УРОК «КИБЕРБЕЗОПАСНОСТЬ»

Составители: специалисты подразделения Кибербезопасности МВД РФ

Этапы урока

В общем зале:

1. Открытие урока в общем зале (собраны ученики всех классов, для которых будет проводиться урок): вступительное слово руководства учебного заведения и представителя подразделения МВД

В классах:

1. Вступительное слово ведущего
2. Краткая лекция о нескольких степенях интернет угроз. В старшие классы от 7 и выше рекомендуется направлять также сотрудника правового подразделения
3. Проверка усвоения материала. Выполнение теста на «киберграмотность». Разбор правильных ответов.
4. Тест «Какой я?»
5. Раздача памяток «Безопасный интернет – детям»
6. Ответы на вопросы ребят. Подведение итогов

Сценарий урока

В общем зале:

1. Открытие урока. Вступительное слово представителя подразделения МВД России, «Основные правила безопасности в сети Интернет»

Интернет – уникальная реальность нашего с вами времени. Это безграничный мир информации, где есть не только развлекательные и игровые порталы, но и много полезной информации для учебы. Здесь можно общаться со своими друзьями в режиме онлайн, можно найти новых друзей, вступать в сообщества по интересам. Информация, оперативно обеспечивающая ваши ежедневные потребности, - все это Интернет.

Почему же полицейские вынуждены предупреждать об опасностях виртуального мира, если в нем так много всего хорошего и полезного?

(Дети дают свои ответы)

Все, что вы сказали совершенно правильно. Достаточно большая часть интернет-пользователей ищет не друзей в Интернете, а свои жертвы.

Дело в том, что недобросовестные граждане - мошенники, наркодилеры, иные злоумышленники, асоциальные и психически нездоровые люди по-своему оценили возможности Интернета. Ведь именно Всемирная паутина дает возможность преступникам действовать анонимно.

Поэтому небезопасное поведение в сети Интернет может нанести вред и вам, и вашим родным и близким людям. Обезопасить себя не так уж и трудно – достаточно серьезно отнестись к проблеме кибербезопасности и соблюдать простые правила, о которых мы сегодня расскажем.

Мы поговорим о трех основных направлениях по обеспечению кибербезопасности:

- защита ваших компьютеров и гаджетов от вирусов и вредоносных программ;
- виртуальное или кибермошенничество;
- нарушение морали и этики в онлайн-общении, троллинг, разрушающий ваше личное пространство.

Мы расскажем, как важно уделять внимание парольной политике, кто может интересоваться вашей страницей В Контакте, и почему не стоит кормить троллей, и чем они в принципе «питаются».

Соведущий, представитель подразделения МВД России:

Начнем мы с трех самых общих правил, которые в наш информационный век должны стать вашими спутниками на всю жизнь:

ПАРОЛИ (ключ от дома)

Используйте всегда индивидуальные и сложные пароли, состоящие из букв, цифр и специальных символов. Исключите использование паролей по умолчанию, не сохраняйте пароли в ваших гаджетах и браузерах. Почему мы говорим об этом в первую очередь? Статистика говорит о том, что люди мало уделяют внимания парольной политике.

Третий год подряд самым популярным паролем в мире является «123456». Подобрать такой пароль к вашим порталам и персональным данным злоумышленнику не доставит труда.

Регулярно осуществляйте смену паролей, обеспечивая каждый раз их конфиденциальность. Это ваш самый большой секрет, как ключ от замка входной двери в ваш дом.

Правило первое: «Ключ от дома должен быть секретным, надежным, и только вашим, личным».

ВИРУСЫ и АНТИВИРУСЫ («моем руки с мылом»)

Любому компьютеру или гаджету могут навредить вредоносные программы (или вирусы). Они могут скопировать, повредить или уничтожить важную информацию, отследить ваши действия и даже украсть средства со счета. Программы «Черви», «Трояны», «Шпионы» - их множество разновидностей и красивых названий, а суть одна – все это вредные вирусы!

Для защиты компьютера на нем устанавливаются специальные защитные программы и фильтры. Использовать можно только лицензионное программное обеспечение с актуальными обновлениями.

Устанавливать надо все обновления, как только они становятся доступными. Нельзя допускать истечения срока действия вашего антивируса.

Не качайте программные продукты из сомнительных источников (файлообменных сетей и торрентов). Не открывайте и не сохраняйте подозрительные файлы – сразу удаляйте. Не отвечайте на непонятные вам рассылки.

И главное - не посещайте ресурсы с сомнительной репутацией, которые вызывают у вас (или у вашей антивирусной программы) подозрения любого толка. Сомневаетесь – не нажимайте «да» или «ENTER».

Здесь можно провести простую параллель – держимся подальше от вирусов, моем руки регулярно, хорошим и качественным мылом. При любой сомнительной ситуации: «Моем руки с мылом, к вирусам не прикасаемся».

