



СЕРИЯ ПАМЯТОК
ПО ПРОФИЛАКТИКЕ ДЕСТРУКТИВНОГО ПОВЕДЕНИЯ
НЕСОВЕРШЕННОЛЕТНИХ

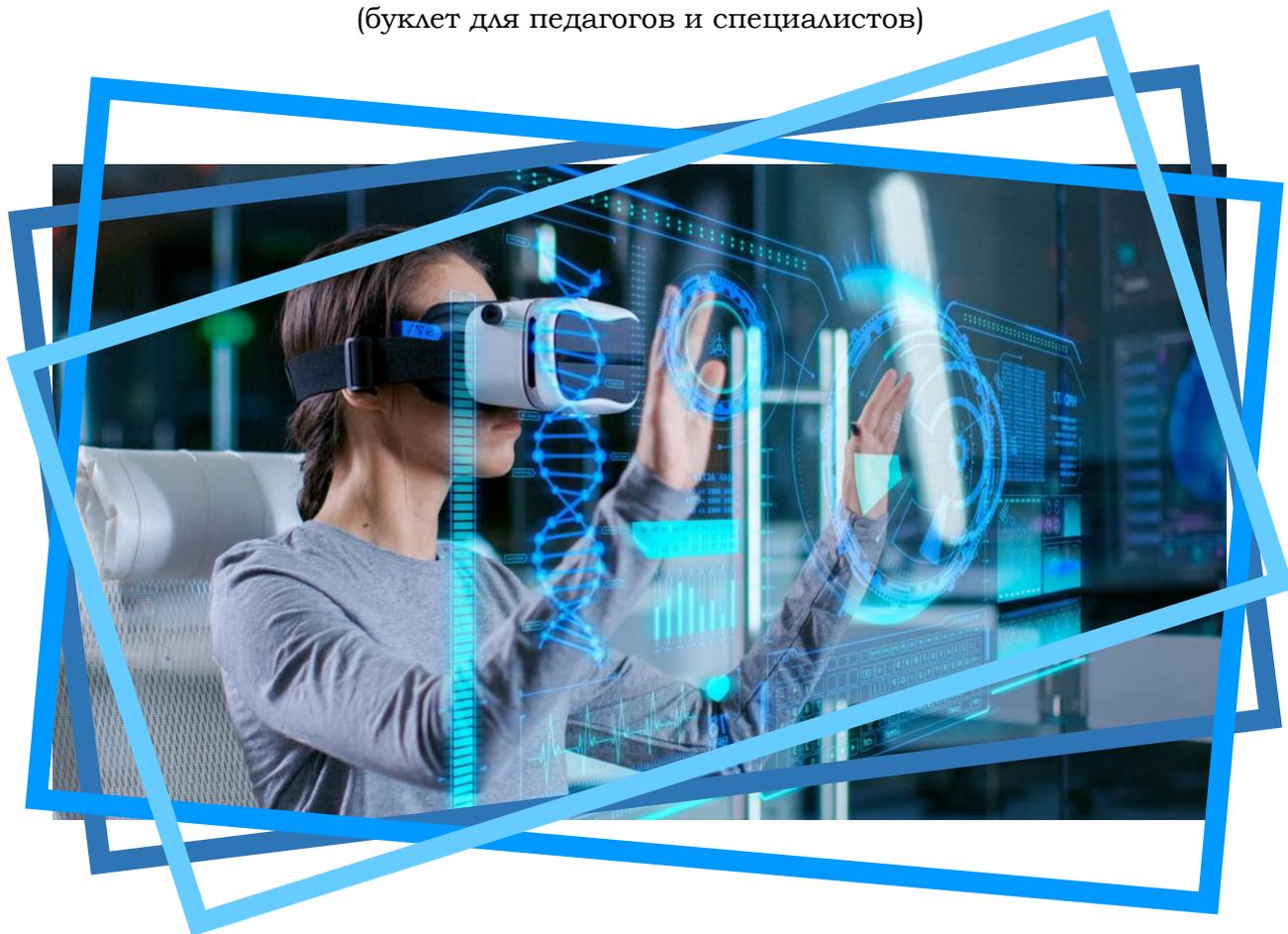
ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ
КОСТРОМСКОЙ ОБЛАСТИ

ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«КОСТРОМСКАЯ ОБЛАСТНАЯ ИНСТИТУТ
РАЗВИТИЯ ОБРАЗОВАНИЯ»

ФАКУЛЬТЕТ
ВОСПИТАНИЯ И ПСИХОЛОГИЧЕСКОГО СОПРОВОЖДЕНИЯ

Пропаганда безопасного поведения в сети Интернет

(буклет для педагогов и специалистов)



КОСТРОМА
2024



СЕРИЯ ПАМЯТОК
ПО ПРОФИЛАКТИКЕ ДЕСТРУКТИВНОГО ПОВЕДЕНИЯ
НЕСОВЕРШЕННОЛЕТНИХ

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ
КОСТРОМСКОЙ ОБЛАСТИ

ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«КОСТРОМСКОЙ ОБЛАСТНОЙ ИНСТИТУТ
РАЗВИТИЯ ОБРАЗОВАНИЯ»

ФАКУЛЬТЕТ
ВОСПИТАНИЯ И ПСИХОЛОГИЧЕСКОГО СОПРОВОЖДЕНИЯ

Пропаганда безопасного поведения в сети Интернет

(буклет для педагогов и специалистов)

КОСТРОМА
2024

Авторы – составители: **Тайгин Олег Валерьевич**, декан факультета воспитания и психологического сопровождения ОГБОУ ДПО «КОИРО»

Адоевцева Ирина Викторовна, доцент кафедры воспитания и психологического сопровождения ОГБОУ ДПО «КОИРО»

Буклет для педагогов и специалистов **«Пропаганда безопасного поведения в сети Интернет»** подготовлен с использованием материалов, разработанных Лигой безопасного Интернета.

Материалы буклета направлены на повышение компетентности специалистов (заместители директора по воспитательной работе, педагоги – психологи, социальные педагоги, классные руководители и кураторы учебных групп) образовательных организаций, а также – специалистов социозащитных учреждений и молодежной политики по вопросам организации просветительской работы, направленной на формирование основ безопасного поведения в сети Интернет у детей, подростков и учащейся молодежи, представителей родительской общественности и специалистов организаций и учреждений детствосбережения.

ВМЕСТО ПРЕДИСЛОВИЯ

Интернет стремительно и быстро вошел в нашу жизнь. Трудно представить человека XXI в., ведущего активный образ жизни, который бы не пользовался Всемирной паутиной.

Сейчас практически у каждого Интернет есть на мобильном телефоне, планшете или другом портативном устройстве. Если нам нужно найти информацию и компанию, узнать новости, уточнить адрес, становится скучно и мы хотим пообщаться с друзьями, посмотреть фильм или видеоролик, поиграть – мы обращаемся к Интернету. Взрослый человек в той или иной мере слышал об угрозах, опасностях в сети, представляет как вести себя в различных сложных ситуациях, а вот младший школьник и подросток слабо представляют, что делать в критических ситуациях.

