Пароли — это ключи, которые открывают доступ к личным данным, хранящимся на компьютере и в учетных записях в Интернете.

Если злоумышленники украдут эти данные, они могут воспользоваться ими для открытия новых счетов кредитных карт, получения кредита или выполнения через Интернет иных действий от вашего имени. Очень часто вы можете не подозревать о таких действиях до тех пор, пока не станет слишком поздно.

К счастью, создать и хорошо защитить надежные пароли несложно.

Что такое надежный пароль?

Для злоумышленника надежный пароль выглядит как случайный набор знаков. Следующие критерии помогут в выборе пароля.

Используйте как можно больше символов. Каждый дополнительный знак увеличивает степень защиты пароля. Пароль должен содержать не менее 8 знаков; 14 знаков и более являются идеальным вариантом.

Так как многие системы позволяют использовать знак пробела при создании пароля, можно составить пароль из нескольких слов — парольную фразу. Такие фразы легче запомнить и труднее подобрать.

Используйте комбинацию из букв, цифр и других символов. Чем больше разных знаков содержит пароль, тем труднее его подобрать. Другие важные сведения:

- **Чем меньше разных символов вы используете, тем длиннее должен быть ваш пароль**. Пароль из 15 случайно выбранных букв и цифр примерно в 33 тысячи раз надежнее, чем пароль из 8 знаков, содержащий разные типы имеющихся на клавиатуре знаков. Если нет возможности включить в пароль символы, следует сделать его значительно длиннее, чтобы обеспечить ту же степень защиты. Идеальный пароль сочетает в себе длину и разнообразие знаков.
- **Используйте все символы клавиатуры**, а не только часто используемые. Цифры и символы, вводимые с помощью клавиши Shift, также часто используются при создании паролей. Пароль будет надежнее, если вы используете все имеющиеся на клавиатуре символы, включая знаки препинания, расположенные не в верхнем ряду клавиатуры, и символы, характерные только для вашего языка.

Используйте слова и фразы, легкие для запоминания, но не очевидные для злоумышленников. Проще всего запомнить пароли и парольные фразы, записав их. Вопреки общепринятому мнению, нет ничего страшного в записи пароля, если данные при этом защищены надлежащим образом.

Пароли, записанные на бумаге, обычно труднее взломать через Интернет, чем пароли, хранящиеся в диспетчере паролей, на веб-узле или в иной программе для хранения данных.

6 этапов создания надежного и легко запоминающегося пароля

Следуйте этим инструкциям для создания надежного пароля.

1. **Придумайте предложение, которое точно не забудете,** Это предложение и будет основой для надежного пароля или парольной фразы. Предложение должно быть запоминающимся (например, "Моему сыну Павлу три года").
2. **Убедитесь, что выбранная вами система проверки пароля допускает использование идентификационных фраз.** Если имеется возможность использовать парольные фразы (с пробелами между знаками), воспользуйтесь ею.
3. **Если использование идентификационных фраз недопустимо в данной системе, воспользуйтесь обычным паролем.** Составьте новое бессмысленное слово из первых букв всех слов, входящих в созданное предложение. В нашем примере получится: "мсптг".
4. **Усложните комбинацию**, используя заглавные буквы, строчные буквы и цифры. Можно поменять местами буквы в слове или намеренно допустить орфографические ошибки. Например, в парольной фразе, приведенной выше, можно допустить ошибку в имени или заменить слово "три" на цифру 3. Имеется множество возможных подстановок, и чем длиннее предложение, тем более надежным будет пароль. Наш пример можно преобразовать так: "Моему сыНу Па8лУ 3 годА". Если компьютер или система не поддерживают парольные фразы, тот же метод можно применить и к простому паролю. Например, "мСп3Г".
5. **Наконец, замените отдельные символы.** Можно использовать знаки, похожие на буквы, объединять слова (удаляя пробел между ними) и т. п. Следуя нашему примеру, мы получаем: "Моему

$ыНуП@в8лУ 3 годА" или "м$п3Г!".

6. **Проверьте свой новый пароль с помощью программы проверки паролей.** Программа проверки паролей на данном веб-узле определит надежность выбранного пароля, как только вы его введете и не сохраните при этом.

Методы создания пароля, которые не следует использовать.

Существуют общепринятые методы, о которых могут знать и злоумышленники. Во избежание создания ненадежного пароля

- **не используйте последовательные комбинации и повторяющиеся символы.** Такие сочетания (например, "12345678", "222222", "abcdefg" или сочетания соседних букв на клавиатуре) не являются надежными паролями.
- **Избегайте использования только замен похожих цифр и символов.** Преступников и иных злоумышленников, обладающих достаточными знаниями для подбора и взлома пароля, не удастся ввести в заблуждение подобными заменами, например "i" на "1" или "a" на "@" в словах "M1cr0$0ft" или "П@р0ль". Однако не стоит пренебрегать такими заменами в сочетании с другими методами повышения надежности пароля, такими как увеличение длины, неправильное написание, использование заглавных и строчных букв.
- **Не применяйте свое имя пользователя в качестве пароля.** Избегайте также использования иных личных данных (своих или своих близких), таких как имя, дата рождения, код социального страхования и т. д. Эти сведения используются злоумышленниками в первую очередь.
- **Избегайте словарных слов на любом языке.** Злоумышленники обладают совершенными средствами, позволяющими быстро подобрать пароли, в основе которых лежат слова из разных языков; слова, написанные задом наперед; распространенные орфографические ошибки и замены, а также все виды ругательств и других слов, которые не произносят при детях.
- **Используйте несколько паролей.** При взломе одного компьютера или системы, где используется определенный пароль, опасности подвергаются все прочие данные, защищенные тем же паролем. Настоятельно рекомендуется использовать разные пароли для различных систем.
- **Не сохраняйте пароль в Интернете.** Злоумышленник, получивший доступ к вашему паролю в Интернете или в компьютерной сети, получает доступ ко всем данным.

