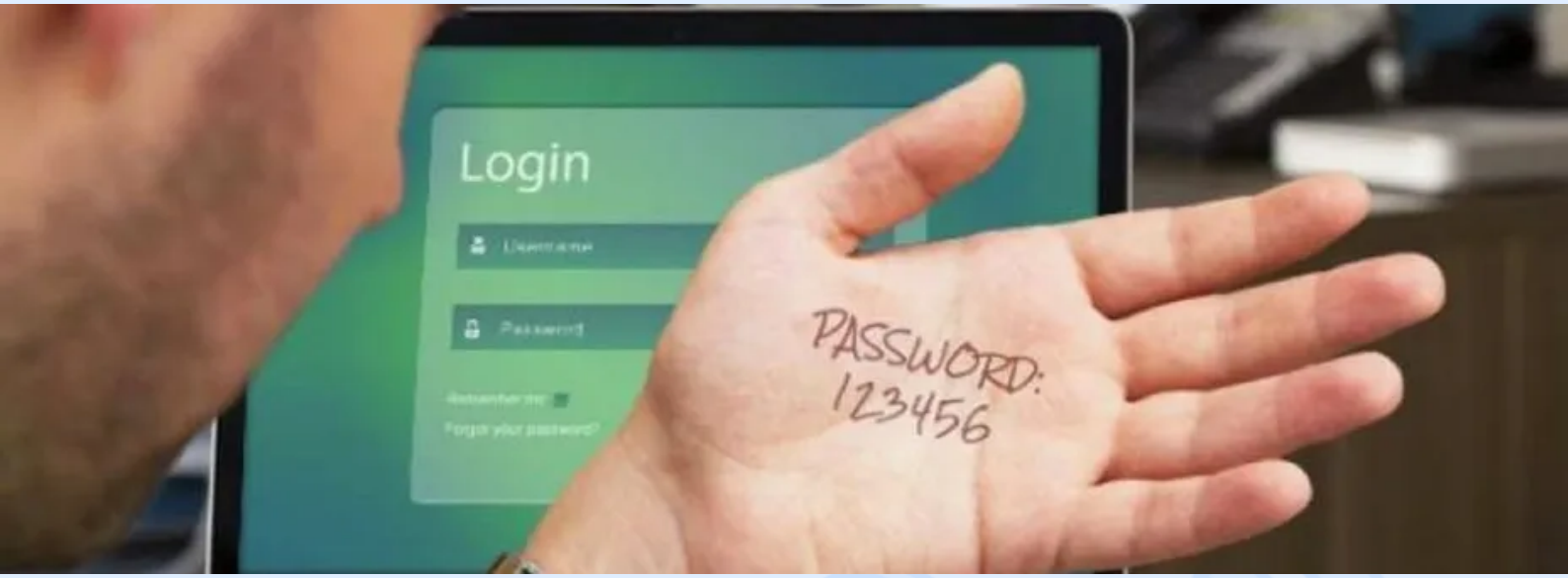


The leakage of the Largest Credential Database

Scandals associated with the theft of passwords and personal data happen regularly - only in the past couple of years the passwords of popular mail services were leaked to the open network, and even the services for storing passwords were hacked.

1.4 Billion passwords were found in a single database - how can you be sure that yours is not there? In this article you will find out what kind of threats your password is open to, and how to protect your personal data with the correct credentials.

All passwords are presented in text form, and the most terrible fact is that most of them are passed as acceptable. Almost all users, interviewed by researchers, confirmed that the passwords were valid.

Researchers compared the data from the leak to other known bases

It was discovered that, although most of the credentials were already known, 14% of the login/password pairs had never been found before.

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk

This new database adds 385 million new accounting pairs, 318 million unique users and 147 million passwords.