Таким образом, актуальным становится вопрос по повышению эффективности работы с детьми, подростками и учащейся молодежью, родительской общественностью по выработке единых подходов и требований к безопасному поведению в сети Интернет.

Информационная безопасность касается защиты жизненно важных интересов любого человека (и более глобально – общества, государства). Ложная, неполная, несвоевременная информация может нанести вред. Исследователи выделяют следующие типы Интернет-угроз:

1). Относящиеся к личной безопасности:

- ознакомление с порнографическими материалами, ненормативной лексикой, информацией суицидального характера, расистского, человеконенавистнического или сектантского содержания;

- угроза получения недостоверной или ложной информации;
- формирования зависимости (игровой, компьютерной, от Интернета);
- общение с опасными людьми (извращенцы, мошенники).
- привлечение к выполнению противоправных действий (хакерство, нарушение прав и свобод других).

2). Касающиеся общей безопасности:

- материалы, существование и использование которых может стать причиной посягательства на безопасность окружающих (например, информация о создании оружия или ядовитых веществ);
- сознательное и бессознательное введения в заблуждение других;
- совершение противоправных действий, влекущих за собой ответственность согласно действующему законодательству;
- кибербуллинг – сознательная травля и унижение, прежде всего сверстников.

3). Связанные с утечкой персональной информации:

- разглашение личной и конфиденциальной информации (фамилии, имени, контакты, данные кредитных карт, номера телефонов);
- угроза заражения ПК вирусами различной категории;
- опасность загрузки программ с вредными функциями.

Это наиболее распространенные типы угроз, с которыми может столкнуться не только ребенок, но и взрослый в Интернете, выкладывая или просматривая сомнительную информацию. От некоторых из них можно защититься техническими средствами, но большинство требуют комплексного подхода.

Для формирования устойчивого безопасного поведения в Интернет-среде при планировании и проведении практико-ориентированных занятий, индивидуальных и групповых консультаций с участниками образовательных отношений необходимо использовать материалы, подготовленные с учетом всех требований действующего законодательства Российской Федерации.

Инструментарий пропаганды безопасного поведения в сети Интернет

Во все времена плакаты, листовки были одним из самых распространенных средств массовой агитации и информации, они призывали к определенным действиям, информировали о событиях в стране, указывали на хорошие и плохие стороны жизни, воспитывали в людях чувство патриотизма, любовь к Родине и т.д.

Наглядная агитация используется как дополнительное средство внушения, убеждения, воспитания, обучения. Практически каждый компетентный специалист может самостоятельно разработать материалы, которые планирует использовать в работе с детско-подростковыми, молодежными или родительскими коллективами.

Если рассматривать общие требования к агитационным (информационно-просветительским) материалам, то можно отметить следующее:

1). По содержанию агитационные материалы должны быть актуальными, информация – новой, художественное решение – эмоциональным. Изображенная ситуация должна быть типичной, выглядеть привлекательно. Всегда должна быть четко определена агитационная идея. Например, указать на явления, вызывающие положительное отношение. Или показать негативные факты и их последствия, побудить отрицательное отношение к изображенному.

2). Главное – это понятная, образная трактовка темы. Предпочтительнее использовать симметричные, законченные формы – круг, квадрат, прямоугольник. Хуже воспринимаются абстрактные формы.

Изображения людей и животных, автомашин, оружия привлекают больше внимания, чем вид бытовых предметов. Средства наглядной агитации эффективнее, если в изображении отдельных объектов или ситуаций присутствует сатира, юмор.

3). Текст должен быть кратким, энергичным, доходчивым. Хорошо воспринимаются и запоминаются призывы, состоящие из коротких фраз, особенно рифмованных.

В тоже время, можно воспользоваться и материалами, разработанными компаниями и организациями, специализирующимися в вопросах Интернет-безопасности и пропаганды безопасного поведения пользователей сети Интернет.

Так, при проведении информационной кампании или индивидуально-групповой работы с обучающимися и родителями (законными представителями), направленной на формирование основ безопасного поведения в сети Интернет, в образовательных организациях и социозащитных учреждениях можно рекомендовать использование материалов, разработанных **Лигой безопасного Интернета**, учрежденной в 2011 году при поддержке МВД России, Минкомсвязи и Комитета Государственной Думы по вопросам семьи, женщин и детей.

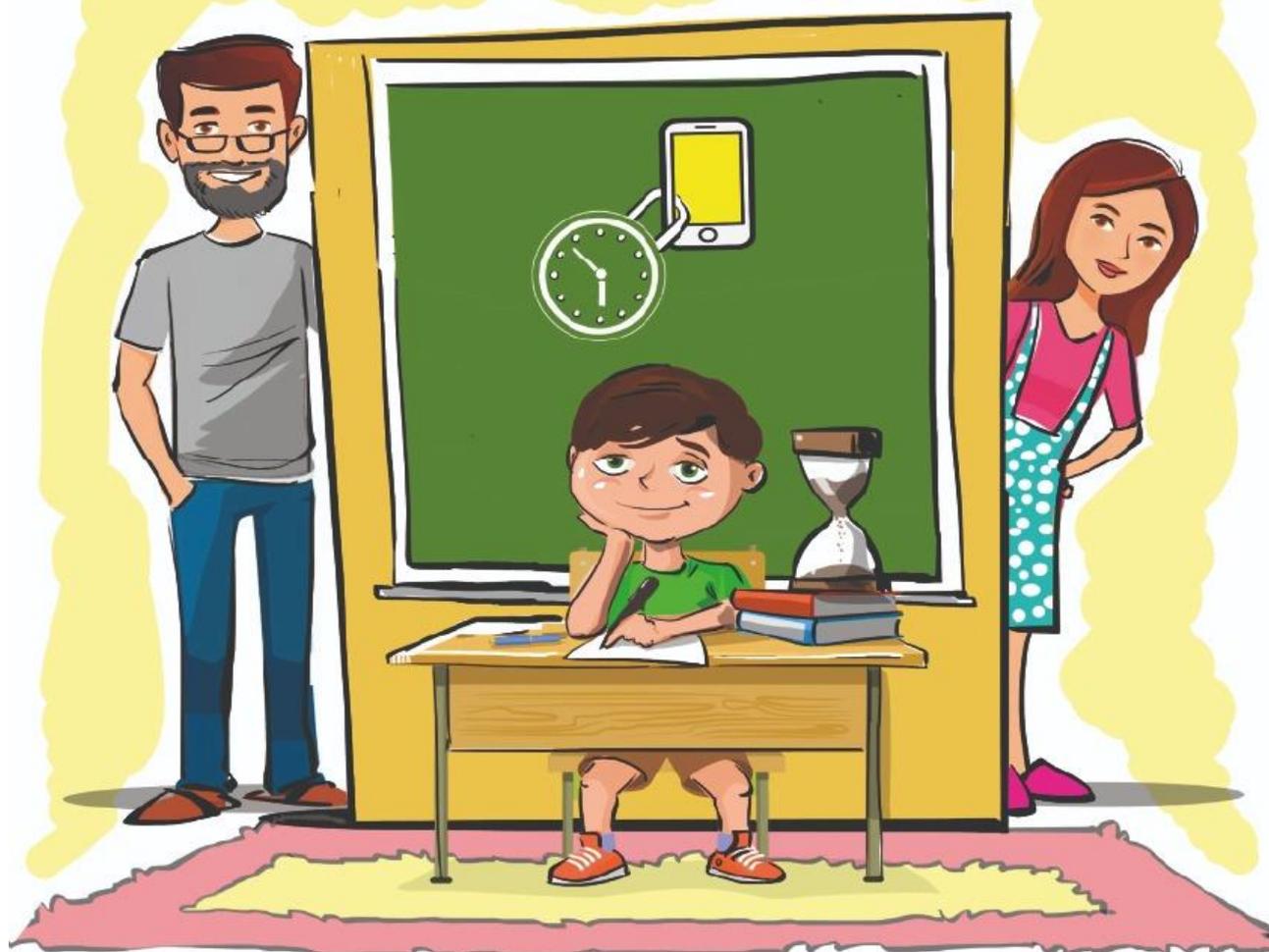
Примеры информационно-просветительских материалов представлены в приложениях:

