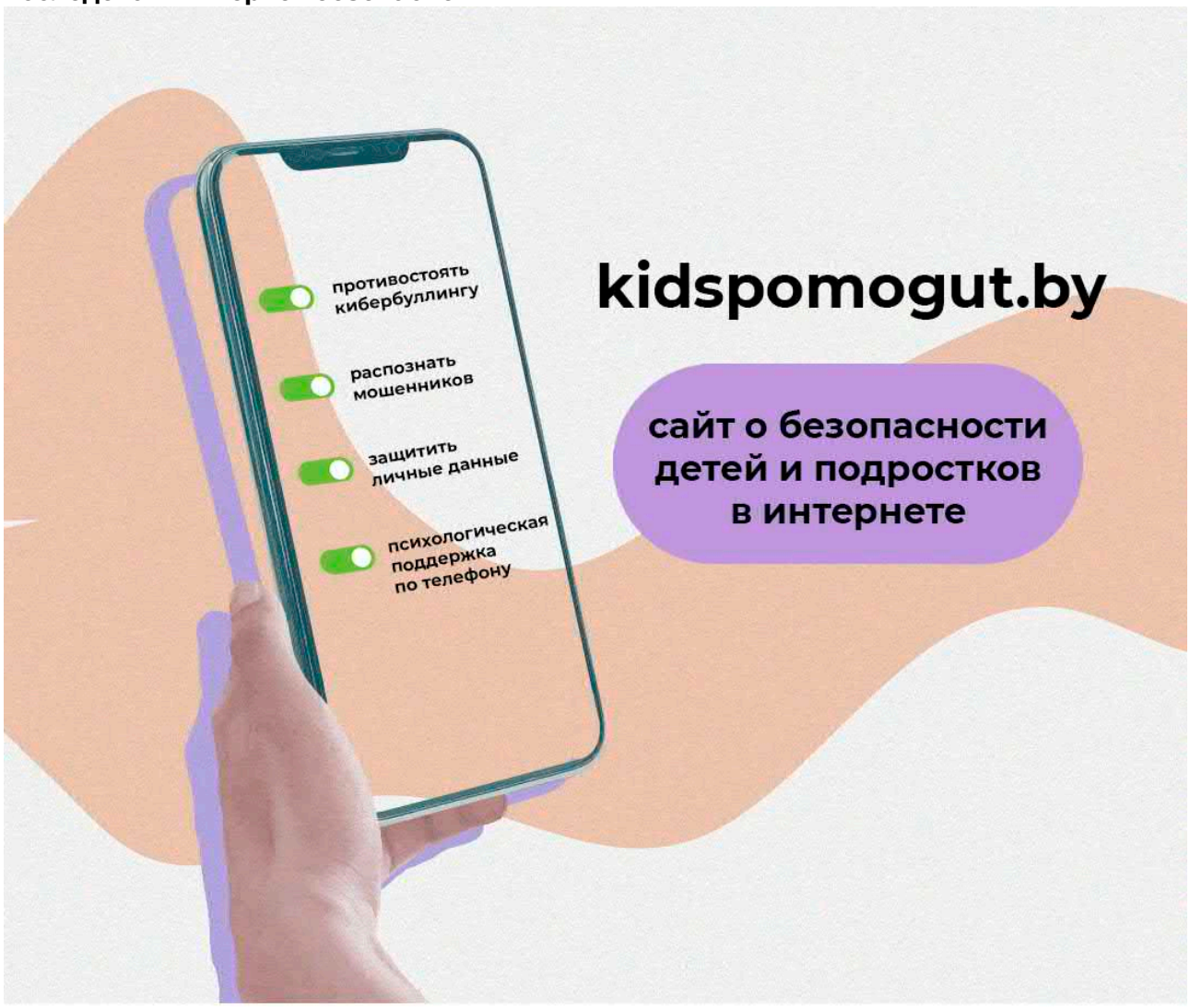
Полезно знать детям и родителям!

•

Интернет – это море информации. Полезной и опасной, интересной и травмирующей.

KIDS POMOGUT.BY | безопасность детей в сети

На ресурсе kidspomogut.by собрана экспертная информация, которая поможет детям исследовать интернет безопасно.



МИНСКИЙ ГОРОДСКОЙ ИСПОЛНИТЕЛЬНЫЙ КОМИТЕТ

kaspersky

Беларусь ЮНИСЕФ для каждого ребенка

Здесь можно узнать, как противостоять кибербуллингу, как распознать мошенников, защитить личные данные: есть адаптированная информация как для детей и подростков, так и для родителей и учителей.
Если вы уже столкнулись с угрозой или насилием, всегда можно написать об этом специалистам в онлайн-чат на сайте или позвонить по телефонам:
8 801 100 16 11, 8 (029) 367 32 32. Эксперты дадут совет и поддержат!

> Круглосуточная линия экстренной психологической помощи

В Беларуси работает новый короткий номер — 133, по которому каждый может получить экстренную психологическую помощь абсолютно бесплатно. Линия функционирует круглосуточно, и вызов бесплатный с любых телефонов — как мобильных, так и стационарных.

Кому поможет 133?

