Основные виды мошенничества

1. Подставной оффер

Мошенники отправляют сообщения (спам) с предложением купить внутриигровой товар дешевле чем в официальном магазине, выдавая себя за настоящие видеоигровые компании или партнеров, например, Steam, Roblox, Minecraft, и тд.

2. Фишинг

Мошенники отправляют пользователю сообщение с вопросом «Это твой профиль?» и ссылкой на фальшивый сайт, похожий на Steam. Кликнув на ссылку, пользователь попадает на поддельную страницу, где его просят ввести логин и пароль.

! Важно всегда проверять адрес сайта и не вводить свои данные на подозрительных ресурсах.

3. Скам

Мошенники могут сначала завоевать доверие, предлагая купить, например, скин, или прокачать аккаунт, азатем просто отобрать его. Мошенники используют расширения для браузеров, которые показывают ложную информацию, чтобы обмануть пользователей.

4. Ложные страницы видеоигр

Мошенники создают поддельную страницу на платформе видеоигр, которая выглядит точно так же, как страница популярной игры (продажа поддельных копий, кодов пополнения, продажи игровой валюты и тд).

Общие правила безопасности

1 Защита устройств

Антивирус + фаерволл:

- Установите антивирус от проверенных производителей (Kaspersky, ESET). Он блокирует вирусы, трояны и фишинг-сайты.
- Фаерволл контролирует, какие приложения могут выходить в интернет, предотвращая утечки данных.

Обновления ПО:

- Регулярно обновляйте ОС и приложения (браузеры, игры). Доработки часто закрывают уязвимости, которые используют мошенники.

2 Пароли

Правила составления:

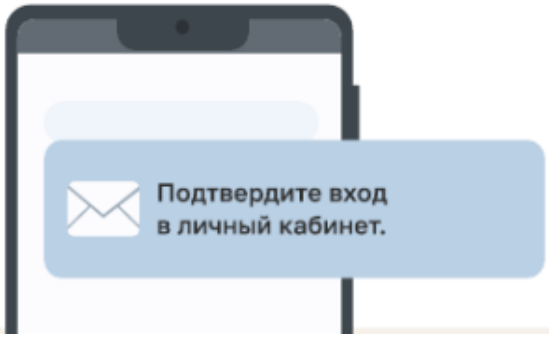
- **Сложность:** Минимум 12 символов, буквы (верхний/нижний регистр), цифры, спецсимволы (например: Kl#5x9&vP@z!L7).
- **Уникальность:** Для каждого сервиса (почта, соцсети, банк) — свой пароль.
- **Обновление:** Меняйте пароли каждые 3–6 месяцев.

Хранение паролей:

- **Нельзя:** Сохранять в заметках, браузере, файлах с названиями Пароли_2024.txt или Мои_данные.doc — их легко взломают.
- **Можно:** Используйте менеджеры паролей. Они шифруют данные и генерируют сложные комбинации автоматически.

3 2FA (двухфакторная аутентификация)

Двухфакторная аутентификация — это защита аккаунта с помощью двух факторов: пароля и дополнительного кода (из СМС или приложения).



4 Поведение в сети

Не кликайте:

- На сообщения с подозрительными темами («Ваш аккаунт заблокирован!», «Видео с вами»).
- На ссылки в письмах, даже если они пришли «от банка» — проверяйте через официальное приложение.

Не скачивайте:

- Файлы с расширениями .exe, .bat, .js от незнакомцев (с читами, дополнениями, подключениями к серверам и т. д.).
- Документы (Word, Excel) с макросами — они могут запускать вредоносный код.

Акции и розыгрыши:

- «Скидка 90% на PlayStation» — требуют ввести данные карты.
- «Бесплатная игра» — выманивают логин/пароль от Steam.

Правда: Официальные акции всегда есть на сайте сервиса, а не в личных сообщениях.

Дополнительные меры безопасности

Читы и внешние программы

Риски: читы, трейнеры и другие внешние программы могут внедрить вирусы на ваш компьютер.

Совет: откажитесь от использования таких программ, даже если они обещают лёгкие преимущества в игре.

Безопасные способы оплаты

Избегайте банковских карт: не пользуйтесь банковскими картами для покупок в играх и не сохраняйте их данные, проверяйте сумму для списания.

Используйте веб-кошельки: оплачивайте через разнообразные сервисы, такие как PayPal или российские «ЮMoney».

Осторожность с внутриигровыми операциями

Торговля предметами: разработчики осуществляют торговлю внутриигровыми предметами на своих сайтах, но в сети много независим площадок.

Риски: виртуальные транзакции могут оказаться обманом, и вы можете потерять реальные деньги, покупая украденные предметы.

Совет: не ввязывайтесь в торговлю внутриигровыми предметами за реальные деньги, особенно если вы новичок.
Не соглашайтесь на предложения, которые слишком хороши, даже если они по вашему мнению очень похожи на правду