Мошенники стали чаще атаковать российских геймеров. Они заманивают онлайн-игроков на фишинговые сайты под видом распродажи популярных игр. «Известия» выяснили, какие схемы чаще всего используют киберпреступники и как любителям игр защитить свои аккаунты, данные и деньги.

Всплеск атак

Всплеск активности мошенников эксперты заметили в мае. Киберпреступники стали создавать много фейковых магазинов с играми, которые якобы продаются с большими скидками, аккаунтами к ним и коллекционными предметами, рассказали в банке ВТБ.

Такие сайты мошенники продвигают через SMS-рассылки, чаты в мессенджерах и поисковые системы. После того как доверчивые игроки переходят по ссылке, их просят ввести данные карты на сайте (якобы для покупки товара), а по факту деньги уходят преступникам.

Помимо денег и данных карт, мошенников интересуют номера телефонов, данные паспортов и СНИЛС. Они обычно используются в рамках социальной инженерии.

Почему мошенники выбирают геймеров

Специалист по информационной защите компании «Код безопасности» Мария Фесенко называет геймеров идеальной мишенью для кибермошенников. Дело в том, что главная задача таких преступников — сделать так, чтобы у жертвы не возникло никаких подозрений. Для этого они всячески пытаются отвлечь ее внимание, заставляя совершать необдуманные действия (срочно купить что-то со скидкой или, например, попробовать бесплатную версию ChatGPT).

— У геймеров в этом плане изначально ослаблен «фокус», потому что многие вместо того, чтобы купить игру легально,

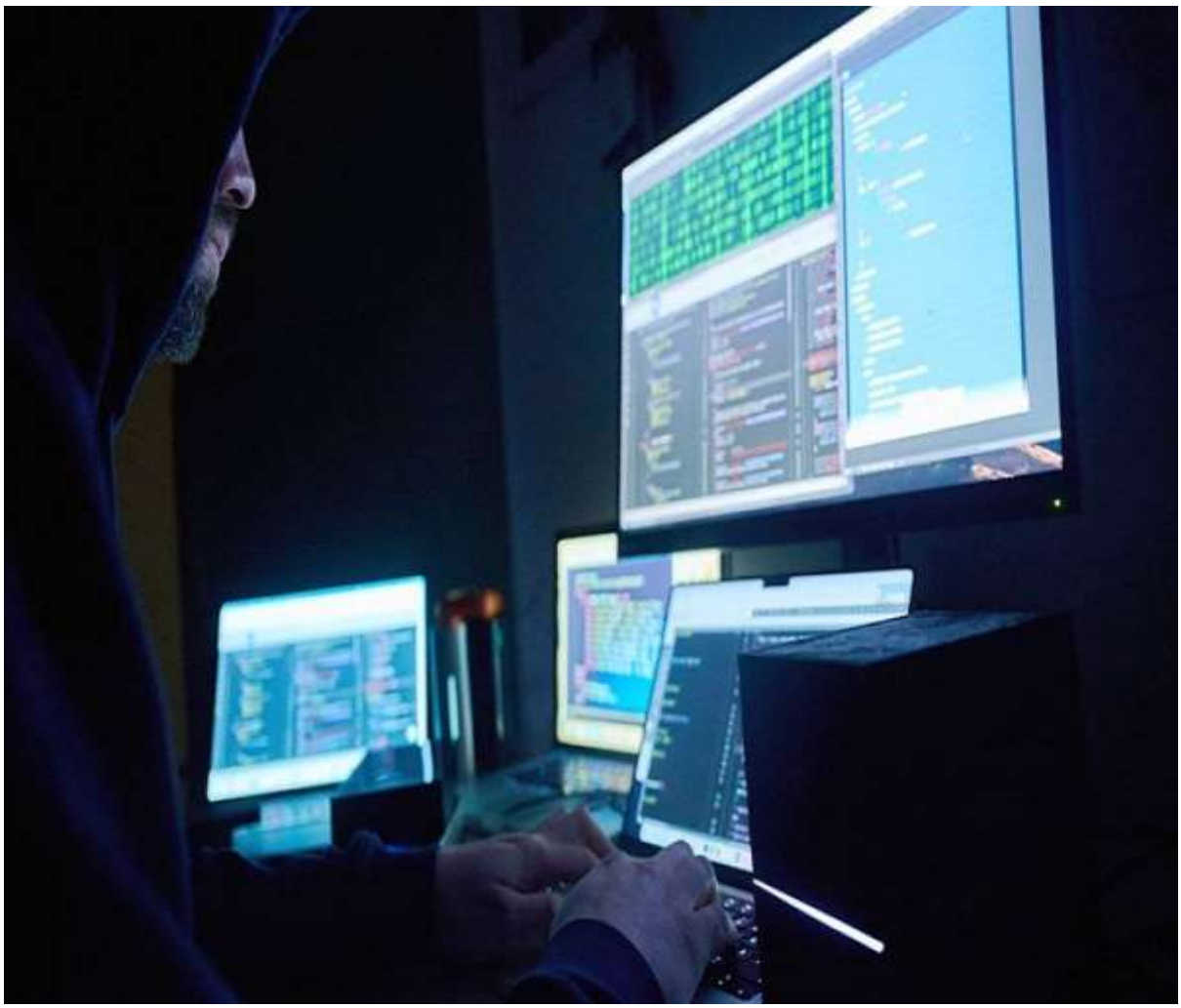
ищут ее «кряки» на различных сайтах. По сути, они сами приходят в «сети», и мошенникам остается лишь подобрать грамотный способ, чтобы пользователь ввел данные своей карты на фишинговом сайте (например, с помощью того же варианта «до конца акции остался час») или перешел по ссылке, откуда на его компьютер автоматически скачается вредоносное ПО, — говорит собеседница «Известий».