Новый номер подключен к Центру экстренной психологической помощи, который создан на базе Республиканского научно-практического центра психического здоровья. Инициатива ориентирована на людей, оказавшихся в сложной жизненной ситуации — будь то кризис, тревога, стресс или острая эмоциональная перегрузка.

По словам представителей учреждения, каждый звонок автоматически перенаправляется в регион, откуда он поступает, чтобы обеспечить быструю и максимально эффективную помощь.

Что важно знать?

Номер: 133

Время работы: 24/7

Стоимость: бесплатно

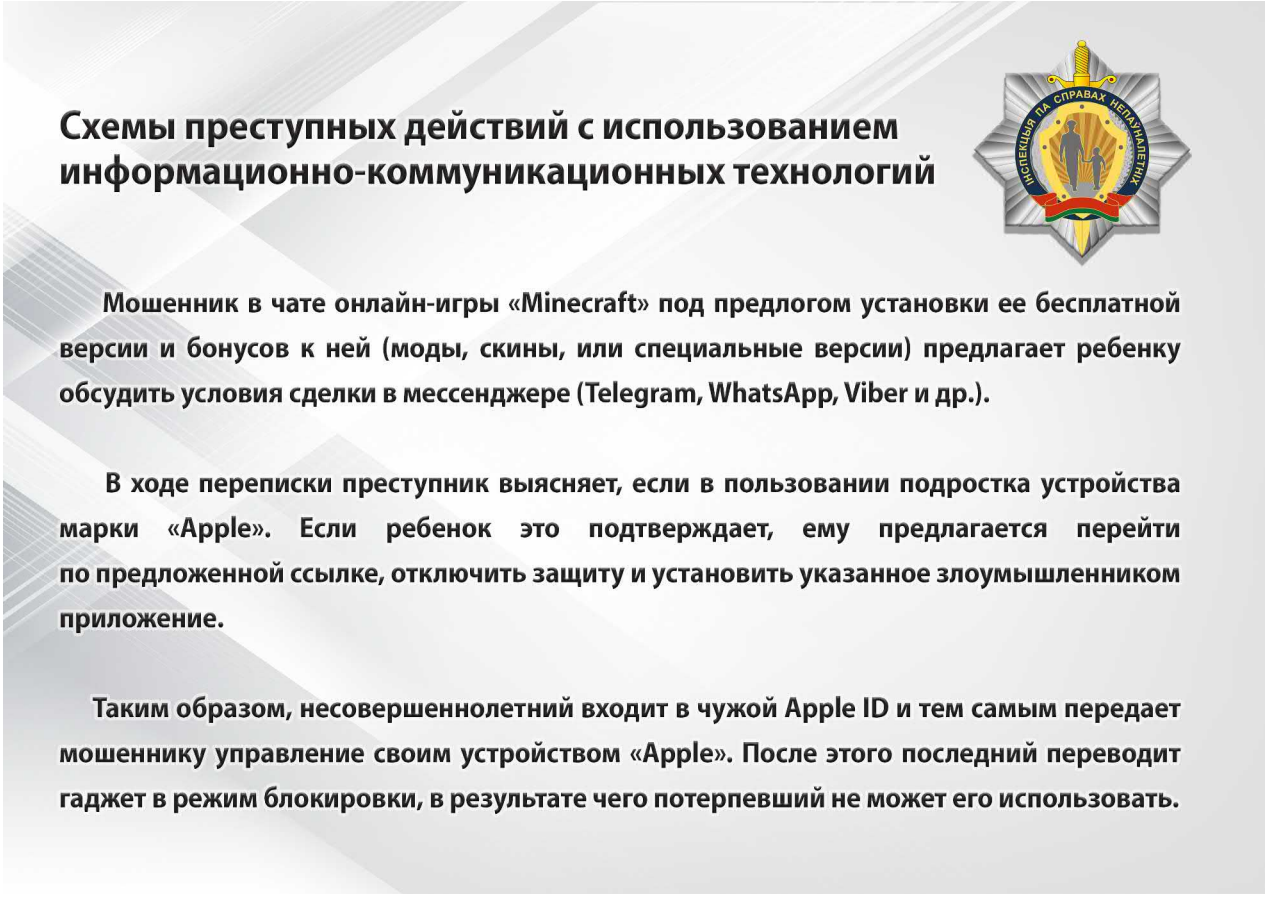
Доступность: с мобильных и стационарных телефонов

Формат помощи: разговор с профессиональным психологом

Почему это важно?

В стрессовые периоды жизни возможность поговорить с квалифицированным специалистом может стать критически важной. Новый номер делает эту помощь ближе, понятнее и оперативнее.

БЕЗОПАСНОСТЬ В ИНТЕРНЕТ-ПРОСТРАНСТВЕ



Схемы преступных действий с использованием информационно-коммуникационных технологий

Злоумышленник знакомится с несовершеннолетним в мессенджере, социальных сетях или чатах онлайн-игр.

В ходе общения выясняет возраст собеседника, а потом выдает себя за сверстника. В беседе будущей жертве предлагается в обмен на бонусы к играм (моды, скины, или специальные версии, игровые деньги и т.д.) отправить мошеннику личные фотографии или видеозаписи интимного характера.

