

Фейковые сайты онлайн-покупок

Мошенники создают поддельные сайты продажи виртуального инвентаря для онлайн-игр: персонажей, одежды, предметов и т.п.

Если ввести на таком сайте реквизиты карты, то можно потерять деньги.

А если ввести пароль своего игрового аккаунта или соцсети, то мошенники и их могут украсть.



Совет №1

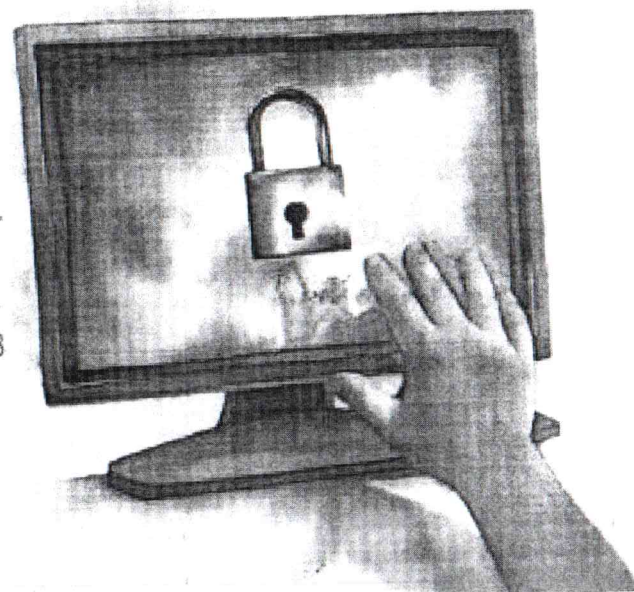
Научите ребёнка правилам безопасности для виртуальных покупок

Не переходить по ссылкам на незнакомые сайты.

Не вводить на незнакомых сайтах пароли от игр, соцсетей, реквизиты карты и коды из sms.

Покупать виртуальные
товары только
в официальных приложениях.

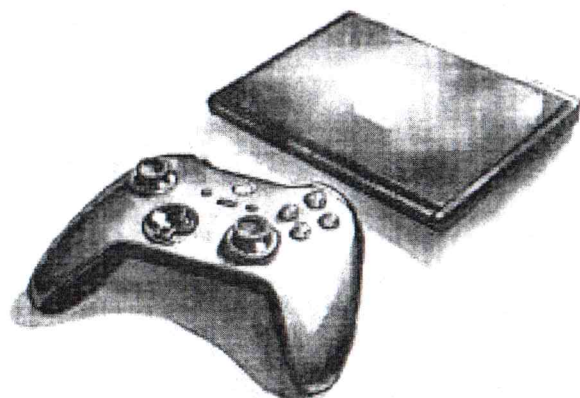
Не оплачивать покупки через
боты в соцсетях.



Совет №2

**Объясните детям, что обещания
лёгких денег — это всегда тревожный знак**

Если ребёнку необходимы деньги на покупку дорогой вещи, то расскажите ему, как он может сам накопить нужную сумму.



Если копить придется долго, посоветуйте положить деньги на вклад или накопительный счёт, чтобы получать проценты на свои сбережения.

Совет №3

Поговорите с подростком об опасностях дропперства

Нельзя никому передавать свою карту
или её реквизиты.

Если незнакомец прислал ребёнку
деньги якобы «по ошибке»
и просит перевести их,
этого делать нельзя!

Родители должны обратиться
в банк, чтобы тот вернул
сумму отправителю.

За дропперство предусмотрена
уголовная ответственность!



Совет №4

Помогите ребёнку усвоить правила кибергигиены

Прежде чем выполнять просьбы «друга», лучше позвонить ему. Скорее всего, он не в курсе переписки.

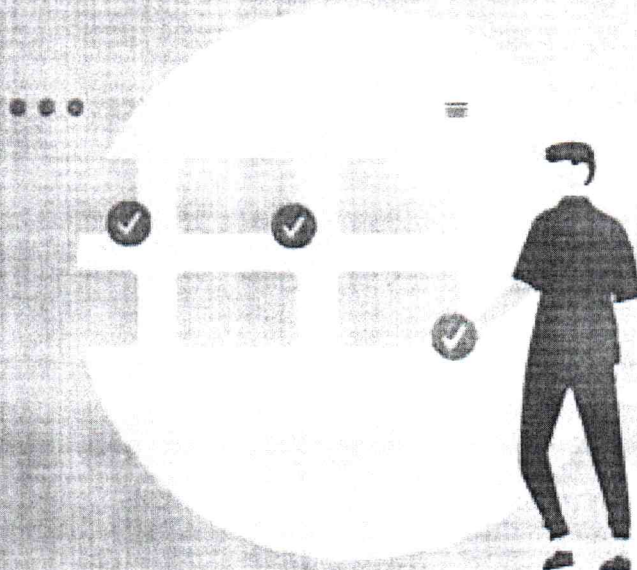
Защититься от вредоносных ссылок помогут антивирусные приложения. Не забывайте обновлять их.