- 1). Плакаты (приложения 1 – 5);
- 2). Памятки для детей (приложения 6 – 10);
- 3). Памятка для родителей (приложение 11);
- 4). Материалы для специалистов (приложения 12 – 13).

Все информационно-просветительские (оригинал-макеты) и методические материалы размещены на официальном сайте **Лиги безопасного Интернета**:

<https://ligainternet.ru/>

НА УРОКЕ БЕРИ ТЕТРАДЬ, А НЕ ТЕЛЕФОН!



НЕ УТОНИ В СВОЕМ ТЕЛЕФОНЕ!



Реальная
ЖИЗНЬ
гораздо интереснее!



**ТЫ
ЗНАЕШЬ,
КТО СЛЕДИТ
ЗА ТОБОЙ
В ИНТЕРНЕТЕ?**



НАЦИОНАЛЬНЫЙ
ЦЕНТР ПОМОЩИ
ПРОТАЯВШИМ И ПОСТАРАДАВШИМ ДЕТИМ
НАИПРИБЛИЖЕНА.РФ



лига
безопасного
интернета



Сайт
ligainternet.ru

ПИШУТ НЕЗНАКОМЦЫ?



СКАЖИ РОДИТЕЛЯМ!



НАЦИОНАЛЬНЫЙ
ЦЕНТР ПОМОЩИ
ПРЕСТАВЛЯЕМ И ПОСТРАДАВШИМ ДЕТЯМ
НАТЕРИЯВНА.РФ



лига
безопасного
интернета



Сайт
ligainternet.ru

ИНТЕРНЕТ ПОМНИТ ВСЁ!

Цифровой след –
не шутка!



НАЦИОНАЛЬНЫЙ
ЦЕНТР ПОМОЩИ
ПРОБЛЕМАМ И ПОСТРАДАВШИМ ДЕТЯМ
НАТТЕРВОССКА.РФ



лига
безопасного
интернета



Сайт
ligainternet.ru

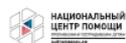
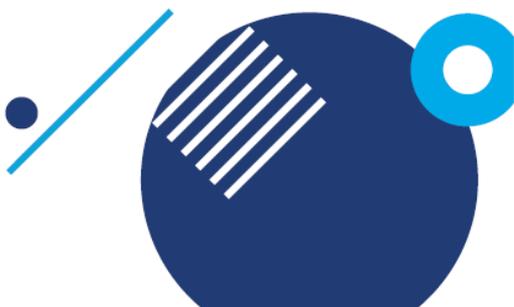
Памятка для обучающихся «10 советов для детей»

Тебе может показаться, что не иметь профиля в социальной сети – это странно, но на самом деле все вовсе не так. Если у тебя нет профиля в соцсети – поздравляем! Ты уже победил! Ведь теперь у тебя будет гораздо больше времени на полезные вещи: учебу, спорт, настоящую, не сетевую дружбу!

Все больше россиян признаются, что соцсети приносят им больше негативных эмоций: печаль, обиду, зависть. Отказ от соцсетей поможет стать по-настоящему счастливым.

Современные соцсети созданы не для общения. Они созданы для рекламы, для продажи товаров и услуг, навязывания чужого мнения. А если у тебя нет соцсетей – ты мыслишь и думаешь самостоятельно!

**НЕ ПОГРУЖАЙСЯ
В ИНТЕРНЕТ С ГОЛОВОЙ!
ЖИВИ РЕАЛЬНОЙ ЖИЗНЬЮ!**



СКОЛЬКО ВРЕМЕНИ СТОИТ ПРОВОДИТЬ В ИНТЕРНЕТЕ?

1. Для развлечения и общения с настоящими друзьями Интернет не нужен, нужна реальная жизнь. Сокращай время пользования Интернетом! Отводи для общения в виртуальном мире не более 1 часа в день. Не позволяй социальным сетям отбирать у тебя здоровье и перспективы!
2. Анонимность в сети - миф. Всё, что мы выкладываем в Интернете, остаётся там навсегда.



3. Проводи больше времени в реальной жизни: общайся с друзьями, родителями, найди себе действительно интересное увлечение, читай, занимайся спортом, придумывай и реализуй полезные социальные проекты, помогай людям, включайся в общественную деятельность, смелее используй свои таланты.
4. Будь бдителен! В Интернете много мошенников, которые охотятся за твоими деньгами и данными. Есть и такие преступники, целью которых является испортить как можно больше детей или загубить их жизнь. Некоторые делают это за большие деньги, продавая снимаемые детьми видео и фотографии, а некоторые потому, что психически больны. Однако понять это, общаясь в Интернете, невозможно. Просто не подпускай к себе незнакомых людей и не позволяй им сделать из тебя свою жертву.
5. Не выкладывай свои персональные данные в Интернет! Помни, что отправлять их не стоит даже друзьям.
6. Закрой свои страницы в соцсетях от посторонним! Будь осторожен с незнакомцами в Интернете, а если кто-то из них задает тебе странные вопросы, навязывает общение или ведет себя агрессивно – блокируй такого человека и не продолжай общение.
7. Не бойся рассказать родителям о своих проблемах! Если кто-то решил тебя обидеть, травить, угрожать тебе, даже если ты попадешься на удочку мошенников, родители смогут помочь тебе и подскажут, как надо поступить.
8. Помни, что из Интернета ничего не удаляется! Если ты не хочешь, чтобы какие-то твои фото или посты увидели все друзья и знакомые – лучше вообще их не выкладывай.
9. Не верь всему, что написано в Интернете! В сети много вранья, многие заголовки пишутся просто для того, чтобы привлечь внимание. Если есть сомнения по поводу новости – лучше проверь, скорее всего это фейк.
10. Соблюдай в Интернете все те же правила, которые ты соблюдаешь в реальной жизни. Общайся с людьми так же, как хотел бы, чтобы они общались с тобой.

НЕ СЛЕДУЙ МОДЕ!

Социальные сети – самый верный способ «убить время». Сетевые развлечения поглощают его без остатка. Но с головой погружаясь в виртуальный мир, мы забываем про друзей, близких, учебу, работу, активный отдых и развитие.

