

KASPERSKY®

# Онлайн мошенничество

KASPERSKY®

**Что такое онлайн  
мошенничество?**

# Онлайн мошенничество

Онлайн мошенничество— это действия киберпреступников, направленные на овладение информационными данными или финансовыми средствами пользователя сети Интернет

Категории онлайн-мошенничества:

- **Фишинг.** С его помощью кибермошенники пытаются выманить у человека конфиденциальные данные или вынудить его на какие-либо нежелательные действия. С этой целью злоумышленники используют мгновенные и почтовые сообщения и специально созданные поддельные веб-сайты
- **Кража личности.** Незаконное использование чужих персональных данных для получения выгоды

# Каналы распространения

- Почта
- Whatsapp
- Twitter, Instagram
- Facebook
- Поисковая выдача

The image shows a Google search result for 'sparkster ico'. The search bar contains the text 'sparkster ico'. Below the search bar, there are tabs for 'All', 'Images', 'Videos', 'News', 'Shopping', and 'More'. The search results show 'About 31,400 results (0.40 seconds)'. The first result is an advertisement for 'Sparkster presale finished | Main sale live now | sparkster.be'. The ad text includes 'Ad www.sparkster.be/', 'Hurry up to get a 15% discount. Only today 1 Spark = 0.12\$', 'View Pricing · Sign Up Online', and a list of links: 'Highlights: Creating Innovative Solutions, Free Individual License Available', 'Contact Us · View Technology · About Us · Solutions Offered · Meet Our Team · Pricing Information'.

Below the search results is a Facebook post. The post features an image of several Russian 500 Ruble banknotes. The text on the image reads 'Получи денежное вознаграждение за 6 вопросов!'. The post is from 'MIKKTORINA.TILDA.WS' and has the text 'Жмите Подробнее'. There is a 'Learn More' button. The post has 2 likes and 1 comment. At the bottom of the post are icons for 'Like', 'Comment', and 'Share'.

# Онлайн угрозы

# Случай 1: Фишинг

Эта схема проста, но наиболее результативна, так как рассчитана на невнимательность и неосведомленность пользователей

Официальные домены Steam – steamcommunity.com и steampowered.com. Мошенники регистрируют очень похожие домены для усыпления бдительности жертвы. К примеру:

