**Доклад: Вовлечение подростков в мошеннические схемы в сети Интернет**

В настоящее время с учетом цифровизации (внедрение цифровых технологий) нашей повседневной жизни – важной темой для обсуждения становятся вопросы, связанные с практиками медиабезопасности.

**Данные медиа-угрозы могут быть потенциально реализованы в следующих проблемных формах:**

* *контентные* – материалы (тексты, картинки, аудио, видеофайлы, ссылки на сторонние ресурсы), содержащие насилие, агрессию, нецензурную лексику и т.д.;
* *коммуникационные* (связаны с межличностными отношениями интернет- пользователей), например, незаконный контакт, домогательство, киберпреследование, кибербуллинг (травля, оскорбления или угрозы, высказываемые жертве с помощью средств электронной коммуникации, в частности, сообщений в социальных сетях, мгновенных сообщений, электронных писем и СМС);
* *электронные* – возможность столкнуться с хищением персональной информации, риск подвергнуться вирусной атаке, онлайн-мошенничеству, спам-атаке, шпионским программам и т.д.;
* *потребительские* – злоупотребление в интернете правами потребителя.

***Мошенничество – это преступление, которое заключается в присвоении чужих денег путём обмана или введения в заблуждение.***

В 2023 году участились случаи вовлечения учащихся образовательных организаций, в том числе и нашего города, в преступные мошеннические схемы. Подростки ищут возможность заработать "легкие деньги", не задумываясь откликаются на предложения злоумышленников через социальную сеть ВКонтакте, мессенджер Телеграм и устраиваются курьерами.

Дистанционные мошенники действуют по старой знакомой схеме: "Ваш родственник попал в ДТП, нужны деньги, чтобы всё прекратить", обманывая доверчивых пожилых людей.  Адрес психологически подготовленной жертвы направляется курьеру-подростку. Последний забирает с адреса деньги, выполняя дальнейшие указания мошенников, переводит полученные средства на электронные счета и одновременно становится соучастником тяжкого преступления, не задумываясь об уголовной ответственности! Конечно, ведь он «за работу» оставит себе до 10% «выручки».

Часто несовершеннолетние совершают правонарушения, а также общественно опасные деяния, не задумываясь о последствиях.

Возмещать причинённый ущерб в данном случае будет его семья в соответствии с Гражданским кодексом РФ. С 16 лет такие несовершеннолетние курьеры могут быть привлечены к уголовной ответственности по статье 159 УК РФ и провести в воспитательной колонии до 2 лет. До достижения этого возраста, при установлении причинно-следственной связи, к ответственности будут привлечены родители по ч.1 ст.5.35 КоАП РФ за ненадлежащее исполнение обязанностей по воспитанию ребёнка, а сам юный мошенник - отправиться в специальное учебно-воспитательное учреждение закрытого типа на срок до 3 лет.

**Причины формирования правонарушений среди несовершеннолетних:**

• Негативное влияние семьи, существенные изъяны в воспитании.

• Негативное влияние окружения со стороны, как взрослых, так и сверстников. Включает в себя проникновение в сознание несовершеннолетнего путем СМИ, бесконтрольного нахождения в сети Интернет, личными бытовыми контактами неверных стандартов поведения (жестокости, распущенности и т. п.).

• Отсутствие занятости ребенка.

• Желание самоутвердиться.

• «Получение острых ощущений».

**Основные советы по безопасности в социальных сетях:**

1. Ограничить список друзей. У вас в друзьях не должно быть случайных и незнакомых людей.
2. Защищать свою частную жизнь. Не указывайте пароли, телефоны, адреса, дату рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как вы и ваши родители планируете провести каникулы.
3. Защищать свою репутацию - задавайте себе вопрос: хотели бы вы, чтобы другие пользователи видели, что вы загружаете? Подумайте, прежде чем что-то опубликовать, написать и загрузить.
4. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее
5. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если вас взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

**Основные советы по безопасной работе с электронной почтой:**

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге.
2. Используйте двухэтапную авторизацию (это когда помимо пароля нужно вводить код, присылаемый по SMS).
3. Выберите сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль.
4. Если есть возможность придумать самому свой личный вопрос, используйте эту возможность.
5. Используйте несколько почтовых ящиков. Отдельный необходимо иметь для частной переписки с адресатами, которым вы доверяете - этот электронный адрес не надо использовать при регистрации на форумах и сайтах.
6. Не открывайте файлы и другие вложения в письмах даже если они пришли от ваших друзей. Лучше уточните у них, отправляли ли они вам эти файлы.
7. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудьте нажать на «Выйти».

**Основные советы для безопасности мобильного телефона:**

1. Будьте осторожны, ведь когда вам предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги.
2. Думайте, прежде чем отправить SMS, фото или видео. Вы точно знаете, где они будут в конечном итоге?
3. Необходимо обновлять операционную систему твоего смартфона.
4. Используйте антивирусные программы для мобильных телефонов.
5. Не загружайте приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение.
6. Периодически проверяйте, какие платные услуги активированы на вашем номере.
7. Давайте свой номер мобильного телефона только людям, которых вы знаете и кому доверяете.
8. Bluetooth должен быть выключен, когда вы им не пользуетесь. Не забывайте иногда проверять это.