После их получения, преступник угрожает размещением указанных материалов в общем доступе в сети Интернет, направлением их родителям, знакомым или одноклассникам, если потерпевший не переведет ему деньги.

Схемы преступных действий с использованием информационно-коммуникационных технологий

В ходе онлайн-игр (Minecraft, Roblox и др.) в игровых чатах преступниками размещается информация о возможности приобретения улучшений, позволяющих развить игровых персонажей.

Мошенники обещают детям предоставить их после перевода оговоренной суммы денежных средств.

Вместе с тем после оплаты переписка с потенциальным продавцом удаляется, а его контакты блокируются.

Схемы преступных действий с использованием информационно-коммуникационных технологий

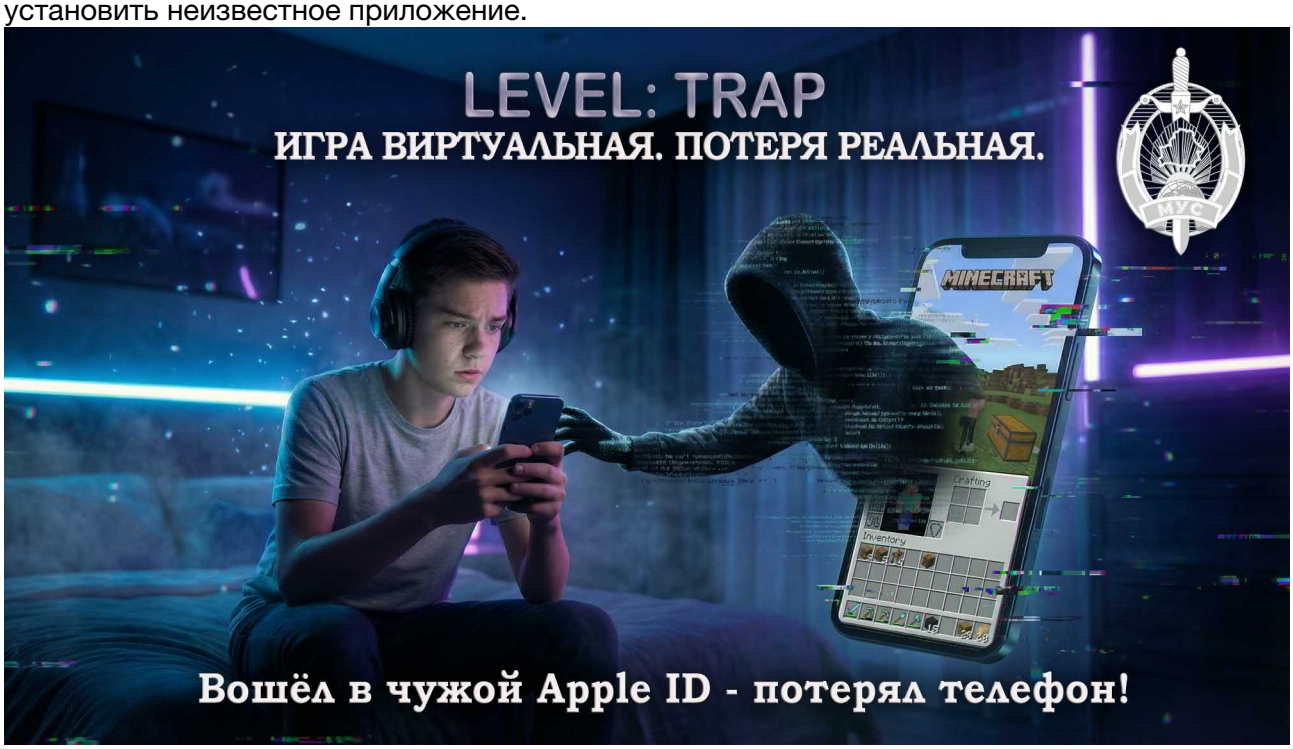
Ребенку в мессенджере поступает звонок от имени работника РУП «Белпочта» или операторов сотовой связи, которые под различными предлогами пытаются узнать персональные данные родителей. После их получения осуществляется второй звонок якобы от представителя правоохранительных органов. Несовершеннолетнему сообщается о том, что он предоставил персональные данные родителей мошенникам, в результате чего на их имя оформлены банковские счета, через которые перечислены крупные суммы денег, добытые преступным путем.

Затем подростку угрожают привлечением родителей к уголовной ответственности из-за него. Чтобы этого избежать, предлагается «спасти родителей», для чего необходимо выполнить процедуру обязательного «декларирования» денежных средств, находящихся дома. Далее ребенку под угрозой ареста или заключения под стражу родителей предлагается передать имеющиеся в доме денежные средства или оставить их в указанном злоумышленником месте для проведения процедуры «декларирования» или зачисления на «безопасный счет». При этом детям категорически запрещают рассказывать об этом кому-либо. После передачи сбережений сведения о входящих звонках и переписке удаляются преступником.

ВАЖНО ЗНАТЬ ДЕТЯМ

Уважаемые ребята! В интернет-пространстве нужно быть предельно бдительными – всегда! Вступая в онлайн-диалог с незнакомыми пользователями, руководствуйтесь главным правилом: **«Никогда не доверяй! Проверяй!»**.