ПЕРСОНАЛИЗАЦИЯ (документы в сейфе)

Никому не передавайте свои конфиденциальные данные (логин, пароль), свидетельство о рождении, паспортные данные, адрес и прописку, и даже ваши фотографии. Такие «цифровые следы», если их создать, могут тянуться за вами всю жизнь. Могут навредить вам на пути к достижению поставленной цели. Игнорируйте в сети Интернет подобные запросы.

Получается странно – дома и на работе мы храним свои документы в сейфе, закрываем на ключ. Мы понимаем их важность. А потом по непроверенному запросу открываем сейф, достаем документы, фотографируем и посылаем посредством ресурсов в сети Интернет. Количество лиц, которые могут получить доступ к таким посланиям, даже трудно прогнозировать.

Давайте запомним третье правило: «Наши документы всегда в сейфе».

Давайте повторим правила:

- Ключ от дома (это наши пароли)
- Моем руки с мылом (качественно защищаемся от вирусов)
- Документы в сейфе (не раскрываем персональные данные в Сети)

Далее учащиеся расходятся по классам

В классах:

1. Вступительное слово ведущего

«В этом году, ровно через 2 недели, российская полиция будет отмечать свое 300-летие. Все три столетия полицейские охраняют граждан, общественный

порядок, обеспечивая безопасность граждан и стабильность в стране. Полицейские раскрывают преступления и разыскивают тех, кто их совершает.

А есть сотрудники, задача которых не менее важна – профилактика преступности и информирование граждан о деятельности полиции. Это сотрудники Управления общественных связей МВД России, которые пришли сегодня к вам и подготовили этот урок.

Тема у нас с вами сегодня очень интересная – обеспечение безопасности в Интернете. При чем тут полиция, можете вы спросить?

Надо понимать, что полицейская служба, правоохранительная деятельность не стоит на месте, развиваясь вместе с прогрессом всего человечества. Например, только сто лет назад появилась экспертная служба, без которой сегодня трудно себе представить работу полицейского. Информационные центры, которые хранят все сведения и являются сегодня фундаментом для работы полиции, создавались в последние десятилетия. Работа МВД России стала высокотехнологичной, и наши полицейские теперь расследуют как преступления, совершенные физически, в реальном пространстве, так и в сети Интернет.

Как только появилась киберпреступность, в МВД России были созданы специальные подразделения по противодействию незаконным деяниям, совершенным как в сети Интернет, так и с использованием интернет-технологий, либо мобильных сервисов связи. Управление «К» - или киберполицейские, как их иногда называют коллеги.

Может и кто-то из вас вырастет и станет «киберполицейским». По этой специальности начато обучение специалистов в Московском университете МВД России им.Кикотя. Выпускники факультета информационной безопасности – уникальные профессионалы, будущее нашей полиции, которые понимают все в новых видах преступлений, мошенничеств во Всемирной сети. Мы готовы дать отпор киберпреступности.

А сегодня об опасностях для граждан и преступлениях в сети Интернет нам расскажет главный администратор интернет-сайта территориального органа МВД России.

2. Краткая лекция о нескольких степенях интернет угроз. Выступление специалиста подразделения МВД России: «ТРОЛЛИ – ХАКЕРЫ – ЗЛОДЕИ»

ЧАСТЬ 1 – ТРОЛЛИНГ и БУЛЛИНГ

Давайте поговорим о тех, кто чаще всего доставляет вам огорчение при общении в Интернете. Это разнообразные хулиганы, главная цель которых – уколоть вас, испугать, огорчить или заставить грубить в ответ.

Прежде всего, мы расскажем о категории интернет-вредителей – это граждане, имеющие преступные намерения в отношении вас лично, или просто злые, невоспитанные люди, выходящие сначала за грань воспитанности, а затем и за грань закона.

Самый распространенный вид хулиганства в Сети – это троллинг.

