OUCH! Август 2023

Ежемесячный информационный бюллетень по безопасности

Возможности менеджеров паролей

Вы разочарованы в использование паролей?

Как и большинству людей, вы, вероятно, сочтете создание, управление и запоминание всех ваших разных паролей сложной задачей. Кажется, что каждый веб-сайт имеет разные правила пароля, и многие из них требуют дополнительных мер безопасности, таких как контрольные вопросы. Было бы здорово, если бы существовало единое решение для всех ваших проблем с паролями? Существует. Это называется менеджер паролей.

Менеджеры паролей упрощают и защищают вашу цифровую жизнь

Менеджеры паролей — это программное решение, которое хранит ваши пароли в защищенной базе данных, иногда называемой хранилищем. Менеджер паролей шифрует содержимое хранилищ и защищает его мастер-паролем, который знаете только вы. Когда вам нужен один из ваших паролей, вы просто вводите свой основной пароль в свой менеджер паролей, чтобы разблокировать хранилище. Менеджер паролей часто интегрируется в ваш веб-браузер, автоматически извлекает правильный пароль и безопасно регистрирует вас на веб-сайте. Это позволяет вам легко поддерживать уникальный пароль для каждой из ваших учетных записей, что имеет решающее значение для обеспечения безопасности вашей цифровой жизни.

Кроме того, большинство менеджеров паролей включают возможность синхронизации между несколькими устройствами. Таким образом, когда вы обновляете пароль на своем ноутбуке, эти изменения синхронизируются со всеми другими вашими устройствами. Наконец, большинство менеджеров паролей определяют, когда вы пытаетесь создать новую учетную запись в Интернете, и могут создать и сохранить для вас новый уникальный пароль.

Единственный пароль, который вы должны помнить, — это основной пароль, который вы используете для доступа к вашему менеджеру паролей. Очень важно сделать этот пароль длинным и уникальным. Фактически, мы рекомендуем сделать ваш мастер-пароль парольной фразой - длинным паролем, состоящим из нескольких слов или фраз. Если ваш менеджер паролей поддерживает многофакторную аутентификацию, используйте и ее. Наконец, крайне важно помнить свой основной пароль, чтобы избежать блокировки вашего менеджера паролей.

Выбор менеджера паролей

Есть много менеджеров паролей на выбор. В разделе ''Ресурсы'' мы предоставляем ссылку на обзоры менеджеров паролей. Между тем, пытаясь найти то, что лучше для вас, помните следующее:

- Ваш менеджер паролей должен быть простым в использовании. Если вы находите решение слишком сложным для понимания, найдите другое решение, которое лучше соответствует вашему стилю и опыту.
- Хороший менеджер паролей должен быть совместим со всеми вашими устройствами и синхронизироваться с ними.
- Используйте только известные и надежные менеджеры паролей. С осторожностью относитесь к программам, которых не было в течение долгого времени или без отзывов пользователей.
- Убедитесь, что поставщик активно обновляет менеджер паролей, и убедитесь, что вы всегда используете самую последнюю версию.
- Менеджер паролей должен предоставить вам возможность хранить конфиденциальные данные, такие как ответы на секретные вопросы, информацию о кредитной карте и номера часто летающих пассажиров.
- С подозрением относитесь к менеджерам паролей, которые позволяют восстановить ваш основной пароль или позволяют их службам технической поддержки изменить его для вас.

Вы можете записать свой основной пароль, хранить его в запечатанном конверте и хранить конверт в защищенном месте на случай, если вы его забудете.

Менеджеры паролей не для вас?

Мы понимаем, что некоторым людям менеджеры паролей могут показаться слишком громоздкими и сложными в использовании. Тем не менее, для обеспечения безопасности для каждой учетной записи по-прежнему необходим уникальный пароль. Как кто-то может безопасно запомнить все эти уникальные пароли? Один из вариантов — записать эти пароли. Это не вариант для рабочих паролей. Но это может быть альтернативой использованию дома для личных учетных записей, если менеджеры паролей просто не подходят. Ключевым шагом является обеспечение безопасности этого ноутбука. Если вы или ваш близкий человек используете блокнот для записи паролей, убедитесь, что блокнот хранится в безопасном месте, доступ к которому есть только у вас или доверенных членов семьи.

Приглашенный редактор

Нурин Ньороге — специалист по кибербезопасности с большим опытом работы в многогранной, сложной и быстро меняющейся среде как в государственном, так и в частном секторах. Она является стратегическим мыслителем с проверенным опытом руководства по вопросам, касающимся новых технологий. Нурин — лидер, который также увлечен наставничеством других. LinkedIn: https://www.linkedin.com/in/noureennjoroge/.

Ресурсы

Обзор менеджера паролей: https://www.pcmag.com/picks/the-best-password-managers
Многофакторная аутентификация: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/

Роман Полаков