Мошенники могут подстерегать вас в чате игры «Minecraft». Под предлогом установки ее бесплатной версии и бонусов к ней (моды, скины, или специальные версии), предложить обсудить условия сделки в мессенджере (Telegram, WhatsApp, Viber). В ходе переписке преступник выясняет, есть ли у вас в пользовании устройства марки «Apple». Если вы это подтверждаете, злоумышленник предлагает войти в чужой Apple ID, отключить защиту и установить неизвестное приложение.



Таким образом, вы передаете преступнику управление своим устройством «Apple». После этого последний переводит устройство в режим блокировки, в результате чего вы не сможете его использовать. Для разблокировки устройства преступник потребует денежное вознаграждение!

В сети действуют те же правила безопасности, что и в реальном мире:

Не рассказывай о себе много!

Ни за что и нигде не раскрывай свои личные данные. Никогда не пиши в интернете свои настоящие имя, фамилию, дату рождения, адрес, место своей учебы, место работы родителей. Этой информацией могут воспользоваться воры и мошенники не только в виртуальной, но и в реальной жизни. Придумай себе забавный никнейм для Интернета!

Общайся только с теми, кого ты действительно знаешь!

Не отвечай в мессенджерах на сообщения от незнакомых тебе людей! Расскажи родителям или любому другому взрослому, которому ты доверяешь, если тебе предлагает переписку человек, которого ты не знаешь в реальной жизни. К сожалению, в сети попадаются плохие люди, злодеи-обманщики и киберпираты, которые могут прикрываться милыми именами, но общение с которыми может быть опасным

Не стоит встречаться в реальной жизни с людьми из переписки в интернет.

Ты можешь быть уверен, что тот, с кем ты играешь в онлайн игру, твоего возраста. А на самом деле может оказаться, что это сорокалетний дядька, который хочет обокрасть вашу квартиру. Никогда не приглашай интернет-знакомых к себе домой, и не соглашайся ходить в гости к ним. Тебя могут похитить или сделать тебе больно. Обязательно расскажи родителям или другим взрослым, которым ты доверяешь, если кто-то из интернета настойчиво приглашает тебя встретиться.

Никому нельзя показывать фотографии своего тела.

Расскажи взрослым, если кто-то предлагает тебе сфотографировать себя и отправить фотографии ему. Ты должен знать, что твое тело — от кончиков волос до ногтей на ногах — принадлежит только тебе. И никто не имеет права оказывать на тебя давление. Точно также как в реальной жизни, ты имеешь право запретить другим людям трогать тебя, так и в виртуальном мире ты не должен никому себя показывать.

Ты не обязан хранить секреты!

Если тебе от тайны, которую тебя просят хранить, делается не по себе, ты не обязан ее хранить. Если кто-то попросит тебя держать что-то в секрете, а тебе это не нравится, расскажи об этом родителям или педагогу.

Будь вежливым в общении в интернете!

Виртуальное пространство — такое же общественное место, как улица, школа или метро. Поэтому не стоит вести себя плохо в отношении других людей: обижать кого-то, писать обидные слова, оскорблять и угрожать.

Нельзя верить всему, что пишут в интернете.

К сожалению, в интернете очень много лжи. Кто-то пишет неправду от скуки, кто-то намеренно обманывает других людей, чтобы нанести им вред. Мы не можем понять, почему люди совершают плохие поступки. Но мы можем себя от них уберечь.

Никогда не открывай подозрительные письма или спам!

И ни в коем случае не переходи по ссылкам в них. В таких письмах могут быть спрятаны опасные вирусы или вредоносные программы. Они могут не только сломать твой компьютер или гаджет. Но и получить доступ к личной информации вашей семьи, и потом, например, списать все деньги с банковских карточек.

Если тебе страшно, просто отключи интернет.

Посещай только те сайты, играй только в те игры, которые тебе разрешают родители. Переходя по незнакомым ссылкам, ты можешь случайно натолкнуться на страшные видео и фотографии. Насмотришься такого, а потом не заснешь неделю. Если вдруг ты увидел что-то в Интернете, что пугает или беспокоит тебя, обязательно поговори со взрослыми. Задай родителям вопросы, которые тебя волнуют. Если ты разберешься в том, что случилось, ты перестанешь волноваться и бояться.

Если тебе страшно, просто отключи интернет.

Бывает пугающий тебя ролик или программу показывают снова и снова много раз. Страх и волнение от этого только растут. Отключи свои гаджеты. Займись другими обычными вещами. И ты и не заметишь, как то что тебя пугало и волновало, перестанет казаться таким ужасным. Помни, что жестокие или неприличные видео, не имеют отношение к реальности. Это как страшное кино, в котором показывают то, чего не бывает в обычной жизни. Просто закрой браузер, отключи интернет и расскажи родителям.

ПОЛЕЗНАЯ ИНФОРМАЦИЯ

- Безопасность персональных данных в компьютерных играх
- Безопасность в социальных сетях
- Кибербуллинг
- Приватность и как защитить личные данные в интернете?

