Урок безопасного интернета.

Для подростков 13-15 лет

Материалы от РОЦИТ (Региональный общественный центр интернет технологий )

*Пояснение: Практика Молодежной Интернет-Палаты свидетельствует, что подростковая аудитория предпочитает стиль информационно-просветительских материалов, максимально приближенный к ориентированному на совершеннолетнюю аудиторию — ввиду того, что в этот период происходит самоидентификация подростка как «взрослого».*

**Тема 1.**

Российская аудитория интернета стремительно растет – дети, подростки, молодежь составляют ее значительную часть. Сейчас уже практически каждый подросток старше 12 лет присутствует в онлайне. Сегодня детям доступно то, что лет пятнадцать назад было под силу лишь профессионалу или даже государству – создать собственную телестудию, получить картинку или музыку из-за тридевяти земель, поуправлять собственным мультфильмом. Через интернет дети и подростки открывают для себя мир, формируют собственную личность. Интернет дает пользователю огромные возможности как высокотехнологичный источник коммуникации, как инструмент поиска и получения информации. Для того чтобы эффективно использовать этот инструмент, нужны как умения обращаться с ним, так и определенный жизненный опыт, позволяющий не захлебнуться в океане неограниченных возможностей интернета, вовремя разглядеть подводные камни, рифы и водовороты виртуального пространства. С развитием интернета резко возросло число тех, кто использует его возможности в неблаговидных целях. Хорошо знакомые виды преступлений перешли в сеть, появились новые виды преступлений, порожденные интернетом.

Интернет — это куча возможностей, которые доступны не выходя из дома. Или вообще «из кармана» - через смартфон. Молодое поколение чаще всего выходит в интернет с мобильного телефона.

Интернет — это:

- Покупки в онлайн-магазинах и пополнение баланса на электронных счетах;

- Просмотр видео и прослушивание аудио;

- Съемка собственных клипов и публикация их в Сети;

- Самопрезентация и общение в социальных сетях;

- Общение в мессенджерах, чатах и микроблогах;

- Поиск полезной информации — для домашнего задания и не только;

- Онлайн-игры;

- Написание собственных программ;

И многое, многое другое.

**Тема 2.**

В Сети хорошо, когда безопасно. Когда ничто и никто тебе не угрожает, можно спокойно заниматься любимым делом. Это как везде, но в Интернете — особенно.

В Интернете могут угрожать:

- Твоей репутации, то есть тому, насколько хорошо тебя воспринимают друзья и вообще окружающие;

- Твоим деньгам и деньгам твоих родственников;

- Твоему компьютеру или смартфону.

Все как на улице. Поэтому главное правило безопасности в Сети — нужно вести себя КАК НА УЛИЦЕ. То есть — так, чтобы тебе было безопасно.

**Тема 3. Киберунижение**

Киберунижение — главная, самая многогранная и самая массовая контентная угроза в Сети. Сюда входят любые оскорбления, любая травля, и публикация фото и видео со сценами унижения и насилия. Да, «фотожабы» - это тоже про это.

Самая «типовая» форма киберунижения в Интернете — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов. Сюда же можно отнести и распространение фото или видео со сценами унижений и издевательств.

Последствия от киберунижения очень тяжелые. Для жертвы, но и для агрессора тоже. В Интернете никто не бывает анонимным, так что заниматься киберунижением — себе дороже.

«Золотое правило» общения в Сети: «Общайся с другими так, как ты хотел бы, чтобы другие общались с тобой».

**Тема 4. Жертва киберунижения**

Что делать, если ты стал(а) жертвой киберунижения?

- Для начала, можно пожаловаться модератору или администрации сервиса. Для этого в соцсетях и мессенджерах есть специальные кнопки - «Пожаловаться». Пожаловаться можно на пост, на фото или на видеоклип.

- Если кто-то начал вести себя неподобающе на твоей странице в соцсети или в группе (чате), которую ты администрируешь — такого «кого-то» лучше забанить.