Троллинг — форма провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в

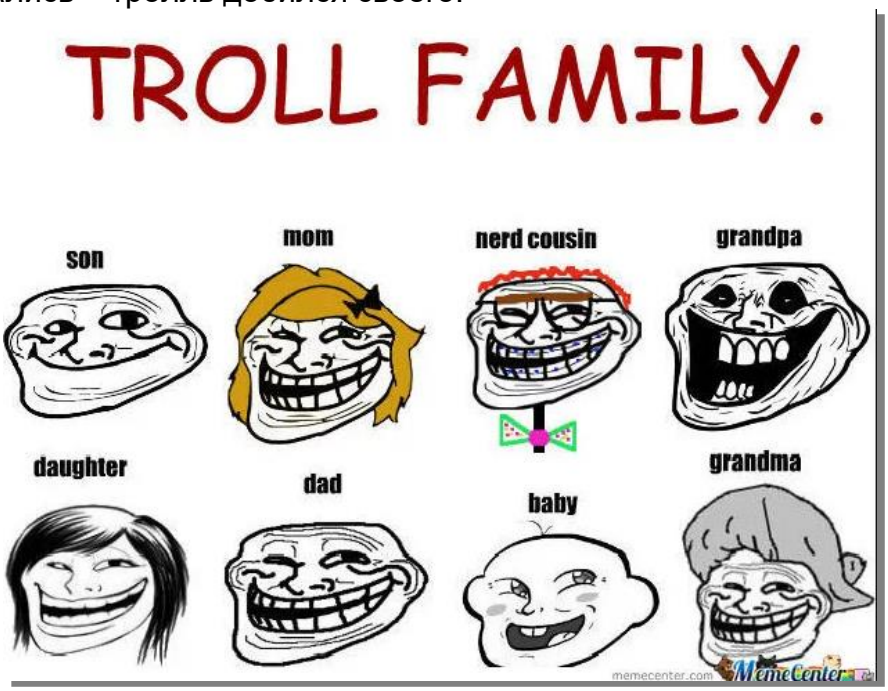
большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации.

Прямую аналогию из обычной жизни для явления троллинга подобрать нелегко. Ближайшие понятия — это искушение, провокация и подстрекательство — то есть сознательный обман, клевета, возбуждение ссор и раздоров, призыв к неблаговидным действиям

Термин «троллинг» происходит из сленга участников виртуальных сообществ. В дословном переводе англ. trolling означает «ловлю рыбы на блесну». В качестве цели таких действий могут выступать волны правок (постмодерация сообщений, тем, новостей) — флейм (от англ. flame — «пламя, огонь»), либо бесцельная конфронтация — «холивары» (от англ. holy war — «священная война»). В отношении пользователя, осуществляющего троллинг, утвердилось обозначение «тролль».

Это слово приобрело популярность из-за другого его значения — «троллей» как существ, упоминаемых в скандинавской мифологии. Мифологические существа тролли, особенно в детских рассказах, изображаются в качестве уродливых, неприятных существ, созданных для причинения вреда и сотворения зла.

Посмотрите (показывается «портрет» тролля из мультика или компьютерной игры). Это тролль. Он живет под землей или в пещере, и питается героями сказок, мультиков или игр. Но это сказочный тролль. Реальный тролль в Интернете питается вашими негативными эмоциями. Он задает вам каверзные вопросы и потом издевается над вашими ответами, он цепляется к вашей аватарке и высмеивает вашу внешность, он дразнит вас за рост, возраст, пишет обидные вещи про ваших родных или друзей… Как только вы обиделись, огорчились или испугались – тролль добился своего.



Давайте запомним простое правило: НЕ НАДО КОРМИТЬ ТРОЛЛЕЙ. Если вы заметили, что кто-то в Сети ведет себя как тролль – вы можете легко победить его. И ваша победа будет заключаться в том, что вы перестанете его кормить – не спорьте с ним, не пытайтесь оправдаться или что-то объяснить. Не кормите тролля! Единственное, что ему нужно – это ваша реакция. Как только вы перестанете реагировать – он очень быстро потеряет к вам интерес.

Гораздо опаснее ситуация, когда вас начинают обижать люди, которые знают вас лично. В случае, когда вы видите, что против вас начинается коллективная

травля – ни в коем случае не расстраивайтесь и не замыкайтесь. В Сети людям свойственен стадный инстинкт, и многие из тех, кто включается в травлю, лично против вас ничего не имеют. Они просто поддались стадному чувству, и это говорит о них очень красноречиво – значит, у них нет своего мнения, и они являются послушными куклами в чужих руках.

Тебя начинают атаковать – просить фотографии или персональные данные, тебе начинают угрожать с разной аргументацией, против тебя организуется коллективное преследование. Оскорбления, угрозы, искажение ваших изображений – все это не безобидные шутки. Это – буллинг или для сети Интернет – кибербуллинг.

Если вы столкнулись с кибербуллингом – немедленно сообщите об этом своим близким или учителям! Если для травли используют ваши прошлые ошибки или неправильное поведение – гораздо проще сразу признаться в этом перед старшими, чем загонять проблему внутрь.

Кибербуллинг (англ. bullying) — агрессивное преследование в сети Интернет одного из членов коллектива (особенно это актуально сейчас для коллектива школьников) со стороны остальных членов коллектива или его части. При травле жертва оказывается не в состоянии защитить себя от нападок, таким образом, травля отличается от конфликта, где силы сторон примерно равны. Кибербуллинг - травля в психологической форме. Проявляется во всех возрастных и социальных группах. Буллинг приводит к тому, что жертва теряет уверенность в себе. Также это явление может приводить к разной тяжести психическим отклонениям, а также психосоматическим заболеваниям, и может явиться причиной самоубийства.

