Q.1) How Firewall helps to secure pc?

Ans : A firewall is a system designed to prevent unauthorized access to or from a private network. You can implement a firewall in either hardware or software form, or a combination of both. Firewalls prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets. All messages entering or leaving the intranet (the local network to which you are connected) must pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

In protecting private information, a firewall is considered a first line of defense; it cannot, however, be considered the only such line. Firewalls are generally designed to protect network traffic and connections, and therefore do not attempt to authenticate individual users when determining who can access a particular computer or network.

Several types of firewalls exist:

- **Packet filtering:** The system examines each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
- **Circuit-level gateway implementation:** This process applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
- **Acting as a proxy server:** a proxy server is a type of gateway that hides the true network address of the computer(s) connecting through it. A proxy server connects to the internet, makes the requests for pages, connections to servers, etc., and receives the data on behalf of the computer(s) behind it. The firewall capabilities lie in the fact that a proxy can be configured to allow only certain types of traffic to pass (for example, HTTP files, or web pages). A proxy server has the potential drawback of slowing network performance, since it has to actively analyze and manipulate traffic passing through it.
- **Web application firewall:** A web application firewall is a hardware appliance, server plug-in, or some other software filter that applies a set of rules to a HTTP conversation. Such rules are generally customized to the application so that many attacks can be identified and blocked.

Q.2) if you are a system admin what steps/precautions will you take to secure it?

Ans :

basic security practices that are best to configure before or as you set up your applications they are as follows:

The security of the property that a charity's computer system is housed in is a basic check. Is the building or room secured with smoke and burglar alarms? Can people walk in and out without being checked? Are your computers secured to their desks or are all portable items locked away from sight when not in use?

A mobile device (such as a laptop) should never be the sole place where your important data is stored and should always be password protected. Better still is to encrypt the data held on the computer.

When travelling with your mobile device be extra vigilant and don't take any risks when using it in public places such as cafes or on public transport.

If you need to connect to the internet from a public WiFi hot-spot always check it is a trusted network or via a reputable supplier and be cautious about making financial transactions over these networks.

Use strong passwords:

After the physical security of your office, passwords are the next most important thing to consider. Use strong passwords with a combination of uppercase and lowercase characters, numbers, and symbols. This will help you defend against hackers who make random and systematic guesses that are based on commonly used words.

Use different passwords for different websites, use password management software (e.g.LastPass) to help you remember them. To thwart unauthorized password recovery that's based on commonly known information (your date of birth, the model of your first car, or your pet's name), consider whether you can use related but nonsense answers, for example the colour of your friend's car or name of your neighbour's pet.

Don't write down your passwords and put them in your drawer or attach to your monitor on a sticky-note!

Ensure robust user authentication and firewall protection:

Enhanced security can also come about through a process called dual factor authentication (2FA), which identifies individuals through a combination of user name, password and information known only to them.
As for firewalls: the best come at an enterprise level price, but – as with all aspects of security – small and medium size charities absolutely shouldn't be left out as discounted firewall software is available through the Technology Trust.

Get the right security software:

Another basic is the software needed to safeguard not only data and information, including passwords etc but also the computers themselves. Malware can make computers run very slowly; viruses can render them unusable.
Off-the-shelf security products, or their free versions, can be very useful but enterprise-grade equivalents, which also make life more difficult for hackers and automated hacking programs, are a step up. See this guide on protecting your charity with security software.

Another improvement from the basics is high end online filtering, which protects staff, data and information from malicious websites. Even innocuous-looking websites can contain threats that need to be neutralised. A trusted website might have been compromised by malware, which is ready to infect any computer that accesses it over the internet.

Safe browsing:

Educate staff to not forward on spam e-mails to colleagues or open suspect attachments. Don't click on spoof phishing links (even though they may seem plausible) and don't believe all the Facebook links that are just tricks or which are promising the earth! If in doubt check this helpful referencing site.

Consider moving data to the cloud:

The cloud is a great leveller, bringing data storage prices down to affordable levels and enabling organisations of any size to share in the same levels of technology security. It has achieved that by allowing charities and other organisations which have outsourced their IT to share all costs, including those of the physical security of the data centre, where the data and information is kept.

Using a cloud services provider that is ISO 27001 accredited will ensure that all processes during and after the move to cloud computing are compliant with it. This accreditation offers assurance that standards are adhered to.

However, exercise caution when accessing cloud services or granting access to another person for your files. Satisfy yourself that the cloud service provider is legitimate and will take good care of your data. Also check where data is stored, both physically in a well-protected data centre.

Make sure all staff use individual login passwords to cloud based websites.