

«Лови секретную ссылку, тут голда и шмот дешевле!»

Валя, Санкт-Петербург

Мы с ребятами из школы подсели на одну онлайн-игру, там можно общаться между собой и знакомиться с другими игроками. Игра сама по себе бесплатная, но чтобы быть наравне с топами, нужно платить за лучший шмот и пушки. В игре есть свой магазин, где все это можно купить.

Однажды мне написал в игровой чат какой-то парень, мы поболтали, и он по секрету скинул мне ссылку на неофициальный магазин, где можно гораздо дешевле купить тот же самый шмот и игровое золото. Он давно там закупается, все норм работает.

Я посмотрела, классный выбор, и правда дешевле. Выбрала интересные мне штуки, стала оплачивать и у меня сняли сразу 1000 рублей! А я набрала только на 130 рублей. Я быстро пишу этому парню, а он уже не отвечает.

Друг, который тоже играет, сказал, что это развод и что нельзя ничего покупать по левым ссылкам. Короче, я очень расстроилась, потому что мне мама эту тысячу переводила на новые наушники. Не знаю, как ей теперь об этом сказать.

Совет эксперта по противодействию мошенничеству:

Мошенник притворился участником игры и прислал в чат Вале ссылку на фишинговый сайт, замаскированный под страницу с объектами для игры.

Незнакомцем мог быть и не реальный человек, а чат-бот, которого хакеры создали для рассылки сообщений пользователям.

Иногда киберпреступникам удается распространять фишинговые ссылки через всплывающие баннеры в самой игре. Реклама обещает пользователям бесплатные предметы для игры или футболки, кепки, браслеты с лого или персонажами. Но в результате пользователи теряют доступ к своему аккаунту в игре, за который потом у них требуют выкуп.

Если вы, как и Валя, ввели данные банковской карты на мошенническом сайте, постарайтесь как можно скорее ее заблокировать. Например, позвоните по номеру горячей линии банка — он указан с обратной стороны карты — и следуйте инструкциям оператора.

Если карта оформлена на паспорт подростка, то он сможет самостоятельно получить новую перевыпущенную карту в банке. Если же карта привязана к счету родителей, то забрать новую в офисе смогут только они. Подробнее о том, как это сделать, можно узнать из текста «Банковские карты для детей».

Чтобы обезопасить свои деньги от мошенников, важно следовать правилам финансовой безопасности:

Никому ни под каким предлогом не сообщайте данные банковской карты, включая трехзначный код с обратной стороны, а также ПИН-коды и пароли из сообщений от банка.

Прежде чем совершать покупку в интернете, всегда проверяйте, безопасен ли сайт. Подробнее о том, как распознать мошенническую страницу, читайте в тексте «Фишинг: что это и как от него защититься».

Подключите СМС или push-оповещения по всем карточным операциям, чтобы сразу узнавать о подозрительных транзакциях.

Установите антивирус на всех гаджетах, которыми пользуетесь.

Не храните много денег на карте, которой регулярно расплачиваетесь в интернете. Лучше завести отдельную карту для онлайн-покупок и каждый раз переводить на нее нужную сумму. Родители могут ограничить сумму или количество списаний с детской карты.