How to securely host a website

1. Installing secure socket layer (SSL) certificates

Any information and data that is sent to and from the website is encrypted, translating this information into a language that is difficult to decipher by third parties.

2. Select a good hosting service.

Look for hosting services that include web application firewalls (WAFs), file transfer protocols (FTPs) or secure FTPs, especially if the website can upload files. Consider if you are selecting a shared hosting plan. Sharing a server with other websites could impact our website if other websites on that server are being attacked.

3. Enable site data backups

This can be done manually or automatically and can be stored inside a secure cloud/physical server.

4. Practice good online habits

This means using strong passwords, regularly updating software, enabling two-factor authentication to ensure that our website is most safe and up to date. Look out for any suspicious activity, or anything that looks abnormal on the website, and do not click on anything that looks weird.

5. Use anti-malware software

Adding an anti-malware software adds another layer of security to our website. Some of the services that certain options offer includes web scanning, malware detection and removal.

Potential challenges with securely hosting a website:

1. Cost

Hosting a website can become costly. This could incur from the hosting service you select, to all the add-ins/plug-ins including anti-malware systems and servers we need for our website to run safely and smoothly.

2. Hackers & Threats

There are a variety of threats and viruses that attackers use to destroy websites, including ransomware, gibberish hacks, Denial of Service (DoS), phishing, etc. This is why it is important to practice good online habits.