ITGLOBAL.COM
MANAGED IT. WORLDWIDE

БЕЗОПАСНОСТЬ ПАРОЛЕЙ

Чтобы узнать пароли пользователей, злоумышленники используют различные приемы и инструменты взлома, которые находятся в свободном доступе в интернете.

Мы подготовили советы по безопасности паролей для пользователей, которые также помогут улучшить безопасность вашей системы.

Как взламывают пароли...

Кража паролей

Если пароль хранится небезопасно, его могут украсть. Пример: пароль на бумаге, спрятанный рядом с устройством.

«Механический подбор»

Программа перебирает сотни миллионов вариантов, пока не найдет правильный пароль.

Подбор вручную

Пользователи часто используют в паролях личные данные (например, имя и дату рождения), и такие пароли легко угадать.

Shoulder Surfing или «Подсматривание через плечо»

Злоумышленники могут подсмотреть, как вводят пароль.

Поиск по инфраструктуре

В ИТ-инфраструктуре ищут пароли, которые хранятся в электронном виде.

Социальная инженерия

Злоумышленники прибегают к техникам социальной инженерии и выведывают пароли обманом.

Перехват на устройстве

Программа-перехватчик запоминает пароли, которые вводит пользователь.

Перехват в сети

Пароли перехватывают во время передачи по сети.

...и как улучшить безопасность системы

Как помочь вашим пользователям?

- Используйте пароли только там, где они действительно нужны.
- Внедряйте технические решения, чтобы снизить нагрузку на пользователей.
- Предоставьте пользователям средства для безопасных записи и хранения паролей.
- Сброс пароля должен быть легким, быстрым и экономным.
- Запрашивайте смену паролей при подозрении на компрометацию, но не реже установленного срока.

22

СРЕДНЕЕ КОЛИЧЕСТВО ПАРОЛЕЙ, КОТОРЫЕ ПОЛЬЗОВАТЕЛИ ХРАНЯТ ОНЛАЙН

Предоставьте надежный инструмент генерации паролей

- Внедрите технические средства защиты, чтобы можно было использовать более сложные пароли, более простым способом.
- Помните о том, что возможности инструментов проверки надежности пароля ограничены.
- Поощряйте пользователей использовать разные пароли для рабочих и домашних устройств.
- Расскажите сотрудникам, почему не нужно пользоваться паролями, которые легко подобрать.
- Расскажите о последствиях использования предсказуемых паролей и запретите наиболее распространенные варианты.

...и как улучшить безопасность системы

Отслеживайте неудачные попытки входа в систему, обучите пользователей сообщать о подозрительной активности

Уделяйте особое внимание учетным записям администратора и удаленных пользователей

Добавьте в черный список самые распространенные варианты паролей

Не храните пароли в текстовом формате

4 СРЕДНЕЕ ЧИСЛО ВЕБ-САЙТОВ, ДЛЯ КОТОРЫХ ЗАДАН ОДИНАКОВЫЙ ПАРОЛЬ

Смените все пароли, установленные поставщиком по умолчанию, и только потом пользуйтесь устройством или ПО

Используйте средства блокировки, регулирования или мониторинга учетных записей, чтобы предотвратить попытки подбора паролей

Больше информации на сайте: www.itglobal.com

ITGLOBAL.COM
MANAGED IT. WORLDWIDE