Arturo Alquicira

Common Vulnerability Research

DoS Attack – Makes a machine or network unavailable to intended users made by two or more persons or bots. DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers.
Involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic, or responds so slowly as to be rendered essentially unavailable.

In order to fix this problem firewalls can be set up to have simple rules such to allow or deny protocols, ports or IP addresses.

Code injection - is the exploitation of a computer bug that is caused by processing invalid data. Code injection can be used by an attacker to introduce (or "inject") code into a computer program to change the course of execution. The results of a code injection attack can be disastrous. For instance, code injection is used by some computer worms to propagate.

In order to fix this problem you can enforce language separation via Regular Expressions, Input validation and input encoding.

Phishing Attack - The usual technique is to send out spam email to thousands of recipients. The email will contain a link to a malicious site that has been set up to look like, say, a regular bank's site. When the user enters thier credentials in the login form, it actually is captured by the malicious site and then used to impersonate that user on the real site.

In order to fix this problem is to never click on links in an email. If an email says that you need to reset your password or else and provides a link, you type in the link to the bank directly in the web browser and then verify the information on the bank website.
Another thing to remember is to never trust emails even from people you know. Their email account could have been hacked and an unauthorized person could be send that email.