Памятка для обучающихся «Как обманывают в Интернете»

КАК ОБЕЗОПАСИТЬ СЕБЯ ОТ МОШЕННИКОВ?

1. **Настрой в мессенджерах и соцсетях двухфакторную (двухэтапную) аутентификацию.** При попытке входа в свой профиль тебе на почту или в сообщения будет приходить код подтверждения.
2. **Перепроверяй на официальных сайтах номер телефона, с которого тебе позвонили.** Если тебе позвонили, например, из банка или из полиции, представились сотрудником, ты можешь самостоятельно найти в Интернете телефоны этих организаций, перезвонить и спросить у них, действительно ли там работает такой человек, и звонил ли он по твоему номеру и с какой целью.
3. **Проверяй адрес сайта.** Мошенники рассчитывают на невнимательность пользователей и часто делают сайт похожий на оригинал. В адресе сайта может отличаться одна буква или символ.
4. **Обращай внимание на наполнение сайта.** Мошенники часто допускают ошибки в словах и тексте, так как делают сайты-подделки на скорую руку.
5. **Не переходи по неизвестным ссылкам.**
6. **Не открывай файлы из писем или сообщений, которые прислали неизвестные люди.**
7. **Если же ты стал жертвой мошенников, то следует сразу же сообщить об этом родителям.**

**ЧТОБЫ НЕ ПОПАСТЬСЯ
МОШЕННИКАМ – МЫСЛИ
САМОСТОЯТЕЛЬНО!**

КАК ОБМАНЫВАЮТ В ИНТЕРНЕТЕ



КАК ОБМАНЫВАЮТ В ИНТЕРНЕТЕ?

Современные мошенники в Интернете действуют не так, как мы обычно привыкли. Сейчас злоумышленники не крадут у нас деньги напрямую. Вместо этого мы сами им их отдаем. Мошенники манипулируют нами, нашей доверчивостью, страхом или жадностью, а современные технические средства позволяют подделать все, в том числе, сайт или номер телефона.

КАКИЕ СХЕМЫ МОШЕННИЧЕСТВА СУЩЕСТВУЮТ?

1. **Взлом аккаунтов в соцсетях и рассылка сообщений от друзей.** Мошенники придумывают разные ситуации и просят срочно перевести деньги.
2. **Сайты-подделки.** Это могут быть копии страниц социальных сетей и Интернет-магазинов. При покупке товара на сайте-подделке ты не получишь ничего, а деньги отправятся напрямую в руки преступников.
3. **Рассылка писем по электронной почте и в соцсетях с выигрышем.** Мошенники вынуждают ввести свои данные для получения выигрыша или отправить им комиссию за получение награды.
4. **Звонки с поддельных номеров.** Мошенники могут представиться кем угодно – работником банка, полиции, госструктуры, врачом, даже твоим родственником.
5. **Шантаж.** Украденные персональные данные или фотографии мошенники могут использовать чтобы вымогать деньги у жертвы. При этом особое внимание преступников направлено на интимные или иные компрометирующие человека фотографии или сведения, которые они крадут, взламывая почту или личную страницу в социальных сетях.

Современные технические средства позволяют мошенникам подделать любой номер телефона, любой сайт, взломать почту или личную страницу. Будьте бдительны и перепроверяйте информацию. Никогда не отправляйте свои интимные фотографии даже хорошо знакомым людям, которым вы доверяете. Знайте, что ваши откровенные фотографии, легкомысленно направленные кому-либо, могут быть украдены, в том числе, для рекламы разного рода неприличных или противоправных услуг. Вы можете узнать об этом только когда ваши близкие или знакомые увидят вас и составят о вас негативное мнение. Впоследствии подобные фотографии также могут быть существенным препятствием для зачисления в ряд ВУЗов или устройства на хорошую работу.



В своей работе мошенники активно используют социальную инженерию. Они сделают все, чтобы ты сам отдал свои деньги. Для этого они используют нашу невнимательность и доверчивость.

Знаешь ли ты, что никому нельзя сообщать свои пароли, пин-коды, коды из СМС и сообщений? В наше время это знают все, но мошенники могут обхитрить неосторожного пользователя. Они позвонят тебе и представятся сотрудником банка, расскажут о том, что прямо сейчас кто-то пытается украсть твои деньги со счета. А чтобы этого не случилось, ты должен сообщить им код из СМС, которая сейчас придет на твой номер. Естественно, никто твои деньги не крадет. А вот если ты передашь мошенникам этот код, то они получат полный доступ к твоему счету, карте и всем деньгам, которые на ней лежат.

Мошенники не обязательно запугивают. Они могут сообщить о крупном выигрыше. Допустим, в 300 тысяч рублей. Но чтобы получить этот выигрыш, надо заплатить небольшую комиссию – всего лишь 300 рублей. Многие люди в такой ситуации теряют бдительность и думают, что 300 рублей – маленькая цена за такой большой выигрыш. Однако приз, естественно, они не получают, а лишаются своих денег.

Памятка для обучающихся «Травля в Интернете»

4. Заблокируй обидчика и внеси его в черный список, чтобы у него больше не было возможности оскорбить тебя или задеть ложными и неприятными высказываниями.
5. **Никогда не оставайся сторонним наблюдателем, если травле подвергнулся кто-то другой.** Собери в группе (в чате), в которой вы общаетесь команду единомышленников, обговори с ними стратегию действий против обидчика. Вам необходимо выступать единым фронтом против любых оскорбляющих действий и требовать прекращения недопустимого поведения. Как правило, обидчики не осмеливаются идти против большой группы людей, действующих заодно, у них не хватает на это смелости. Если действия обидчика не прекратятся и в этом случае, следует всей команде единомышленников демонстративно выйти из группы (чата), это окажет психологическое воздействие на остальных участников, а также будет поддержкой для жертвы травли. Попробуй выйти на личное общение с жертвой травли и поддержать ее. Если жертвой травли стал твой знакомый, расскажи об этом учителю или его родителю. Тем самым ты можешь помочь человеку, который самостоятельно не видит выхода из сложившейся ситуации и страдает.

**ПРОВОДИ БОЛЬШЕ ВРЕМЕНИ
В РЕАЛЬНОЙ ЖИЗНИ!**



ТРАВЛЯ В ИНТЕРНЕТЕ



ТРАВЛЯ В ИНТЕРНЕТЕ

Травля в Интернете является большой проблемой для всех пользователей. Травлю в сети еще называют кибербуллинг. Она включает в себя издевательства, оскорбления, унижения, преследование человека.

Некоторым кажется, что травля – это всего лишь безобидные шутки. На самом деле это не так. Травля может привести к проблемам со здоровьем, к психическим травмам и другим проблемам. Иногда обижая других, обидчик стремится самоутвердиться за чужой счет. Очень часто обидчик сам является глубоко несчастным, нереализованным и затавленным человеком, который таким деструктивным способом пытается отомстить окружающим за свои проблемы. А, находясь под мнимой защитой Интернета, позволяющей сохранять определенную анонимность, обидчик смело оскорбляет других. Как правило, в реальной жизни обидчик не сможет в открытую сказать тебе ни одного обидного слова.

