МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РД
ГБПОУ РД «КОЛЛЕДЖ ЭКОНОМИКИ И ПРАВА»

ОТЧЕТ
о проведении классного часа
группы 39 ИСП 2
кл. руководитель - Наджафова А.С.

12 мая 2023

КЛАССНЫЙ ЧАС

«Безопасность подростков в сети Интернет: виды интернет-преступлений и способы их предупреждения»

ХОД КЛАССНОГО ЧАСА

Часто подростки подвержены негативному влиянию из вне, а так как Интернет на данный момент является неотъемлемой частью жизни, то именно там современных школьников и студентов и подстерегает большое количество опасностей.

1) Мошенничества, связанные с Интернет-магазинами.

Через Интернет могут предложить приобрести все, что угодно, а распознать подделку при покупке через сеть бывает сложно.

2) Фишинг.

Вид интернет-мошенничества, цель которого – получить данные, содержащиеся на вашей пластиковой карте. Злоумышленники рассылают электронные письма от имени банков или платежных систем. Пользователю предлагается зайти на сайт, который является точной копией настоящего сайта банка, где можно увидеть объявления, например, об изменении системы безопасности банка. Для дальнейшей возможности использовать свою пластиковую карту просят указать пин-код и данные, содержащиеся на карте. Впоследствии эти данные используются для изготовления поддельной пластиковой карты и обналичивания денежных средств, содержащихся на вашем счете.

3) Интернет-попрошайничество.

В Интернете могут появляться объявления от благотворительной организации, детского дома, приюта или просто от родителей с просьбой о материальной помощи больным детям. Злоумышленники создают сайт-дублер, который является точной копией настоящего, меняют реквизиты для перечисления денег.

4) Вирусы.

Сущность вируса – переадресация со страницы запрашиваемого ресурса на фиктивную, скопированную с настоящей. Подмена осуществлялась для самых популярных ресурсов Рунета: Яндекс, Рамблер, Майл, ВКонтакте, Одноклассники. Набирая на «зараженном» компьютере адрес одного из указанных ресурсов, пользователь попадает на сервер-подмену, где ему предлагается страница для входа в систему (имя и пароль). С учетом того, что в адресной строке указано корректное имя, а внешний вид скопирован с оригинального сервера, у большинства пользователей не возникает подозрений в подлинности страницы. После ввода имени и пароля отображается иная страница, где уже говорится о необходимости «подтверждения» или «активации» учетной записи за смс на короткий номер, стоимость которого минимальная или якобы бесплатная. Таким образом, злоумышленники не только снимают денежные средства со счетов абонентов, но и получают логин и пароль доступа пользователя к указанным популярным ресурсам, что позволяет им в дальнейшем отправлять от имени «жертвы» различные сообщения,

5) Социальные сети.

Социальные сети являются одним из способов вовлечения студентов в шантаж или же запрещенные РФ группы, подталкивающие молодых людей к совершению каких-либо противозаконных действий (насилие, жестокость). Социальные сети активно используются злоумышленниками для вовлечения детей и подростков в распространение порнографических материалов с участием несовершеннолетних посредством сети Интернет. В ходе электронного общения создаются условия, побуждающие подростка направить свои откровенные фотографии. После их получения данные изображения распространяются на тематических форумах, файлообменных системах и фото и видеопорталах.

6) Кибербуллинг.

Зачастую злоумышленнику становятся известны анкетные данные подростка, и тогда происходит так называемый «тро́ллинг» или травля (размещение в Интернете на форумах, в дискуссионных группах, в вики-проектах провокационных сообщений с целью собственного развлечения и созданием конфликтов между участниками). Это необходимо для установления круга знакомых, учителей и родителей подростка с целью направления им полученных провокационных фотографий, а возможно и с целью шантажа и вымanивания определенной денежной суммы.

7) Интернет-знакомства.

Мошенники с сайтов знакомств – это особый тип людей, способный втираться в доверие к людям, очаровывать их с целью завладеть деньгами, имуществом. Им свойственно обычно глубокое знание психологии, умение построить общение так, что жертвы сами, добровольно отдают им материальные ценности. Причем в такую ловушку могут попасть как девушки, так и юноши.

6) Звуковые наркотики.

Особую популярность звуковые наркотики приобрели в 2009 году., однако и в 2018 данный вид интернет-мошенничества имеет место. Реклама аудионаркотиков осуществляется посредством массовой рассылки писем на электронные почтовые адреса пользователей и на номера в системах быстрого обмена сообщениями. Доступ к прослушиванию аудио-файлов возможен после введения специального цифрового кода, получение которого происходит исключительно после оплаты в виде отправки смс-сообщения. Ресурсы, предлагающие такого рода продукцию, располагаются на площадях зарубежных провайдеров и зарегистрированы по фиктивным анкетным данным.

ЗАКЛЮЧЕНИЕ

Впервые мир узнал о компьютерных преступлениях в начале 70-х годов, когда в Америке было выявлено довольно большое количество таких деяний. Как известно – наиболее опасные преступления – это те, которые носят экономический характер. Изначально, как показывает история, органы уголовной юстиции боролись с ней при помощи традиционных правовых норм о преступлениях против собственности: краже, присвоении,

мошенничестве, злоупотреблении доверием и тому подобное. Однако вскоре практика показала, что такой подход не отвечает всем требованиям сложившейся ситуации, поскольку многие преступления в сфере компьютерной деятельности не охватываются традиционными составами преступлений. Принятый в недавнем прошлом кодекс содержит целую главу, включающую в себя три статьи, связанные с интернет-преступлениями.