В этом случае очень важно объяснить человеку, что его травят злоумышленники, травят без основательно и нет причин для расстройства, снижения самооценки. Надо показать, как действовать в сложившейся ситуации.

Обязательно сообщите взрослым о преследовании вас в сети Интернет и примите вместе решение об обращении в полицию. Не переживайте в тайне от родителей такие ситуации.

И никогда не принимайте сами участие в таких интернет-кампаниях против кого-либо.

На этом уровне интернет-угроз – ваше достойное поведение является главной защитой и гарантом вашего спокойствия, и ваших близких.

Часть 2 – ХАКЕРЫ НЕ ДРЕМЛЮТ

Ребята, Интернет сейчас стал местом, где многие проводят большую часть своей жизни. Помимо общения, Интернет дает очень много возможностей: например, через Интернет можно совершать покупки, платежи за разные услуги, даже с государством сейчас стало удобнее и быстрее общаться не лично, а в Сети.

На следующем, более технологичном уровне в сети Интернет возникает угроза несанкционированного доступа к вашим интернет-ресурсам, компьютерам, гаджетам, банковским и иным картам, даже к вашим аккаунтам в онлайн-играх. Все это работа хакеров разного толка, цель которых – материальная нажива. Незаконная деятельность по отъему виртуальным способом денег и иных ценностей у граждан.

Здесь вы можете столкнуться с мошенничеством, прежде всего, а также с блокировкой компьютера с дальнейшим вымоганием денег (за разблокировку), с прямым хищением средств и ценностей с ваших счетов и аккаунтов.

И в последнее время появилось много мошенников, которые выманивают у людей деньги, пользуясь их неграмотностью или невнимательностью при работе в Интернете.

Самый распространенный вид интернет-мошенничества – ФИШИНГ. Это работает так. Вам на почту приходит с виду совершенно безобидное письмо, например, из телефонной компании, о том, что необходимо заполнить какие-то формы у них на сайте. Вы проходите по ссылке в письме – и попадаете на сайт, внешне неотличимый от настоящего, один в один! Вы заполняете форму, оставляете свои личные данные, номер телефона, реквизиты своей кредитной карты – и с нее разом списываются почти все деньги! Оказывается, что сайт поддельный, и к настоящему сайту никакого отношения не имеет. Найти таких мошенников бывает очень сложно – ведь таких сайтов они создают десятки тысяч, и существуют они один-два дня, после чего исчезают вместе с вашими деньгами.

Сейчас активно растет игровая индустрия. Поднимите руки, кто из вас активно играет в онлайн игры? А кто из вас имеет платный аккаунт? Кому из вас родители дарят премиальный доступ к играм? Так вот, имейте в виду, что игровое мошенничество – тоже очень развитой бизнес. Даже виртуальные, неощутимые наощупь вещи – такие, например, как купленный танк или игровое оружие с сказочной стратегии – представляют собой ценность, которую можно украсть и потом перепродать, как обычный велосипед.

Запомните очень четко – родители должны быть в курсе всех ваших действий в Сети, связанных с онлайн-платежами. Только взрослые могут быстро отменить ошибочный или неправильный платеж и обратиться в полицию в случае мошенничества.

Никогда, ни при каких обстоятельствах не сообщайте никому реквизиты пластиковых карт, ваших или родительских. Особенно защищенными должны быть PIN-коды (они нужны для использования в банкоматах) и CVV-коды, написанные на обороте карты

(они используются при интернет-платежах и потому не должны быть известны никому).

Фишинг

Фишинг - кража любых персональных данных, владение которыми позволяет преступникам получать выгоду. Это серии и номера паспортов, реквизиты банковских карт и счетов, пароли для входа в электронную почту, платежную систему и аккаунты в социальных сетях. Персональную информацию мошенники используют для получения доступа к аккаунтам, к которым привязаны банковские карты, что позволяет похищать с их счетов денежные средства.

Для кражи персональных данных фишеры массово рассылают электронные письма от имени государственных органов или известных компаний, например, крупных банков или онлайн-магазинов. Их цель - заставить получателей перейти по указанной в письме ссылке на поддельный сайт компании, интерфейс которого внешне не отличим от настоящего сайта, и ввести свои личные данные. Для привлечения внимания к письму в теме указывается на перспективу большой выгоды или на проблему, требующую срочного разрешения.

Подставные страницы действуют недолго - как правило, не более одной недели, ввиду частого обновления базы антифишинговых программ и фильтров. Однако мошенники, следуя отлаженной схеме, создают всё новые и новые сайты-фальшивки для сбора персональных данных.

Так, спамеры активно рассылали по всему миру фальшивые уведомления о выигрыше в лотереях, приуроченных к Чемпионату Европы по футболу, Олимпиаде в Бразилии и Чемпионатам мира по футболу в 2018 и 2022 годах. Для получения денег получателю письма предлагалось ввести на сайте несуществующей лотереи персональную информацию.

