

**123456**

Maggie Van Nortwick

The password "123456" is the most common in the world, having been found over 23 million times in the information stolen from countless internet platforms and services in recent data breaches. This piece seeks to explore the complexity and security of such passwords, as well as the process of publicizing private data.

In the case of a breach, user data is publicized with explicit malicious intent, yet, unless the passwords are stored in plaintext (which is the fault of the service that's been breached), the data is usually hashed and/or encrypted, of which both processes are used specifically to obfuscate the information and prevent it from being read. This form of publication, in which secret, private data is made public while maintaining, to some degree, its secrecy, is unique to data breaches.

This piece takes 1 million hashed passwords, ranked by the number of times they've been used, from a database of over 300 million passwords leaked in recent breaches. It then uses these passwords to make a binary pattern, in which the scale of the pattern reflects the prevalence of the passwords used. In this way, larger, more "zoomed in" patterns are created from passwords that are less common and thus likely more complex, in which case the created pattern is less apparent. This speaks to the positive correlation between complexity and security, while the uniformity of the patterns despite the varying passwords addresses the effectiveness of existing security measures.

Placing these patterns, and thus, the passwords concealed within them, in the immensely public setting of the Ars Electronica Centers' façade mimics the obfuscated yet publicizing nature of data breaches.