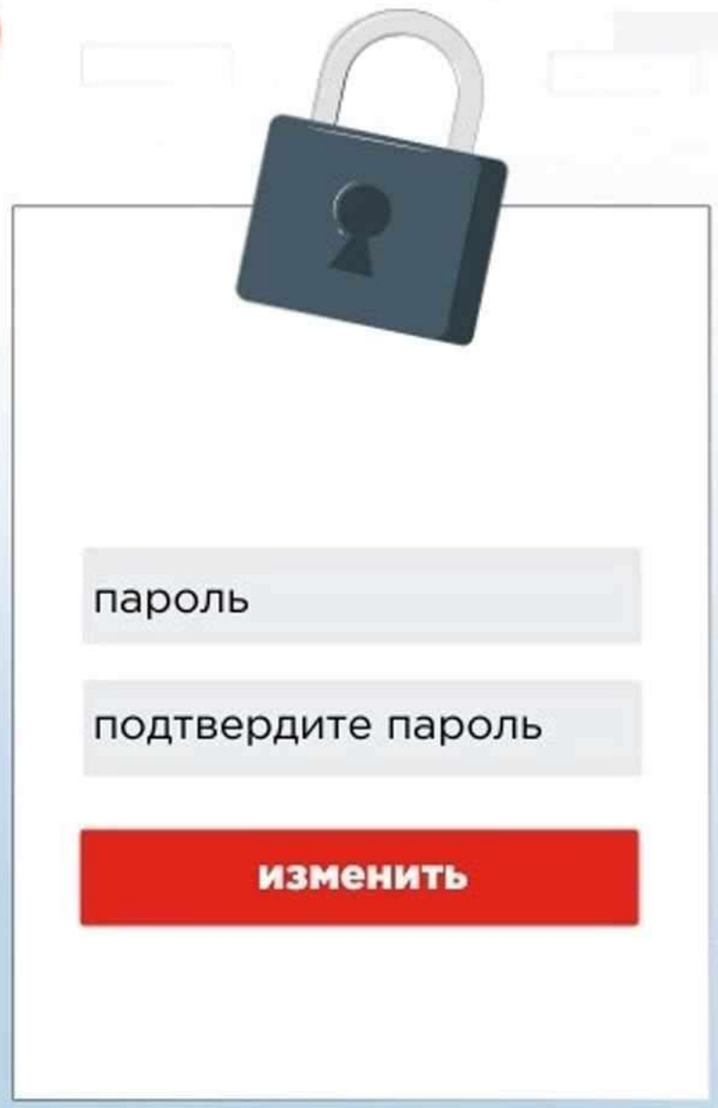
ПРОФИЛАКТИКА
федеральный центр

БЕЗОПАСНОСТЬ ПАРОЛЕЙ: ЧТО НУЖНО ЗНАТЬ?



ПРОФИЛАКТИКА
федеральный центр

КАК МОГУТ УКРАСТЬ МОЙ ПАРОЛЬ?

Злоумышленники изобрели целую плеяду способов хищения цифровых данных. Вот лишь несколько из них:

ФИШИНГ

Обычно фишинговые ссылки ведут на поддельные сайты, на которых требуется ввести личные данные. Неважно, кто отправил вам письмо: **всегда внимательно смотрите на веб-адреса**, которые вам присылают.

АТАКИ ЧЕРЕЗ БРАУЗЕР

Нередко пароли крадут через **уязвимости** браузеров или через браузерные расширения.

ВНЕШНИЕ УТЕЧКИ

Утечки часто происходят и в удаленных интернет-сервисах, которыми мы пользуемся. В результате взлома такого сайта хакеры могут получить огромную базу пользователей вместе с их паролями и персональными данными. **Поэтому стоит обновлять пароль хотя бы раз в 2-3 месяца**

КАК МОГУТ УКРАСТЬ МОЙ ПАРОЛЬ?

Злоумышленники изобрели целую плеяду способов хищения цифровых данных. Вот лишь несколько из них:

ТРОЯН

Эти тихие шпионы, которые могут попасть на ваше устройство через **программу, загруженную в Интернете.** Чем дольше они остаются незамеченными, тем дольше смогут выполнять свою работу — передавать злоумышленникам украденные у вас данные.

ПУБЛИЧНАЯ СЕТЬ WI-FI

Злоумышленники могут перехватить данные, отправляемые по сети, если вы используете сеть Wi-Fi **без шифрования или защищенную старым протоколом WEP.**

ЗАЧЕМ ВООБЩЕ НУЖЕН СЛОЖНЫЙ ПАРОЛЬ? КОМУ НУЖНЫ МОИ СТРАНИЦЫ, Я ЖЕ НЕ ЗНАМЕНИТОСТЬ?

Переписка пользователей, их личные данные всегда была объектом интереса различных сторон.
В социальных сетях мы часто делимся самым сокровенным, а для мошенников это отличная возможность узнать о нас побольше, чтобы потом использовать данные в преступных целях.

Взламывают не только аккаунты известных личностей, но и простых людей. ***Поэтому защищать свою страницу нужно вне зависимости от того, как много у вас подписчиков и как часто вы общаетесь в сети.***

ПРОФИЛАКТИКА
федеральный центр

Я ЗАБЫЛ СВОЙ ПАРОЛЬ, А СЕРВИС ЗАСТАВЛЯЕТ МЕНЯ СОЗДАВАТЬ НОВЫЙ. ПОЧЕМУ МНЕ НЕ МОГУТ НАПОМНИТЬ ПРОШЛЫЙ?

Ни один сервис не знает, какой у вас на самом деле пароль. По ту сторону экрана он выглядит как **хэш-значение** — рандомный набор букв и цифр определенной длины.

Вот пример преобразования одного из знаменитых паролей:

admin ⇄ **21232f297a57a5a743894a0e4a801fc3**

Такие хэш-значения хорошо известны взломщикам, именно поэтому не стоит использовать просты пароли при защите аккаунта.

ПРОФИЛАКТИКА
федеральный центр

ПРАВИЛА ЗАЩИТЫ ВАШЕГО АККАУНТА:

1. Чем больше символов, тем пароль надежней.

2. Идеальный пароль содержит всего понемножку: цифры, большие и маленькие буквы, специальные символы. Буквы не должны образовывать слово.

3. Хороший пароль невозможно запомнить, поэтому лучше довериться менеджеру паролей.

4. Для пароля сойдёт и длинная фраза, только никаких цитат.

5. Один аккаунт – один пароль.

6. Не забывайте периодически менять пароль.

КАК ТОГДА ЗАЩИТИТЬ СВОЙ АККАУНТ ПРАВИЛЬНО?

Для начала запомните, что не стоит использовать простые слова: клички любимых питомцев, дата рождения, футбольный клуб, за который вы болеете — всю эту информацию часто можно найти в открытом доступе.

Не стоит пользоваться и известными фразами:

123456

123456789

qwerty

password

admin