Жители России получали письма, замаскированные под уведомления от Федеральной налоговой службы и Пенсионного фонда РФ, примерно следующего содержания: «Уважаемый налогоплательщик! У вас выявлена задолженность. Срок погашения долга до 23.12.2016 г. Подробнее Вы можете ознакомиться, перейдя по

ссылке… » или «Осуществлен перерасчет пенсионных накоплений. Обязательно ознакомьтесь по ссылке…». После перехода на поддельный сайт государственного органа для получения более подробной информации пользователю предлагалось ввести свои персональные данные.

Обратите внимание, что личную информацию можно вводить только при безопасном соединении. Всегда смотрите в адресную строку - URL веб-сайта должен начинаться с «https://», а в интерфейсе браузера должна появиться иконка замка.

Не используйте общественные беспроводные сети и устройства для работы с личной информацией. Не посылайте по почте и через интернет-мессенджеры копии своих документов. Даже родственникам и друзьям.

Мошенники, используя электронные адреса, схожие с адресами легальных организаций, рассылают от их имени сообщения, содержащие ссылку на скачивание открытки, музыки, картинки, архива или программы. Запуск вложения или переход по ссылке может инициализировать установку на устройство вредоносносной программы (вымогателя-блокиратора, шифровальщика, троянской программы) или же оформление подписки на платную услугу. Выполняйте регулярно резервное копирование важной для вас информации, чтобы перезагрузка вашего компьютера, или вынужденная смена программного базиса вашего компьютера (хакерские атаки – это не редкость, и не фантастика), не стала для вас слишком чувствительной.

Скимминг

Считывание данных карты при помощи устанавливаемого на банкомат специального устройства (скиммера). С помощью него злоумышленники копируют информацию с магнитной полосы карты (имя держателя, номер и срок действия карты). Для считывания пинкода преступники устанавливают на банкомат миниатюрную камеру или накладку на клавиатуру.

Завладев информацией о карте, мошенник изготавливает ее дубликат и распоряжается денежными средствами держателя оригинальной карты.

«Покупки» в Интернете

Мошенники привлекают потенциальных жертв низкими ценами на товары известных брендов. Покупателей просят внести предоплату, как правило, перевести денежные средства на электронный кошелек. В течение нескольких дней магазин обещает скорую доставку товара, после чего бесследно исчезает.

Схожий способ мошенничества используется при продаже товаров или услуг на электронных досках объявлений, интернет-аукционах, форумах, сервисах бронирования недвижимости. Как и в случае с интернет-магазинами, мошенники привлекают своих жертв низкими ценами и требуют перечисления предоплаты на электронный кошелек или банковскую карту.

Звонки и «выигрыши»

«Ваш выигрыш». С помощью массовой рассылки электронных писем и смс-сообщений мошенники оповещают потенциальных жертв о выигрыше ценных призов. Для их получения злоумышленники просят перевести на электронные счета некоторую сумму денег, объясняя это необходимостью уплаты налогов, таможенных пошлин или транспортных расходов.

«Благотворительность». Мошенники размещают в социальных сетях или на форумах подложные объявления о сборе средств тяжелобольным детям или бездомным животным или делают репосты реальных объявлений, но с подложными банковскими реквизитами.

«Звонок из банка». Представляясь сотрудниками банка, преступники обзванивают клиентов и под различными предлогами выясняют у них номера карт,

одноразовые пароли и коды доступа, необходимые для проведения операций по банковским картам. Также с номера-двойника банка мошенники массово рассылают клиентам банка смс-сообщения о блокировке карты. Для разблокировки им предлагают перевести деньги на счет или отправить смс-сообщение на короткий номер. Этот способ мошенничества является наиболее новым. Злоумышленники оформляют облачную АТС на одноразовую сим-карту, а затем через веб-интерфейс меняют телефонный номер своей станции на телефонный номер банка.

Защита банковской карты

- никому не сообщать пин-, CVC- или CVV- коды банковской карты и одноразовые пароли (В противном случае мошенники могут получить реквизиты карты, либо сделать копию при помощи специальных устройств и использовать их в дальнейшем для изготовления подделки);

- в случае потери банковской карты немедленно позвонить в банк для блокировки - это поможет сохранить денежные средства;

- при вводе пин-кода прикрывать клавиатуру;

- в случае некорректной работы банкомата - если он долгое время находится в режиме ожидания или самопроизвольно перезагружается - рекомендуется отказаться от его использования. Велика вероятность того, что он перепрограммирован злоумышленниками.

ЧАСТЬ 3 – ЗЛОДЕЙ протягивает к вам руки в ВИРТУАЛЬНОМ МИРЕ

А теперь мы поговорим о третьем, самом опасном уровне интернет-угроз, где целью являетесь уже именно вы, а не ваш кошелек. Именно вас хочет виртуальный злодей вовлечь в преступную, противозаконную деятельность.

