**Основные опасности в онлайн-играх**

1. Кража персональных данных - пожалуй, самый распространенный вид онлайн-мошенничества.
2. Кража денег: игровая валюта, предметы игры и настоящие деньги в виртуальном кошельке - основной интерес мошенников. Специалисты предупреждают, что для геймера риск подвергнуться мошенничеству наиболее высок, когда он открывает счет для оплаты, без чего нередко многие игры вообще не «запускаются». 48% случаев мошенничества приходится как раз в момент оплаты.
3. Кража аккаунта: украв аккаунт, мошенники начинают шантажировать пользователя, требовать деньги за возврат аккаунта.
4. Вредоносное программное обеспечение. Например, пользователю предлагается скачать плагин для какой-то игры. Не подозревая подвоха, он переходит по ссылке на другой сайт, где запущено вредоносное программное обеспечение. Цель такого ПО - нанести ущерб безопасности и конфиденциальности устройства пользователя. Кроме того, в файлы игры могут быть встроены вирусы, и по незнанию пользователь может впустить их в свою систему во время установки.
5. Нарушение приватности. Сопоставив данные, полученные из игр и других источников, злоумышленники могут получить доступ к другим вашим учетным записям, например, в социальных сетях, а также зарегистрировать на ваше имя новые учетные записи или даже создать цифровые личности.

6) Скрытые сборы. Некоторые онлайн-игры выпускаются в условно бесплатной версии: часть контента предоставляется бесплатно, а для получения доступа ко всем возможностям и функциям необходимо заплатить. Для этого необходимо привязать банковскую карту к своей учетной записи, и оплата будет автоматически списываться с карты при покупке пользователем новых предметов или услуг. Самые распространенные мошеннические схемы:

1. Перенаправление игроков на фейковые сайты, которые, как правило, выглядят, как настоящие сайты для покупки аддонов (экипировки, силы, новых способностей и прочее) и игровой валюты. На самом деле основная цель этих сайтов, как и любых фишинговых, - обманом заставить пользователя перевести деньги за товар, который он никогда не получит.
2. Атаки на IP-адреса игроков (уникальные адреса пользователя в интернете), узнав который, мошенники могут вычислить ваш фактический адрес, имя, фамилию и другую закрытую личную информацию. Имея эти данные, они могут украсть вашу финансовую информацию или игровые учетные данные.
3. Фишинговые рассылки, цель которых - обманом выведать у пользователя данные его учетной записи. Мошенники могут рассылать игрокам письма по электронной почте о необходимости подтвердить свои данные для входа в систему. Переходя по ссылке из такого письма, игроки попадают на поддельную страницу входа в систему, где их просят ввести текущий пароль и имя пользователя. В итоге учетные данные оказываются в руках мошенников.

А могут и направляться ссылки на вредоносное ПО, причем самым разнообразным способом:

* на форуме игроков (публикуются ссылки на вредоносную программу под видом ссылки на патч игры);
* в самой игре (проводятся рассылки ссылок на вредоносную программу под видом «нового патча»);
* по электронной почте (рассылается спам с самой вредоносной программой либо со ссылками на нее);
* вредоносные программы распространяются через файлообменные сети;
* используются уязвимости веб-браузеров (для загрузки вредоносных программ при посещении игровых сайтов.)
* чаще всего злоумышленники публикуют на игровом форуме или в игре ссылки на вредоносную программу с заманчивыми комментариями.

4. Поддельные мобильные версии популярных онлайн-игр. После загрузки
такие приложения устанавливают вредоносное ПО на смартфоны или
компьютеры жертв. Мошенники используют такое ПО для перехвата данных
учетных записей, используемых для совершения покупок на популярных
игровых платформах и приставках. Далее эти данные используются для кражи конфиденциальной информации пользователя, включая данные банковской карты, домашнего адреса и номера телефона.

Основные правила безопасности в онлайн-играх

Для совершения любых игровых покупок пользуйтесь только официальными сайтами, при этом внимательно проверяя доменное имя сайта, так как мошенники часто используют созвучные с брендом доменные имена.

Узнавая о новой возможности в игре или приложении не из официального источника, поищите больше информации по этой теме. Чаще всего уже есть люди, которые с этим сталкивались и поделились своим положительным или отрицательным опытом.

Ищите и проверяйте информацию об акциях и выгодных предложениях на официальных источниках или у официальных представителей.

Никогда не переходите по ссылкам, ведущим на сторонние сайты.

Не отвечайте на электронные письма или запросы на переписку, в которых вас просят указать банковские, финансовые или персональные данные, даже если вам кажется, что сообщение отправлено от игровой платформы. Настоящая компания не будет запрашивать у вас информацию через сообщения.

Не делитесь персональной информацией, не передавайте данные учетной записи по интернету. Не пересылайте ваши учетные данные даже друзьям.

Используйте надежный пароль для входа в игру и никогда не используйте один и тот же пароль для нескольких учетных записей.

Не забывайте о двухфакторной аутентификации. Она надежнее защищает вас и усложняет злоумышленникам задачу.

Не забывайте регулярно обновлять антивирусное ПО.

Одним из способов защиты может быть VPN (Virtual Private Network, виртуальная частная сеть). Она делает ваше интернет-соединение приватным. VPN-приложения легко устанавливаются, не требуют сложной настройки и обладают рядом преимуществ:

* защищают от атак, например, DDoS, которые могут предприниматься против соперников в онлайн-играх, особенно в случае конкурентной борьбы;
* обеспечивают дополнительную безопасность при передаче данных и совершении банковских операций, поскольку VPN-соединение невозможно отследить.

Некоторые VPN-приложения распространяются бесплатно, однако они могут ограничивать передачу данных и не обеспечивать полноценную безопасность. Перед тем как выбрать VPN, нужно четко понимать, на что будет распространяться его защита. Для этого ознакомьтесь с условиями предоставления услуг, в том числе с политикой конфиденциальности. Несмотря на то что некоторые VPN-сервисы обещают защищать вас от вредоносного ПО и фишинговых сайтов, они не гарантируют такого же уровня защиты, какой дает самостоятельный антивирус, поэтому оптимальный вариант - иметь и то, и другое.