

Кошелек или кибержизнь: как защитить детей от мошенников

Цифровые мошенники все чаще связываются с жертвой через мессенджеры, причем действуют через детей. Это напоминает сетевой маркетинг: подростков убеждают за вознаграждение передать свой аккаунт во временное пользование аферисту, а тот с арендованного аккаунта начинает вымогать деньги у других пользователей соцсетей. В числе которых, опять же, дети. Чтобы оградить ребят от преступной «паутины», следует объяснять им, как она работает и почему важно соблюдать приватность в интернете. Рассказываем, как мошенники обманывают подростков, какие уловки сегодня в ходу у киберпреступников и как научить ребенка осторожности.

Зачем мошенникам нужны подставные аккаунты

В мессенджере Telegram сложилась экосистема, которая позволяет получить доступ к аккаунтам мессенджера WhatsApp. В них заинтересованы организаторы колл-центров, расположенных за пределами России. Такие данные приводят в Управлении по организации борьбы с противоправным использованием информационно-коммуникационных технологий УБК МВД России. Именно это подразделение отвечает за борьбу с киберпреступлениями.

В 2024 году полиция изъяла порядка 2 тыс. SIM-банков и 2 млн SIM-карт, применявшихся для связи с потенциальными жертвами. С начала 2025-го Роскомнадзор заблокировал около 9,5 млн SIM-карт, принадлежащих иностранцам, кроме того, введено ограничение количества «симок», доступных одному абоненту. Но злоумышленники тоже ищут обходные пути.

В погоне за трафиком колл-центров мошенники стали практиковать массовую аренду аккаунтов. Для этого они создают в Telegram каналы, где предлагают от 4 до 15 долларов за пользование чьим-то личным аккаунтом WhatsApp. Пользователю достаточно сообщить арендатору номер телефона, указанный при регистрации, и код авторизации. При этом SIM-карта остается у владельца, доступу к другим сервисам и приложениям ничто не препятствует.

Оперативники УБК МВД России выяснили, что с сентября 2024 по март 2025 года через один из Telegram-каналов состоялась передача порядка 11,4 тыс. аккаунтов. Организаторов задержали. Следствие установило, что участники группы могут быть причастны к совершению на территории России порядка 1 тыс. преступлений, связанных с мошенничеством и неправомерным доступом к учетным записям портала госуслуг. Ущерб оценивается не менее чем в 400 млн рублей.

Всего сейчас насчитывается порядка 3 тыс. таких каналов, среднее количество их подписчиков – около 2 тыс. человек.

Почему дети могут стать жертвами мошенников?

На предложение сдать аккаунт в аренду охотно откликаются дети и подростки: карманных денег много не бывает. Слухи о легком заработке распространяются в чатах онлайн-игр, в фан-клубах популярных блогеров, в тематических каналах. Получив первое вознаграждение, ребята, сдавшие свои аккаунты в аренду, втягивают в «дело» друзей и одноклассников.

«Многие не до конца понимают, что сдача аккаунтов в аренду — это не безобидный способ заработка. За этим стоят реальные преступления: мошенничество, шантаж, вербовка в запрещенные группировки и даже поддержка террористической деятельности. Проблема усугубляется тем, что тех, кто предоставляет свои аккаунты, редко привлекают к ответственности, что создает у них ложное чувство безнаказанности», — отмечает председатель Альянса по защите детей в цифровой среде Елизавета Белякова.

Заполучив чужой аккаунт в пользование, киберпреступники выходят через него на своих жертв. Зачастую ими становятся другие дети. Мошенники используют разные схемы и постоянно совершенствуют способы манипулирования детской психикой. Расскажем про самые распространенные ловушки, с помощью которых мошенники обманывают детей в интернете.

Виды интернет-шантажа

Страх перед экзаменами. Старшеклассникам предлагают купить «ответы» на задания ЕГЭ. Получив деньги, аферисты присылают ответы на варианты прошлых лет или просто не выходят на связь.

Кому-то приходит сообщение о том, что камера видеонаблюдения якобы зафиксировала списывание на ЕГЭ. Выпускнику предлагают выкупить запись. После перечисления средств связь обрывается, аккаунт мошенника блокируется.