Мал мала больше: названы самые опасные схемы мошенничества против детей

Банки дали советы о том, как защитить подростков от обмана

При этом она добавляет, что «кряки», то есть версии игры, в которых ключ активации уже вшит «пиратами», опасны сами по себе. Во-первых, в них может быть вредоносное ПО, а во-вторых, при их установке часто требуется отключить антивирус, что снижает защищенность системы.

По словам преподавателя кафедры киберспорта факультета игровой индустрии и киберспорта университета «Синергия», кандидата педагогических наук Алексея Ермакова, в последнее время с возникшими ограничениями на покупку игр в России в интернете появилось много «помощников», готовых решить эту проблему.



— Естественно, что среди них есть те, кто пытается обманом завладеть деньгами доверчивых игроков. Защитить себя в такой ситуации не так уж сложно: нужно каждый раз спрашивать себя, насколько ваши действия надежны и безопасны и нужна ли вам сделка на самом деле, — советует эксперт.

Геймерские схемы

Самая популярная схема, которую используют хакеры в отношении геймеров, — это сайты, на которых пользователь якобы может скачать популярную игру бесплатно. Но в итоге человек платит гораздо больше, чем она стоит — ведь, вводя свои данные, геймер дает злоумышленникам доступ к личному кабинету, говорит Мария Фесенко.

Малыш на миллион: мошенники придумали новые схемы обмана игроманов

Как подросток-геймер в Москве отдал злоумышленникам 2,5 млн рублей

— Часто на фишинговых сайтах пользователь может скачать вместо игры вредоносное ПО, которое обладает самыми разными функциями: от считывания нажатия клавиш клавиатуры до кражи паролей из браузера, — рассказывает она.

Есть и другие махинации с геймерским уклоном, которые скорее относятся к фишингу. Например, когда мошенники создают копию сайта известного киберспортивного турнира, присылают приглашения игрокам на регистрацию и затем крадут их учетные данные.

