**Security Precautions**

**Encryption**

Encryption is used on the internet to protect user information that is sent between a browser and a server, this includes, passwords, payment information and other personal information that is considered private.

**How encryption works**

Unencrypted data, often known as plaintext, is encrypted using an encryption algorithm and an encryption key. This process then generates ciphertext that can only be seen in its original form if decrypted with the correct key. Decryption is simply the inverse of encryption, following all the same steps but in reverse order in which keys are applied.

**Benefits of encryption**

The main purpose of encryption is to protect the confidentiality of digital data that is stored on computer systems or transmitted from the internet or any other computer network.

**Types of encryption**

AES (Advanced Encryption Standard)

The Advanced Encryption Standard, is a symmetric encryption algorithm and the most secure. This method uses a block cipher, which encrypts data one fixed-size block at a time.

3DES (Triple Data Encryption Standard)

Triple Data Encryption Standard, is a current standard, and it is a block cipher. 3DES is a symmetric-key encryption that uses three individual 46-bit keys, it encrypts data three times, meaning your 46-bit key becomes a 168-bit key.

Twofish

Twofish is a symmetric block cipher. Twofish has a block size of 128-bits to 256 bits.

RSA

RSA is an asymmetric algorithm. Most RSA keys are 1024-bits and 2048-bits long.