Использование пустого пароля

Пустой пароль (отсутствие пароля) более эффективен, чем ненадежный, такой как, например, "1234". Простой пароль легко разгадать, но на компьютерах с Windows XP к учетной записи, не защищенной паролем, нельзя получить доступ через локальную сеть или Интернет (данная функция недоступна в ОС Microsoft Windows 2000, Windows Me и в более ранних версиях). Пустой пароль для учетной записи на компьютере можно использовать, если выполнены перечисленные ниже требования.

- У вас один или несколько компьютеров, но вам не нужен доступ с одного компьютера на другой.
- Ваш компьютер физически защищен (вы доверяете всем, кто имеет доступ к вашему компьютеру).

Не всегда рекомендуется использовать пустой пароль. Например, переносной компьютер скорее всего физически не защищен, и на нем лучше использовать надежный пароль.

ДОСТУП К ПАРОЛЯМ И ИХ ИЗМЕНЕНИЕ УЧЕТНЫЕ ЗАПИСИ В ИНТЕРНЕТЕ

Веб-узлы имеют различные политики, регулирующие доступ к учетной записи и изменение пароля. На домашней странице веб-узла найдите ссылку (например "Учетная запись"), служащую для перехода на страницу веб-узла, где выполняется управление паролем и учетной записью.

Пароли на компьютере

Сведения о создании и изменении учетных записей, защищенных паролями, а также о доступе к ним и о том, как установить защиту паролем при загрузке компьютера, обычно имеются в файлах справки операционной системы. Можно также попытаться найти эти сведения на веб-узле производителя программного обеспечения. Например, в ОС Microsoft Windows XP сведения об управлении паролями, их изменении и т. д. можно найти в системе интерактивной справки.

Хранение паролей в секрете

Относитесь к паролям и парольным фразам так же серьезно, как к данным, которые они защищают.

- **Никому не сообщайте пароль.** Держите пароль в секрете от своих близких (особенно от детей) и друзей, которые могут сообщить его кому-либо еще. Исключением являются пароли, которые необходимо знать вашим близким, например пароль к вашему банковскому счету в Интернете, который можно сообщить жене или мужу.
- **Храните пароль в надежном месте.** Будьте внимательны, если записали пароль на бумаге или какой-либо другой носитель. Не оставляйте записку с паролем там, где вы не оставили бы данные, которые он защищает.
- **Никогда не пересылайте пароль по электронной почте.** Любое сообщение электронной почты, содержащее запрос пароля или требующее перейти на веб-узел для подтверждения пароля, почти наверняка является мошенническим. Это относится и к сообщениям такого типа, полученным от надежной компании или человека. Сообщение электронной почты может быть перехвачено, а отправитель запроса может быть совсем не тем, за кого себя выдает. В фишинг-аферах используются мошеннические сообщения электронной почты, обманным путем заставляющие раскрыть имя пользователя и пароль и позволяющие злоумышленникам завладеть идентификационными данными и т. п. Дополнительные сведения о фишинг-аферах и о защите от мошенничества в Интернете.
- **Регулярно меняйте пароли.** Это поможет ввести злоумышленников в заблуждение. Чем надежнее пароль, тем дольше можно его использовать. Пароль из 8 знаков или менее можно применять в течение недели, в то время как сочетание из 14 и более знаков может служить несколько лет, если оно составлено по всем правилам, приведенным выше.
- **Не вводите пароли на чужих компьютерах.** Компьютеры в интернет-кафе и лабораториях, системы общего доступа, интерактивные терминалы, а также компьютеры на конференциях и в залах ожидания аэропортов не могут считаться безопасными и подходят только анонимного выхода в Интернет. Не пользуйтесь такими компьютерами для проверки электронной почты, банковского счета, доступа в виртуальные комнаты для разговоров и доступа к другим учетным записям, где запрашивается имя пользователя и пароль. Злоумышленники применяют недорогие и быстро устанавливающиеся устройства, записывающие последовательность нажатий на клавиши. Такие устройства позволяют мошенникам получать через Интернет все данные, введенные в компьютер. Помните, что ваши пароли и парольные фразы так же важны, как и данные, которые они защищают.

Действия в случае хищения пароля

Отслеживайте все данные, защищенные паролями: финансовые отчеты за месяц, отчеты о кредитных операциях, данные о покупках через Интернет и т. д. Надежные, легко запоминающиеся пароли помогают защититься от мошенничества и хищения идентификационных данных, но не являются абсолютной гарантией защиты. Вне зависимости от того, насколько надежным является пароль, если мошенникам удастся взломать систему, где он хранится, они его узнают. Если вы заметили подозрительные действия, которые могут означать, что кто-то получил доступ к вашим данным, как можно скорее сообщите об этом в соответствующие органы. Дополнительные сведения о действиях в случае хищения идентификационных данных или подобного мошенничества