семь советов по информационной безопасности

Они помогут защитить личные данные и свой аккаунт от взлома и других угроз.

правило 1/7

не предоставляйте доступ к личной информации посторонним

Если злоумышленники завладеют вашими личными данными, они смогут украсть и взломать вашу страницу ВКонтакте, доступы к электронным адресам, кабинету в онлайн-банке.

Поэтому первое и главное правило — нельзя делиться личной информацией с посторонними. Под личной информацией мы понимаем любые данные, с помощью которых злоумышленники могут получить доступ к вашим страницам в соцсетях, электронным почтам, сообществам и так далее. Например, логины, пароли и ответы на секретные вопросы.

правило 2/7

создавайте надёжные пароли и обеспечивайте их безопасность

1/4

Никогда и никому не сообщайте свои пароли. Помните, что иногда это можно сделать случайно: например, если едете в автобусе и вводите в смартфоне свой пароль от почты. Его могут увидеть и запомнить другие люди.

2/4

Не храните пароли в открытом виде: например, в блокноте или в приложении для текстовых заметок. Если на компьютер или смартфон попадёт вредоносное ПО, то любые ваши данные могут стать доступны злоумышленнику. А ещё можно случайно открыть файл при посторонних. Вместо этого следует использовать менеджеры паролей — это программы, которые помогают хранить логины и пароли от разных сервисов в одном месте. Вам достаточно будет держать в голове один мастер-пароль, который нужен для доступа к программе со всеми данными.

3/4

Создавайте длинные и надёжные пароли. Короткие варианты злоумышленники легко могут подобрать в специальных программах. Вот небольшой чек-лист, который поможет создать надёжный пароль:

чек-лист

Длина пароля — **12 символов** минимум.

В пароле одновременно используются цифры, специальные символы, строчные и прописные буквы. Примеры специальных символов: **#, %, *.**

В пароле отсутствуют популярные и простые сочетания. Например, последовательность цифр или букв: **123456, qwerty.**

В пароле нет ваших личных данных. **Например, имени, фамилии, отчества, даты рождения, серии или номера паспорта.**

Лёгкий способ придумать сложный пароль

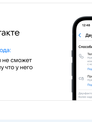
Придумайте парольную фразу – **dobroe utro strana.**
Замените буквы на спецсимволы – **dobroe!utro_$trana.**
Добавьте пару цифр – **d0bro!eutro0_$trana.**
Готово!*

*Этот пароль нельзя использовать, потому что он засветился в открытом источнике.

Изменить пароль можно на странице ВКонтакте:

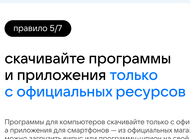
настройки → безопасность → пароль

Когда вы укажете новый пароль, система подскажет:



4/4

Не используйте одинаковые пароли для разных сервисов. В этом случае злоумышленник может взломать один ресурс, а получить доступ сразу к нескольким. Представьте, что человек регистрируется на сайте онлайн-кинотеатра, по привычке вводит пароль от своей страницы ВКонтакте. Если эта видеоплощадка подвергнется атаке киберпреступников, то пароли и другие данные пользователей могут попасть в интернет. А это уже чревато тем, что злоумышленники получат доступ сразу к нескольким сервисам, в которых пользователи зарегистрированы.



*пример уведомления

правило 3/7

используйте двухфакторную аутентификацию

Надёжный пароль — это необходимый минимум. В качестве дополнительной защиты используйте двухфакторную аутентификацию.

Аутентификация — это особая процедура проверки. Когда вы заходите на свою страницу ВКонтакте, то вводите логин и пароль. В этот момент система сравнивает введённую информацию со своей базой данных, которая хранится в зашифрованном виде. Если информация совпадает — аутентификация прошла успешно, вы заходите в аккаунт.

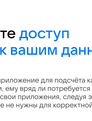
В большинстве сервисов аутентификация двухфакторная: для входа, помимо логина и пароля, пользователю необходимо ввести код. Его получают на телефон или с помощью специального приложения для генерации кодов.

Подключить двухфакторную аутентификацию ВКонтакте:

настройки → безопасность → двухфакторная аутентификация

Двухфакторная аутентификация ВКонтакте

Это более безопасный способ входа:
если кто-то украдёт пароль, то он не сможет авторизоваться в аккаунте, потому что у него не будет кода.



правило 4/7

регулярно обновляйте антивирус и проверяйте компьютер на наличие вредоносных программ

Регулярное сканирование всех файлов и программ на вашем компьютере позволит избежать утечки данных и других неожиданных последствий.

правило 5/7

скачивайте программы и приложения только с официальных ресурсов

Программы для компьютеров скачивайте только с официальных сайтов, а приложения для смартфонов — из официальных магазинов. В противном случае можно загрузить вирус или программу-шпион на свой устройство, они могут украсть ваши логины, пароли и другие данные. Скачивание из официального магазина приложений не является стопроцентной гарантией, но существенно снижает риски.

правило 6/7

контролируйте доступ приложений к вашим данным

Например, если у вас есть приложение для подсчёта калорий и контроля за здоровым образом жизни, ему вряд ли потребуется отправлять СМС-сообщения. Проверьте все свои приложения, следуя этой логике, и ограничьте им доступ к данным, которые не нужны для корректной работы.

правило 7/7

пользуйтесь открытыми сетями Wi-Fi с осторожностью

Лучше не пользоваться ими вовсе: они не всегда безопасны, а злоумышленники с их помощью могут украсть данные ваш и ваших устройств вредоносным программным обеспечением.

Если вам всё же приходится работать с общественным Wi-Fi, подключайте надёжные VPN-сервисы. Так ваши данные будут зашифрованы и скрыты от других участников этой сети.