**P3 - Website Security and Performance**

**How security affects performance**Security is an important a part of a websites performance, from protecting users to keeping the server operational. If there is little or no security, hackers or viruses can gain access to the server, using it to harm users, steal data, or shut down the website.

**Hacking**  
Hackers are people who gain unauthorised access to computer systems, in this case webservers. Once they have gained access, they can change the website, steal or destroy files and access user data. They may damage the reputation of the website, or stop it from operating completely.

**Viruses**  
Viruses are usually aimed at users rather than servers, but if one does infect a server it can spread to all of the server’s clients. It may harvest data, use the server to infect other machines, or simply crash the website

**Protection**  
Servers tend to have a lot of security - more so than most users. This is because they are much more exposed on the internet, and are the target of a lot of hackers. In addition, the hardware itself is very expensive, so it requires physical protection.

**Firewalls**  
Firewalls are a set of rules that determine which traffic is allowed through which ports. For example, port 80 (http) is usually open, but 25 (telnet) may be closed. The direction of the traffic is also specified, so outgoing traffic can be allowed while incoming traffic is blocked, and vice-versa.   
This prevents attackers from connecting to the server on an unsecured port, and limits incoming traffic during a DDOS attack (in which a server is spammed with requests in order to deny service to other users).

**Passwords**  
Servers are administrated with passwords, to prevent attackers from messing with the server. These passwords should be generated with a password generator, and not shared upon request to prevent social engineering attacks. For example, a hacker posing as a sysadmin could claim to have forgotten the password to the server he is 'administering', and ask a legitimate sysadmin for it. If the real sysadmin just gives out the password without checking who is asking, then all the security will have been invalidated.

**Data Protection Act**  
The Data Protection Act is a set of laws that defines how any organisation that stores customer data must keep it protected. This includes only keeping relevant data for as long it is needed, not giving it to third parties without the customers permission (this is usually covered in the terms and conditions), and having a level of security appropriate for the sensitivity of the data.  
While companies must follow the DPA, it is for the benefit of the end user more than the company.