Однако защищенность обидчика в Интернете на самом деле имеет мнимый характер. Обидчик думает, что его никто не сможет найти, и последствий за его действия не будет. На самом деле это не так. Найти обидчика в сети для специалистов сегодня не составляет никаких проблем.

КАК ВЫГЛЯДИТ ТРАВЛЯ В ИНТЕРНЕТЕ?

1. Оскорбительные и угрожающие сообщения, изображения или видео;
2. Передразнивание, бойкоты или унижительные комментарии в сети, в которых упоминается личность человека;
3. Распространение неприятных слухов и обсуждение человека за его спиной;
4. Создание поддельных аккаунтов от имени конкретного человека с целью обмануть или унижить его;
5. Специально смонтированные фото или видео с изображением человека.



ЧТО ДЕЛАТЬ, ЕСЛИ ТЫ СТОЛКНУЛСЯ С ТРАВЛЕЙ В ИНТЕРНЕТЕ?

1. **Поговори с родителями или учителями об этой ситуации.** Они не оставят тебя одного в неприятном состоянии и помогут наилучшим способом разрешить любую ситуацию. Расскажи им, что ты воспринимаешь эту ситуацию серьезно и объясни какие чувства ты испытываешь.
2. **Постарайся сохранять спокойствие и не отвечать обидчику.** Как правило, его цель – вывести тебя на эмоции. Помни, что твой обидчик распускает о тебе слухи, оскорбляет тебя не потому, что на самом деле считает тебя таким, а потому, что у него самого серьезные проблемы (возможно даже с психикой).
3. **Вместе с родителями собери доказательства:** сделай скриншоты переписки, скопируй ссылки на аккаунты обидчика, тебе это может пригодиться в случае обращения в полицию.

Памятка для обучающихся
«Цифровой след в Интернете»



Внимательно посмотри на свой телефон. Ты знаешь, что современные смартфоны – те же самые компьютеры? Они обладают такими же функциями, а в чем-то даже превосходят компьютер или ноутбук. Наши телефоны включены круглосуточно. И все это время они собирают о нас информацию. Больше всех информацию собирают приложения соцсетей и мессенджеров. Фото, видео, история переписок, хобби и увлечения, даже места, в которых ты бываешь – все это приложения собирают и хранят. А все, что однажды попало в Интернет, остается там навсегда и удалить это невозможно.

ДЛЯ ЧЕГО ИСПОЛЬЗУЕТСЯ ВСЯ ЭТА ИНФОРМАЦИЯ?

1. Соцсети, поисковые сайты, Интернет-магазины и прочие крупные Интернет-ресурсы собирают данные для того, чтобы потом показывать своим пользователям рекламу. Чем точнее реклама попадает в интересы и увлечения каждого конкретного пользователя, тем она качественнее и дороже.
2. За этими данными охотятся злоумышленники. Они могут использовать их для того, чтобы как можно больше узнать о жертве, выяснить, где человек работает, в каком банке у него открыт счет, как его зовут и так далее.
3. Соцсети собирают информацию буквально о каждой твоей активности. Под какими постами ты ставишь лайки, сколько времени ты читаешь новость, какие заголовки тебе нравятся больше, с какими людьми ты дружишь и общаешься, какую музыку ты слушаешь, какие видео тебе нравятся. У соцсетей есть информация даже о том, что ты пишешь и какие фото отправляешь друзьям.

Вся эта информация называется цифровым следом, который каждый из нас оставляет в сети. Невозможно пользоваться Интернетом и не оставлять след. Даже если ты решишь ничего не публиковать, ничего никому не писать, в любом случае прочитанные и просмотренные посты будут формировать длинную историю твоей активности. Этот след уникален для каждого человека, двух одинаковых быть не может. О каждом из нас в Интернете настолько много информации, что можно создать настоящего цифрового двойника.

В Интернете, как и в реальной жизни, нужно быть очень внимательным со своими словами и действиями. Особенно осторожно следует относиться к публикуемым и пересылаемым личным фотографиям. Ни в коем случае никому не отправляй фотографии интимного характера! Из Интернета, как мы помним, ничего не удаляется. Всегда помни: чем меньше мы используем гаджеты – тем лучше!

ЖИВИ РЕАЛЬНОЙ ЖИЗНЬЮ!

Памятка для обучающихся
«Что такое фишинг»



ЧТО ТАКОЕ ФИШИНГ?

Фишинг с английского переводится как «рыбалка». Это самый распространенный вид мошенничества в Интернете. С помощью фишинга мошенники выуживают у пользователя данные и потом используют их в своих целях. В Интернете существует огромное множество фишинговых сайтов. Они могут копировать страницу какого-либо известного сайта: Интернет-магазина или соцсети.

Существует несколько подсказок, при помощи которых можно точно понять, настоящий это сайт или сайт-подделка:

- 1. Проверь адрес сайта.** Мошенники рассчитывают на невнимательность пользователей и часто делают похожий на оригинал сайт. В адресной строке сайта может отличаться одна буква или символ.
- 2. Обращай внимание на предупреждение браузера о небезопасном сайте.** Проверь, есть ли в адресной строке символ замка, если его нет, то это может быть признаком ненадежного сайта.
- 3. Внимательно смотри на наполнение сайта.** Зачастую сайты мошенников, где продается товар, который ты ищешь, имеют ограниченный ассортимент товаров или вовсе могут быть одностраничными сайтами.
- 4. Обращай внимание на правильность написания слов в текстах.** Мошенники часто допускают ошибки в словах и тексте, так как делают сайты-подделки на скорую руку.

Базовые правила, которые помогут тебе уберечь себя от поддельных сайтов:

- 1. Будь внимателен и тщательно обдумывай ситуацию.** Если у тебя возникают сомнения в надежности сайта – лучше им не пользоваться.
- 2. Не игнорируй предупреждения!** Большинство браузеров имеют встроенные системы защиты, предупреждающие, что сайт, на который ты собираешься перейти, может быть небезопасен.
- 3. Не вводи личные данные** (имя, фамилию, номер телефона, домашний адрес, номера и пароли банковских карт, свои фотографии и пр.) на незнакомых сайтах и не сообщай их посторонним.
- 4. На некоторых сайтах есть возможность вместо регистрации зайти через свой профиль в социальной сети. Не пользуйся этой функцией.** Если преступники получают доступ к твоему профилю в соцсети, то они получают доступ и ко всем сайтам, куда ты через него заходил.
- 5. Если ты стал жертвой мошенников, то следует незамедлительно обратиться за помощью к родителям.** Они помогут написать заявление в полицию. Чаще всего преступников удается поймать. Однако вернуть средства гораздо сложнее.

Памятка для родителей «Манипуляции в Интернете»

МАНИПУЛЯЦИИ В ИНТЕРНЕТЕ: ФЕЙКИ, ЛОЖЬ, НЕДОСТОВЕРНАЯ ИНФОРМАЦИЯ

Что такое «фейк»?

Проблема верифицированных источников информации сейчас стоит очень остро не только в России, но и во всем мире. Фейк – целенаправленно распространяемая ложная информация под видом достоверной. Может выражаться в самых разных формах, таких как текстовые материалы, новостные статьи, аудио- и видеозаписи, передачи, а иногда и целые фильмы, снятые в документальном или псевдодокументальном жанре.