- Доксинг: что это такое и как избежать?
- Безопасные покупки в интернете

ВАЖНО ЗНАТЬ РОДИТЕЛЯМ

Безопасность детей в сети – это не просто запреты, а создание защищенной среды и обучение правильному поведению. В семье необходимо выстраивать доверительные отношения с ребенком. Дети не должны искать понимания у незнакомцев в сети, а быть уверены, что могут рассказать родителям о любой странной или неприятной ситуации в сети без страха быть наказанным.

Важно договориться и установить четкие правила: какие сайты можно посещать, сколько времени проводить онлайн, какие приложения можно использовать. Для младших детей рекомендуется создавать аккаунты вместе и знать их пароли.

Использование специализированного программного обеспечения **родительского контроля** позволит ограничивать время за экраном, фильтровать контент, блокировать нежелательные сайты. Программ "родительского контроля" существует большое количество как для контроля мобильных телефонов детей, так и для компьютеров или ноутбуков. Их можно скачать и установить бесплатно. Эти приложения ограничивают те или иные функции гаджетов. В них возможно оградить ребенка от неблагоприятных сайтов, длительного пребывания в интернете или играх. С их помощью - отследить его активность в интернете и недопустить ознакомления с нежелательным контентом, а также оградить от поиска запрещенных или ограниченных к обороту веществ, предметов, услуг. Также установить, где находится ребенок в любой момент по геолокации и многое другое. Существует множество преступных схем, используемых кибермошенниками в отношении несовершеннолетних детей.

Способы киберпреступлений в отношении детей и подростков:

- **«бесплатные» подарки и розыгрыши,** когда ребенку для получения выигрыша предлагается перейти по ссылке и ввести платежные и иные данные его родителей. Основная цель – украсть данные банковских карт или учетных записей;
- **«фейковые» запросы от друзей**, когда с использованием взломанного аккаунта друга ребенка просят помочь (перевести денежные средства), а ребенок, желая помочь, может не усомниться в личности просящего;
- **«груминг»,** когда взрослый злоумышленник под видом сверстника втирается в доверие к ребенку в соцсетях или играх, постепенно выведывает личную информацию, манипулирует, вызывает чувство близости, а затем может выпрашивать интимные фото/видео или назначать личную встречу, что может привести к совершению в отношении ребенка действий сексуального характера, которые ребенок в силу возраста не может оценивать, как социально-значимые, считая происходящее игрой;
- **«сексторшен»**, когда преступник, получив интимные фото или видео (добровольно отправленные ребенком или через взлом камеры), начинает шантажировать ребенка, вымогая как материальные блага, так и услугу, в том числе сексуального характера;
- **кибербуллинг (или травля),** когда создаются группы и паблики для насмешек, унизительных комментариев, отправляются угрозы в личных сообщениях, чтобы причинить ребенку психологическую боль, что нередко может закончится депрессией или даже самоубийством;
- **вовлечение в опасные сообщества**, пропагандирующие депрессивные течения, суицид, анорексию, насилие или экстремизм, которые преподносятся ребенку как что-то «модное», «крутое» и «запретное».

Уважаемые родители! Если у вас возникают подозрения, что в сети Интернет в отношении вашего ребенка совершены противоправные действия, необходимо сразу же обратиться в милицию по телефону 102 или сообщить в чат-бот МВД «Мы всегда рядом».

Безопасность в социальных сетях

Социальные сети – пространство для общения, поиска информации, ведения своих блогов и многого другого. Но здесь спрятано и множество рисков: кибербуллинг, мошенничество, груминг и др.
Давайте сформируем перечень советов, которые помогут детям и родителям защитить свои данные в социальных сетях.

Сделайте свой аккаунт приватным

Закройте свой аккаунт, чтобы быть уверенным: контент, который вы публикуете, доступен только друзьям и знакомым. По данным исследования «Лаборатории Касперского» «Взрослые и дети в интернете: альтернативные цифровые реальности», 79% детей

получают заявки на добавление в друзья от незнакомых людей в социальных сетях, а 23% случаев – это незнакомые взрослые.
Некоторые незнакомцы могут оказаться злоумышленниками. Они могут узнать у вас личную информацию или прислать фишинговые ссылки на сервисы, чтобы украсть личные данные. Логичным следующим шагом будет запрет на отправку сообщений от незнакомых вам людей.

Используйте антивирусные решения на всех своих устройствах

Технические меры защиты, установленные на ваших устройствах, помогут вам уберечь свои данные от действий зловредного программного обеспечения (вирусов, троянов, шифровальщиков и др.).
Кроме того, стоит позаботиться и о том, чтобы регулярно устанавливать обновления для вашей операционной системы, мобильных приложений и защитных решений. Разработчики программных продуктов периодически находят уязвимости в своем коде и стараются максимально быстро выпустить обновления. Зачастую этого может оказаться недостаточно, ведь о существовании уязвимости знают не только разработчики, но и злоумышленники, которые могут эти уязвимости эксплуатировать в своих целях. Например, они могут получить доступ к данным, которые хранятся на вашем устройстве (фото, видео, переписка).
Антивирус помогает быстро «отловить» все опасности, которые могут угрожать вашим данным. Например, обнаружить зловредное программное обеспечение, заблокировать переход по фишинговой ссылке или отфильтровать спам-письмо в электронной.
Устанавливать защитные решения нужно не только на персональные компьютеры, но и на мобильные устройства.

