Не оставляйте безопасность паролей на волю случая

Как запомнить огромное количество паролей, которые приходится использовать каждый день? Ведь они не должны быть слишком простыми, чтобы их нельзя было отгадать и использовать в неблаговидных целях. Ниже даны некоторые рекомендации по выбору безопасных паролей, обеспечивающих конфиденциальность ваших данных.

Интернет давно перестал быть только средством связи. Почта, банковские операции, подписка на ленты новостей и даже подача налоговой декларации — теперь практически любые данные можно передавать в электронном виде через Интернет. А для доступа к любой из этих служб необходимо указывать пароль. Каким образом следует хранить или запоминать пароли? Записывать в отдельный файл на своем ПК? Это одна из тех ошибок, о которых предупреждают эксперты. Пароль не должен быть записан где бы то ни было, так как существует реальная угроза того, что он будет украден хакером.

Как выбрать надежный пароль?

Хакер или любой другой недоброжелатель, пытающийся получить доступ к вашим данным, в первую очередь попробует использовать примитивные варианты пароля (ваше имя, кличка собаки или дата рождения). Поэтому пароль должен быть длинным, сложным и, кроме того, регулярно изменяться. Эти три заповеди нужно неуклонно соблюдать. Однако, чтобы обезопасить себя полностью, этого недостаточно. Для подбора пароля хакеры используют специальные утилиты, составляющие различные сочетания слов и цифр. База данных этих программ включает все содержимое словаря, в том числе имена собственные. Поэтому использовать в качестве пароля вариант «иванпетров» также небезопасно. Для того чтобы минимизировать риск, рекомендуется выбирать пароль длиной не менее восьми символов (это уже существенно затруднит его подбор) и включать в его состав такие символы, как +, #, |, * (к сожалению, не все программы и ресурсы допускают использование подобных символов в поле для ввода пароля). Как же запомнить такую сложную комбинацию, особенно если она не должна содержать знакомых слов?

Шифрование для усиления безопасности

Хотя способы, описанные во врезке «Примеры безопасных паролей», позволяют подобрать таковой, они не гарантируют защиту от программ, копирующих ввод с клавиатуры или пытающихся получить другие конфиденциальные данные, например номера банковских карт. Помимо современной антивирусной программы и брандмауэра, которые абсолютно необходимы для защиты компьютера, неплохо иметь средства, предназначенные для защиты личной информации. Это специальное ПО, позволяющее хранить такие данные в зашифрованном виде. Например, разработки компаний Symantec и Aladdin не только обеспечивают безопасность хранения конфиденциальной информации, но и позволяют создать отдельный профиль для каждого члена семьи. Даже если компьютер используют несколько человек, пароли будут храниться таким образом, чтобы их не могли узнать другие пользователи. Кроме того, эти программы могут автоматически заполнять поля форм, когда для доступа к электронной службе требуется указать пароль или какую-либо другую информацию (например, адрес или номер банковской карты).

По материалам, предоставленным компанией Symantec.

Е. Т.

Примеры безопасных паролей

Можно составить пароль по первым буквам слов в предложении и добавить к нему несколько специальных символов или цифр. Например, «Приключения Шерлока Холмса» дает буквы «пшх» в качестве первой части пароля. Добавим к ним число букв в каждом слове предложения: 11, 7, 6. На первый взгляд пароль «пшх 1176» заучить трудно, однако все, что вам нужно сделать, — это вспомнить о Шерлоке Холмсе и сосчитать число букв.

Еще один способ — заменить гласные в слове на строку запоминающихся символов. Допустим, слово «конституция» можно заменить на «к+нст*т!ц#я» или «к1нст2т3ц45». И не забывайте регулярно изменять пароль!