

«Хочешь прокачать игровой аккаунт? Скажи данные карты родителей и коды от банка»

Дарья, Саранск

История о том, как игра дочки обошлась мне почти в полмиллиона рублей. Милане девять, и для своего возраста она очень рассудительная девочка, поэтому таких сюрпризов точно от нее не ждала.

В воскресенье я встала попозже, заглянула к дочке — она по планшету разговаривала с какой-то взрослой девушкой по видеосвязи. В руках у Миланы почему-то был мой смартфон, а на столе лежала моя банковская карта. Стоило мне появиться, собеседница мигом отключилась.

Попытка быстро узнать у дочери, что происходит, не принесла успеха. Я схватила свой телефон, зашла в приложение банка: 460 000 рублей, которые мы накопили на ремонт, ушли пятью переводами неизвестным людям. Тут же позвонила в банк, заблокировала онлайн-доступ к счетам, но переводы отменить не удалось.

Когда успокоилась, стала выяснять у Миланы, что же произошло. Оказалось, она пыталась заработать виртуальную валюту для онлайн-игры, которой увлеклась неделю назад. Игровые деньги нужны для покупки одежды своему персонажу, «усилителей» для перехода на новый уровень и многого другого. Я один раз пополняла ее счет в игре, но там была небольшая сумма.

Выяснилось, что Милана подписалась на канал фанатов этой игры и сегодня утром ей пришло сообщение от другой подписчицы. Она предложила поучаствовать в челлендже: выполняешь задания и взамен получаешь игровую валюту бесплатно. Дочка согласилась.

Сначала поручения были простые и относились только к игре. Например, зайти в игровой магазин и сделать скрин того, что хочешь купить. Потом они попросили дочку прислать мое фото. Затем нужно было раздобыть мой телефон и сделать снимки экрана. Милана знала пароль для разблокировки, так что выполнила и это задание. А заодно сообщила мой номер.

После этого «подруга по игре» объявила, что Милана прошла челлендж, и предложила созвониться по видеосвязи. Якобы так быстрее объяснить, как получить призовые деньги. Девушка сказала, что скинет деньги на мою карту, а уже оттуда их можно перевести в игру.

Милана взяла мою карту, продиктовала собеседнице все цифры с нее и сказала еще несколько кодов, которые пришли на мой телефон. Потом появилась я, девушка сбросила звонок, а вся переписка с ней тут же исчезла.

В банке мне сказали, что деньги не возвратят, потому что я нарушила правила безопасности — фактически из-за моей беспечности все секретные данные попали преступникам. Хочу предупредить других родителей, чтобы они были готовы к подобным историям и не потеряли деньги, как я.

Совет эксперта по противодействию мошенничеству:

Через онлайн-игры мошенники выходят на доверчивую аудиторию. Дети и подростки часто не задумываются о ценности денег, особенно когда речь идет о достижениях в любимой игре. И преступники используют этот азарт в своих целях. В частности, чтобы получить доступ к кошелькам родителей.

Обманщики ищут детей в чатах самой игры, в тематических каналах и сообществах, а затем переходят на личное общение в мессенджерах. Они обещают игрокам разные бонусы: атрибуты для персонажей, ключи активации для бесплатной установки платных игр, виртуальную валюту или даже реальные деньги. Чтобы получить приз, нужно выполнить задания, которые поначалу просты и связаны с игрой.

Когда участник втягивается, поручения аккуратно меняют вектор. Мошенников начинают интересовать вещи, которые помогут открыть им доступ к деньгам на картах родителей или самих детей. Задания могут быть крайне странными, совсем не связанными с игрой или реальной целью аферистов. Например, спрашивают, чем сейчас занимаются родители. Затем просят тайком их сфотографировать. С одной стороны, подогревают игровой азарт, с другой — проверяют, может ли ребенок завладеть родительским телефоном и картой.

В итоге преступники всегда подводят ребенка к тому, чтобы он выдал секретные данные: реквизиты карты, пароли от устройств и аккаунтов, коды из уведомлений.

Через дочь Дарьи аферисты узнали ее номер телефона и карты. По скринам смартфона поняли, какими банковскими приложениями она пользуется. Затем вошли в ее онлайн-банк, сменили пароль с помощью номера карты и кодов, которые продиктовала девочка, и перевели деньги на свои счета.

Некоторые банки блокируют вход в мобильное приложение или личный кабинет на сайте, если это происходит с нового устройства. Доступ открывают только после звонка сотрудника банка: он должен удостовериться, что именно сам клиент меняет пароль. Чтобы обойти такую защиту, иногда обманщики убеждают ребенка самого зайти в банковское приложение на телефоне родителей и перевести им деньги. Пошаговую инструкцию они дают по видеосвязи.

Чтобы не потерять деньги, соблюдайте правила финансовой безопасности и научите им ребенка:

- Ограничьте доступ к своему телефону. Например, установите вход по паролю или отпечатку пальца, если вы этого еще не сделали. Старайтесь никому не раскрывать свои пароли, в том числе детям.
- Объясните ребенку, что банковская карта — личная вещь, ее нельзя брать без разрешения. А данные, которые указаны на карте, и коды из сообщений банков дают доступ к банковским счетам. Если выдать эту информацию посторонним, они могут украсть все деньги.
- Расскажите, что существуют поддельные сайты и приложения. Если ввести там данные карты, это тоже грозит потерей сбережений.
- Предупредите ребенка о том, что преступники используют хитрые способы втереться в доверие. Например, заводят дружбу в социальных сетях, начинают общение в тематических каналах, а затем под разными предлогами выманивают секретную информацию.