|  |  |
| --- | --- |
| желательно приложить какие-то доказательства в виде скринов;3. Не указывай личную информацию в профайле игры;4. Уважай других участников по игре;5. Не устанавливай неофициальные патчи и моды;6. Используй сложные и разные пароли;7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твойкомпьютер могут заразить.**Основные советы по безопасной работе с электронными деньгами:**1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способвосстановить доступ к счету. Привязанный телефон поможет, если забудешьсвой платежный пароль или зайдешь на сайт с незнакомого устройства;2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебеуже не будет угрожать опасность кражи или перехвата платежного пароля;3. Выбери сложный пароль. Преступникам будет не просто угадать сложныйпароль. Надежные пароли — это пароли, которые содержат не менее 8 знаков ивключают в себя строчные и прописные буквы, цифры и несколько символов,такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;;4. Не вводи свои личные данные на сайтах, которым не доверяешь.**Основные советы для безопасности мобильного телефона:**1. Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебепредлагают бесплатный контент, в нем могут быть скрыты какие-то платныеуслуги;2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где онибудут в конечном итоге?3. Необходимо обновлять операционную систему твоего смартфона;4. Используй антивирусные программы для мобильных телефонов;5. Не загружай приложения от неизвестного источника, ведь они могут содержатьвредоносное программное обеспечение;6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди внастройки браузера и удали cookies;7. Периодически проверяй какие платные услуги активированы на твоем номере;8. Давай свой номер мобильного телефона только людям, которых ты знаешь икому доверяешь;9. Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывайиногда проверять это.https://rostokpriut.uln.socinfo.ru/media/2019/05/22/1262391086/Risunok1.jpg | Picture background**Советы по информационной безопасности*****МКОУ «СОШ№2 им.Дж.Т.Хагажеева»*** ***с.п.Лечинкай*****e-mail: lechin.school.2 @yandex.ru , тел.: (886630) 75-2-81****http:// lechinkay.ucoz.ru** |
| **НЕЛЬЗЯ**1. Всем подряд сообщать свою частную информацию (настоящие имя, фамилию,телефон, адрес, номер школы, а также фотографии свои, своей семьи и друзей);2. Открывать вложенные файлы электронной почты, когда не знаешь отправителя;3. Грубить, придираться, оказывать давление — вести себя невежливо и агрессивно;4. Не распоряжайся деньгами твоей семьи без разрешения старших – всегда спрашивайродителей;5. Не встречайся с Интернет-знакомыми в реальной жизни - посоветуйся со взрослым,которому доверяешь.**ОСТОРОЖНО**1. Не все пишут правду. Читаешь о себе неправду в Интернете — сообщи об этомсвоим родителям или опекунам;2. Приглашают переписываться, играть, обмениваться – проверь, нет ли подвоха;3. Незаконное копирование файлов в Интернете – воровство;4. Всегда рассказывай взрослым о проблемах в сети – они всегда помогут;5. Используй настройки безопасности и приватности, чтобы не потерять свои аккаунтыв соцсетях и других порталах.**МОЖНО**1. Уважай других пользователей;2. Пользуешься Интернет-источником – делай ссылку на него;3. Открывай только те ссылки, в которых уверен;4. Общаться за помощью взрослым – родители, опекуны и администрация сайтоввсегда помогут;**Основные советы по безопасности в социальных сетях:**1. Ограничь список друзей. У тебя в друзьях не должно быть случайных инезнакомых людей;2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, датутвоего рождения и другую личную информацию. Злоумышленники могутиспользовать даже информацию о том, как ты и твои родители планируетепровести каникулы;3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел быты, чтобы другие пользователи видели, что ты загружаешь? Подумай, преждечем что-то опубликовать, написать и загрузить;4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имяи другую личную информации: имя, место жительства, место учебы и прочее;5. Избегай размещения фотографий в Интернете, где ты изображен на местности,по которой можно определить твое местоположение; | 6. При регистрации в социальной сети необходимо использовать сложные пароли,состоящие из букв и цифр и с количеством знаков не менее 8;7. Для социальной сети, почты и других сайтов необходимо использовать разныепароли. Тогда если тебя взломают, то злоумышленники получат доступ только кодному месту, а не во все сразу.**Методы защиты от вредоносных компьютерных программ:**1. Используй современные операционные системы, имеющие серьёзный уровеньзащиты от вредоносных программ;2. Постоянно устанавливай почти (цифровые заплатки, которые автоматическиустанавливаются с целью доработки программы) и другие обновления своейоперационной системы. Скачивай их только с официального сайта разработчикаОС. Если существует режим автоматического обновления, включи его;3. Работай на своем компьютере под правами пользователя, а не администратора.Это не позволит большинству вредоносных программ инсталлироваться на твоемперсональном компьютере;4. Используй антивирусные программные продукты известных производителей, савтоматическим обновлением баз;5. Ограничь физический доступ к компьютеру для посторонних лиц;6. Используй внешние носители информации, такие как флешка, диск или файл изинтернета, только из проверенных источников.**Советы по безопасности работе в общедоступных сетях Wi-fi:**1. Не передавай свою личную информацию через общедоступные Wi-Fi сети.Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;2. Используй и обновляй антивирусные программы и брандмауер. Тем самым тыобезопасишь себя от закачки вируса на твое устройство;3. При использовании Wi-Fi отключи функцию «Общий доступ к файлам ипринтерам». Данная функция закрыта по умолчанию, однако некоторыепользователи активируют её для удобства использования в работе или учебе;4. Не используй публичный WI-FI для передачи личных данных, например длявыхода в социальные сети или в электронную почту;5. Ипользуй только защищенное соединение через HTTPS, а не НТТР, т.е. принаборе веб-адреса вводи именно «https://»;6. В мобильном телефоне отключи функцию «Подключение к Wi-Fiавтоматически». Не допускай автоматического подключения устройства к сетямWi-Fi без твоего согласия.**Основные советы по безопасности твоего игрового аккаунта:**1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируйего в списке игроков;2. Пожалуйся администраторам игры на плохое поведение этого игрока, |