Glossary

Hampshire Alerts: A platform which allows the public receive messages of information, crime alerts and witness appeals local to their area in which they live or work in a way that suits their needs and lifestyle by email, text or telephone.

Word Cloud: Is an image composed of words used in a particular text or subject, in which the size of each word indicates its frequency or level of importance

Denial of service: A method of taking a website out of action by overloading of 'flooding' the server.

Phishing: A method of accessing valuable personal details, such as usernames and passwords, often through bogus communications such as emails, letters, instant messages or text messages.

Pharming: A method of deceiving an individual into ending up at a fake website, even though the correct URL has been entered.

Spoofing: Masquerading as another individual or entity by falsifying data, thereby gaining an illegitimate advantage.

Doxing: Discovering and publishing the identity of an internet user, obtained by tracing their digital footprint.

Malware: A program or malicious software that consists of programming, for example code or scripts, designed to disrupt the performance of PCs, laptops, handheld devices, etc.

Whaling: A type of spear phishing (i.e. specifically directed) attack, such as an e-mail spoofing attempt, that targets senior members ('big fish') of a specific organization, seeking unauthorized access to confidential data.

Ransomware: A type of malware that prevents the use of a system, either by locking the system's screen or by locking the users' files unless a ransom is paid.

Social Engineering: In a cyber security context, the general art of manipulating people online so they give up confidential information.

Theft of data: Stealing computer-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information.