



Старая песня о главном

отчаянные возгласы?!» – спросите вы. Судите сами...

Человек удивительно настойчивое в стремлении к самообману существо. И все с детства известные нам поговорки, вроде «Пока жареный петух не клюнет...», ещё долго будут актуальны для абсолютного большинства из нас. «К чему эти

Есть такой сайт – www.leakedsource.com. На нём находятся базы данных, включая пары «логин/пароль», различных взломанных по всему миру ресурсов. В том числе очень крупных (например, LinkedIn.com и Twitter.com) и в том числе российских (VK.com, Rambler.ru, Mail.ru). На этом же сайте, кстати, можно проверить, была ли взломана ваша учётная запись и, если да, сделать запрос на её удаление из базы. Что же выясняется по итогам анализа логинов и паролей взломанных аккаунтов? А выясняется то, что пользователи массово пренебрегают элементарнейшими, всем давно известными и миллион раз повторенными правилами составления паролей! Вроде тех, что длина пароля должна быть не менее 8 символов, что должны использоваться цифры и буквы различного регистра, и ещё, желательно, спецсимволы. А также, что нельзя использовать в качестве пароля своё имя, личные данные и распространённые сочетания клавиш вроде «qwerty» и «123456».

К примеру, возьмём базу взломанных учётных записей «ВКонтакте» (VK.com) объёмом 100,5 млн. записей и посмотрим насколько неизобретательны были, без преувеличения можно сказать, мы с вами. Чаще всего использовался пароль «123456» - 709067 пользователями, второй по популярности пароль «123456789» был у 416591 пользователя, на третьем месте – (бинго!) пароль «qwerty», 291645 пользователей. Сермяжный коллективный разум 33 тысяч человек даже каким-то образом вывел на 32-е место рейтинга пароль, который не знающие великого и могучего авторы www.leakedsource.com не постеснялись написать полностью.

Ещё пример – топ-5 статистики паролей 98 млн. взломанных записей Rambler.ru:

Место	Пароль	Количество использовавших его пользователей
1	asdasd	723039
2	asdasd123	437638
3	123456	430138
4	000000	346148
5	666666	249812

Учётные записи с такими паролями ломаются простейшими программами-подборщиками паролей за секунды! А ведь сколько раз каждый пользователь слышал наставления о необходимости использования сложных паролей? Все всё знают – и тихо надеются, что «этого со мной не случится».

Легко может случиться. Ибо работа злоумышленников поставлена на поток – учётные записи взламываются в автоматизированном режиме, после чего полученные данные или продают, или сразу используют для рассылки спама, вредоносного ПО и прочей преступной деятельности.

Вы не хотите, чтобы кто-то рылся в вашей личной переписке? И даже не хотите порадовать своих знакомых рассылкой свежих вирусов?

Что ж, тогда мы ещё раз призываем вас обратить внимание на используемые (для рабочих информационных систем и ресурсов, для социальных сетей и личных почтовых ящиков) пароли, на то как вы их используете и когда последний раз меняли:

- Достаточно стойкий к взлому пароль должен состоять из не менее 8 символов, среди которых должны быть буквы обоих регистров, цифры и спецсимволы (% , \$, ! и т.п.);
- Не используйте при составлении пароля имя и личную информацию (дата рождения, email, адрес и т.д.);
- Не используйте распространённые буквосочетания и словарные слова;
- Не используйте последовательности клавиш на клавиатуре (123456, qwerty, asd и прочие и их обратное написание);
- Не используйте пароли по умолчанию;
- Регулярно меняйте пароли и не используйте повторно старые пароли;
- Используйте разные пароли для разных сайтов и систем.