Exposed Unique Attributes	1.4B Credentials DB	Exploit.in + Anti Public	#Difference	%Diff
Username/Password pairs	1,400,553,869	1,015,261,204	385,292,665	28%
Users	1,163,976,485	845,167,132	318,809,353	27%
Passwords	463,619,984	316,143,487	147,476,497	32%

Since the data is organised in alphabetical order, the main problem is easily detected - the **reuse of passwords**:

********chu@epost.de: l369888369
********chu@gmx.de: l369888369
********chu@lycos.de: l369888369
********chu@web.de: l369888369
********chu@yahoo.com:l369888369
********chu@yahoo.de: l369888369

Here is the list of 40 most popular passwords:

+44 20 7183 5820
info@magora.co.uk
sales@magora.co.uk

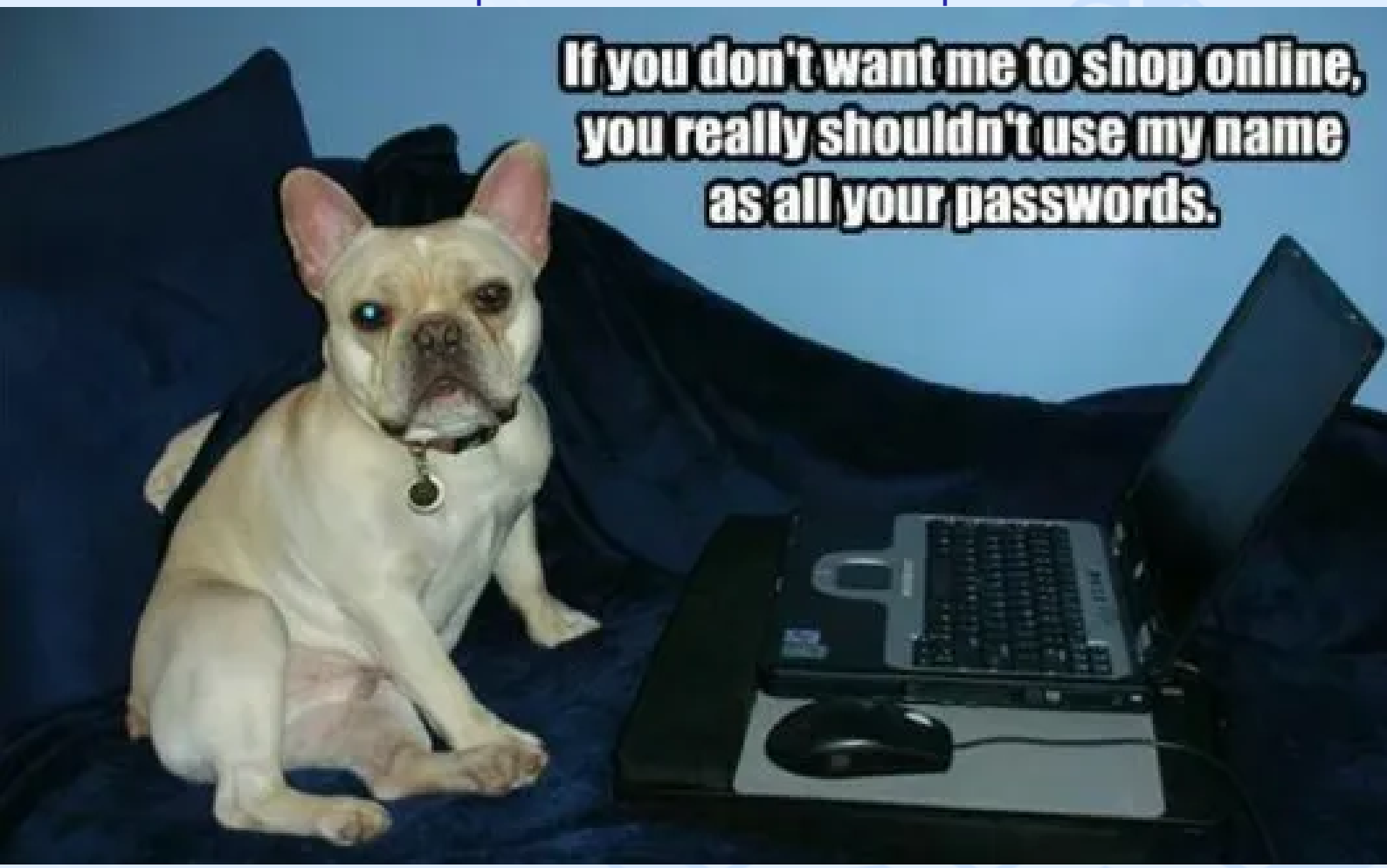
	Count	Password		Count	Password
1	9218720	123456	21	370652	666666
2	3103503	123456789	22	354784	123
3	1651385	qwerty	23	347187	monkey
4	1313464	password	24	343864	dragon
5	1273179	111111	25	311371	1qaz2wsx
6	1126222	12345678	26	300279	123qwe
7	1085144	abc123	27	299984	121212
8	969909	1234567	28	298938	myspac
9	952446	password1	29	291132	a123456
10	879924	1234567890	30	276473	qwe123
11	866640	123123	31	270488	1q2w3e4r
12	834468	12345	32	268121	zxcvbnm
13	621078	homelesspa	33	263605	7777777
14	564344	iloveyou	34	255079	123abc
15	527158	1q2w3e4r5t	35	250732	qwerty123
16	470562	qwertyuiop	36	241721	qwerty1
17	468554	1234	37	241495	987654321
18	417878	123456a	38	227701	222222
19	398114	123321	39	226785	555555
20	371627	654321	40	220363	112233