Ключевой вопрос:
Жизнь в век дезинформации.
Фейки и ложь в сети

Основным местом концентрации фейков является Интернет. Подобные материалы чаще всего распространяются через интернет-мессенджеры, а уже оттуда попадают в социальные сети или «желтые» средства массовой информации.

Фейки могут распространяться с самыми разными целями:

1. Ради шутки или создания повышенного внимания какому-либо событию.
2. Для увеличения посещаемости сайта («накручивания счетчика просмотров»). Создаются «громкие» заголовки-приманки, кликнув на который пользователи переходят на сайт и таким образом увеличивают трафик этого сайта.
3. С целью дезинформации читателей о реальной ситуации: изменения настроения в обществе, отношения людей к какому-либо вопросу, создания паники или волнения среди людей.

Внимание!

Самый распространенный формат фейков, с которым сталкивался практически каждый – **фейковые новости**. Миллионы людей, подвергаясь регулярному воздействию фейков, начинают верить ложной информации, что в перспективе приводит к негативным последствиям. Лишь 49% россиян, согласно опросу, проведенному ВЦИОМ, уверены, что смогут отличить фейк от настоящей новости.

С **фейками в интернете** сталкиваются не только взрослые, но и дети. Ребенок может увидеть заголовок на сайте, содержащий ложную информацию. Фейки могут целенаправленно рассылаться пользователям в мессенджерах или соцсетях. Кроме того, иногда происходят взломы официальных сайтов или страниц известных организаций. В таком случае злоумышленники могут рассылать ложную информацию от их лица.

Как правило, в информационном пространстве **фейки живут относительно недолго – 3-4 дня**. Для искусственного поддержания интереса к подобному материалу совершаются «вбросы» – ложная информация поступает в Интернет через специальные каналы, откуда распространяется в настоящие СМИ, либо же расходит по пользователям и распространяется с помощью пересылки друг другу.

Кроме **фейков существуют и самые настоящие «ментальные вирусы»**. Ментальные вирусы – это какие-либо тексты, статьи или новости, а иногда аудио- или видеозаписи, содержащие в себе определенную идею. Как и настоящие вирусы, они способны заражать сознание людей и целого общества, внедряя вредную, опасную и разрушительную идею.



Источники опасности:

- **У каждого фейка есть конкретная цель** – могут провоцировать людей на совершение опростраченных поступков.
- **С учетом специфики Интернета - очень большой охват аудитории, скорость распространения.**
- **Могут представлять угрозу жизни и здоровью людей.**
- **Инструмент манипуляции.** Создатели фейка могут управлять подвергнувшимся воздействию как организованной структурой.

Как распознать фейк?

1. Сообщение быстро распространяется в соцсетях или мессенджерах.
2. Сообщение очень эмоциональное, вместе с тем не содержит факты, которые возможно перепроверить.
3. Передаются сведения об угрозе жизни и здоровья большого числа людей, а также о наличии многочисленных жертв.
4. Присутствует указание на то, что власти скрывают информацию во избежание паники или волнений. Именно поэтому вы не найдете ничего в СМИ. Подчеркивается, что значимая для общества информация специально утаивается.
5. Присутствует просьба о максимальном распространении информации, либо о сокрытии (ведь автор сообщил ее вам «по секрету»).
6. Присутствует указание на лицо, сообщившее новость (врач больницы, водитель скорой, учитель школы, знакомый знакомого), либо информация о месте, где что-то произошло (номер больницы, название города, адрес школы).
7. Источник информации сложно установить.

При проверке информации есть ряд маркеров, на которые очень важно обратить внимание:

1. **Оригинал всегда лучше любого пересказа**, поэтому всегда важно искать оригинальный источник информации и задумываться на сколько этому источнику информации можно доверять. Не является ли, например, источником новости желтое СМИ или какая-то из «тизерных» сеток, которые занимаются привлечением трафика пользователей с помощью «кликбейтных», то есть громких заголовков.
2. **При работе с оригинальными источниками важно смотреть взаимосвязь между этими источниками информации.** Если информация опубликована в разных источниках, то как они сами между собой связаны. Не является ли это партнерской сетью ресурсов или единой сетью распространения информации.
3. **Чаще всего разнообразие фейковых сообщений очень низкое**, постоянно публикуется фактически одно и то же сообщение. Практически все фейки являются перепостами.
4. **При сравнении оригинальной настоящей новости и фейка, у настоящей новости всегда очень много свидетелей**, очень много участников, они по-разному рассказывают своими словами о том, что произошло. Настоящая новость имеет очень много серьезных верифицированных источников информации. Сейчас ни одна заслуживающая внимания новость не проходит мимо ведущих средств массовой информации.
5. **Очень важно обратить внимание на контекст новости** и проверять полную суть любой цитаты, которая используется в том или ином сообщении. Не стоит доверять ссылкам на громкие и авторитетные имена. Проверять нужно как цитаты, так и факты, кому бы они не принадлежали, какая бы известная фамилия ни была озвучена.
6. **Очень важно обращать внимание на суть, смысл самого материала**, а не на мелкие детали, которых очень много в фейках. Они, таким образом, отвлекают внимание от содержания, придавая некую достоверность материалу.
7. **В новой информационной реальности важно научиться доверять серьезным средствам массовой информации, официальным источникам**, которые дорожат своей репутацией и ответственно относятся к распространению новых сведений и данных.

Полезные советы

Если вы получили или обнаружили недостоверную информацию, есть простые шаги, с помощью которых можно защитить себя, своих друзей и родственников от массового распространения этого сообщения:

1. Стоит дождаться официального подтверждения или опровержения громкой новости, прежде чем пересылать что-то друзьям и знакомым.
2. Обратитесь в службу поддержки и направьте туда все имеющиеся у вас ссылки, скриншоты и т.д.
3. Обратитесь в полицию, Роскомнадзор и прикрепите ссылки и скриншоты страниц, содержащих недостоверную информацию.
4. Если вы считаете, что сообщение или публикация является общественно опасной, вы можете прислать скриншот и ссылку в Лигу безопасного Интернета по адресу: info@ligainternet.ru или в сообщениях ВК: vk.com/liga.

Внимание!

В случае обнаружения фейковой информации не стесняйтесь и пользуйтесь кнопкой «Пожаловаться» (в случае с социальными сетями или мессенджерами). Мессенджеры и соцсети должны оперативно блокировать такие сообщения и публикации.



