Как не стать жертвой кибербуллинга и мошенничества

1. Защита от кибербуллинга

Кибербуллинг — это травля, запугивание или оскорбление человека в интернете через соцсети, мессенджеры, форумы и игры.

Советы:

1. **Не делитесь личной информацией**

✓ Не публикуйте домашний адрес, номер телефона, пароли, фотографии документов.

2. **Настройка приватности**

✓ В соцсетях закройте профили для посторонних, ограничьте круг людей, кто может писать сообщения или видеть публикации.

3. **Игнорируйте провокации**

✓ Не вступайте в конфликты с агрессором, не отвечайте на оскорбления.

4. **Сохраняйте доказательства**

✓ Скриншоты оскорбительных сообщений могут понадобиться при жалобе администрации платформы или полиции.

5. **Блокируйте и жалуйтесь**

✓ Используйте функции блокировки и жалобы в соцсетях, мессенджерах, на игровых платформах.

6. **Обратитесь за поддержкой**

✓ Родители, учителя, школьный психолог или милиция — люди, которые могут помочь.

Как защить себя от мошенничества в интернете

Мошенничество — попытка незаконно получить ваши деньги, данные или доступ к аккаунтам.

Советы:

1. **Будьте осторожны с ссылками и файлами**
    - Не переходите по подозрительным ссылкам и не открывайте вложения от незнакомых людей.
2. **Не отправляйте деньги и данные**
    - Никому не переводите деньги по просьбе в интернете, не сообщайте логины, пароли, данные карт.
3. **Проверяйте сайты и контакты**
    - Официальные компании имеют проверенные сайты и контактные данные. Подозрительные письма или сообщения — почти всегда мошенничество.
4. **Используйте сложные пароли и двухфакторную аутентификацию**
    - Пароль должен быть уникальным, длинным, с буквами, цифрами и символами.
5. **Обучайтесь и информируйте других**
    - Чем больше вы знаете о типах мошенничества (фишинг, скам, лжерекламные акции), тем легче распознать угрозу.

Общие принципы безопасности

- Думайте перед тем, как что-то опубликовать или ответить.
- Проверяйте информацию и источники.
- Обсуждайте подозрительные ситуации с доверенными взрослыми.
- Помните: в интернете важна осторожность — часто легче предотвратить проблему, чем решать последствия.

Чек-лист: Защита от кибербуллинга и мошенничества

1. Личная информация

- Не делитесь адресом, телефоном, паролями, личными документами.
- Настройте приватность в соцсетях и мессенджерах.

2. Поведение в интернете

- Не вступайте в перепалки с оскорбителями.
- Игнорируйте провокации и угрозы.
- Сохраняйте скриншоты оскорбительных сообщений.

3. Работа с подозрительными сообщениями

- Не переходите по неизвестным ссылкам.
- Не открывайте файлы от незнакомцев.
- Не сообщайте данные банковских карт, пароли и коды подтверждения.

4. Деньги и покупки

- Никому не отправляйте деньги по просьбе в интернете.
- Проверяйте официальные сайты и контакты перед оплатой.

5. Пароли и аккаунты

- Используйте сложные, уникальные пароли.
- Включите двухфакторную аутентификацию.

6. Поддержка и помощь

- Блокируйте и жалуйтесь на агрессивных пользователей.
- Обращайтесь к родителям, учителям, школьному психологу или милиции при угрозе.
- Обучайтесь типам мошенничества (фишинг, скам, лжереклама).

7. Общие правила

- Думайте перед публикацией и ответами.
- Проверяйте информацию и источники.
- Бережливость и осторожность — лучшая защита.