Также мошенники создают фейковые сайты и группы в соцсетях, выдавая себя за сотрудников приемных комиссий вузов. С абитуриента берут плату за поступление на бюджетное место. Разумеется, никакого отношения к университетам преступники не имеют.

Псевдо-босс. Мошенники звонят школьникам, представляясь завучем, классным руководителем или врачом медицинского кабинета школы. Под предлогом проведения корректировок в электронном дневнике, медкарте или записи на прием они просят передать код из СМС, который используют для авторизации на портале госуслуг под видом родителей ребенка.

Мама в беде. Неизвестные могут связаться с ребенком через мессенджер и сообщить, что мама или папа попали, например, в автокатастрофу, сейчас находятся в больнице и нужно срочно собрать денег на дорогие лекарства.

Чем младше дети, тем они доверчивее, поэтому такой прием наиболее эффективно действует на детей до 10-12 лет. Мошенники, убедившись, что родителей нет дома, могут попросить ребенка включить видеосвязь, чтобы дистанционно руководить поисками в квартире. Когда дети находят деньги или драгоценности, преступники требуют открыть дверь и передать их курьеру.

Развод через онлайн-игру.

В любой онлайн-видеоигре всегда есть риск столкнуться с мошенничеством.

Одна из самых популярных подростковых онлайн-игр — Roblox. Это платформа, где пользователи могут создавать свои миры, зарабатывать внутриигровую валюту и общаться с другими игроками. И киберпреступники наживаются на подобной популярности.

Аферисты заходят в тематические сообщества — форумы, чаты, соцсети — с предложением, например, купить игровую валюту вне официального магазина по заниженной цене. Надо лишь взять родительский смартфон, сделать фото банковской карты мамы или папы и ввести код подтверждения перевода денег. Или задействовать собственную карту, если она у подростка уже есть.

После этого аферист ничего не отправляет, но получает доступ к карте и может выводить с нее деньги.

Чтобы завоевать доверие, преступники могут задействовать поддельные аккаунты популярных стримеров и блогеров.

Обещание бесплатных бонусов тоже должно насторожить игрока. «Перейди по ссылке — получи 700 алмазов!», «Бесплатные скины!», «100 000 монет за пять минут!» — такие сообщения часто ведут на вредоносные (фишинговые) сайты, которые воруют пароли. Мошенник меняет пароль и получает полный доступ к профилю, в том числе к привязанным платежным средствам.

Еще одна приманка — сообщение «Ты выиграл приз! Отправь мне данные аккаунта». Получение настоящих призов никак не связано с предоставлением паролей. Официальные награды приходят только через систему уведомлений игры (например, в игре Fortnite — через «Турниры»).

Нажав на подозрительную ссылку, можно заразить компьютер вирусом, потерять доступ к аккаунту или лишиться всех внутриигровых ценностей.

Модный приговор. Через Telegram распространяются схемы, связанные с якобы выгодными покупками с китайского маркетплейса Poizon. Подростку обещают выкуп брендовой одежды по низкой цене. Деньги уходят мошенникам на карту, но товар не приходит. Более того, жулики требуют оплату «пошлины», чтобы «растаможить товар».

Дроппинг. В переводе на русский — распыление похищенных средств по каплям. На банковскую карту подростка поступает перевод, которого он не ждал. Затем с ним связывается некий гражданин, говорит, что ошибся и просит вернуть деньги. Делать этого нельзя, иначе есть вероятность стать соучастником мошеннической схемы с отмыыванием денег или даже спонсированием терроризма. Возврат осуществляется только через банк, куда надо будет зайти вместе с родителями и написать заявление об отказе от непонятного перевода.

Рандеву у банкомата. Это тоже разновидность дроппинга, хотя «зачин» происходит в оффлайне. На подходе к банкомату подростка может подкараулить незнакомый человек, который попросит помочь ему срочно снять деньги, так как свою карту он забыл дома. Предложит воспользоваться вашей: мол, на нее родственник или друг этого незнакомца сейчас переведет деньги, а вы просто снимете наличность.

Опасность здесь многоплановая: жертва не только сообщит свои реквизиты третьему лицу для совершения перевода, но и может быть втянута в сложную цепочку вывода денег, полученных преступным путем.