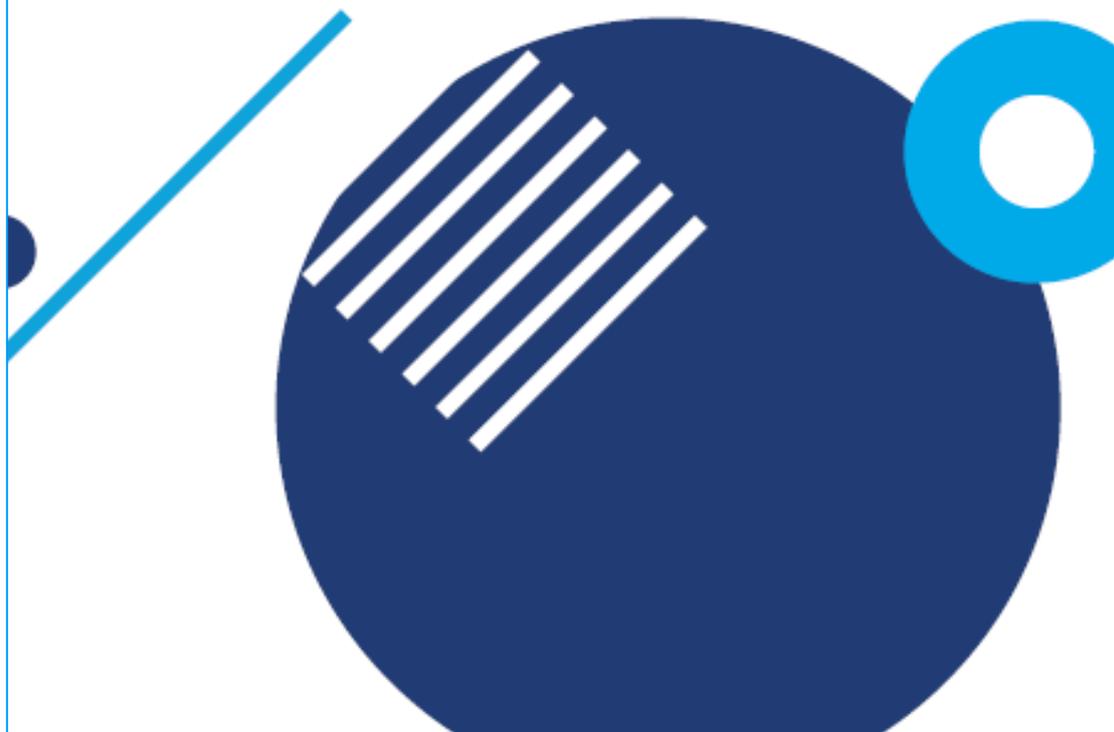
НАЦИОНАЛЬНЫЙ
ЦЕНТР ПОМОЩИ
В БОРЬБЕ С УГРОЗАМИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



лига
безопасного
интернета



Сайт
ligainternet.ru



Материалы для специалистов «Опасные сообщества цифрового мира»

ОПАСНЫЕ СООБЩЕСТВА ЦИФРОВОГО МИРА: КАК ИЗБЕЖАТЬ СЕТЕВОЙ МАНИПУЛЯЦИИ

Деструктивные сообщества в сети – проблема реального мира

В Интернете существует большое количество опасных групп, сообществ, которые распространяют опасные для жизни, здоровья, нравственности человека идеологию, увлечения, движения, в том числе, вовлекают в экстремистскую деятельность и совершение иных преступлений. К таким группам относятся:

Суицидальные сообщества – группы, в которых публикуется контент, связанный с тематикой самоубийств. Сообщества суицидальной направленности часто маскируются, тем не менее, их можно выявить по таким признакам: романтизация смерти и идей самоубийств; героизация людей, совершивших самоубийство и подражание им; практика «селфхарма» (причинения вреда самому себе); распространение деструктивно-суицидальной информации разного вида разнообразными способами. Например, часто пропагандируется такой контент через аниме, идеи анорексии идеологию ЛГБТ сообщества и др. 46% россиян убеждены, что Интернет значительно увеличил число самоубийств (по данным ВЦИОМ).

Аутодеструктивные сообщества – группы, распространяющие идею и практики причинения самому себе физического или психологического вреда. Например, группы «селфхарма». Часто бывают подготовительным этапом для вовлечения детей в суицидальные группы.

Сообщества школьных расстрелов (скулшутинг) – движение, ставшее популярным в США. Эти сообщества романтизируют и продвигают идею массовых убийств и, в особенности, массовых убийств среди детей и подростков в школах. К таким относится, например, движение «Колумбайн», признанное террористическим на основании решения Верховного суда Российской Федерации. По данным исследователей, скулшутинг пропагандируется даже через «кровавое аниме».



Сообщества по криминальной идеологии – продаигают идеалы из криминальной среды среди подростков. Наиболее известным примером является движение АУЕ (признано экстремистским и запрещено на территории Российской Федерации). В таких сообществах романтизируется не только криминальный, но и тюремный образ жизни и быт, а также криминальные герои книг, фильмов и сериалов.

Сообщества по пропаганде наркотиков – данные сообщества пропагандируют не только употребление наркотиков, романтизируя наркопотребление и образ жизни наркоманов, но и вовлекают своих членов в распространение наркотиков. Для этого пользователям массово рассылаются предложения о «подработке», где обещают высокую заработную плату. Бывают случаи и втягивания в эту деятельность детей и подростков. При этом несовершеннолетние, решившие подработать курьером, как правило, устанавливаются правоохранительными органами (в отличие от их работодателей-преступников) и получают реальные сроки лишения свободы.

Экстремистские сообщества – сообщества, занимающиеся публикацией и распространением экстремистского контента, пропагандирующие экстремистские идеи, а также привлекающие своих подписчиков к совершению преступлений на почве политики, расовой, национальной или религиозной ненависти.

Ключевой вопрос

Как помочь ребёнку не попасть в деструктивное сообщество?



Внимание!

На что обратить внимание...

- Наличие в сообществах, которые посещает ребенок, или в ленте новостей его аккаунта, фотографий увечий: порезы, ссадины, кровь, травмы и т.п.
- Наличие фотографий в мрачных тонах, с депрессивным содержанием.
- Наличие в ленте цитат, обесценивающих жизнь или традиционные духовно-нравственные, в том числе, семейные ценности; содержащих пренебрежительные/неуважительные высказывания по отношению к родителям, деторождению, служению Отечеству, исторической памяти народа России, ценности жизни человека, руководству страны и принимаемым решениям.
- Наличие в подписках у подростка или в ленте новостей его аккаунта сообщества, посвященных скулшутингу, а также лицам, которые совершали эти преступления.
- Интерес к «аниме» у ребенка или его друзей.
- Ребенок стал часто проводить время вне дома, скрывать информацию о том, где и с кем проводит время, при этом вы не знаете телефонов его друзей и их родителей, его успеваемость в школе упала.
- У ребенка появились денежные средства или дорогие вещи, происхождение которых вы не знаете или он пользуется вещами, которые ему, якобы, дал временно поносить товарищ.

Последствия вовлечения в деструктивные движения

- Снижение способности самостоятельно думать и принимать решения.
- Отказ от личной ответственности.
- Отрицание авторитетов, в том числе родителей, учителей и знакомых.
- Обесценивание норм морали и общечеловеческих ценностей.
- Выраженная симпатия к антигероям, антидвижениям.
- Выраженное стремление к разрушению и деструктиву.
- Снижение успеваемости в школе.
- Неуважение и травля учителей.
- Нарушение коммуникации и конфликты со сверстниками.
- Формирование школьных банд или радикальных группировок.
- Политизация детей и подростков.
- Рост преступлений среди детей и подростков.
- Рост наркомании среди подростков.
- Попытки самоубийства и причинения себе вреда.