Для безопасности маленьких детей можно настроить программы родительского контроля.



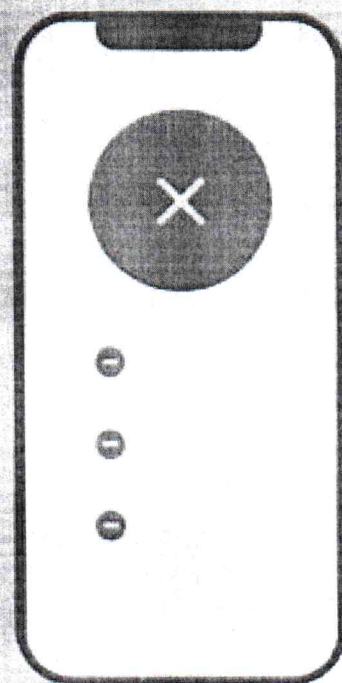
Безопасный способ удостовериться
в действительности информации –
самостоятельно позвонить в организацию,
сотрудником которой представился звонящий.

Официальные контакты есть на её сайте.



Не доверяйте звонкам и сообщениям
с незнакомых номеров.

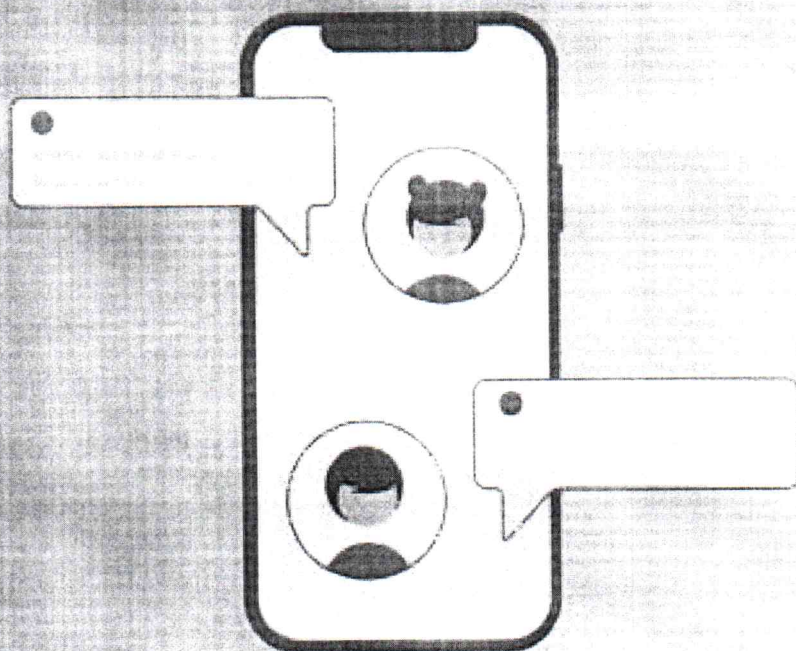
Не совершайте никакие
банковские операции
по просьбе или
указанию других.



Аферисты пишут людям якобы
от имени их начальника.

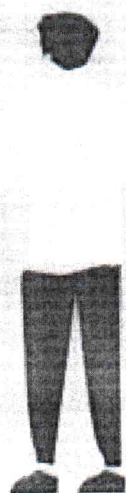
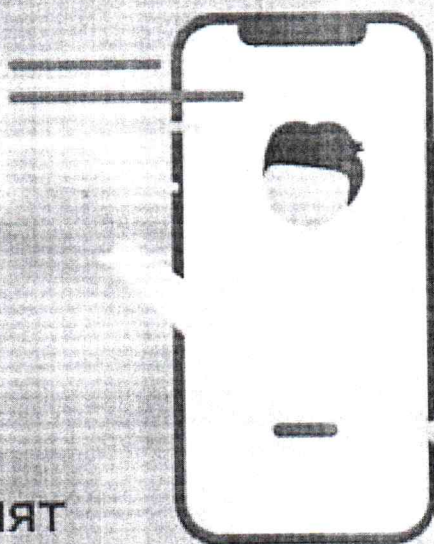
Чтобы вызвать доверие,
лжеруководитель обращается
в переписке по имени и отчеству.