Рекламируя замечательный заработок по распространению наркотиков, обещая деньги за прибытие на митинги и марши, запрашивая у вас интимные фото за большие деньги – все эти экстремисты, наркодилеры, извращенцы – нарушают закон. Все это реальные уголовно наказуемые деяния, и интернет здесь – лишь виртуальная ниточка к вам, протягиваемая настоящими преступниками.

Так за последнее время резко возросло количество преступлений с использованием социальных сетей в Интернете. Большая часть детей, ставших объектом такого преступного насилия, не достигли 16-летнего возраста. Тут стоит обратить Ваше внимание на то, что в Российской Федерации установлен общий 16-летний возраст уголовной ответственности (ч. 1 ст. 20 УК РФ), а за отдельные преступления с 14-летнего возраста (ч. 2 ст. 20 УК РФ) (смотри справку).

Широкое распространение мобильных, средств связи, доступность использования сети Интернет, отсутствие в виртуальном мире «территориальных» границ, неограниченная возможность анонимного общения и быстрого обмена фото и видео позволяют лицам, имеющим преступные намерения, совершать противоправные действия в отношении Вас как несовершеннолетних. В силу возраста, любопытства и чувства безопасности в домашних условиях легко вступить в разговоры на запретные темы, в том числе развращающего характера.

У Вас могут обманным путем узнать номер вашей кредитной карточки, и это вызовет финансовые потери, также могут склонить к совершению поступков,

нарушающих права других людей, что в конечном счете приведет к возникновению у вашей семьи проблем, связанных с нарушением законов.

Также могут уговорить сообщить конфиденциальную информацию. Сведения личного характера, такие как Ваше имя и фамилия, адрес, возраст, пол и информация о семье, могут легко стать известными злоумышленнику. Даже если сведения о Вас запрашивает заслуживающая доверия организация, все равно нужно заботиться об обеспечении конфиденциальности этой информации. И обязательно сообщить родителям о подобных случаях.

Иногда из-за Вашей невнимательности можно открыть непонятное вложение электронной почты или загрузить с веб-узла небезопасный код и в компьютер может попасть вирус, «червь», «троян», «зомби» или другой код, разработанный со злым умыслом.

Одной из важнейших угроз является вовлечение через различные социальные сети в распространение наркотиков. Подростки и даже их родители не до конца осознают всей полноты ответственности, которая последует. Более того, на самом первом этапе некоторые закладчики воспринимают происходящее как некий увлекательный «квест».

Как правило, сами они наркотики не употребляют, многие - из вполне благополучных семей. А вот срок, который грозит им по статье за сбыт и распространение наркотиков 8-15 лет (ч. 1 ст. 20 УК РФ).

Вот один из примеров: В Екатеринбурге полицейские задержали 16-летнюю Софью. Гуляя с трехлетним братом по городу, она раскладывала синтетические наркотики, носила их с собой в пакете из «Макдоналдса». В квартире у нее нашли еще 6,2 килограмма «синтетики». Софья говорит, что не хотела зависеть от родителей и решила подзаработать. По ее словам, поначалу не понимала, что распространяет наркотики. А когда осознала и решила отказаться, наркодилеры стали ей угрожать: мол, у них есть ее паспортные данные и не дай бог что-то случится с ее родственниками... Как оказалось до этого Софья не привлекалась, хорошо училась, закончила восемь лет музыкальной школы на скрипке. Теперь ей грозит 10 лет тюрьмы.

Ведущий урока: «Подводя итог всему сказанному, мы попросим вас - будьте бдительны точно так же, как и в реальной жизни.

Незнакомец – каждый, кого вы не знаете лично. Не доверяйте интернет-знакомствам! И не ждите, что преступник сразу покажет свое лицо, и с аватарки на вас будет смотреть Бармалей. Скорее, напротив.

Подсказкой вам должно стать содержание первой же просьбы или предложения.

Что-то вас насторожило? Прекратите общение, никаких дискуссий, снимите скриншот, заблокируйте этого собеседника и сообщите обязательно родителям об этом факте.

3. Проверка усвоения материала

А теперь давайте вместе проверим, как вы усвоили информацию и проведем тест по вопросам кибербезопасности.

Тесты вам знакомы? Наверняка это ваш любимый вид работы на уроке.

Мы раздаем вам тесты и попросим дать быстро собственные ответы, не заглядывая в ответы соседа».