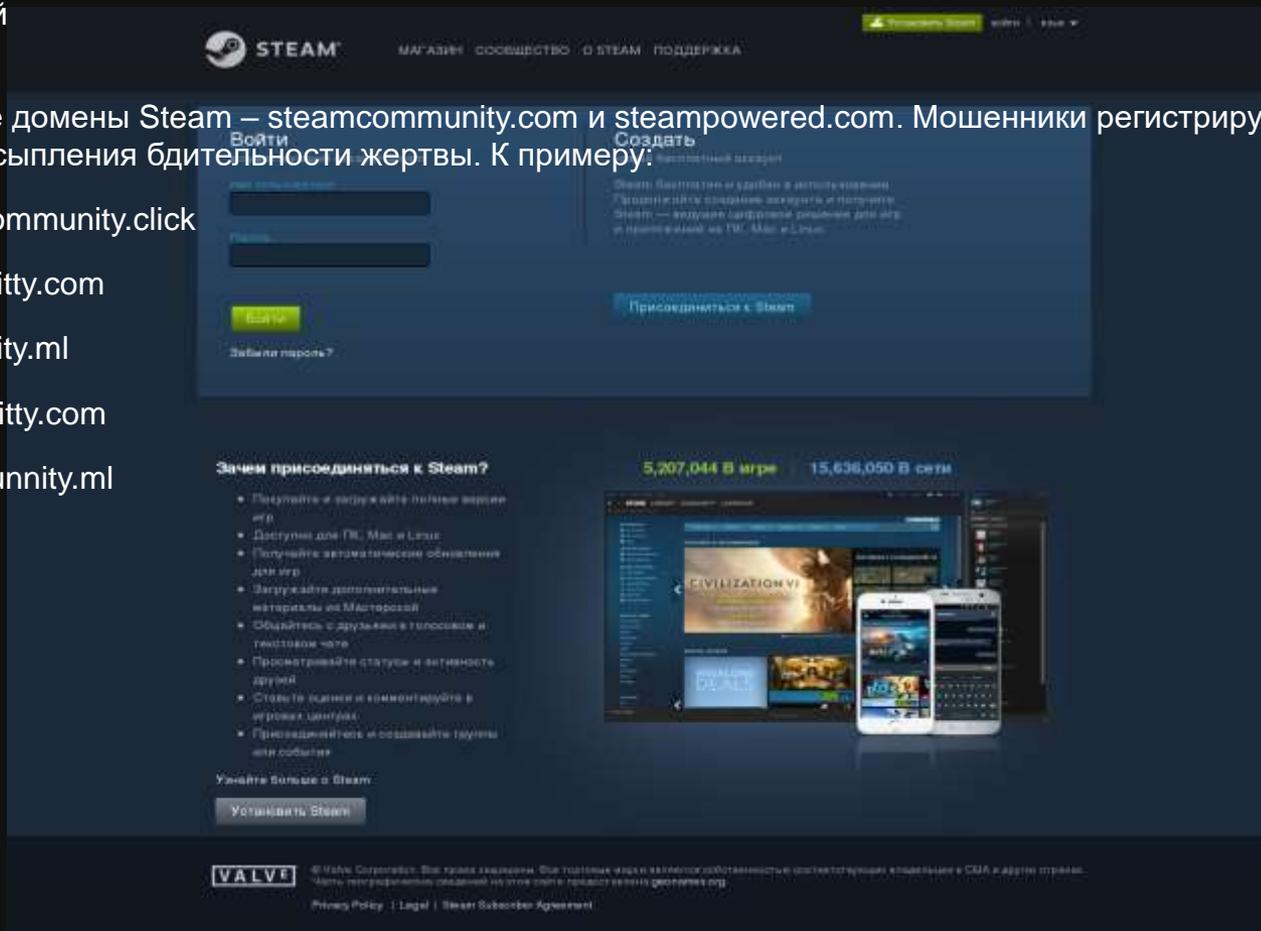
steam.stearncommunity.click

steamcammunnitty.com

steamcammunity.ml

steamcamrnunnitty.com

steamcommunnitty.ml



## Случай 2: Продажа/розыгрыш невалидных ключей

В Сети огромное количество магазинов, предлагающих приобрести ключи. Покупка ключа – это всегда кот в мешке, до момента активации невозможно узнать, рабочий он или нет. Здесь можно рассчитывать только на добросовестность продавца. Часто пользователи в погоне за новой игрой и привлекательным ценником забывают простые правила безопасности и приобретают ключи на сомнительных площадках

The screenshot shows a website interface for selling Steam keys. A modal window titled "Оплата товара" (Payment of goods) is open, displaying the following information:

- Название: Случайный Steam ключ «Золотой» (Name: Random Steam key «Gold»)
- Ваш email: [Input field: Введите Email адрес для доставки товара] (Your email: [Input field: Enter email address for delivery of goods])
- Купон: [Input field: Если есть] (Coupon: [Input field: If any])
- К оплате: 60 руб. (Amount to pay: 60 rub.)
- Согласен с Правилами и Условиями (Agree with Terms and Conditions)
- ОПЛАТИТЬ И ИГРАТЬ (PAY AND PLAY)