- Если ты оказался(ась) в таком месте, где модератор не реагирует на жалобы — из такого пространства лучше просто уйти. В Интернете точно есть куча таких же пабликов, сообществ, групп и чатов, на ту же самую тему — но без унижения. Ничего «трусливого» в таком поведении нет — ведь на улице ты тоже наверняка отойдешь подальше от проблемного персонажа.

- Не скатывайся на ответные оскорбления. 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. И вообще, веди себя вежливо.

- Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии.

- Очень полезно обратиться за помощью к родителям. Если будет нужно, они смогут подключить психолога, который поможет успокоиться и вернуться в обычный ритм жизни.

- Если речь идет о сценах унижения и насилия — обязательно сообщи родителям, они обратятся в полицию. Проблемное видео уберут, а злоумышленникам точно не поздоровится.

И да, любителям киберунижения стоит помнить:

«Мне нет 16, а значит, ничего не будет» - это не работает, накажут по полной. Да так, что будет аукаться и через 10 лет, и через 20 — например, при поиске работы.

«Меня не найдут» - в Интернете абсолютной анонимности не бывает. Ни VPN, ни Tor ее не гарантируют. Найдут. Да и в Интернет-сервисе забанят.

В общем, не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно.

**Тема 5. Поиск популярности в Сети**

Снять «крутой ролик», выложить его в TikTok и набрать кучу лайков? Идея неплохая. Но сначала надо кое-о чем подумать.

- Экстремальные видео, типа руфинга или зацепинга — точно не вариант. Шансы разбиться насмерть ОЧЕНЬ велики — даже если ты думаешь, что «все просчитал». Всегда «что-то может пойти не так», но тут цена этого — твоя жизнь. Которая не игра, тут «сейвов» нет.

- Видео в стиле «пляжная одежда» - тоже не то. Толку от таких лайков не будет, а вот травли обычно бывает много. Да и вообще, могут «не так понять» - и репутация среди знакомых «съедет в ноль».

- Еще хуже — видео с неприличным поведением, издевательствами или насилием. Такой ролик, скорее всего, просто не пройдет модерацию. А какие будут последствия — мы уже знаем.

Лучше всего снимать что-то познавательное, откуда зритель узнает для себя много нового. Вот такие ролики действительно поднимают популярность.

**Тема 6. Приватность в Интернете**

Приватность — это та часть нашей жизни, которая «чисто для нас», «не для всех». Далеко не всем следует делиться в Интернете — даже если кажется, что это прибавит нам популярности.

Личные данные — очень ценный товар для злоумышленников. Почти такой же, как деньги. И они за ними охотятся очень активно.

Что точно не надо публиковать в соцсетях и оставлять на разных сайтах в Сети:

- Слишком много данных о себе. Лучше публиковать минимум информации — фамилия, имя, возраст, город. Сведения о школе, увлечениях, кружках и секциях, а тем более домашний адрес — точно не публичная информация.

- Чекиниться тоже надо с осторожностью. Это может помочь злоумышленникам понять, когда и сколько времени тебя нет дома.

- Точно не надо публиковать фото и видео со всяких тусовок и вечеринок - «не так поймут».

- Бывают сайты, которые предлагают «легкий заработок» или «выплаты» и просят для этого личные данные. Это точно мошенники.

- Лучше не публиковать фото изнутри своего дома, из ближайших окрестностей. Или из школы. Преступники тоже умеют думать головой, и по этим фото могут легко определить, где человек живет. А также оценить уровень достатка — и спланировать кражу.

**Тема 7. Друг и «френд»**

«Френд» - в переводе с английского значит «друг». Но вот друг в реале и френд в виртуале — «две большие разницы».

Очень часто в Интернете «френдят» людей, которых никогда не видели в реале. А вот доступ к личной информации такие «френды» получают такой же, как хорошие знакомые в оффлайновой жизни. То есть… мы допускаем «вглубь своей жизни» совершенно незнакомых людей. И как они распорядятся «информацией не для всех» - можно только гадать…

- То, что мы активно общаемся с кем-то в Сети, не делает этого «кого-то» таким же другом, как тот, кого мы видим каждый день.

- Френдить в Сети лучше тех, кого знаешь в реале. Или для френдов можно создать отдельный аккаунт — в котором публиковать только то, что можно «отдать на общий доступ».