ТЕСТ Проверь свою киберграмотность

1. КАКОЙ ПАРОЛЬ НЕОБХОДИМО ПОСТАВИТЬ К УЧЕТНЫМ ЗАПИСЯМ В ИНТЕРНЕТЕ?
    - такой, чтобы было легко его запомнить
    - **максимально длинный пароль, с содержанием цифр, спецзнаков и заглавных букв**
    - пароль, уже используемый в других учетных записях

2. КАК ЧАСТО НУЖНО МЕНЯТЬ ПАРОЛИ?
    - никогда не менять.
    - менять в том случае, если аккаунт был взломан
    - менять не реже, чем 1 раз в 2 месяца

3. КОМУ МОЖНО ПРЕДОСТАВЛЯТЬ ПЕРСОНАЛЬНЫЕ ДАННЫЕ (ФИО, дата рождения, данные документов (в том числе паспорт и банковская карта), адрес, место работы родителей и прочее) В ИНТЕРНЕТЕ?
    - никому
    - официальным представителям государственных органов
    - людям, которых Вы знаете лично

4. КОГО СЛЕДУЕТ ДОБАВЛЯТЬ В ДРУЗЬЯ В СОЦИАЛЬНЫХ СЕТЯХ?
    - людей, которых Вы знаете лично и хотите с ними общаться
    - только родственников.
    - людей, которые просятся к Вам в друзья.

5. КОМУ МОЖНО РАССКАЗЫВАТЬ В ИНТЕРНЕТ-ЧАТАХ О СВОИХ ДУШЕВНЫХ ПЕРЕЖИВАНИЯХ?
    - людям, которые готовы обсудить их с Вами и поддержать Вас
    - людям, которых Вы знаете
    - только родителям

6. ПОЧЕМУ ЧЕЛОВЕК НЕ ПУБЛИКУЕТ СВОИ ФОТОГРАФИИ В АККАУНТЕ И НЕ НАЗЫВАЕТ НАСТОЯЩЕЕ ИМЯ И ФАМИЛИЮ?
    - он стесняется или что-либо скрывает
    - у него имеются преступные намерения относительно жизни и имущества других людей
    - любой из перечисленных **вариантов, поэтому не стоит ему доверять**

7. ЧТО ДЕЛАТЬ, ЕСЛИ ВАМ ПОСТУПАЮТ НАВЯЗЧИВЫЕ ПРЕДЛОЖЕНИЯ ИЛИ УГРОЗЫ В ЛИЧНЫХ СООБЩЕНИЯХ?
    - ответить, что Вы не боитесь угроз, и вступить в переписку
    - не отвечать ничего, только читать
    - отказаться от общения и обязательно сообщить об этом родителям

Разбор вопросов.

Всем, кто не переступил за «черту безопасности», можно вручить наклейки-смайлики

4. Тест «Какой я?»

Что самое опасное именно для вас в Интернете, зависит во многом от вашего характера. Хотите узнать свои сильные и слабые стороны? (Отвечают)

Давайте узнаем, какие мы, чтобы быть всегда начеку, общаясь в сети Интернет.

Я буду диктовать вопросы, а вы ставите записывайте номер вопроса и ставьте цифру: «1» - это если да, если утверждение именно про вас. Цифра «2», если иногда вы именно так поступаете, так чувствуете. Цифоа «3», если сказанное вовсе не про вас, если это твердое «нет».

ТЕСТ Какой я?

За каждое «да» — 1 балл, «иногда» — 2, «нет» — 3.	
1. Я радуюсь, если мне дают поручение выступить с докладом на уроке.	1 2 3
2. Я не боюсь врачей и сразу иду с родителями к доктору, если что-то беспокоит.	1 2 3
3. Всегда интересно поехать в новый коллектив, где раньше никогда не был.	1 2 3
4. Я спокоен и не нервничаю, если мне предстоит серьёзный разговор с важным для меня человеком.	1 2 3
5. Я люблю делиться своими переживаниями и мечтами с попутчиками в транспорте, в поезде или самолете.	1 2 3
6. Я не раздражаюсь, если незнакомый человек обращается ко мне с просьбой.	1 2 3
7. Я уверен, что людям разных поколений вовсе не трудно понимать друг друга.	1 2 3
8. Я обязательно возмущусь и скажу об этом вслух, если мне дали не вкусное и некачественное блюдо.	1 2 3
9. Если я вступлю в беседу с незнакомым человеком в Сети, то очень огорчусь, если он мне не ответит.	1 2 3
10. Длинная очередь или большое скопление людей меня не пугает.	1 2 3
11. Я готов стать активным участником группы/чата в соцсети, где рассматриваются конфликтные ситуации.	1 2 3
12. Я не принимаю никаких чужих суждений о музыке, книгах, имея свое мнение.	1 2 3
13. Прочитав в соцсети явно ошибочное высказывание, я вступлю в спор.	1 2 3
14. Я люблю помогать одноклассникам разбираться в том или ином учебном вопросе.	1 2 3

15. Мне удобнее излагать свою точку зрения устно, а не в письменной работе.	1 2 3

Теперь сложите все цифры и получите итоговый балл. Мы не будем подводить итоги этого теста здесь, мы предлагаем вам самостоятельно прочитать характеристику вашего результата и взять на вооружение советы и рекомендации специалистов.