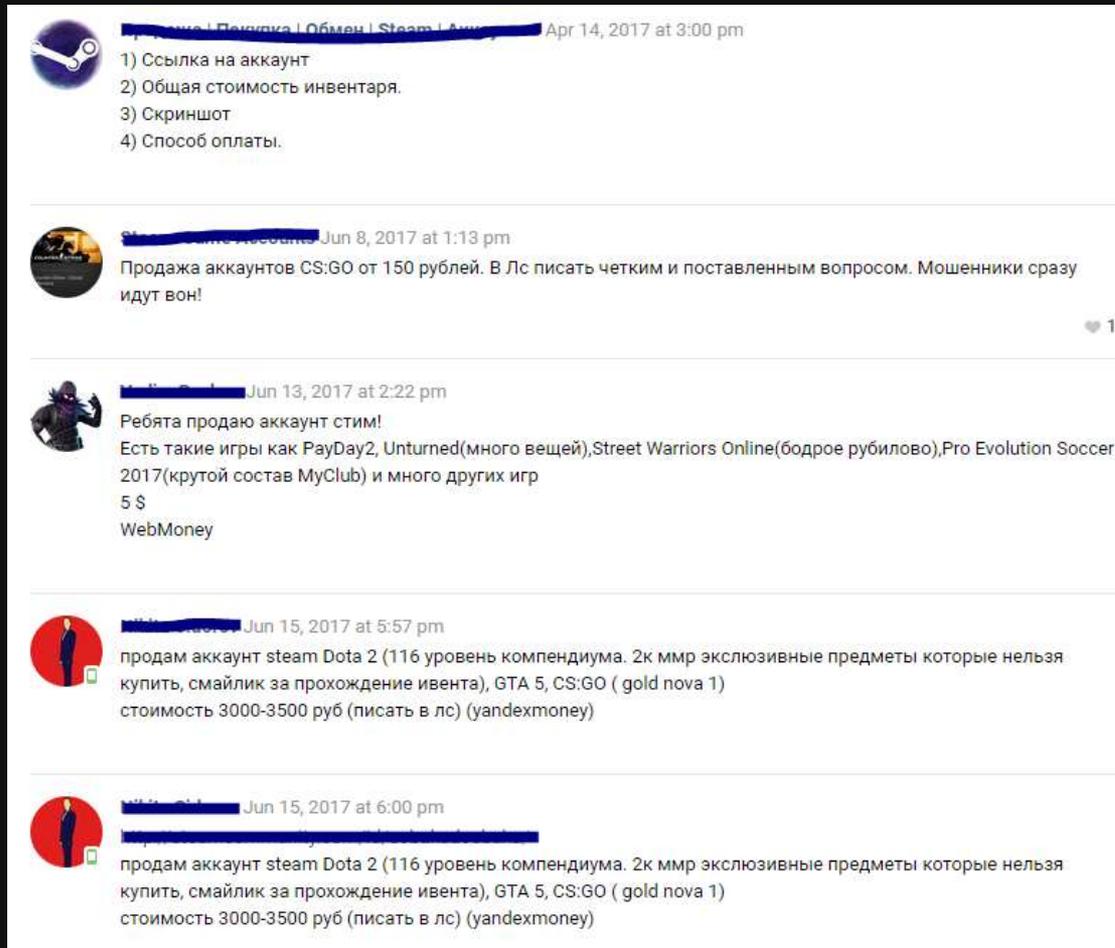
Below the modal, three key options are visible:

- Серебряный (Silver): 2 stars, price 40 rub.
- Золотой (Gold): 3 stars, price 60 rub.
- Premium: 5 stars, price 90 rub.

Each option includes a "купить" (buy) button. At the bottom, a note reads: "Наведите курсор на товар, чтобы получить информацию о нем" (Hover over the item to get information about it).

# Случай 3: Покупка/продажа аккаунта

Еще один способ получить игры дешевле, чем они стоят собственно в Steam, — купить у кого-нибудь уже существующий аккаунт. Продают их зачастую те же самые сомнительные магазины, которые торгуют дешевыми ключами. Почему же находятся покупатели на такой товар? Сделав приличную скидку на купленные игры и внутриигровые предметы, продавец отдает пользователю готовый профиль.



The screenshot shows a forum thread with five posts. Each post includes a profile picture, a redacted name, a date and time, and the text of the post. The posts are as follows:

