

ТЕСТ "СКЛОНЕН ЛИ ТЫ СТАТЬ ЖЕРТВОЙ КИБЕРМОШЕННИЧЕСТВА"?

1. Как часто ты используешь одинаковые пароли для разных аккаунтов?
а) Никогда
б) Иногда
в) Часто
2. Делишься ли ты личной информацией (например, адресом, номером телефона) в социальных сетях?
а) Никогда
б) Иногда
в) Часто
3. Проверяешь ли ты ссылки, прежде чем на них кликнуть?
а) Всегда
б) Иногда
в) Никогда
4. Используешь ли ты двухфакторную аутентификацию для своих аккаунтов?
а) Да, всегда
б) Иногда
в) Нет, никогда
5. Насколько сильно ты беспокоишься о безопасности своих данных в интернете?
а) Очень беспокоюсь
б) Иногда беспокоюсь
в) Совсем не беспокоюсь

РЕЗУЛЬТАТЫ

Больше ответов «а»: Ты достаточно осторожен в интернете и принимаешь меры для защиты своих данных.

Больше ответов «б»: У тебя есть некоторые привычки, которые могут подвергнуть тебя риску. Обрати внимание на безопасность своих аккаунтов.

Больше ответов «в»: Тебе стоит серьезно задуматься о своей безопасности в интернете и изменить некоторые привычки.

БУДЬ В ТЕМЕ, ЧТОБ НЕ ПОПАСТЬ В РУКИ КИБЕРМОШЕННИКОВ!

© Выполнено представителями "КиберЪОко" под научным руководством: Сыромля Ларисы Борисовны - заведующего кафедрой прокурорского надзора за исполнением законов в оперативно-розыскной деятельности и участия прокурора в уголовном судопроизводстве Дальневосточного юридического института (филиала) Университета прокуратуры Российской Федерации, советника юстиции, кандидата юридических наук

5

минут в день и ты узнаешь:

- как не стать жертвой кибермошенничества;
- что делать, если ты или твои знакомые попались «в руки» злодея;
- какие еще опасности ожидают нас в цифровом пространстве и многое другое.

Для слепых и слабовидящих



СТОП КИБЕРМОШЕННИЧЕСТВУ

Безопасность детей
в цифровом мире

ЧТО ТАКОЕ КИБЕРМОШЕННИЧЕСТВО?



«Это не игра. Это реальная угроза»

- Фейковые «бесплатные» игры или подарки.
- Поддельные конкурсы и опросы.
- Мошенничество через стримы и стримеров.
- Угрозы с требованиями денег или действий.

ПРИМЕР

Пишет одноклассница: «Привет, это Маша! Мой аккаунт в ВКонтакте взломали, можешь, пожалуйста, помочь мне и сообщить код, который придет на твой телефон».

5 ПРАВИЛ ЗАЩИТЫ



ПАРОЛЬ-МОНСТР

Используй буквы, цифры и символы.
Пример: «БЕЗопасно24!»



НЕ КЛИКАЙ НА СТРАННОЕ

Ссылки от незнакомцев = вирусы.



АНОНИМНОСТЬ

Не указывай школу, адрес, график занятий.

БЛОКИРУЙ АГРЕССОРОВ

Не бойся жаловаться в поддержку соцсети.



ДУМАЙ

Если что-то кажется подозрительным – так и есть!

ЧТО ДЕЛАТЬ, ЕСЛИ ПОПАЛ В БЕДУ?

1. Не паникуй и не удаляй переписку.
2. Сделай скриншот – это доказательство.
3. Расскажи взрослым: Родители, учитель, психолог.
4. Позвони:
 - В полицию по номеру 02 (сам или через родителей);
 - В горячую линию «Дети России» по номеру 8-800-2000-122 (круглосуточно, анонимно).

«Защищён тот, кто осведомлён!»