Ключ к тесту

Суммируй баллы. Определи по классификатору к какой категории интернет-пользователей относишься ты.

15 - 19 баллов: Ты весьма общителен, порой, быть может, даже сверх меры, что создает очень высокий уровень угрозы контакта в сети Интернет со злоумышленниками.

Любопытен, разговорчив, эмоционален и любишь высказываться по разным вопросам, что дает возможность злоумышленнику легко включить тебя в интернет-дискуссию или прямой диалог.

Легко увлекаешься и охотно заводишь в Сети новые знакомства, не анализируя направленность интересов собеседника. Именно таков основной контингент групп в Сети, организуемых администраторами с нелегитимными целями.

Тебе недостает внимательности, терпения и силы воли при столкновении с незнакомым и сомнительным сегментом в Сети. Хотя, если сильно захочешь, ты сможешь себя заставить не включаться в неоднозначные дискуссии и онлайн-чаты с незнакомцами.

20 - 25 баллов: Твоя коммуникабельность в норме.

Ты любознателен, охотно слушаешь интересного собеседника, ты желанный онлайн-собеседник по многим вопросам. Без волнения идешь на онлайн-контакт с новыми людьми, но анализируешь все сказанное собеседником.

Ты терпелив и тактично отстаиваешь свою точку зрения.

Однако если к тебе найти «подход», то злоумышленники в твоем лице могут обрести вполне активного участника нелегитимных групп в соцсетях.

Помни, что твоя сильная сторона в том, что ты не любишь экстравагантных и сомнительных персонажей в Сети, а многословие, обращенное к тебе, вызывает у тебя подозрение.

26-31 балла: Ты в известной степени общителен и в незнакомой обстановке чувствуешь себя вполне уверенно. Но с новыми людьми ты сходишься с оглядкой, в спорах участвуешь неохотно.

Завлечь именно тебя в онлайн-группы и подчинить своим целям злоумышленникам будет крайне затруднительно.

В твоих высказываниях порой неоправданно много сарказма. Но этот недостаток исправим, помни об этом.

Будь более доброжелателен с твоими настоящими, а не виртуальными друзьями.

32-38 баллов:

Ты замкнут и предпочитаешь одиночество, и поэтому у тебя не много друзей. В Сети именно таких «одиночек» пытаются привлекать создатели запрещенных и незаконных сообществ. Увы, но участие в таких онлайн-группах может тебя привлечь благодаря иллюзии обретения «настоящих верных друзей», которые тебя понимают и принимают со всеми твоими недостатками.

Ты должен проанализировать эту особенность своего характера, найти свои сильные стороны, сделать на них акцент и обрести свой круг общения в офлайн.

Поверь, в твоей власти преодолеть себя. Разве не бывает, что, сильно увлекшись, ты вдруг становишься очень коммуникабельным и душой компании?

39—45 баллов: Ты явно некоммуникабелен и сверстникам с тобой нелегко, а вот администраторы незаконных сообществ, использующие молодых людей и детей для своих противоправных действий в Сети, ищут именно таких, как ты.

Запомни, что новые знакомства в Сети, прежде чем ты поймешь истинную цель интереса к твоей персоне, дадут ощущение внутренней уверенности и душевного равновесия. Но это лишь ощущение, которое затруднит возможность самореализации в обществе и развития социально включенной личности.

Старайся быть общительнее, контролируй себя. Сократи время, которое ты проводишь в Интернете. Найди дело по душе и своих единомышленников в реальной жизни.

5. Раздача памяток «Безопасный интернет – детям»

Кроме того, мы хотим оставить вам на память об этом уроке, для полного усвоения услышанной информации памятки от МВД России – «Безопасный интернет – детям».

Раздаем после ответов всем памятки «Безопасный интернет», куда вложена страница с ключом к тесту. Пусть дети спокойно дома осмыслят, какие они в общении. Раздаем вместе с памятками.

Мы хотели бы, чтобы вы рассказали, как можно большему количеству своих сверстников о правилах безопасности в Интернете, обо всем, что сегодня услышали. И сделали в своих аккаунтах посты о сегодняшнем уроке и репосты памятки с хештегами #безопасныйинтернет #мвдроссии.

В нашу следующую встречу мы обязательно отметим самые лучшие из этих постов – мы их найдем по хештегам #безопасныйинтернет #мвдроссии ».

6. Ответы на вопросы ребят. Подведение итогов

Ведущий урока:

«А теперь мы готовы ответить на ваши вопросы и о киберпреступности, и о службе в полиции».

Ответы на вопросы ребят – отвечают те из сотрудников, кому дает слово ведущий урока.