- В соцсетях можно управлять настройками видимости постов. То есть — какой-то конкретный пост могут видеть не все френды. Этой полезной опцией следует пользоваться, если в ком-то из френдов ты не уверен.

- Нужно помнить, что даже человек, знакомый по реалу, может репостнуть закрытый контент — тогда он станет виден другим. Поэтому нужно тщательно продумывать контент, доступный даже близким друзьям.

- Нельзя делиться информацией «только для себя» в Интернете — и вообще, такой контент лучше не переводить в цифровую форму.

- Если френд начинает требовать контент определенного рода, угрожать, вымогать деньги — лучше от него избавиться. Или, что надежнее, посоветоваться с родителями.

**Социальные сети**

Социальная сеть - это сайт, который предоставляет возможность людям осуществлять общение между собой в интернете. Чаще всего в них для каждого человека выделяется своя личная страничка, на которой он указывает о себе различную информацию, начиная от имени, фамилии и заканчивая личными фотографиями. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

1. Как уже говорилось, ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;

2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;

3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;

4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;

5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;

6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;

7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

**Тема 8. Покупки.**

В Интернете можно легко покупать все, что нравится. От подписок на любимые онлайн-сервисы до модной одежды. Можно за деньги «прокачать» своего персонажа в онлайн-игре или продвинуть свой ролик на площадке. Но и тут есть свои особенности…

- Для начала, нужно завести свою собственную банковскую карту. Да, она будет привязана к родителям, и денег там будет немного. Но небольшие покупки с ней делать будет можно. Это безопаснее.

- Точно не надо «подсматривать» данные банковских карт родителей. Мошенники могут таким образом оставить их вообще без денег. Впрочем, если у родителей подключена двухфакторная аутентификация, то подсматривать данные родительской карты бесполезно вообще.

- Покупать лучше в проверенных магазинах. Сильная скидка в малоизвестном магазине — признак возможного мошенника. Это же касается «непонятных» сайтов, предлагающих платный доступ к фильмам и музыке. Особенно внимательным надо быть с Интернет-аукционами — там риск мошенничества выше, чем в обычных онлайн-магазинах.

- Покупки следует тщательно продумывать. Иначе денег может не хватить.

- Криптовалюты — штука до сих пор не очень понятная, и жульничеств с ними пока хватает. Не лучший выбор для «подъема денег».

- И да, надо проверять адрес магазина в адресной строке — особенно если ты перешел туда по внешней ссылке. Бывает, что мошенники подменяют букву в адресе и переводят людей на мошеннический сайт, точно копирующий по дизайну известный магазин.

- Покупка чего-то противоправного в Интернете — худший вариант. Мало того, что это само по себе может быть преступлением, так еще и обычно такие вещи в Сети предлагают… обычные мошенники. И деньги заберут, и покупки не будет.

**Электронные деньги**

Электронные деньги — это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги. Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах. В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов - анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в не анонимных идентификации пользователя является обязательной. Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;

2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;

3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли — это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, StROng!;

4. Не вводи свои личные данные на сайтах, которым не доверяешь

**Тема 9. Фактчекинг.**

В Интернете публикуется куча информации. Но далеко не вся она правдива. Обмануть в Интернете легко. Можно «подправить» себе внешность, можно вообще выдать себя за другого человека. Можно написать что-то, чего в реале вообще не было. Или для шутки, или по недомыслию — а бывает, что и для злонамеренного обмана. Все это очень часто встречается в Сети.

Бывает, что ложную информацию публикуют «для паники». Например, чтобы все кинулись покупать что-то по завышенной цене. Или чтобы люди стали вести себя определенным образом.

Как защитить себя от фальшивой информации?

- Проверять информацию в других источниках. Например, на сайтах СМИ — ведь журналисты несут ответственность за правдивость информации. Если это касается, скажем, сообщения в групповом чате об отмене контрольной — нелишне перепроверить у самого учителя.

- Это же касается фото или видео. Нередко бывает, что публикуются «обрезанные» или «отредактированные» видео, в том числе с использованием искусственного интеллекта (дипфейки). Даже обычный поисковик может помочь найти реальный первоисточник.

