Ежемесячный информационный бюллетень по безопасности

Сила парольной фразы

Вам надоело постоянно придумывать сложные пароли? Разочарованы необходимостью запоминать и вводить все эти буквы, символы и цифры? Что ж, у нас есть для вас решение: сильная парольная фраза!

Парольные фразы

Вы можете этого не осознавать, но пароли являются одним из основных векторов атак киберзлоумышленников. Злоумышленники нацелены на ваши пароли, и если они смогут правильно угадать или взломать правильный пароль, они смогут легко получить доступ к вашей электронной почте, банковским счетам или, возможно, украсть всю вашу личную информацию. Чем слабее ваши пароли, тем легче их взломать. Таким образом, надежные пароли являются одним из наиболее эффективных способов защиты ваших учетных записей и цифровой жизни в Интернете. Традиционно вас учили использовать очень сложные пароли. Идея заключалась в том, что чем выше сложность, тем сложнее киберзлоумышленникам и их автоматизированным программам угадать пароль. Но проблема в том, что сложные пароли сложно запомнить и точно ввести. Еще лучший способ создать надежный и безопасный пароль — это так называемая парольная фраза. Вместо сложности они сильны из-за своей длины. Вот пара примеров:

Время крепкого кофе!
потерянная-улитка-ползет-пляж

Парольные фразы представляют собой не что иное, как серию слов и могут содержать более двадцати символов, если это разрешено сайтом. Это может показаться много, но оба приведенных выше примера содержат более двадцати символов, и, в отличие от паролей, парольные фразы гораздо легче запомнить и их проще вводить. Чем длиннее парольная фраза, тем она безопаснее. В некоторых ситуациях вас могут попросить усложнить парольную фразу, например, добавить символы, заглавные буквы или цифры. Самый простой способ сделать это — изменить некоторые буквы вашей парольной фразы с помощью символов или цифр. Например, если заменить букву ''е'' на цифру ''3'', приведенные выше примеры станут более сложными, но их все равно будет достаточно легко запомнить и напечатать:

Вр3мя крепкого коф3!
потерянная-улитка-полз3т-пляж

Сохраняйте уникальность

Чтобы парольная фраза была по-настоящему безопасной, она также должна быть уникальной для каждой учетной записи. Если вы повторно используете одну и ту же кодовую фразу или фразу, содержащую легко идентифицируемый шаблон, для нескольких учетных записей, вы подвергаете себя опасности.

Все, что нужно сделать киберзлоумышленнику, — это взломать один веб-сайт, который вы часто используете, украсть кодовую фразу, которую вы используете для этого конкретного веб-сайта, и, если все ваши пароли/парольные фразы одинаковы, он получит доступ ко всем остальным вашим учетным записям. Не можете запомнить все эти длинные уникальные фразы-пароли для каждой из ваших учетных записей? У нас есть решение для вас: менеджеры паролей.

Менеджеры паролей — это специальные компьютерные программы, которые надежно хранят все ваши пароли в зашифрованном хранилище, защищенном основным паролем. Чтобы получить доступ к хранилищу, вам нужно запомнить только основной пароль. Менеджер паролей может автоматически получать ваши пароли, когда они вам понадобятся, и автоматически входить на веб-сайты вместо вас. Менеджеры паролей эволюционировали и теперь содержат другие функции, в том числе хранение ответов на секретные вопросы, предупреждение вас, когда вы повторно используете пароли или попадаете на поддельный веб-сайт, использование генераторов, которые будут создавать для вас надежные пароли или парольные фразы, и многое другое. Большинство менеджеров паролей также безопасно синхронизируются практически с любым компьютером или устройством, поэтому независимо от того, какую систему вы используете, у вас есть простой и безопасный доступ ко всем вашим паролям.

Последний шаг – многофакторная аутентификация

Последним шагом к тому, чтобы сделать ваши парольные фразы по-настоящему надежными, является добавление к ним второго уровня защиты — так называемой многофакторной аутентификации (MFA). MFA требует, чтобы у вас было два документа, удостоверяющих личность, при входе в свои учетные записи. Это может быть ваш пароль и биометрические данные, например отпечаток пальца; или это может быть ваш пароль и автоматически сгенерированный цифровой код, который будет отправлен на другое устройство или на другую учетную запись электронной почты. Код каждый раз уникален и может быть сгенерирован с мобильного телефона или другого доверенного устройства. Этот процесс гарантирует, что даже если злоумышленник получит ваш пароль, он все равно не сможет попасть в ваши учетные записи. Включите эту опцию, когда это возможно, особенно для наиболее важных счетов, таких как банк или пенсионные счета или доступ к вашей электронной почте. Если вы используете менеджер паролей, мы настоятельно рекомендуем защитить его надежной парольной фразой и двухэтапной проверкой.

Парольные фразы — отличный способ упростить безопасность и защитить ваши учетные записи. Чтобы сделать вашу цифровую жизнь в Интернете еще проще и безопаснее, мы предлагаем объединить возможности менеджеров паролей и MFA для ваших парольных фраз.

Приглашенный редактор

Кинтана Паттерсон — менеджер по ИТ-клинике и обеспечению соответствия требованиям медицинского кампуса Аншутца Университета Колорадо и председатель комитета WiCyS (Женщины в кибербезопасности) по защите прав справедливости. Она стремится обеспечить, чтобы женщины в этой отрасли чувствовали себя нужными, поддерживаемыми и ценными.

Ресурсы

Менеджеры паролей: https://www.sans.org/newsletters/ouch/power-password-managers/
Биометрия: https://www.sans.org/newsletters/ouch/biometrics-making-security-simple/
Многофакторная аутентификация: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/

Роман Полаков