О пределах человеческой памяти или Как запомнить все эти пароли?

Ранее мы уже писали, что несмотря на все увещевания «безопасников» большинство пользователей упрямо используют в качестве паролей простейшие буквосочетания, нарушая тем самым даже самые базовые правила составления паролей – например, особенной популярностью неизменно пользуются пароли «123456» и «qwerty». Даже для самых сокровенных систем и данных – онлайн-банкинга и персональных данных. Не говоря уже о рабочих компьютерах и корпоративных информационных системах.

Понятно, «безопасники» в ужасе и продолжают в который раз взывать чуть ли не к чувству гражданского самосознания пользователя. А пользователь смиренно слушает, что пароль должен быть не менее 8 символов, содержать заглавные и строчные буквы и спецсимволы и не являть собой словарные слова и распространённые буквосочетания и… продолжает вводить «123456».

И ведь всем (и, по секрету, «безопасникам» тоже!) понятно почему: потому что нормальный человек просто физически не в состоянии запомнить все эти 125 паролей к разным компьютерам, сайтам и системам, составленные по всем правилам информационной безопасности. А если их ещё и менять каждые 90-180 дней, как этого, опять же, требуют «безопасники»!? Тут только запомнил пароль – и как раз подходит время его менять…

Как жить дальше?

Реалистичных с практической точки зрения вариантов не так много:

1. Использовать для всех 125 компьютеров, сайтов и систем два или, максимум, три пароля. А лучше один и никогда его не менять. Самый распространённый и самый, конечно, рискованный вариант – узнав этот один пароль злоумышленник, понятно, получает доступ сразу ко всем вашим системам, сайтам и данным. В этом случае вам сильно «не повезёт»!
2. Использовать различные пароли и записывать их куда-нибудь. Куда записывать? В файл? Крайне опрометчиво: то же вредоносное ПО первым делом сканирует компьютер на наличие файлов с паролями. На бумажку? Бумажку надо где-то хранить, её банально можно потерять, да и вообще – не слишком это удобно.
3. Использовать специальные программы – менеджеры паролей. Это, по сути, та же «бумажка», но данные она хранит зашифрованными стойким к взлому алгоритмом шифрования (большинство современных менеджеров паролей используют алгоритм, для расшифровки которого даже суперкомпьютеру потребуются миллиарды лет вычислений).

Третий вариант – наиболее целесообразный, так как позволяет и доступ пользователя в различные системы обезопасить и запоминать придётся лишь один пароль, теперь уже для доступа к менеджеру паролей. Правда, и тут не без рисков - если вы забудете этот «главный» пароль, недоступными станут сразу все остальные пароли. Но идеальных решений нет – с точки зрения информационной безопасности человек всегда был и, видимо, будет «слабым звеном».

Наиболее распространённый на сегодня менеджер паролей, с широким функционалом, надёжной защитой, работающий почти в любой операционной системе и к тому же ещё и бесплатный - программа KeePass. В отличие от многих других менеджеров паролей, которые являются расширениями браузеров, это – отдельно устанавливаемая и независимо от других работающая программа. Обладает развитыми средствами управления паролями и их сменой, позволяет безопасно синхронизировать базу паролей через DropBox.

Другой вариант – расширение для браузера LastPass. Очень удобен для активных пользователей интернета, есть функция автозаполнения форм «логин-пароль». Имеет мобильную версию для iOS, Android и Windows Phone. Базовая версия бесплатна, премиум-версия стоит $12 в год.

Есть, конечно, и другие в той или иной степени аналогичные менеджеры паролей – 1Password, DashLane, RoboForm и другие. В интернете также можно найти и несколько обзоров менеджеров паролей (достаточно набрать в поисковике «менеджер паролей обзор»).

Выбор - за вами!