- Вообще же, лучше пользоваться проверенными источниками. Как уже говорилось, теми же СМИ. Для разнообразия картины можно пользоваться медиа с разными «редакционными позициями» - так представление о событии получится объективнее.

**Тема 10. «Вирусы» и «зловреды»**

Программно-технические угрозы — самый старый и по-прежнему очень опасный вид угроз. Вредоносные программы способны замедлить работу устройства, вывести его из строя вообще, изменить данные на нем, украсть эти данные. Могут заставить устройство «шпионить» за своим владельцем. Могут красть деньги с подключенных счетов. А могут и заблокировать устройство, вымогая деньги за разблокировку.

Если говорить конкретно о вирусах, то компьютерный вирус - это разновидность вредоносных компьютерных программ, отличительной особенностью которой является способность к саморазмножению (копированию). Благодаря этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет — и могут заражать другие компьютеры с уже зараженных машин.

Самое «слабое звено» здесь — обычно сам пользователь. Как правило, преступники делают все, чтобы сам пользователь «пустил их к себе» - убеждают скачать или запустить некую программу. Делается это при помощи специальных убеждающих текстов (например, рекламы).

Для защиты от таких угроз нужно принимать определенные меры предосторожности:

- Использовать современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;

- Постоянно устанавливать патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;

- Работать на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;

- Скачать и регулярно обновлять защитные программы (их обычно называют «антивирусы», но сейчас они защищают от целого спектра разных угроз).

- Не скачивать и тем более не запускать программы с малоизвестных сайтов и ресурсов. Даже если они маскируются под «загрузчик», нужный для скачивания интересной игры или фильма.

- Не «вестись» на различные рекламные предложения, предлагающие «кликнуть» куда-то или «скачать» что-то. Там может прятаться вредоносное ПО.

- Видеокамеры на устройствах реально лучше заклеивать. И это уже давно не смешно.

- Все это касается и «умных устройств» - если, конечно, вы не хотите, чтобы они превратились в «домашних шпионов».

- И да, гаджеты подвержены зловредам в той же мере, что и компьютеры с ноутбуками. Антивирус должен присутствовать и на смартфоне, и на планшете.

**Тема 11. Мошенники в чатах и в телефоне**

«Вася, я попал, перекинь мне 1000 рублей. Петя». Или «Маш, кинь мне денежку на раскрутку канала. Вика». Получив такое сообщение в чате или мессенджере, надо трижды подумать. Мошенники часто рассылают такие сообщения «наудачу» - авось из ста тысяч людей найдется тысяча Вась, и сто из них переведут деньги. Бывает и так, что у жуликов есть Ваши персональные данные — взятые из Вашей соцсети или украденные из какой-то базы данных. Такие мошенники представляются менеджерами сотовой сети, сотрудниками банков, даже полицейскими. Помимо мессенджеров и чатов, они могут звонить просто по телефону. Цель у них одна — собрать Ваши данные, достаточные для доступа к деньгам.

Самый простой способ избежать проблем — проверить информацию. Перезвонить Вашему другу Пете или подруге Вике по телефону, который давно «зашит» у вас в память телефона. И уточнить, что происходит. Если друг сразу не отвечает — можно перезвонить чуть позже. И точно не пересылать никакие деньги без подтверждения. Потому что иначе они почти стопроцентно попадут не другу, а мошеннику.

**Фишинг или кража личных данных**

Главная цель фишинга - вида Интернет-мошенничества - состоит в получении конфиденциальных данных пользователей — логинов и паролей. На английском языке phishing читается как фишинг (от fishing — рыбная ловля, password — пароль).

Основные советы по борьбе с фишингом:

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 проверенных 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;

7. Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы

**Тема 12. Завершение.**

В Сети удобно и полезно, когда безопасно. Как на улице.

Идя по улице, мы принимаем меры предосторожности. Не рассказываем каждому встречному о себе, не размахиваем банковской картой… В Интернете нужно делать то же самое. Знание правил безопасности помогает взять от возможностей Сети максимум — без риска и без проблем.