— Пользуется популярностью и стандартная социальная инженерия, только в случае с геймерами мошенники прикидываются службой поддержки игрового портала или игры. Они присылают письма на почту игрока и под разными предлогами пытаются выманить пароль от аккаунта или опять же заставить ввести данные банковской карточки. Такие письма выглядят весьма убедительно — на них есть и официальные логотипы, и типичное оформление, — говорит собеседница «Известий».

Впрочем, по ее словам, иногда используются и совсем простые методы социнжинерии, на которые могут клюнуть новички: человеку пишет некто с просьбой дать данные учетные записи, чтобы с помощью некоего бага сгенерировать большое количество игровой валюты. После того как жертва дает данные, «учетку» просто крадут.

В пылу азарта: хакеры атакуют любителей играть на смартфонах

Как распознать нечестных геймеров или мошенников в мобильных приложениях

— Такая кража — очень популярный ход у мошенников, — отмечает Алексей Ермаков. — Когда игроку не хватает терпения и способностей самому развивать аккаунт, он передает его в управление другому лицу, которое, как предполагается, будет опытным игроком и сможет легко достичь требуемого высокого уровня. А в итоге доверчивый любитель игр лишается всего и вынужден покупать новый доступ.

Еще один оригинальный способ обмана геймеров связан с платформой YouTube. Мошенники загружают туда видео с инструкцией взлома различных игр, а в описание добавляют ссылку на скачивание «необходимых для взлома программ». Ссылка действительно ведет на страницу, где можно скачать архив, однако в нем содержится вредоносное ПО.

Кто чаще становится жертвами

По данным исследования «Лаборатории Касперского», с мошенничеством, связанным со взломом аккаунта, в России сталкивался каждый пятый любитель игр. Жертвами обмана

становятся и взрослые, и дети: последние более склонны доверять интернет-знакомым и заходить на фишинговые страницы, просто потому что у них нет личных средств на покупку игр. С другой стороны, взрослые тоже часто ищут «пиратские» пути, поэтому заражают свои устройства вредоносным ПО.

Для того чтобы защитить себя от кибермошенников, Мария Фесенко советует покупать игры только в официальных магазинах. Что касается социнженерии — важно помнить о том, что никогда нельзя вводить свои конфиденциальные данные — и логины-пароли, и банковские — на сайтах, на которые привела ссылка из некоего письма, поста в Telegram или YouTube-видео.
Бесплатные игры, инструкции по взлому, «кряки» тоже могут быть уловками, которые потенциально ведут к заражению ПК.

— Также вы можете пассивно защитить свои игровые и любые другие аккаунты с помощью сильного пароля. Он должен иметь 11 и более знаков, среди которых есть буквы разного регистра, цифры и обязательно спецсимволы, например %, №, $. Пароли для аккаунтов должны быть разными. Кроме того, нужно

добавлять двухфакторную аутентификацию там, где это возможно, — говорит собеседница «Известий».

Секс, ложь и видео: в полиции фиксируют рост киберпреступности

Основные криминальные тренды цифровой сферы — телефонный обман и эпистолярное вымогательство

Как защитить ребенка

Говоря о том, как защитить ребенка, эксперты призывают родителей чаще интересоваться, в какие игры он играет и какие риски это может нести. В случае с маленькими детьми можно установить на ПК функцию «родительского контроля», чтобы система блокировала попытки захода на определенные сайты.
— Кроме того, необходимо обучать ребенка кибергигиене: не переходить по ссылкам, присланным от друзей из Сети, из неизвестных ТГ-каналов и других источников, не вводить данные учетной записи или любую другую конфиденциальную информацию без ведома родителей, не скачивать моды или обновления, если они неофициальные. Кстати, сегодня существует множество курсов по кибергигиене, которые

оформлены в виде игры или мультиков, — говорит Мария Фесенко.

Взрослым стоит защитить детский компьютер техническими средствами, например антивирусом, который способен заблокировать большинство угроз и не позволит установить вредоносную программу.