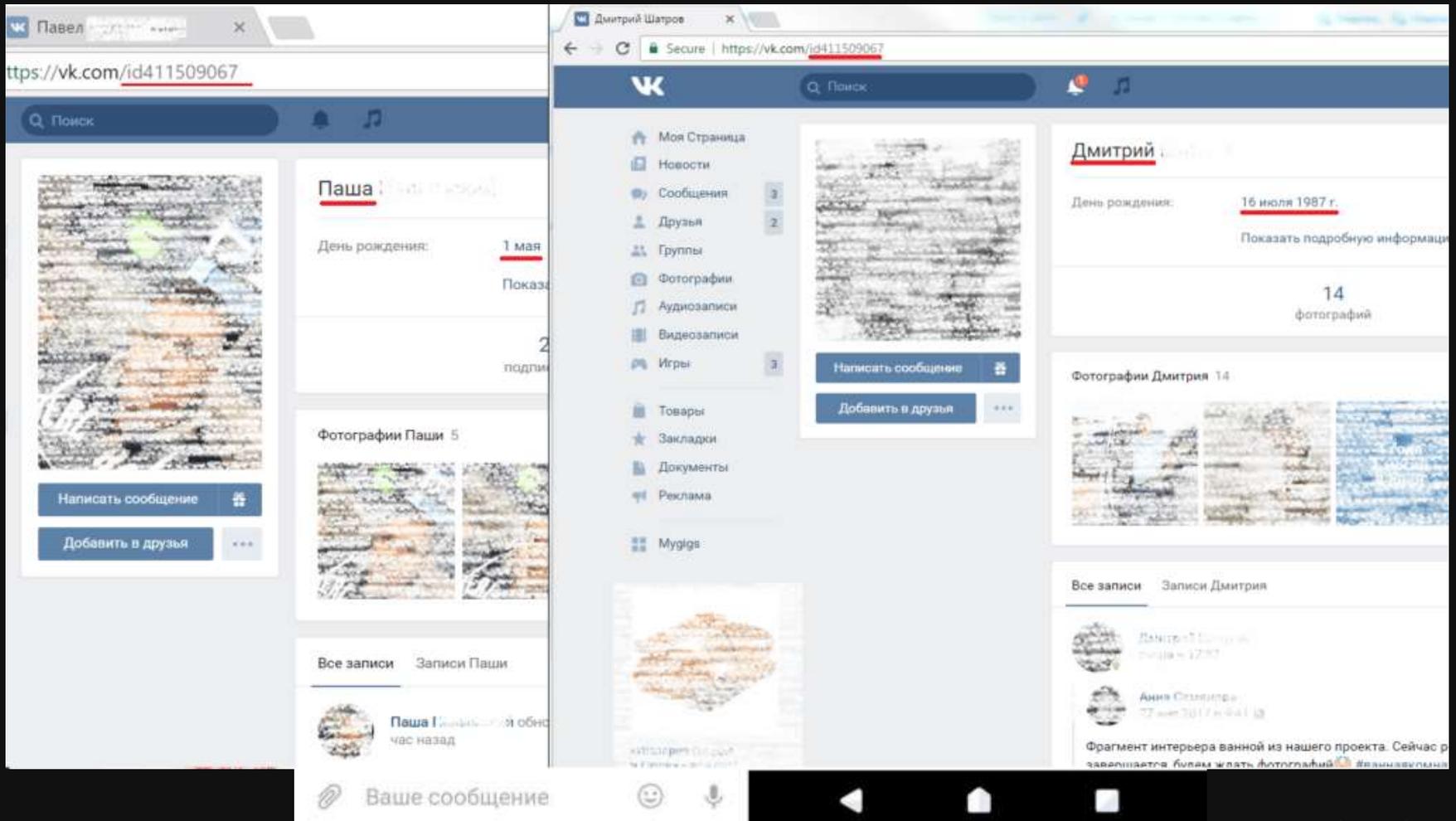
- Post 1:** Profile picture: Steam logo. Name: [Redacted]. Date: Apr 14, 2017 at 3:00 pm. Text: 1) Ссылка на аккаунт  
2) Общая стоимость инвентаря.  
3) Скриншот  
4) Способ оплаты.
- Post 2:** Profile picture: CS:GO logo. Name: [Redacted]. Date: Jun 8, 2017 at 1:13 pm. Text: Продажа аккаунтов CS:GO от 150 рублей. В Лс писать четким и поставленным вопросом. Мошенники сразу идут вон! (1 like)
- Post 3:** Profile picture: Dota 2 logo. Name: [Redacted]. Date: Jun 13, 2017 at 2:22 pm. Text: Ребята продаю аккаунт стим!  
Есть такие игры как PayDay2, Unturned(много вещей),Street Warriors Online(бодрое рубилово),Pro Evolution Soccer 2017(крутой состав MyClub) и много других игр  
5 \$  
WebMoney
- Post 4:** Profile picture: Dota 2 logo. Name: [Redacted]. Date: Jun 15, 2017 at 5:57 pm. Text: продам аккаунт steam Dota 2 (116 уровень компендиума. 2к ммр эксклюзивные предметы которые нельзя купить, смайлик за прохождение ивента), GTA 5, CS:GO ( gold nova 1)  
стоимость 3000-3500 руб (писать в лс) (yandexmoney)
- Post 5:** Profile picture: Dota 2 logo. Name: [Redacted]. Date: Jun 15, 2017 at 6:00 pm. Text: продам аккаунт steam Dota 2 (116 уровень компендиума. 2к ммр эксклюзивные предметы которые нельзя купить, смайлик за прохождение ивента), GTA 5, CS:GO ( gold nova 1)  
стоимость 3000-3500 руб (писать в лс) (yandexmoney)

