Материалы для проведения мероприятий с детьми 14-18 лет / для обучающихся старших классов общеобразовательных организаций (8-11 класс), обучающиеся профессиональных образовательных организаций

По материалам к уроку безопасного интернета, разработанным Лигой безопасного Интернета.

№	Этапы урока	Сценарий к презентации «Материалы к уроку в старших классах. Презентация.» (**http://www.ligainternet.ru/encyclopedia-of-security/parents-and-teachers/parents-and-teachers-detail.php?ID=3652**)
1.	**Опасность сайтов-подделок**	Добрый день! С ростом активности в Интернете, доступности всемирной сети все большему количеству пользователей, пропорционально активизируются и мошенники. Самые распространенные аферы в сети – выманивание (вымогание) денег, распространение вредоносного программного обеспечения и кража паролей посредством использования сайтов-подделок (сайтов-ловушек). Что они из себя представляют? Как вы думаете? *Ответы* Неопытному пользователю иногда довольно сложно сориентироваться в сети Интернет и не попасть на такие сайты. Особенно опасны поддельные сайты социальных сетей, банковских и финансовых организаций. Зафиксировано множество поддельных сайтов банков, аукционных домов, популярных файлообменников, социальных сетей. А ведь там, зачастую, требуется ввод паролей, номеров пластиковых карт и так далее. Ребята, только представьте, что вы сообщите эти конфиденциальные данные злоумышленникам, попав на сайт-подделку! Как же отличить сайт-подделку от сайта-оригинала? Как вы считаете? *Ответы* *Переход к следующему слайду*
2.	**Осторожно: сайты-ловушки!**	Как же обманывают в Интернете? • Просят подтвердить логин/пароль. • Предлагают бесплатный антивирус, а устанавливают вредоносное программное обеспечение, вирусы. • Просят отправить платное СМС. Если вы не можете зайти на страницу какого-либо сайта под своим аккаунтом, вам говорят, что вы заблокированы, необходимо выполнить следующие действия: - закрыть страницу, убедиться, что блокировка пропала; - проверить систему антивирусом; - авторизоваться под своими аккаунтами и убедиться, что все в порядке; - сменить используемые к аккаунтам пароли. *Переход к следующему слайду*

3.	**Осторожно: спам!**	Скажите,- а как часто вы сталкиваетесь со спамом? *Ответы* Спам – это нежелательные рекламные электронные письма, приходящие ежедневно миллионам пользователей Интернет. Как же обезопасить себя от этих ловушек? Как вы считаете? *Ответы* Давайте запомним простые правила безопасности: - удаляйте письма с незнакомых адресов; - игнорируйте неизвестные ссылки; - игнорируйте отправку СМС, если вас просят это сделать; - используйте кнопки «Это спам», «Заблокировать отправителя»; - настроить безопасность браузера и используемой почтовой программы; - используйте дополнительные расширения браузеров, которые позволяют блокировать СПАМ и рекламные блоки - используйте антивирусные программы; - проверяйте надёжность поставщика услуг, используя информационные сервисы «who is». *Переход к следующему слайду*
4.	**Персональные данные и личная информация в Интернете**	Практически каждый из вас зарегистрирован в социальных сетях, общается посредством этих сайтов со своими родными, друзьями, одноклассниками, знакомыми и незнакомыми людьми. Поднимите руки те, у кого нет личной страницы ни в одной социальной сети. *Ответы* Вот видите, к сожалению, живое общение сейчас все сильнее вытесняет он-лайн общение в Интернет. Но это одна сторона проблемы. А задумывались ли вы о том, что активно посещая социальные сети, вы подвергаете опасности собственную безопасность? Скажите, о чем идет речь? *Ответы* Правильно! Миллионы пользователей, заходящих в социальные сети, могут видеть вас. И очень важно проверить и настроить свою страницу так, чтобы личную (конфиденциальную) информацию могли видеть (если это действительно необходимо) самые близкие люди, необходимо настроить приватность. Очень часто указанная вами личная и контактная информация используется интернет-мошенниками, преступниками для кражи паролей, в целях шантажа, вымогательства, оскорбления, клеветы, хищения. Создавая свою личную страницу в социальной сети, будьте осторожны! Используйте только Имя или Псевдоним (ник), не публикуйте информацию о своем местонахождении и материальных ценностях, и уж тем более какую-то очень личную информацию. *Переход к следующему слайду*

5.	**Анонимность в Интернете**	В социальных сетях множество мошенников, зарегистрированных под именем известных личностей или даже ваших знакомых. Многие зачастую скрываются под маской анонимности, будьте предельно осторожны! Ведь анонимность в Интернете – это миф. Задумайтесь, с кем вы общаетесь в сети, кто скрывается за тем или иным ником и почему. Сталкивались ли вы когда-нибудь с подобным и, если да, то чем это закончилось? *Ответы* Общаясь с незнакомцами в социальной сети, вы даже не подозреваете, что среди них могут быть: • маньяки, педофилы, извращенцы, склоняющие к совершению развратных действий; • интернет-ХАМЫ (тролли), провоцирующие на необдуманные поступки и необоснованную агрессию; • киберпреступники, зачастую обманом похищающие чужое имущество; • хакеры, использующие анонимность для распространения вредоносного программного обеспечения, завладения учётными данными, платёжными реквизитами, персональной информацией. Кроме того, виртуальное общение, как и общение в реальной жизни, требует соблюдения правил этикета. Как вы считаете, почему? *Ответы* *Переход к следующему слайду*
6.	**Открытые сети, чужая техника**	Как вы считаете, насколько безопасна работа за чужим компьютером? *Ответы* Верно, довольно опасно оставлять свои учётные данные на устройстве, которое тебе не принадлежит, этими данными могут воспользоваться даже в преступных целях. Также будьте осторожны в открытых и небезопасных сетях. Подключение к ложной сети может моментально лишить вас всей персональной информации, хранящейся в вашем электронном устройстве: преступнику станут доступны пароли и другая информация. Запомните несколько правил, если вы пользуетесь чужой техникой или выходите в открытые сети: 1. При работе с публичным устройством используйте пункт «чужой компьютер». 2. Используйте режим «приватного просмотра» в браузере. 3. Всегда используйте кнопку «выйти» при завершении работы с ресурсом. 4. Отказывайтесь от сохранения пароля при работе на «чужом компьютере». 5. Используйте безопасное соединение с почтой и сервисами (безопасное соединение обозначено замком с зелёным текстом). 6. Не оставляйте без присмотра устройства доступа в сеть (телефон, планшет, ноутбук). 7. Используйте шифрованные хранилища данных, которые помогут защитить ваши личные файлы. 8. Используйте сложные пароли, состоящие из прописных и заглавных латинских букв и цифр, а также символов. 9. Используйте только такие сети, в надежности которых вы уверены. *Переход к следующему слайду*

7.	**Условия использования программного продукта**	Устанавливая тот или иной программный продукт (особенно от неизвестных производителей), внимательно читайте тексты соглашений, ведь после принятия соглашения вся ответственность и последствия использования программного продукта ложатся на вас! Как вы считаете, чем грозит бездумное принятие соглашения на установку программы? *Ответы* Итак, подтверждая соглашение «вслепую», вы рискуете: - оформить платные подписки/услуги; - предоставить приложению/программе обширные права; - лишиться персональных данных, хранящихся на электронном устройстве; - стать звеном СПАМ сети; - стать жертвой мошенников. При установке/использовании нового программного продукта соблюдайте следующие правила: - используйте лицензионные продукты проверенного производителя; - внимательно знакомиться с лицензионным соглашением; - не используйте подозрительное программное обеспечение. *Переход к следующему слайду*
8.	**Мобильные устройства / Мобильный Интернет**	Скажите, пожалуйста,- а что вы понимаете под словосочетанием «мобильный Интернет»? *Ответы* Сегодня все современные технологии мобильной связи представляют свои решения в сфере доступа к сети Интернет. Поэтому мобильный Интернет – это технология для подключения к глобальной сети практически из любого места. Пользуясь мобильными приложениями, будьте внимательны и осторожны, ведь в вашем телефоне много важной информации, которая может стать легкодоступной для других лиц. Соблюдая следующие правила, вы обезопасите себя: - следите за своим мобильным телефоном или планшетом; - установите пароль на включение мобильного телефона; - установите мобильный антивирус; - игнорируйте звонки и СМС с незнакомых номеров; - установите приложения, шифрующие ваши личные данные; - отключите функцию автоподключения к открытым Wi-Fi сетям; - используйте только защищённые Wi-Fi сети; - правильно завершайте работу с публичным Wi-Fi; - внимательно изучай права, запрашиваемые мобильными приложениями; - используйте только проверенные мобильные сервисы *Переход к следующему слайду*

9.	**Осторожно, мошенники: что такое кардинг и фишинг**	А кто из присутствующих здесь сегодня слышал такие определения, как «кардинг» и «фишинг»? Что вы об этом знаете? *Ответы* Кардинг – способ мошенничества с использованием банковских карт. Преступники похищают реквизиты карты со взломанных серверов интернет-магазинов, платежных систем или с персонального компьютера пользователя. Фишинговые сообщения – это уведомления, отправленные от имени администраторов банковских или других платежных систем. Они призывают пользователей пройти по фальшивой ссылке, чтобы украсть конфиденциальные данные. Как только преступники получают необходимую им информацию, они моментально используют ее для доступа к банковскому счету. Будьте предельно осторожны, оказавшись на сомнительном сайте! *Переход к следующему слайду*
10.	**Осторожно, мошенники: предупрежден – значит, вооружен!**	Интернет-мошенники действуют и таким образом: - отправляют уведомление о крупном выигрыше с целью выманить деньги (якобы налог) за получение выигрыша; - давят на жалость и отправляют письма с просьбой о помощи якобы от благотворительных организаций или нуждающихся людей; - отправляют так называемые «нигерийские» письма с такой информацией: у автора письма есть много денег, полученных не совсем законным путём, и поэтому он не может хранить деньги на счету в банках своей страны. Ему срочно необходим счет за рубежом, куда можно перечислить деньги. Авторы подобных писем попросят тебя обналичить крупную денежную сумму, в качестве вознаграждения обещая от 10% до 30% от заявленной в письме суммы. Идея мошенничества заключается в том, что пользователь предоставит доступ к своему счету, с которого позже будут списаны все денежные средства. Не ведитесь на эти уловки! *Переход к следующему слайду*
11.	**Средства защиты от Итнернет-мошенничества**	Итак, чтобы не попасться на удочку мошенников: - используйте инструменты браузера: «избранное», «закладки», «быстрый доступ»; - не переходите по ссылкам, указанным в подозрительных письмах; - удаляйте письма, содержащие не относящуюся к тебе информацию, связанную с денежными средствами, особенно от неизвестных людей; - не будьте слишком доверчивыми, проверяйте всю информацию, содержащую просьбы о помощи; - проверяйте адрес сайта; - обратите внимание на настоящий адрес сайта: при наведении мыши реальный адрес отображается во всплывающей подсказке; - внимательно изучите содержимое сайта – наличие дефектов верстки (сдвинутые блоки, картинки, наползающий друг на друга текст и т.д.) и грамматических ошибок явный признак того, что с сайтом что-то не так; - обратите внимание на даты под сообщениями, блоками, новостями – на поддельных сайтах даты, как правило, уже неактуальны, новости – просрочены; - на мошеннических сайтах практически никогда не указываются контактные данные, нет формы обратной связи, либо она просто не работает, либо указанные в контактах данные – пустышка; - мошеннические сайты не имеют гостевых и форумов; - настоящие сайты не просят отправлять СМС на короткие номера; максимум – это запрос вашего номера телефона, на который и проходит код. *Переход к следующему слайду*

12.	**Влияние виртуальной сети на реальную жизнь**	Являясь интернет-пользователями, каждый из вас несет персональную ответственность за соблюдение определенных законов: Федеральным законом от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» к распространению на территории России запрещена следующая информация: **материалы, содержащие публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости, и материалов, содержащих нецензурную брань.** Действующее законодательство устанавливает как уголовную, так и административную ответственность за правонарушения, связанные распространением противоправной информации. ст. 272 УК РФ - **Неправомерный доступ к** охраняемой законом компьютерной информации **компьютерной информации** (до 7 лет лишения свободы); · ст. 273 УК РФ – Создание, использование и **распространение вредоносных программ** для ЭВМ (до 7 лет лишения свободы); ст. 159 УК РФ – **Мошенничество** (до 10 лет лишения свободы со штрафом в размере до одного миллиона рублей); · ст. 242 УК РФ – Незаконное **распространение порнографических материалов** или предметов (до 6 лет лишения свободы); · ст. 242 (1) УК РФ – Изготовление и оборот материалов или предметов **с порнографическими изображениями несовершеннолетних** (до 10 лет лишения свободы); ст. 228.1 УК РФ - Незаконные **производство, сбыт или пересылка наркотических средств**, **психотропных веществ или их аналогов**, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества с использованием электронных или информационно-телекоммуникационных сетей (до 20 лет лишения свободы); · ст. 20.29. Кодекса Российской Федерации об административных правонарушениях – **Распространение экстремистских материалов** (штрафные санкции и административный арест до 15 суток). Помните, за ВИРТУАЛЬНЫЕ преступления отвечают по РЕАЛЬНОМУ закону! Кроме того, в сети Интернет появились сообщества, пропагандирующие кражи в магазинах. Будьте бдительны! Согласно ч.1 Статья 158 Уголовного кодекса РФ: **Кража, то есть тайное хищение чужого имущества**, - наказывается лишением свободы на срок до 2 лет. *Переход к следующему слайду*

13.	**Соблюдение правил безопасности**	Важно помнить, что ваша безопасность в ваших руках. Для этого следуйте следующим простым правилам: • если вы не уверены в своих знаниях, используйте учетную запись с ограниченными правами; • не работай от имени администратора (root) – это убережет от большинства заражений; • используйте антивирусную защиту; • регулярно обновляйте операционную систему и антивирус; • настройте дополнительные функции (блокировку рекламы в браузере, функции антифишинга, блокировку всплывающих окон, режим безопасного поиска); • используйте официальное лицензионное и (или) свободное программное обеспечение; • не заходите на сайты, которые помечены как опасные, не открывайте файлы, которые блокирует антивирус; И самое главное, ограничивайте время работы в Интернете – живите реальной жизнью! *Переход к следующему слайду*
14.	**Как сделать Интернет безопаснее?**	Вы всегда можете «пожаловаться» в соцсетях администратору сайта/группы на размещение опасной/запрещенной информации. Если вы встретили в Интернете противоправную информацию (пропаганда наркотиков, суицида, экстремизма, порнографии и т.п.), можете направить ссылку через сайт Роскомнадзора: http://eais.rkn.gov.ru/feedback/.
15.	**Заключительная часть (Закрепление знаний)**	А теперь, давайте проверим, как вы усвоили материал по теме безопасного Интернета. Предлагаю совместно обсудить следующие вопросы: • Чем опасны сайты подделки? • Как распознать подделку? • Что такое Спам? Как бороться со Спамом? • Какие существуют методы блокировки Спам рекламы? • Что относится к персональным данным, а что к личной (конфиденциальной) информации? • Какую информацию можно публиковать в сети? • Почему не стоит публиковать свои полные данные? • Анонимность в сети: правда или вымысел? • Какие правила поведения в сети нужно соблюдать? • Какие опасности подстерегают нас в открытых сетях? • Как не стать жертвой преступника при использовании открытых сетей? • Какие правила пользования чужой техникой нужно помнить? • Лицензионное соглашение/правила пользования: читать или нет? • Почему важно знать правила использования программного продукта/интернет-ресурса? • Виды интернет-мошенничества (объекты мошенничества)? • Какие виды преступлений распространены в Интернете? • Как не стать жертвой киберпреступника?