А ещё могут писать
работникам
других ведомств.

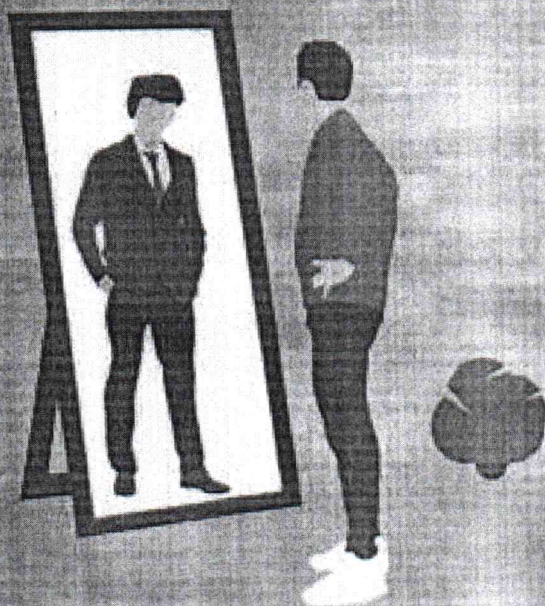


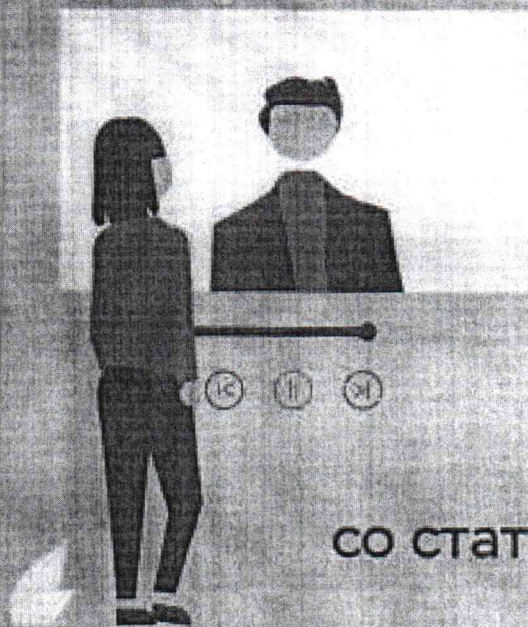
Затем обманщики звонят с неизвестного номера и пытаются узнать **конфиденциальную информацию**, позволяющую получить доступ к деньгам и похитить их.

Аферисты пользуются тем, что лжена начальнику доверяют и боятся отказать в просьбе.



Мошенники создают
поддельные аккаунты
в мессенджерах, выдавая себя
за руководителей министерств,
ведомств и других организаций.



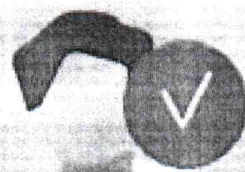


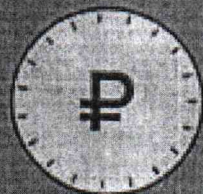
Поддельный аккаунт заводят на имя человека со статусом и **высокой должностью**. Для убедительности используют его фотографию.

Данные легко находят в открытом доступе в Интернете.

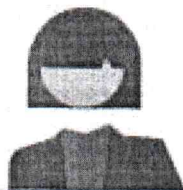
Кем бы ни представлялись незнакомцы,
не сообщайте им:

- паспортные данные;
- данные банковской карты;
- коды из СМС-сообщений;
- логины и пароли от своих
аккаунтов, в том числе
для входа в интернет-банк.

A stylized illustration of a login form. It features two horizontal lines for input fields, one for a username or email and one for a password. The form is enclosed in a rounded rectangle with a small menu icon (three dots) in the top right corner.



Финансовая
культура



ФАЛЬШИВЫЕ АККАУНТЫ

Мошенники под видом руководителя сообщают, что **поступит звонок** из профильного ведомства.

Рекомендуют действовать по инструкции звонящего и никому не рассказывать об этом разговоре.

