(по списку общеобразовательных учреждений)

В целях правового информирования и правового просвещения прошу довести до сведения педагогических работников и обучающихся общеобразовательного учреждения следующую статью:

Распространенные способы мошенничества с применением информационно-телекоммуникационных технологий

В условиях современного мира разновидность преступлений с использованием IT-технологий, весьма обширна. Такие преступления тщательно спланированы и, как правило, совершаются подготовленной организованной преступной группой на протяжении длительного периода времени.

Вот наиболее распространенные из них.

1. гражданину в социальной сети или интернет-мессенджере (ВКонтакте, Telegram, WhatsUp) приходит сообщение от клона профиля знакомого ему лица с текстовым сообщением «Это твои фотографии?/Это ты на видео?/Ты знаешь этого человека?» с приложением ссылки или стороннего файла любого другого формата.

Текст сообщения может варьироваться. В любом случае содержание такого сообщения направлено на побуждении интереса у лица к открытию и прочтению сообщения.

При последующем открытии приложенной ссылки или стороннего файла происходит автоматическое скачивание вредоносного приложения, которое предоставляет мошенникам полный дистанционный доступ к мобильному устройству гражданина, что и позволяет в последующем осуществить хищение принадлежащих ему денежных средств.

Чтобы обезопасить себя от такого типа мошенничества следует помнить, что открывать диалоговое окно с приложенным файлом или ссылкой безопасно, но в последующем следует детально изучить полученное сообщение: установить, является ли профиль отправителя «подлинным», проверить контактны данные, обратить внимание на отсутствие в диалоге иных сообщений и медиа-файлов; обратить внимание на текст ссылки и

Организация

№ рег

формат приложенного файла. Следует остерегаться форматов «exe». Зачастую мошенники прикладывают файл с наименованием «mamont».

В случае открытия вредоносного файла мобильное устройство начнет производить самостоятельные бесконтрольные действия. Попробуйте незамедлительно выключить его длинным нажатием клавиши «блокировка» или физическим извлечением батареи.

Если мошенникам все же удалось похитить денежные средства незамедлительно обращайтесь в полицию. Ни в коем случае не форматируйте мобильное устройство, оставшиеся на нем сведения важны для осуществления расследования.

2. Также все большую популярность приобретает мошенничество в популярных среди детей онлайн играх, примером служит игра Roblox (роблокс).

В ходе игры детям предлагается подписаться на страницу в социальной сети Телеграмм, где разыгрывается пополнение игрового счета. Для перечисления выигрыша, злоумышленники просят ребенка сфотографировать банковское приложение в телефоне родителей (сфотографировать банковскую карту, осуществить перевод денежных средств через приложение банка и пр.), требуют это сделать незамедлительно, объясняя тем, что приз скоро исчезнет. После того, как ребенок выполнит указания, денежные средства со счета родителей уходят к мошенникам.

В основном в такую ситуацию попадают дети в возрасте Самый «удобный» от 7 до 12 лет. Дети этого возраста уже разбираются в компьютерной технике, смартфонах и соцсетях. Если в семье не выстроен доверительный диалог, велика вероятность, что ребенок без спроса возьмет телефон/банковскую карту родителей чтобы получить как можно скорее заветный приз.

Родителям важно защитить детей от мошенников. Необходимо проверять приложения, которые использует ребенок, разговаривать с ним об угрозах в сети и правилах безопасного поведения в интернете. Необходимо объяснить ребенку, что вводить данные банковских карт или делиться иной личной информацией в интернете нельзя

Прокурор района

старший советник юстиции Д.А. Дерябин

Ю.А. Наумова, 8 (342 66) 2-20-33