How Do Hackers break passwords?

There are always at least two ways to crack the password:

- A trivial selection, which takes a huge amount of resources and time, but with the proper luck, will not take an hour.
- The most simple and effortless way is the "pet attack." This is when people choose the name of their pets as a password, making it very easy for hackers.

Recommendations for passwords and their compilation



Actually, in order to complicate the process of hacking a password, a large number of recommendations applicable to its selection and compilation are singled out. We will try to give only some, the most important ones.

Fighting QWERTY

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk

Lower your eyes to the keyboard and see how these keys are located. No doubt, you noticed that they are running in a row. So never do such nonsense. Do not allow more than two characters running consecutively in the password.

For example, passwords like qwinto or abscuro will be quite effective (they are called persistent ones, that is, those that are hard to crack), but passwords like qwento or abco will be ineffective, hacking them takes much less time.

When choosing a password, try to avoid alternating characters (alphabetically or by keyboard layout), this can save you from hacking by selection.

Collisions - What Is It and How to Avoid It

When you come up with the key for encryption, try to avoid such nonsense as repetition of symbols. In itself, the word Collision is already a lousy password, in it we have two consecutive letters L . When encrypted, it will give a lot of duplicate characters. And the repetition of the same character in the password makes it much easier to select.

No matter how much you like it, try to avoid repeated symbols and use the same letters in your password.

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk

Length vs. Efficiency

Some people believe that the names of Icelandic volcanoes are excellent passwords. And let's be honest, are you ready to memorize 15 characters of text, about which you can break a language? And often there are more than a lot of collisions and ordering of symbols in these names.

Compare on the above parameters 2 simple passwords (conditionally simple, of course):

1. Faithful
2. Yokalatarakoyl

Let's see what we have in both cases and what disadvantages there are:

