

## Безопасность аккаунтов.

В предновогодней суете важно не забывать о безопасности.

Увы, даже в праздники, мошенники не дремлют.

### Безопасность Ваших аккаунтов – в Ваших руках

#### Правила по защите информации

- Постарайтесь, чтобы пароль был сложный. Поменяйте пароль и делайте это регулярно. Хороший пароль содержит не менее 8 символов: цифры, буквы разного регистра, спец.символы (например: %, &, #). Он не должен совпадать с паролями на других сайтах.
- Проверьте на наличие вирусов смартфон и компьютер.
- Если используете профиль ВКонтакте, удалите расширения для ВКонтакте: они могут украсть ваши логин и пароль. Например, скачивалки для музыки, «Мои гости».
- В настройках аккаунта VK ID можно посмотреть историю активности:
- <https://id.vk.com/account/#/security> → История активности.
- Здесь можно завершить все сеансы, то есть на всех других устройствах нужно будет вновь войти в аккаунт, чтобы просматривать его и пользоваться.
- Не переходите по подозрительным ссылкам и не вводите свои данные на сомнительных сайтах и в приложениях.
- Важно совершать выход из профиля на компьютере, телефоне, других устройствах, если планируете оставить без присмотра, или оставлять их запароленными.
- Также не стоит предоставлять доступ другим людям к вашему телефону.
- Проверьте, что на Ваших устройствах отключен Bluetooth. (в подавляющее большинство современных стационарных и мобильных операционных систем позволяют злоумышленнику имитировать подключение Bluetooth-клавиатуры к устройству и имитировать нажатие клавиш. Для этого ему не надо знать какие-либо логины и пароли.)

#### ВАЖНО

- Даже при использовании двухфакторной аутентификации (2FA) пользователь может получить одноразовый пароль в SMS-сообщении или в письме на свою электронную почту для подтверждения правомерности использования своей учетной записи какого-либо сервиса, хотя при этом сам его не запрашивал. Что делать в таком случае?
- Если код подтверждения 2FA (его еще называют OTP-код) пришел вам без вашего запроса - это означает, что данные вашей учетной записи стали известны мошенникам. Злоумышленник попробовал войти в сервис (например, в Госуслуги) под вашими данными, однако был остановлен необходимостью подтверждения двухфакторной аутентификации. То есть ваш пароль больше не является тайной.

#### Следует сделать следующее:

- Войти в сервис непосредственно с его страницы, не переходя на него по каким-либо ссылкам. Далее необходимо срочно сменить пароль, который был скомпрометирован мошенниками.
- Если такой же пароль вы использовали для входа в другие учетные записи - смените его и там.