Подработка на каникулах. Часто в интернете попадаются объявления о работе с обещанием «быстрого заработка». Мошенники рассылают информацию о вакансиях, доступных даже подросткам, через СМС или электронные письма. Условия заманчивые: для работы не требуется опыт и образование, удаленная работа с большой

зарплатой, нет четко прописанных обязанностей. Описание вакансии лаконично — «трехчасовой рабочий день в офисе с достойной оплатой», без подробностей. Но и гарантий того, что человек увидит свой заработок, в этом случае тоже нет, хотя реквизиты для получения оплаты он мошенникам оставит.

Из той же серии — вакансия «администратор лотереи», когда предлагается переводить выигрыш «победителям» через собственную карту. Это дроппинг чистой воды.

Как предотвратить обман ребенка в интернете?

Эксперты Альянса по защите детей в цифровой среде подготовили для родителей рекомендации, которые подскажут, как ребенку не попасться на удочку мошенников.

Осведомленность. Объясните ребенку, кто такие мошенники и какие у них бывают цели. Убедите на примерах из жизни, что нельзя сообщать незнакомым людям личные данные: ФИО, адрес, номер школы, номер телефона, пароли. Это основы кибербезопасности для детей.

Сопроотивление шантажу. Расскажите, в чем опасность предложений от незнакомцев «забрать приз», «помочь перевести деньги» или «передать подарок родителям». Поясните, на чем шантажист может подловить жертву, какие приемы психологического манипулирования он использует, как их вовремя распознать и пресечь.

Цифровая гигиена. Объясните, почему нельзя добавлять незнакомцев в друзья в соцсетях или мессенджерах.

Научите не отправлять фото или видео незнакомцам и не тратить деньги, поступившие на счет из непонятного источника.

Исключите «привязку» платежных средств к игровым аккаунтам.

Общение с незнакомцами. Правила безопасности в интернете для детей таковы:

Если знакомый по онлайн-игре предлагает встретиться в реальной жизни, это может быть опасно. Не надо ходить на такие встречи в одиночку, лучше взять с собой друзей или родителей.

Если незнакомец убеждает, что близкие люди попали в беду — перезвонить им и спросить, все ли у них в порядке.

Кодовые слова. Используйте секретное слово или фразу: если кто-то говорит «я от мамы», ребенок должен спросить пароль, о котором он с мамой условился. Например, «белеет парус одинокий».

Ролевые игры и тренировка. Инсценируйте разные ситуации:

Кто-то предлагает забрать из школы;

Кто-то пишет в чате «я друг твоего папы»;

Мошенник звонит и говорит, что с родителями случилось что-то плохое.

Пусть ребенок отрабатывает правильную реакцию: не верить, не паниковать, звонить вам. Критическое мышление пригодится и во взрослой жизни.

Защита аккаунта. Научите детей использовать сложные пароли для аккаунтов и никому их не сообщать.

Как создать надежный пароль:

- 1) Не применяйте очевидные комбинации вроде «12345» или «password»;
- 2) Добавьте спецсимволы и цифры: например, «FireDragon#2025» или «StarRoblox&25»;
- 3) Используйте фразу-пароль, к примеру, «ЯОбожаюСыр!» — такую комбинацию трудно взломать, а вот запомнить — проще простого.

Если аккаунтов несколько, к каждому желательно придумать отдельный пароль. Хранить пароли в смартфоне или в ноутбуке небезопасно: лучше записать их на бумаге и спрятать в тайнике. Там их хакеры точно не найдут.

Настройте родительский контроль на устройствах — это поможет ограничить доступ к нежелательным сайтам и приложениям. Используйте детские версии браузеров и включите безопасный поиск. Объясните ребенку, что нельзя делиться личной информацией, общаться с незнакомцами и переходить по подозрительным ссылкам.

Установите фильтры, блокирующие опасные сайты. Ограничьте время в соцсетях и настройте возрастные ограничения в приложениях. Регулярно проверяйте историю просмотров, но делайте это открыто — так ребенок поймет, что это не слежка, а забота.

Договоритесь о правилах: сколько времени можно проводить онлайн, какие сайты посещать. Используйте технические средства – например, настройки роутера, которые ограничивают доступ. Но главное — будьте в курсе интересов ребенка, чтобы он сам хотел делиться тем, что находит в интернете.

Источник:

<https://объясняем.рф/articles/useful/kak-zashchitit-detey-ot-moshennikov/>