ПАМЯТКА ПО БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

ГРУППЫ СМЕРТИ

В последнее время в сети интернет обрели большую популярность так называемые **«группы смерти»**, склоняющие подростков к самоубийству. Яркий пример – игра «Синий кит», она уносит жизни сотен пользователей. Альтернативные названия: «Море китов», «Тихий дом».

Суть игры заключается в том, что подросток, должен выполнять «испытания», которые раздаёт куратор. Эти задания морально подавляют психику подростка. Многие ребята, оказавшиеся в сложной жизненной ситуации, сами ищут способы уйти из жизни и вступают в такие группы. Хладнокровные анонимы, вместо помощи ещё больше вгоняют человека в депрессию, а если кто-то отказывается от дальнейшего прохождения испытаний, то начинаются угрозы в его адрес.

Как избежать, или как «выйти из игры» вам или вашим близким:

1) Самое лучшее это **обратиться к взрослым**: родителям, психологам или полиции. Они помогут и выведут на чистую воду тех, кто возомнил себя вершителями судеб.

2) Самый **простой вариант прекратить играть** – выйти из чата и всех групп и просто игнорировать сообщения от куратора игры. В этом случае вам могут начать угрожать, писать, что найдут родственников и причинят им вред. Однако следует знать, что кураторы «Групп смерти» не держат своего слова и угрозы не выполняют.

3) Еще один вариант – завести новую страничку и вместе с ней **начать новую жизнь** без китов, кураторов, опасных заданий, без групп смерти.

4) Всегда **нужно понимать, что смерть – это не выход и всегда есть другие пути решения**, даже самых сложных проблем. Не верь тому, кто хочет тебе вреда. Не будь его игрушкой. Если уж ты готов рисковать, то рискни бороться с тем, кто возомнил себя повелителем твоей судьбы. Верни себе право на свою жизнь. Всё может быть по-другому!

Обращайте внимание на своих знакомых в социальных сетях, может они выкладывают подозрительные посты, подписывают хештеги:
#китыплывутвверх, #синийкит, #тихий, #синий, #китом, #жду, #синий_кит, #хочу, #разбуди, #спасименя, #рина, #тихийдом, #4, #китообразный, #Видья, #я_в_игре, #разбуди меня в 4:20.
НЕ ОСТАВАЙТЕСЬ РАВНОДУШНЫМИ, не дайте им издеваться над собой, возможно, им просто не хватает внимания и человеческого тепла.

РОДИТЕЛИ!
Интересуйтесь жизнью своего ребенка, с кем он общается, на каких сайтах он сидит, проведите беседу, не строгую, а душевную, ведь всем детям хочется быть важными, понятыми и услышанными.

ВЕРБОВЩИКИ ИГИЛ

ИГИЛ – это непризнанное суннитское исламское государство на территории восточной Сирии и западного Ирака. Фактически ИГИЛ – большая террористическая группировка, захватившая несколько городов Сирии и Ирака, пользуясь слабостью местных армий, гражданской войной в Сирии.

Как понять, что тебя вербуют в ИГИЛ?

1. Дружелюбный незнакомец

Если в вашем кругу общения «абсолютно случайно» оказался человек, который слишком сильно заинтересован изучением вашей жизни, это уже может быть первым маленьким звоночком. Как правило, такой малознакомый человек пытается узнать у вас много личной информации о текущем состоянии дел (о проблемах, стрессах, заботах, финансовом положении). При этом он демонстрирует высокую осведомлённость о ваших чувствах и эмоциональном состоянии, старается помочь решить ваши проблемы, чтобы в дальнейшем вы чувствовали себя обязанным.

2. Нужный человек

Часто вербовщики стараются занять пустующую нишу в жизни человека. Какая роль будет выбрана, зависит исключительно от вас, так как на начальном этапе целью является удовлетворение ваших потребностей, например, в самоутверждении или желания иметь близкие отношения, желания отомстить и так далее.

3. Спутанные мысли

Появляется разница между прошлой и настоящей жизнью, также возможно ощущение проживания двух жизней одновременно. Вы чувствуете, что вам трудно сформировать конкретное отношение или чёткую позицию в каком-то вопросе. Первостепенная задача вербовщика — сделать человека беззащитным перед манипуляцией, а это достигается запутыванием мыслей, необходимо сделать их нелогичными, заставить человека усомниться в своём мировоззрении, в своих жизненных принципах, идеях.