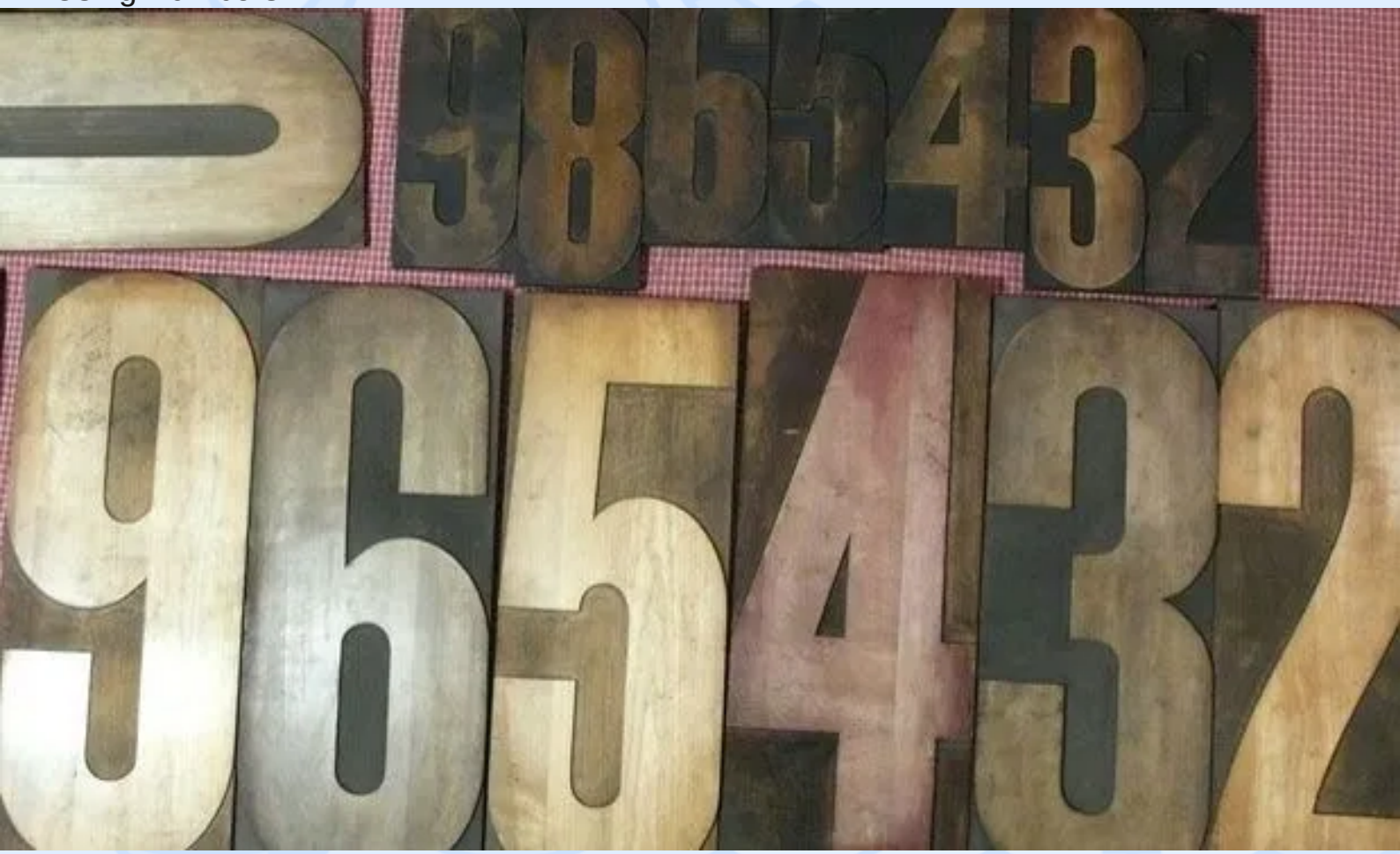
1. A small number of characters, one alphabet is used, no numbers. However, all the symbols are quite scattered in alphabetical order and layout. And in the password we have 6 effective symbols.
2. A large number of characters, one alphabet, no numbers. However, in this password we have two letters "k", "y", "o" and "l". We have four letters "a" at once. Therefore, in fact, in this

+44 20 7183 5820
info@magora.co.uk
sales@magora.co.uk

password there are 6 characters.

You do not need to be a wisecrack to figure out that these passwords are equally reliable, regardless of the number of characters that are used in the second. Therefore, we can safely say that the password is such a thing, where the quantity is very rarely intertwined with quality.

Using Numbers



But how to make the first password more effective? - Simple, but effective advice - to add the numbers.

- Adding to the word "Loyalty" something like "11111" or "666" is, of course, a solution, but generally ineffective. We add more symbols to remember, and we increase the efficiency only by one.
- It is best to follow the rules applicable to letters to pick up 3-4 figures. So, for example, the password "Loyalty1859" will contain 10 effective symbols.
- Each account requires its own password. Even if one of the passwords appears unreliable, hackers won't get access to all your accounts at once.

More complicated and better-protected passwords are the combination of small and capital letters, numbers, special symbols, collected in non-predictable order.

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk

The last, but not the least: do not keep your passwords auto-saved by the browser on your computer or smartphone - it’s the easiest way for hackers to reach them. If you have some points to be discussed - contact our London team or just come for a lovely chat with a cap of tea.

magora

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk