Материалы для проведение занятия курса внеурочной деятельности «Разговоры о важном»

23.01.2023

Тема: КИБЕРБЕЗОПАСНОСТЬ

Цель: формирование культуры безопасного и эффективного использования цифровых ресурсов и устройств, знакомство с основами безопасности в сети и повышение уровня цифровой грамотности.

Формирующиеся ценности: жизнь, права и свободы человека.

Сегодня наше занятие посвящено кибербезопасности. Жизнь современного человека трудно представить без цифровых сервисов и приложений. Мы используем их для решения самых разных повседневных задач. При этом онлайн-среда связана не только с массой полезных возможностей, но и с рисками для безопасности пользователя. Именно поэтому так важно развивать собственную цифровую грамотность, знать о возможных рисках и владеть разными методами защиты, в том числе и технологическими. Также сфера кибербезопасности активно развивается, поэтому это ещё и перспективное направление для профессионального развития. О том, почему важно быть внимательными в цифровом мире, вам расскажет Наталья Ивановна Касперская — глава компании InfoWatch в видеообращении по ссылке: https://razgovor.edsoo.ru/video/1612/

Итак, пользователи интернета подвергаются целому ряду потенциальных угроз. Ландшафт угроз постоянно меняется, а киберпреступники изобретают новые способы атак на интернет-пользователей. Вот лишь основной список опасностей при использовании интернета:

Кража идентификационных данных;

Утечки данных;

Вредоносные программы и вирусы;

Фишинговые и мошеннические электронные письма;

Поддельные сайты;

Интернет-мошенничество;

Мошенничество на сайтах и в приложениях для знакомств;

Неприемлемый контент;

Кибербуллинг.

Неверные настройки конфиденциальности

Согласно статистике, 22% пользователей сталкивались с кражей аккаунтов в социальных сетях или играх, 15% теряли данные из-за компьютерного вируса, 14% отметили, что им писали странные сообщения взрослые, 10% сталкивались с мошенничеством с использованием фальшивых сайтов и писем.

В продолжение занятия предлагаю вам погрузиться в настоящее состязание кибермошенников и специалистов по информационной безопасности. Мы проведем игру и научимся противостоять киберугрозам, разберём типичные сценарии атак и узнаем, как пользователи могут себя защищать. Вы можете выбрать себе любую роль - «Кибермошенники» и «Специалисты по информационной безопасности».

Итак, герой нашей истории молодой ученый Алексей, который давно ведёт свой профиль, у него много подписчиков, интересные и полезные научно-популярные публикации — потерять аккаунт для него будет обидно. Первая угроза: кибермошенники пытаются совершить кражу профиля Алексея через взлом логина/пароля. Команда «Кибермошенников» из своих карточек–действий составляет план атаки. Вам нужно отобрать те действия, которые злоумышленникитипично используют в такой ситуации (можете добавить свои варианты действий). Команда «Специалистов по информационной безопасности» составляет из своих карточек план защиты. Ваша задача – собрать эффективную при такой угрозе модель поведения для пользователя (можете добавить свои варианты действий).

Карточки-задания можно скачать по ссылке: https://razgovor-cdn.edsoo.ru/media/file/media-1011-dop2.pdf

Продолжить игру можно с использованием остальных карточек.

Теперь вы знаете чуть больше о том, как действуют мошенники онлайн и как можно предусмотреть риски. Это была отличная тренировка для вас. Предлагаю вам из тех полезных правил для пользователя, что мы сегодня услышали и из тех, что вы можете назвать самостоятельно, составить список – топ-5 полезных привычек кибербезопасности, которые каждый из нас может начать придерживаться с сегодняшнего дня.

Ответы присылайте на электронную почту преподавателя.

Я предлагаю вам свои 5 правил кибербезопасности:

1.Держите в секрете сведения о себе, данных банковских карт, пароли интернет банка.

2. Проверяйте безопасность интернет – соединения.

3. Не переходите по ссылкам от неизвестных отправителей.

4. Установите антивирус на все устройства.

5. Используйте сложные пароли.

Сегодня мы рассмотрели ситуации, когда пользователи не задумываются о последствиях своих действий и сами ставят себя под угрозу. Наша ответственность как пользователей цифровых сервисов — быть внимательными и стремиться повышать уровень своей цифровой грамотности. Теперь мы можем соблюдать простые правила и внедрять в свою жизнь полезные привычки кибербезопасности. Чтобы узнать больше о том, как с технической стороны обеспечивается наша с вами информационная безопасность, послушаем рекомендации от эксперта компании VK Рустэма Газизова по ссылке: https://razgovor.edsoo.ru/video/1613/

и популярного российского певца Егора Крида по ссылке: https://razgovor.edsoo.ru/video/1611/

Итак, для безопасного пользования интернетом следует запомнить следующее:

Внимательно отнеситесь к созданию и хранению паролей.

Изучите политику конфиденциальности сайтов и приложений, запретите вашему браузеру автоматически сохранять пароли, регулярно удаляйте cookies.

Пользуйтесь блокировщиками рекламы.

Оставляйте личные данные только на сайтах с защищённым соединением. Не пользуйтесь общественными сетями Wi-Fi для передачи конфиденциальной информации.

Если вы столкнулись с травлей в сети, блокируйте пользователя, который отправляет вам агрессивные сообщения. Обратитесь в службу поддержки сайта или социальной сети, сообщите родителям. Не вступайте в дискуссии с агрессивно настроенными пользователями.

Чтобы не стать жертвой интернет-мошенников, перепроверяйте всю информацию, полученную по электронной почте или в сообщениях социальных сетей и мессенджеров, не сообщайте незнакомым людям и не публикуйте в открытом доступе личные данные.

С этими советами надеюсь, вы осознали важность максимальной безопасности работы в интернете. Всегда предполагайте, что вы открыты для атаки и готовы к тому, что неизбежно произойдёт.

Презентации к занятию можно скачать по ссылке:

Защита личной информации: https://razgovor-cdn.edsoo.ru/media/file/media-presentation3.pdf

Защита профиля: https://razgovor-cdn.edsoo.ru/media/file/media-presentation2.pdf

Социальная инженерия: https://razgovor-cdn.edsoo.ru/media/file/media-presentation3.pdf

Фишинговые ссылки: https://razgovor-cdn.edsoo.ru/media/file/media-presentation4.pdf