

В последние годы мошенничество с банковскими картами и мобильными телефонами прочно вошли в нашу жизнь. Стоило появиться играм, предполагающим какие-либо правила, как сразу же нашлись те, для кого выигрыш был важнее честности. Мошенники хорошо знают: любую игру, даже на интерес, человек начинает либо чтобы выиграть, либо чтобы почувствовать себя самым сильным и крутым. А учитывая, что деньги в современных онлайн-играх зачастую вполне реальные, это огромное поле для «деятельности» злоумышленников.

Рассказываем, как, просто играя в интернете в бродилку, ферму, аркаду или РПГ, можно потерять свои деньги.

Главная цель мошенников, которые действуют в сфере игр – подростки. У многих из них уже есть банковские карты, а опыта недостаточно. К тому же если подростку чего-то очень захотелось, его легче убедить предоставить доступ к средствам своих родителей.

В онлайн-играх присутствуют все типы мошенничества, характерные в целом для интернета. Это заманивание пользователей на фишинговые сайты и кража их персональных и платёжных данных, выманивание кодов из СМС, установка вредоносного ПО под видом приложений или дополнений, помогающих в игре, получение доступа к конфиденциальной информации, кража аккаунтов и вымогательство денег за возврат либо получение возможности связи с игровой командой.

Здесь эта опасность даже серьёзнее, чем в соцсетях: в командных играх порой зарождается реальная дружба, возникает «чувство локтя», а возможность коммуникаций зачастую ограничена. Стандартный совет на случай, если кто-то просит о помощи, связаться с ним по другому каналу и уточнить, он ли это, в играх зачастую невыполним.

Сравнительно новая схема в играх связана с предоставлением возможности доната (оплаты игровых товаров реальными деньгами) в играх производителей, которые покинули российский рынок. Сами игры чаще всего доступны, а вот возможность ускоренной прокачки – нет. Разработчики в этом случае действуют себе в убыток, а мошенники этим пользуются. Порой они выманивают крупные суммы.

Значит ли это, что немедленно нужно бросать играть самим и строго запретить такой досуг детям? Разумеется, нет. А вот внимательно изучить самим и объяснить детям правила безопасного поведения в интернете – необходимо.

Сотрудники Отделения МВД России по Шенталинскому району напоминают:

- Нельзя скачивать на компьютер или смартфон неизвестные программы, особенно – якобы дающие доступ к ушедшим из России интернет-ресурсам. В большинстве случаев это программы, крадущие данные или даже перехватывающие контроль над устройством.
- Не устанавливайте расширений для браузеров, облегчающих игровой процесс: они могут навредить точно так же.
- Если вы приняли решение или разрешили ребенку покупать игровые ресурсы за реальные деньги, для расчетов используйте только виртуальную карту с ограниченным лимитом трат!
- Коды из СМС нельзя передавать никому. Вводить их самостоятельно можно только на официальных сайтах. Внимательно оцените функционал сайта, прочтите по символам его адрес, убедитесь, что это не подделка!
- Нельзя вводить коды из СМС на непонятных сайтах, особенно если они созданы недавно. Проверить дату создания можно с помощью сервиса Whois.
- Внимательно читайте содержание СМС: там указывается, куда именно идет платёж, его сумма, указывается, что это – списание средств. Последнее важно, когда обманутый человек пытается вернуть деньги за услугу, которую не получил. Мошенники в таком случае часто требуют назвать код и под видом возврата производят списание денег.
- Не передавайте никому пароли от аккаунта, особенно если он привязан к соцсетям. Если вы по какой-то причине нарушили это правило, смените пароль как можно быстрее.

- Выбрав игру, доступную в соцсетях, заведите для неё отдельный аккаунт и максимально защитите его (например, с помощью двухфакторной аутентификации – подтверждения входа через код в СМС).
- Не покупайте игровые аккаунты с рук

Если против Вас совершены мошеннические действия, незамедлительно звоните в дежурную часть ОМВД России по Шенталинскому району по номеру телефона: 8 (84652) 2-10-06.

Отделени МВД России по Шенталинскому району