Как вовлекают в опасные сообщества?

Для вербовки и привлечения новых людей в движение вербовщики используют своеобразную «Воронку вовлечения».

Как это работает?

Чаще всего вербовка начинается с личного и очень навязчивого общения. Вербовщики пытаются завладеть всем вниманием и временем пользователя. Один из основных способов вербовки – маркетинговая «воронка вовлечения». Суть «воронки» заключается в том, что пользователь сначала привлекается в какую-либо группу по интересам, затем по активности в этих группах или комментариях, он отбирается и через личные сообщения приглашается в тематическое сообщество с более узкими интересами. После этого происходит отбор пользователя в закрытые группы и чаты, где уже происходит вовлечение в опасную и даже преступную деятельность сообщества. Особенностями таких групп может быть персональный доступ к ним только членам сообщества (особенно если общение происходит через мессенджеры). То есть родители или иное лицо не сможет попасть в группу, используя свой телефон или компьютер. После этого пользователи приступают к выполнению заданий в реальном мире.

Это надо знать!

1. **Постоянные флешмобы могут быть опасны** – это регулярные задачи, например: облейся холодной водой, напиши пост и поставь правильный хештег, опубликуй свои фото в конкретных условиях и т.п. Такие активности «дрессируют» пользователей на бездумные массовые действия.
2. **Массовые тесты, квесты, задания** – псевдотесты на IQ, творческие способности, тип личности и т.п. Они не несут никакой пользы и не могут определить ничего из вышеперечисленного, но подталкивают пользователей к ненужной им активности.
3. **Общественные и явно политические задания** могут выражаться в требовании у ребенка поставить на аватар радужный (ЛГБТ) флаг, опубликовать пост с поддержкой или осуждением какого-либо внутривнутриполитического или мирового инцидента, распространить фейковую новость, сдать деньги на поддержку какой-либо организации.
4. **Максимальный репост** служит формированию среди пользователей привычки делать репосты каких-либо публикаций к себе в ленту. Таким образом публикации, в том числе и фейки, могут распространяться лавинообразно, каждый раз захватывая все больше и больше пользователей, которые занимаются их репостом и распространением.
5. **Метод наводнения** – формирование постоянного и плотного информационного поля вокруг какого-либо вопроса. В результате у пользователей складывается ложная уверенность, что какая-либо позиция поддерживается разными независимыми источниками и обсуждается на разных уровнях, а значит эта позиция важна и правдива.
6. **Метод «от вас скрывают, а я расскажу правду»** – придает максимальную правдоподобность сообщению и создает у пользователей чувство избранности, ведь с ними поделились какой-то правдой, которую от всех остальных скрывают.
7. **Виртуальные рейтинги и награды** – в соцсетях, сетевых сообществах и массовых играх используются награды и рейтинги, призванные подстегнуть интерес пользователей, заставить их участвовать в активности не «просто так», а за какую-либо награду, даже если эта награда – символическая позиция в виртуальном рейтинге.

Личный пример

Обращаем внимание на молодёжный сленг и изучаем его! Для этого бывает достаточно посмотреть значение разных слов в Интернете. Так, например, слова «самовыпил» и «выход» могут означать самоубийство. Пора бить тревогу по всем фронтам!

Цифры:

58% убеждены, что современные дети живут в более опасное время, чем они сами (по данным ВЦИОМ).

46% опрошенных считают, что Интернет значительно увеличивает количество самоубийств (по данным ВЦИОМ).

60% опрошенных взрослых уверены, что социальные сети и их контент оказывают вредное воздействие на детей (по данным ВЦИОМ).



НАЦИОНАЛЬНЫЙ
ЦЕНТР ПОМОЩИ
ПРОБЛЕМ И ПОСЛЕДОВАТЕЛЬНОСТИ
ДЕТЕМ



лига
безопасного
интернета



Сайт
ligainternet.ru

Материалы для специалистов «Клиповое мышление»

КЛИПОВОЕ МЫШЛЕНИЕ: ЦЕНА ДЛЯ ЛИЧНОСТИ

Небезопасные клипы

Клиповое мышление – тип мышления, заключающийся во фрагментарном восприятии информации. Люди с преобладающим клиповым мышлением склонны к восприятию информации отрывочно и порционно, небольшими кусками, при этом значительно страдает глубина понимания материала, а также критический подход к информации.

У современных подростков такой тип мышления преобладает. Его формированию активно способствует формат подачи информации в соцсетях, особенно короткие видео (в TikTok, YouTube).

Особенности клипового мышления:

- Фрагментарность;
- Яркость;
- Кратковременность;
- Нелогичность;
- Отрывочность;
- Разрозненность;
- Поддержание общения одновременно с несколькими собеседниками.



Ключевой вопрос: Как бороться с клиповым мышлением?

Внимание!

Основной причиной развития клипового мышления у детей и подростков является особенность преподнесения информации в Интернете. Информация в сети подается отрывочно, в виде коротких статей или видео. Ярким примером является чтение новостей «по заголовкам». В таком случае человек менее склонен сомневаться в информации и перепроверять ее.

Считается, что клиповое мышление преобладает у тех, кто большую часть свободного времени проводит в Интернете ввиду специфики подачи информации. В среднем, современные подростки в возрасте от 12 до 17 лет тратят на Интернет почти 6 часов в день (по данным Mediascope).

У современной молодежи по данным экспертов зафиксированы проблемы, связанные с чтением. При попытке прочитать и усвоить сложный текст, (например, инструкцию), многие подростки начинают испытывать резь в глазах и головную боль.

Что способствует формированию клипового мышления:

- Музыкальные клипы;
- Реклама на ТВ;
- Электронные СМИ;
- Мобильные средства связи;
- Социальные сети и мессенджеры, такие как TikTok, YouTube.

Развитие клипового мышления приводит к следующим проблемам:

- Внушаемость;
- Плохая обучаемость;
- Гиперактивность;
- Дефицит внимания;
- Предпочтение визуальных символов логике и углублению в текст;
- Неспособность к восприятию однородной информации (в т.ч. книжного текста);
- Снижение уровня грамотности у подростков и студентов;
- Вместо логических связей выстраиваются эмоциональные;
- Ослабляется или нивелируется чувство сопереживания, а также ответственности.

Полезные советы

- Контролируйте экранное время ребенка.
- Воспользуйтесь приложениями для тренировки памяти и внимания.

Личный пример

Организуйте «время без гаджетов» - по вечерам или по выходным дням, когда не только ребенок, но и вся семья сможет максимально отвлечься от телефонов, компьютера и Интернета.



НАЦИОНАЛЬНЫЙ
ЦЕНТР ПОМОЩИ
ПРОТИВ БУЛЛИНГА И СОСТАВЛЯЮЩИХ СЕТИ
НАЦИОНАЛЬНЫЙ



лига
безопасного
интернета



Сайт
ligainternet.ru





лига безопасного интернета

Контактная информация



E-mail

info@ligainternet.ru
press@ligainternet.ru



Телефон

8 800 700 56 76



Telegram

<https://t.me/ligainternet>



ВКонтакте

<https://vk.com/liga>

