An attacker may try to bring down an e-commerce website to prevent or deny usage by legitimate customers. DoS attacks are common on the internet, where they have hit large companies such as Amazon, Microsoft, and AT&T. These these attacks are often widely publicized in the media. Several types of attacks can occur in this category. These attacks can deny access to information, applications, systems, or communications. A DoS attack on a system crashes the operation system (a simple reboot may restore the server to normal operation). A common DoS attack is to open as many TCP sessions as possible; This type of attack is called TCP SYN flood DoS attack. Two of the most common are the ping of death and the buffer overflow attack. The ping of death operates by sending Internet control message protocol (ICMP) packets that are lrger than the system can handle. Buffer overflow attacks attempt to put more data into the buffer than it can handle. Code red, slapper and slammer are attacks that took advantage of buffer overflows, sPing is an example of ping of death.  
  
**Distributed Denial-of-service Attacks** - This is similar to a DoS attack. This type of attack amplifies the concepts of DoS attacks by using multiple computer systems to conduct the attack against a single organization. These attacks exploit the inherent weaknesses of dedicated networks such as DSL and Cable. These permanently attached systems have little, if any, protection. The attacker can load an attack program onto dozens or even hundreds of computer systems that use DSL or Cable modems. The attack program lies dormant on these computers until they get attack signal from the master computer. This signal triggers these systems which launch an attack simultaneously on the target network or system.  
  
**Back door Attacks** - This can have two different meanings, the original term back door referred to troubleshooting and developer hooks into systems. During the development of a complicated operating system or application, programmers add back doors or maintenance hooks. These back doors allow them to examine operations inside the code while the program is running. The second type of back door refers to gaining access to a network and inserting a program or utility that creates an entrance for an attacker. The program may allow a certain user to log in without a password or gain administrative privileges. A number of tools exist to create a back door attack such as, Back Orifice (Which has been updated to work with windows server 2003 as well as erlier versions), Subseven,NetBus, and NetDevil. There are many more. Fortunately, most anti-virus software will recognize these attacks.  
  
**Spoofing Attacks** - This is an attempt by someone or something to masquerade as someone else. This type of attack is usually considered as an access attack. The most popular spoofing attacks today are IP spoofing and DNS spoofing. The goal of IP spoofing is to make the data look like it came from a trusted host when it really didn't. With DNS spoofing, The DNS server is given information about a name server that it thinks is legitimate when it isn't. This can send users to a website other than the one they wanted to go to.  
  
**Man-in-the-Middle Attacks** - This can be fairly sophisticated, This type of attack is also an access attack, but it can be used as the starting point of a modification attack. This involves placing a piece of software between a server and the user that neither the server administrators nor the user are aware of. This software intercepts data and then send the information to the server as if nothing is wrong. The server responds back to the software, thinking it's communicating with the legitimate client. The attacking software continues sending information to the server and so forth.  
  
**Replay Attacks** - These are becoming quite common, This occur when information is captured over a network. Replay attacks are used for access or modification attacks. In a distributed environment, logon and password information is sent over the network between the client and the authentication system. The attacker can capture this information and replay it later. This can also occur security certificates from systems such as kerberos: The attacker resubmits the certificate, hoping to be validated by the authentication system, and circumvent any time sensitivity.