Используйте надежный пароль

Правило такое: один сервис, один пароль. Не самой хорошей идеей будет авторизация в социальной сети при помощи аккаунта другой социальной сети, т.к. в случае утечки данных обе учетных записи будут скомпрометированы.
Большое количество паролей запомнить сложно. Чтобы запомнить все коды, можно воспользоваться менеджером паролей. Проверить вашу учетную запись на наличие утечек в сеть можно в сервисе Have I Been Pwnd (HIBP).

Не открывайте подозрительные ссылки

Если вы получили сообщение с такой ссылкой, даже от человека из вашего списка контактов, не торопитесь по ней переходить. Сразу обращайте внимание на подозрительные словосочетания в обращении собеседника. Например, обычно ваш друг даже не здоровается, а сразу переходит к сути вопроса. А в этот раз пишет «доброе утро!» и «как дела?». Сообщение от мошенников может начинаться словами «Дорогой друг…» в начале, вместо обращения по имени и др. В этом же сообщении вас могут просить что-то сделать: проголосовать за рисунок, видеофрагмент, оценить работу художника и т.п. Не спешите это делать, свяжитесь со своим другом, например, по телефону и уточните детали. Или задайте вопрос, ответ на который можете знать только вы вдвоем. Часто злоумышленники, получив доступ к аккаунту пользователя, начинают от его имени отправлять сообщения всей книге контактов. В надежде на то, что кто-то им поверит и совершит действия, которые от него требуются.

Кибербуллинг

Буллинг – это умышленное агрессивное поведение в отношении жертвы, которое носит систематический характер. С таким поведением по отношению к себе может столкнуться буквально каждый, достаточно чем-то отличаться от других, быть не как все, иметь увлечения, которые многие могут не разделять и др.

Кибербуллинг, в отличии от агрессивного поведения в реальном мире, отличается анонимностью. Согласно опросу «Лаборатории Касперского», чаще всего травлю организовывают люди, с которыми жертва не встречалась в реальной жизни (44%). Но в 22% случаев – знакомые или даже друзья.

Еще одно отличие кибербуллинга от буллинга. Травля не имеет никаких временных рамок, т.е. может происходить в любое время суток, без перерывов на выходные и праздники, так как происходит в онлайн среде. Она может включать в себя размещение неприятных по содержанию постов, получение сообщений через личные сообщения или в мессенджерах, в том числе сопровождаться медиаконтентом (фото или видео). Цель таких сообщений – запугать и унизить жертву, нанести ему серьезный эмоциональный урон.

Как снизить риски кибербуллинга?

1. Не выкладывайте в публичный доступ свои личные данные: адреса, приватные фотографии, номера телефонов, адрес почты и тем более логин/пароль от какого-либо сервиса.
2. Не общайся с незнакомцами в офлайн пространстве. Злоумышленники могут «втираться» в доверие с целью грабежа, насилия или киднеппинга.
3. Используй функцию блокировки от неприятных собеседников в социальных сетях. Кроме того, можно сообщить о травле администраторам.
4. Не отвечайте на негативные сообщения. Часто агрессоры преследуют именно эту цель: вывести на эмоцию и на неприятный разговор.
5. Можно уйти на несколько дней из онлайна, отключив аккаунты в социальных сетях или других сервисах.

Если вы считаете, что проблема выходит из-под контроля, не закрывайтесь в себе. Нет ничего зазорного, если вы решите обратиться к родителям, а вместе с ними к профессионалам, например психологам, которые специализируются на подобных проблемах.

Есть бесплатные и круглосуточные телефонные линии, куда можно позвонить в кризисной ситуации:

- детская телефонная линия – 8-801-100-16-11
- линия в Республиканском центре психологической помощи, работающая в рабочее время (с 9 до 18) – 8-017-300-2321

А еще эксперты Республиканского центра психологической помощи БГПУ вместе с ЮНИСЕФ в Беларуси запустили онлайн-платформу talk2ok.by, с помощью которой подростки и молодые люди могут бесплатно и конфиденциально получать квалифицированную психологическую помощь в виде онлайн-консультаций – в комфортном для современных подростков формате аудио- и видеочатов.

Приватность и как защитить личные данные в интернете?

В интернете хранится огромное количество информации, и практически любой человек может получить доступ к тому, что его интересует. Мы пользуемся смартфонами, стационарными компьютерами, планшетами, умными телевизорами, голосовыми помощниками и другими устройствами, которые могут подключаться к сети для своих ежедневных нужд. Поэтому личные данные могут легко «утекать» в интернет.
Приватность данных – это гарантия того, что они будут использованы только теми, кому они предназначены. Другими словами, никто не может получить доступ к вашим данным, если у них нет соответствующих прав.
Вы наверняка встречали рекламу в интернете, которая будто бы подобрана специально для вас. Вы недавно искали информацию о новой модели велосипеда или игровой приставки, и тут видите рекламное объявление с предложением купить именно этот товар. Это не случайно. Поисковые запросы – это просто «клад» для любого человека, который занимается рекламой, ведь на их основе вам могут предложить не только сам товар, но и много сопутствующих. Искали игровой ноутбук, а в итоге можете получить рекламу коврика для мышки или даже шлема виртуальной реальности.
Кроме поисковых запросов вы можете оставить много лишней информации о себе в социальных сетях. Например, при заполнении профиля указать номер телефона или домашний адрес, геометки к фотографиям из мест, которые вы часто посещаете и тд. Попробуйте уже сегодня оценить свой профиль с точки зрения того, какую информацию может получить любой пользователь сети, а какую – только друзья. Само собой, мы рекомендуем всю «чувствительную информацию» (там где есть персональные данные) сделать доступной только тем, кто есть у вас в друзьях.

