

Dyman & Associates Risk Management Projects: 10M Passwords Publicized For Research



We've all heard of this before: a hacker releasing a certain number of passwords and usernames, presumably just for the lulz. But this time, we're talking about 10 million records posted by no less than a [security](#) specialist himself.

Security expert Mark Burnett has published 10 million sets of usernames and passwords online in an effort to equip the security sector with more information, while also getting himself potentially tagged as a criminal.

He clarified that his release of the username-password list is solely for white-hat purposes -- to aid research in making login authentications more effective and fraud-proof. Burnett insisted that he does not intend to help facilitate any illegal activity or defraud people by his actions.

"I could have released this data anonymously like everyone else does but why should I have to? I clearly have no criminal intent here. It is beyond all reason that any researcher, student, or journalist have to be afraid of law enforcement agencies that are supposed to be protecting us instead of trying to find ways to use the laws against us," he said in his post.

Leaking a massive amount of user data into the wild certainly does not sound like great help for most people but for security professionals, it's an important tool for research. For instance, how else would they know that online users are generally bad at choosing passwords?

In his post, he shared that he would often get requests for his password data from researchers but he would just decline them before. But since he also know its importance, he decided to publish a clean data set for the public.

"A carefully-selected set of data provides great insight into user behavior and is valuable for furthering password security. So I built a data set of ten million usernames and passwords that I am releasing to the public domain."

To be fair, [Dyman & Associates Risk Management Projects](#) confirms that analyzing a username-password set seems to be more helpful for the security researchers.

According to him, it was by no means an easy decision but he eventually posted it after weighing down a number of factors. And though Burnett said he believes most of the data are already expired and unused, the domain part of the logins and any keyword that could link it to a certain site were still removed to make it difficult for those with criminal intent.

Besides, Dyman & Associates Risk Management Projects experts agreed with him in saying that if a hacker would need such a list in order to attack someone, he's not going to be much of a threat.

Burnett has previously helped in collecting the recent list of worst passwords to alarm people into adopting better practices when it comes to their login credentials.

Lastly, he imparted the following warning for complacent users: "Be aware that if your password is not on this list that means nothing. This is a random sampling of thousands of dumps consisting of upwards to a billion passwords."