Relatório de Integridade de dados - Email

Email: franciscolopescaldas@gmail.com

Vazado em: Dropbox

Nome do domínio:

dropbox.com

Data do vazamento:

2012-07-01

Dados vazados:

Email addresses, Passwords

Descrição do vazamento:

In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Vazado em: Lastfm

Nome do domínio:

last.fm

Data do vazamento:

2012-03-22

Dados vazados:

Email addresses, Passwords, Usernames, Website activity

Descrição do vazamento:

In March 2012, the music website Last.fm was hacked and 43 million user accounts were exposed. Whilst Last.fm knew of an incident back in 2012, the scale of the hack was not known until the data was released publicly in September 2016. The breach included 37 million unique email addresses, usernames and passwords stored as unsalted MD5 hashes.

Vazado em: LinkedIn

Nome do domínio:

linkedin.com

Data do vazamento:

2012-05-05

Dados vazados:

Email addresses, Passwords

Descrição do vazamento:

In May 2016, LinkedIn had 164

million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

Vazado em: ModernBusinessSolutions

Nome do domínio:

modbsolutions.com

Data do vazamento:

2016-10-08

Dados vazados:

Dates of birth, Email addresses, Genders, IP addresses, Job titles, Names, Phone numbers, Physical addresses

Descrição do vazamento:

In October 2016, a large Mongo DB file containing tens of millions of accounts was shared publicly on Twitter (the file has since been removed). The database contained over 58M unique email addresses along with IP addresses, names, home addresses, genders, job titles, dates of birth and phone numbers. The data was subsequently attributed to "Modern Business Solutions", a company that provides data storage and database hosting solutions. They've yet to acknowledge the incident or explain how they came to be in possession of the data.

Vazado em: MyHeritage

Nome do domínio:

myheritage.com

Data do vazamento:

2017-10-26

Dados vazados:

Email addresses, Passwords

Descrição do vazamento:

In October 2017, the genealogy website MyHeritage suffered a data breach. The incident was reported 7 months later after a security researcher discovered the data and contacted MyHeritage. In total, more than 92M customer records were exposed and included email addresses and salted SHA-1 password hashes. In 2019, the data appeared listed for sale on a dark web marketplace (along with several other large breaches) and subsequently began circulating more broadly. The data was provided to HIBP by a source who requested it be attributed to "BenjaminBlue@exploit.im".