Давайте разберемся, а что можно сделать?

Злоумышленники могут использовать различные базы данных, которые «сливают» в сеть, получить доступ к вашей учетной записи и прочитать вашу переписку с друзьями. Есть случаи, когда подделывают профиль человека, воруя его личность, а затем распространяли информацию от его имени без ведома владельца данных.
Так что же можно сделать?
Даже если вы подключаетесь к различным сервисам через безопасное соединение, поисковые системы или социальные сети могут отслеживать ваши действия в Сети.

- Чтобы предотвратить такое отслеживание со стороны сервисов, переключите браузер в приватный режим. Например, в Chrome он называется «Режим инкогнито», а Firefox — «Приватный просмотр». Если вы работаете за компьютером, доступ к которому есть у других пользователей, например, в библиотеке или школе, приватный режим придется

как нельзя кстати: в таком случае ваши данные и действия не сохранятся на чужом устройстве.

- Не лишним будет установка специальных расширений – плагинов в браузере, которые помогут предотвратить отслеживание с помощью файлов cookie. Они же избавят от назойливой контекстной рекламы. Но будьте внимательны и осторожны: используйте такие расширения только от проверенных разработчиков и скачивайте только в официальном магазине. Злоумышленники часто выдают вредоносные программы за приложения и расширения, предназначенные для защиты.
- Одно из самых важных правил: не забывайте выходить из своих аккаунтов, когда вы их не используете. При этом недостаточно просто закрыть вкладку или браузер. Например, социальные сети могут отслеживать своих пользователей, даже если в их браузере нет открытой вкладки с социальной сетью. Чтобы это прекратить, нужно полностью выйти из аккаунта. Это актуально не только для социальных сетей, но и для других сервисов, например онлайн-банкинга, магазина и т.д.

Ваши данные будут в безопасности, если вы сами будете тщательно отбирать публикуемую информацию и людей, которые смогут ее видеть.

Доксинг: что это такое и как избежать?

Наши действия в интернете, например, на платформах социальных сетей или игровых мирах могут привести к нежелательным последствиям уже в реальном мире. Мы создаем профили в соцсетях и других сервисах, оставляем свои данные на разных ресурсах. Часто сами сервисы просят нас рассказать что-то о своей жизни, поделиться эмоциями, указывать места, которые вы часто посещаете, других людей на фотографии и т.д.
Возможность свободно получать информацию практически о любом человеке заинтересовала злоумышленников, которые стали называть **доксерами**. А сам процесс – **доксингом**. Это поиск и преднамеренное раскрытие информации о человеке с целью получения какой-либо выгоды, шантажа или травли.
Самыми распространенными действиями со стороны таких злоумышленников являются раскрытие данных жертвы: адреса проживания, места работы, медицинских диагнозов, переписки с друзьями и другой информации о пользователе. Кроме того, в общий доступ могут попасть детали личной жизни, которые изначально не предназначались для посторонних глаз.
В виртуальном пространстве информация распространяется мгновенно и после первой публикации удалить ее из сети практически невозможно. Это факт усугубляет опасность доксинга, который представляет собой серьезную угрозу для потенциальной жертвы.

Откуда берется информация

В интернете можно найти все, что вы когда-либо загружали или пересылали, существуют даже специальные сервисы, которые архивируют все веб-ресурсы и фиксируют

изменения, которые на них происходят. Кроме того, количество утечек данных пользователей за последние пару лет резко возросло. Как это не страшно признавать, но стопроцентной защиты от доксинга не существует.

Что же это за данные?

В интернете можно найти все, что вы когда-либо загружали или пересылали, существуют даже специальные сервисы, которые архивируют все веб-ресурсы и фиксируют изменения, которые на них происходят. Кроме того, количество утечек данных пользователей за последние пару лет резко возросло. Как это не страшно признавать, но стопроцентной защиты от доксинга не существует.

Давайте попробуем разобраться на конкретном примере, могут ли сами пользователи как-то повлиять на распространение информации о себе в интернете и какую роль они играют в этом процессе.

Разбираем на примере

Разберем ситуацию, как злоумышленники могут воспользоваться информацией, которую вы размещаете у себя на странице.

Например, вы давно собираетесь купить новый велосипед. Выбрали модель, цвет, подобрали все оборудование. Чтобы ваши старания оценили друзья, публикуете фото еще не купленного «железного коня» у себя на странице с подробным описанием того, что на нем будет установлено. Через несколько дней вы получаете сообщение от пользователя, который давно на вас подписан, но вы его лично не знаете. Он сообщает вам, что ваш выбор – просто отменный. И что он/она сам недавно купил/а себе точно такой же велосипед и с радостью сможет поделиться с вами ссылкой на онлайн-магазин, где был сделан заказ.

