■ СОЦИАЛЬНАЯ СФЕРА АЛТАЙСКОГО КРАЯ

Доверяй, но проверяй!

Мошенники становятся более избирательными в методах обмана

Теперь целью мошенников являются не только взрослые, но и дети. Именно юные пользователи в силу возраста и доверчивости становятся легкой мишенью для реализации преступных замыслов. Чтобы не стать жертвой злоумышленников, обезопасить себя и своих близких от посягательств на персональные данные и личные сбережения, необходимо соблюдать ключевые правила медиабезопасности. Рассказываем о самых распространенных схемах дистанционного мошенничества в отношении подростков и рекомендациях, как противостоять аферистам.

■ Юные пользователи в силу возраста и доверчивости становятся легкой мишенью для реализации преступных замыслов.

Онлайн-игры

Отличить мошенника от обычного пользователя непросто. Вначале злоумышленник выстраивает доверительные отношения с ребенком. Общается в игровом чате, предлагает помощь в прохождении игры и т.д., после чего совершает обман.

Мошенник предлагает детям купить ценный или очень редкий предмет, коллекционный образ героя игры, перейдя по специальной ссылке или оплатив через сторонний сервер. После оплаты он получает доступ к банковским реквизитам и удаляет переписку.

Дропперы

Мошенники начали брать в аренду банковские карты подростков, чтобы выводить с них похищенные деньги. Обычно мошенники крадут деньги у жертв, прося их перевести сбережения на "безопасный счет". Для того чтобы заполучить эти средства, они используют сторонние банковские счета с логинами и паролями в приложениях. И если раньше преступники чаще выкупали чужие карты и после совершения транзакций избавлялись от них, то сейчас стремятся перевести ответственность на изначальных владельцев карт, делая их соучастниками преступления.

Людей, у которых берут карты, называют дропперами или дропами.

Пушкинская карта

Если вам предлагают "купить" или "обналичить" Пушкинскую карту - это мошенники. Законными способами снять деньги с нее нельзя.

Пушкинская карта входит в число социальных, поэтому вывод средств с нее считается нарушением и влечет уголовную ответственность.

Аферисты уточняют реквизиты банковской карты, на которую предлагают "вывести" средства с Пушкинской карты, просят продиктовать код подтверждения и списывают деньги, затем блокируют и не отвечают на сообщения.

Звонок от учителя

Мошенники с помощью диппфейк-технологий подделывают голоса классных руководителей или учителей ребенка. Общаясь со школьником по телефону, они просят его обновить профиль, например, в "Сферуме" (или другой программе) и убеждают его назвать номер из СМС-сообщения.

Код подтверждения используется для получения доступа к аккаунту на портале "Госуслуги" и кражи персональных данных.

Призы от блогеров

Мошенники создают в соцсетях фейковые страницы популярных блогеров и устраивают "розыгрыши" призов (игровые приставки, телефоны, виртуальную игровую валюту и т.д.).

Чтобы получить приз, нужно оплатить доставку и передать свои персональные данные псевдоменеджеру. В результате преступник получает деньги и доступ к аккаунту ребенка.

Работа за лайки

Мошенники заманивают детей через объявления о быстрой и легкой работе. За несколько проставленных реакций (лайков) в различных телеграм-каналах предлагают щедрое вознаграждение.

По завершении работы у ребенка просят реквизиты банковской карты для перечисления "заработанных" средств. В итоге у мошенников оказываются банковские данные ребенка.

Выпуск виртуальных карт

Злоумышленники убеждают завести и добавить в электронный кошелек "специальную" виртуальную карту - человек уверен, что сохранит деньги, перечислив их в "надежное место". Жертва пополняет фальшивую карту через банкомат наличными по присланному мошенниками пин-коду и лишается средств.

Смишинг-мошенничество

Это разновидность дистанционного мошенничества с использованием СМС-сообщений. Аферисты маскируются под легитимные организации и обманом вынуждают своих жертв раскрыть конфиденциальную информацию. В последнее время участились случаи, когда подросткам под видом знакомого в мессенджер присылают ссылку для получения подписки "Телеграм Премиум". После перехода пользователь моментально лишается аккаунта. Фейковый "Телеграм Премиум" имитирует страницу авторизации, благодаря чему мошенники похищают данные пользователя. С его помощью они получают полный доступ к устройству.

Вербовка несовершеннолетних

Вербовка - это целенаправленное воздействие одного человека или группы лиц на другого с целью принуждения к совершению каких-либо действий. Вербовщиков в первую очередь интересуют подростки, испытывающие материальные и социальные трудности. Кураторы деструктивных и радикальных групп сначала собирают в сети информацию о потенциальной жертве, проводят анализ собранного материала, затем вырабатывают и применяют определенные технологии и подходы. Активно интересуются личной жизнью, увлечениями, заботами, финансовым положением, стремятся стать другом, наставником, стараются помочь в решении проблем. После мастерски используют психологические манипуляции, предлагают принять участие в сомнительных мероприятиях, акциях или выполнить поручение за определенную плату, часто ведут беседы на религиозные, мировоззренческие темы, навязывают новые взгляды и, как следствие, вовлекают молодежь в противоправную деятельность.

Как защитить детей от киберпреступников?

1. Расскажите детям о возможных видах мошенничества.

Объясните, как легко сейчас можно попасться на уловки злоумышленников, расскажите о схемах обмана, опасности общения с незнакомыми людьми.

2. Обсудите базовые правила безопасного поведения в виртуальном мире.

Их выполнение и критическое отношение ко всем поступающим в интернете предложениям минимизируют шансы стать жертвой обманщиков.

- Не добавляйте незнакомых людей в друзья.
- Никому не сообщайте личную информацию.
- Не ставьте геометки под фото.
- Перепроверяйте сообщения с просьбами о помощи от друзей и родственников.
- Не надейтесь на быстрое обогащение.
- Не используйте найденную банковскую карту.
- Не переходите по сомнительным ссылкам.
- Используйте сложные пароли.
- Не публикуйте персональные данные в социальных сетях.
- Защитите аккаунт двухфакторной аутентификацией.

Двухфакторная аутентификация предполагает ввод пароля и дополнительного кода, который можно получить на номер телефона, в приложении или на почту. Это надежный барьер от злоумышленников, который усложнит им получение доступа к чужим данным.

3. Помните об ответственности.

Мошенничество - это нарушение закона, за которое предусмотрено наказание по статье 159 Уголовного кодекса Российской Федерации. Если вы узнали, что ребенок или кто-то из ваших близких стал жертвой обмана, то стоит обратиться в полицию.

Подготовлено по заказу Управления печати и массовых коммуникаций Алтайского края совместно с методическим центром сопровождения педагогов по вопросам профилактики распространения идеологии экстремизма и терроризма КАУ ДПО "АИРО им. А.М. Топорова".