Deprecation of Vulnerable Encryption Standards

Behind every authentication, online purchase, and email sent to and from your boss, cryptography algorithms are working in the background to secure your information. Data Encryption Standard (DES) has a long history in cryptography advancement from peer review to find a secure encryption standard for government documents, to furthering education in the field of cybersecurity. Although, with the improvement of technology, the use of DES has met its end. The encryption algorithm's short key length makes it an easier algorithm to decrypt, thus leaving information open to attack. This paper will be addressing and summarizing why DES is no longer being used, how DES is being deprecated, and where the future of algorithmic encryption will be heading to compensate for the loss of this readily used standard for encryption to upkeep cybersecurity protection.

In need of a reputable guideline for cybersecurity standards, I looked to the world leading institute for creating encryption standards in technology, The National Institute of Standards and Technology (NIST). The National Institute of Standards and Technology (NIST) shares and creates publications from their Information Technology Laboratory in an effort to educate and preserve the integrity of the cybersecurity industry. The National Institute of Standards and Technology (NIST) gave notice of when DES will further be disallowed from certain protocols such as TLSS, IPsec, and others through their publications and published many guidelines, frameworks, and updates on how to move to a more secure encryption algorithm. The updated algorithm in question is currently the Advanced Encryption Standard (AES) because of its longer key length. Understanding what information to look for and where to keep up to date on standards in cryptography can prevent a company or personal information from being compromised because of invalidity with traffic protocols.