4. Кругом враги

Часто вербовщики стараются представить социум и ближайшее окружение враждебными, глупыми, деградирующими людьми. Вы можете услышать такие фразы: «Кажется, твои друзья совсем не понимают тебя и не могут оценить твои таланты! Ты достоин большего!» и т. д. Если вам вдруг стало невыносимо ваше привычное общество (друзья, родные, коллеги), прежде чем «сжигать все мосты», постарайтесь найти у себя в воспоминаниях именно тот момент, когда ваши близкие стали вызывать у вас подобные чувства, и проанализируйте, что тогда произошло.

5. Беседы о религии

Частые разговоры о религии, возможное обесценивание собственной веры или навязывание иных трактовок. Также формирование кармической, духовной связи с Богом, гуру, идолом: «Бог с тобой», «Учитель тебе поможет», «С Богом ты не один», «Учитель придаст тебе сил» и пр.

6. Готовые ответы на сложные вопросы.

Изменение смысла общих понятий, представлений и предоставление готовых образцов и смыслов. Например: смысл жизни — быть счастливым, а счастье есть чистое преданное служение ИГИЛ. То есть достичь счастья можно через хорошее внешнее поведение. Или: месть — это восстановление справедливости, справедливость — это истина, Бог любит истину, он за тебя!

7. Жажда мести

Вас призывают к чувству вины, долга, мести. Например, отомстить за смерть близкого человека или за то, что в этом обществе не находится признания, благополучия, справедливости и т. д.

8. Ты избранный

Вам пытаются внушить принадлежность к «просветлённому обществу», к «избранным». Для этого может предлагаться различная атрибутика в виде одежды, значков, каких-либо других предметов, символизирующих принадлежность к группе, а также журналов, книг, музыки.

9 . Ты — неотъемлемая часть группы

Один из способов воздействия — это создать ощущение принадлежности к группе и потери собственной индивидуальности. Для этого человека аккуратно могут начать контролировать, как и его время, его мысли. Не давать принимать решения самостоятельно: «Посоветуйся с нами, без нас ты можешь меньше!».

10. Странные просьбы

Когда степень доверия уже велика или манипулятор видит, что перед ним человек, который не умеет говорить «Нет!», могут возникнуть странные просьбы. Например, вас попросят отнести чемодан, содержимое которого вы не знаете, неизвестным людям. Сопровождая просьбу поддерживающими фразами: «Ты же мой друг!», «Ты что, мне не доверяешь?», «Сделай доброе дело!» и пр. Всегда узнавайте, что вы передаёте и кому! Тут же можно говорить о таких предложениях, как, например, выпить «просветляющий напиток» или вкусить «особое лакомство их сообщества».

11. Сомнительные встречи

Вас зовут на какое-либо мероприятие, не объясняя точного смысла и целей этого собрания. Само мероприятие кажется вам странным, в обычной жизни вы бы вряд ли его посетили. Вас могут просить оставлять эти встречи в тайне. Или наоборот — распространять их в массы.

12. Поэтапный допуск

На ваши вопросы отвечают неоднозначно, сообщают о том, что истину можно узнать, только заслужив её. Далее постепенно предоставляют порционно информацию, подчёркивая вашу ответственность за полученные знания и заслуженную степень доверия.

КИБЕРБУЛЛИНГ ИЛИ ВИРТУАЛЬНОЕ ИЗДЕВАТЕЛЬСТВО

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет - сервисов.

Основные советы:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт.
2. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом.
3. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;
4. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.
5. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов.
6. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

ЦИФРОВАЯ РЕПУТАЦИЯ

Цифровая репутация – это негативная или позитивная информация в сети о тебе. Компрометирующая информация, размещенная в интернете, может серьезным образом отразиться на твоей реальной жизни. «Цифровая репутация» - это твой имидж, который формируется из информации о тебе в интернете. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;
3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

ИНТЕРНЕТ-МОШЕННИЧЕСТВО

Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься «любимым» делом.

Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого, состоит в получении конфиденциальных данных пользователей – логинов и паролей.

Основные советы:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее.
2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем.
3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем.
4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты.
5. Установи надежный пароль (PIN) на мобильный телефон.
6. Отключи сохранение пароля в браузере.

МОБИЛЬНЫЙ ТЕЛЕФОН

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало.

Основные советы для безопасности мобильного телефона:

1. Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги.
2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут 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 содержать вредоносное программное обеспечение.
6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies.
7. Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

ОБЩИЕ МЕРЫ ПРЕДОСТОРОЖНОСТИ ПРИ РАБОТЕ В ИНТЕРНЕТЕ

Основные советы:

1. Никогда не сообщайте свои имя, номер телефона, адрес проживания или учебы, пароли или номера кредитных карт, любимые места отдыха или проведения досуга.
2. Используйте нейтральное экранное имя, не содержащее сексуальных намеков и не выдающее никаких личных сведений, в том числе и опосредованных: о школе, в которой вы учитесь, места, которые часто посещаете или планируете посетить, и пр.
3. Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу.
4. Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений.
5. Никогда не соглашайтесь на личную встречу с людьми, с которыми вы познакомились в Интернете.
6. Прекращайте любые контакты по электронной почте, в системе обмена мгновенными сообщениями или в чатах, если кто-нибудь начинает задавать вам вопросы личного характера или содержащие сексуальные намеки.

БЕЗОПАСНОСТЬ РАБОТЫ В ОБЩЕДОСТУПНЫХ СЕТЯХ WI-FI

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные Wi-Fi сети не являются безопасными.

Основные советы:

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 ты обезопасишь себя от закачки вируса на твое устройство;
3. При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам»;
4. Не используй публичный Wi-Fi для передачи личных данных, например для выхода в социальные сети или в электронную почту;
5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
6. В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически».

ONLINE ИГРЫ

Современные онлайн-игры – это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, закрываются уязвимости серверов. В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков.
2. Пожалуйся администраторам игры на плохое поведение этого игрока, 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, твой компьютер могут заразить.

АВТОРСКОЕ ПРАВО

Современные подростки – активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

Термин «интеллектуальная собственность» относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права – это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

ДЛЯ РОДИТЕЛЕЙ

КАК УЗНАТЬ, НЕ СТАЛ ЛИ РЕБЕНОК ПОТЕНЦИАЛЬНОЙ ЦЕЛЬЮ ПРЕСТУПНИКА?

1. Ребенок проводит много времени в Интернете.
2. В компьютере появились материалы откровенного содержания.
3. Ребенку звонят люди, которых вы не знаете, или он сам звонит по номерам, которые вам незнакомы.
4. Ребенок получает письма, подарки или посылки от неизвестного вам лица.
5. Ребенок сторонится семьи и друзей и быстро выключает монитор компьютера или переключается на другое окно, если в комнату входит взрослый.
6. Ребенок использует чью-то чужую учетную запись для выхода в Интернет.

ЧТО ДЕЛАТЬ, ЕСЛИ РЕБЕНОК СТАЛ ПОТЕНЦИАЛЬНОЙ ЦЕЛЬЮ ПРЕСТУПНИКА?

1. Регулярно проверяйте компьютер на наличие материалов откровенного характера или каких-либо свидетельств об общении с сексуальной окраской – это настораживающие признаки.
2. Контролируйте доступ ребенка ко всем средствам общения, работающим в режиме реального времени, таким, как чаты, мгновенные сообщения и электронная почта. Обычно Интернет-преступники впервые встречают своих потенциальных жертв в чатах, а затем продолжают общаться с ними посредством электронной почты или мгновенных сообщений.

3. Не вините детей. Если, несмотря на все меры предосторожности, ваши дети познакомились в Интернете со злоумышленником, вся полнота ответственности всегда лежит на правонарушителе. Предпримите решительные действия для прекращения дальнейших контактов ребенка с этим лицом.
4. Если ребенок получает фотографии откровенного характера или подвергается сексуальным домогательствам, сохраните всю имеющуюся информацию, включая адреса электронной почты, адреса сайтов и чатов, чтобы иметь возможность ознакомить с ней представителей власти.