Это сопровождается красивой легендой о том, откуда такая низкая стоимость. Например, склад закрывается или распродажа «только для своих». После этого вам присылают ссылку: она будет фишинговой, т.е. будет приводить пользователя на поддельный сайт интернет магазина. Ошибки в имени сайта будут допущены специально и никогда не будут идентичными настоящей площадке. Если вы понимаете, что это ненастоящий ресурс, то ни в коем случае не вводите свои данные и тем более не совершайте оплату. Даже если такой «знакомый» вернется спустя некоторое время, чтобы поинтересоваться, как все прошло. Можете просто не обращать внимания на такие сообщения.

Стоит ли говорить, что никакого велосипеда вы не получите, зато злоумышленники получат данные банковской карты. В этой ситуации может быть и другой сюжет, разные действующие лица, но итог будет один. Вас попытаются обмануть, используя за основу ту информацию, которую вы сами размещаете у себя в профиле.

Поэтому всегда проверяйте адреса ресурсов, на которые вы заходите, даже если они как две капли воды похожи на настоящие. Если не уверены, всегда можете открыть поисковую страницу и проверить, как пишется адрес веб-ресурса, который вас интересует.

Безопасные покупки в интернете

Интернет-магазины входят в топ-5 самых посещаемых детьми ресурсов в интернете. Часто родители могут сами знакомить с такими площадками, например, чтобы ребенок выбрал себе подарок к празднику.

Вы наверняка читали статьи с информацией о том, что ребенок потратил огромную сумму родительских денег на покупки в компьютерной игре, оформил дорогую подписку на онлайн-сервис или случайно заказал много игрушек (мягкие игрушки, конструкторы и т.п.) на одном из маркетплейсов.

Давайте разбираться, как избежать недоразумений и неприятностей и пользоваться такими сайтами безопасно.

Вот ряд простых правил, которые позволят держать в безопасности свои виртуальные финансовые средства:

— не кладите на карту сразу большую сумму, а лучше пополняйте ее небольшими и регулярными переводами.

— установите лимит на списание денежных средств. Можно посчитать ориентировочную сумму трат в день, например, на проезд или обеды в школе, и дальше принимать решение о том, какой дневной лимит нужно установить.

— запомните, что данные банковской карты (номер, фамилия и имя владельца, срок действия и CVV/CVC – код, который как правило находится на обратной стороне карты) это строго конфиденциальная информация, и ее никому нельзя сообщать.

— не стоит заходить в онлайн-банкинг, если вы подключены через общественные Wi-Fi сети без пароля, например в транспорте, кафе или кинотеатрах.

Вот еще несколько примеров (ситуаций), на которые стоит обратить внимание

Покупки в игровых мирах

Многие бесплатные игры содержат внутриигровые покупки, и это делает их очень дорогими. За дополнительные опции, например игровой инвентарь, новые доспехи, любые внутриигровые ресурсы приходиться платить совсем не виртуальными финансами. Практически во всех игровых мирах есть своя игровая валюта, но приобретается она за вполне реальные деньги. Каждый раз, когда решаете что-то купить, обязательно взвесьте все за и против этой покупки, ведь по большому счету все это остается исключительно в игровом мире. Попробуй найти аналогию в реальном мире перед тем, как сделать покупки. Например, что можно купить на эти деньги в реальном мире, а не в виртуальном.

Пока не разобрались с деталями оплаты, можно поставить техническое ограничение на такие покупки.

Кроме того, обращайте внимание на то, как вы получили предложение внутри игры. Это рассылка сообщений от разработчиков игры или кто-то из других игроков рассылает сообщения о «выгодной покупке» инвентаря. Ведь за такими сообщениями могут скрываться мошенники. Под предлогом покупки интересующего вас товара или

внутриигровой валюты, злоумышленники могут рассылать сообщения с щедрыми предложениями. Цель одна – чтобы вы поверили и перешли по ссылке. Дальше все зависит от целей: кража денег или кража данных, установка на ваше устройство зловредного программного обеспечения и т.д. Всегда критически относитесь к исключительно щедрым предложениям, которые вы получаете от других игроков.

Онлайн-шоппинг

Несколько простых правил, которые помогут сохранить свои средства в безопасности:

1. Никому не сообщайте данные банковской карты и называйте верификационные кода из смс и push-уведомлений. Даже если у вас их попросит человек, который представится сотрудником банка или онлайн-магазина.
2. Не стоит доверять слишком привлекательным предложениям, например, если площадка выглядит подозрительно, появилось много рекламы (баннеров) и визуальных элементов, которых вы раньше не замечали, адрес страницы немного отличается от настоящего, но вас об этом предупредили и уверяют, что все нормально, так и должно быть. Скорее всего вы столкнулись с фишинговым сайтом. (Фишинг – мошенничество, направленное на кражу данных)
3. Не вносите предоплату за товар, который вы еще не получили.
4. Не переходите по внешним ссылкам, которые вы получили от продавцов. Стройте общение только на самой площадке.