ПРОФИЛАКТИКА
федеральный центр

БЕЗОПАСНОСТЬ ПАРОЛЕЙ: ЧТО НУЖНО ЗНАТЬ

Пароль — это ключ ко всей личной информации вашего ребенка в сети. Если злоумышленник получит доступ к аккаунтам, он сможет украсть личные данные, фотографии, переписки, деньги и даже воспользоваться именем вашего ребенка для мошеннических действий.

- Используйте длинные пароли от 8 символов.
  Пример: «NekotoryySlOzhnyParol123»
- Создавайте уникальные комбинации с буквами разного регистра (заглавные и строчные), цифрами и специальными символами (!@#$%^&*).
  Пример: «7mYpAsSwOrDwItHSpEclaLSymBoL$»
- Не используйте имена, фамилии, даты рождения, номера телефонов или любые легкоугадываемые слова и последовательности («qwerty», «password»).
- Меняйте пароли регулярно (минимум раз в полгода).
- Не записывайте пароли на бумаге или в незашифрованных файлах на компьютере. Используйте специализированные менеджеры паролей.
- Используйте двухфакторную аутентификацию.
- Объясните опасность фишинга. Расскажите детям о рисках перехода по подозрительным ссылкам и ввода персональных данных на незнакомых сайтах.
- Ограничьте доступ к публичным сетям Wi-Fi.

Важно регулярно напоминать эти советы своим детям, ведь безопасность — дело первостепенной важности!