Cyberlitica
Threat Intelligence Services

Dark Web Search Technical Overview:

Our Dark Web Search exists to help make passwords more secure, not less. While no Internet-connected system can be guaranteed to be impregnable, we keep the risks to an absolute minimum and firmly believe that the risk of unknowingly using compromised passwords is far greater.

Since our database of compromised passwords is far larger than what could be downloaded to the browser, the compromised password check we perform must occur server-side. Thus, it is necessary for us to submit a hashed version of your password to our server. To protect this data from eavesdropping, it is submitted over an SSL connection. The data we pass to our server consists of three unsalted hashes of your password, using the MD5, SHA1, and SHA256 algorithms.

While unsalted hashes, especially ones using MD5 and SHA1, are NOT a secure way to store passwords, in this case that isn’t their purpose – SSL is securing the transmitted content, not the hashes. Many of the passwords we find on the web are not plaintext; they are unsalted hashes of the passwords.

Since we’re not in the business of cracking password hashes, we need these hashes submitted for more comprehensive lookups. We do not store any of the submitted data. It is not persisted in log files and is kept in memory only long enough to perform the lookup, after which the memory is zeroed out.

Our server-side infrastructure is hardened against infiltration using industry standard tools and techniques and is routinely tested and reviewed for soundness.