## Случай 4: Приложения

Примерно так же работают схемы с приложениями, которые обещают повысить безопасность аккаунта, добавить какие-то дополнительные функции или, скажем, обещают испортить репутацию в Steam кому-то. Таких программ огромное количество, но доверять им не стоит — по точно тем же причинам: они крадут данные

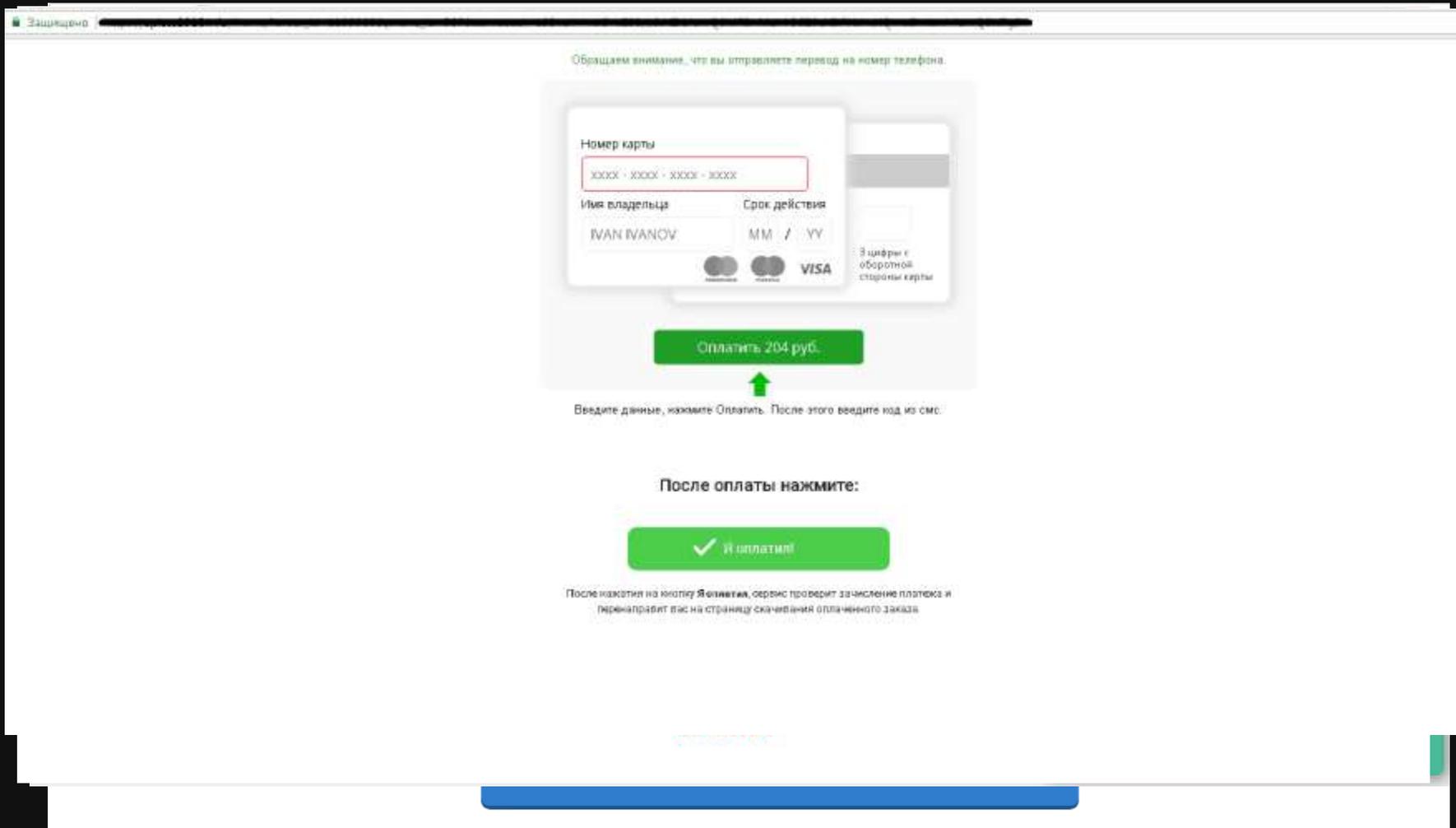
# Случай 5: Кража личности

Термин «кража личности» появился более 50 лет назад и обозначает вид мошенничества с использованием персональных данных человека для осуществления различных операций от его имени с целью получения материальной выгоды. Подобный способ мошенничества из года в год становится все более популярным.



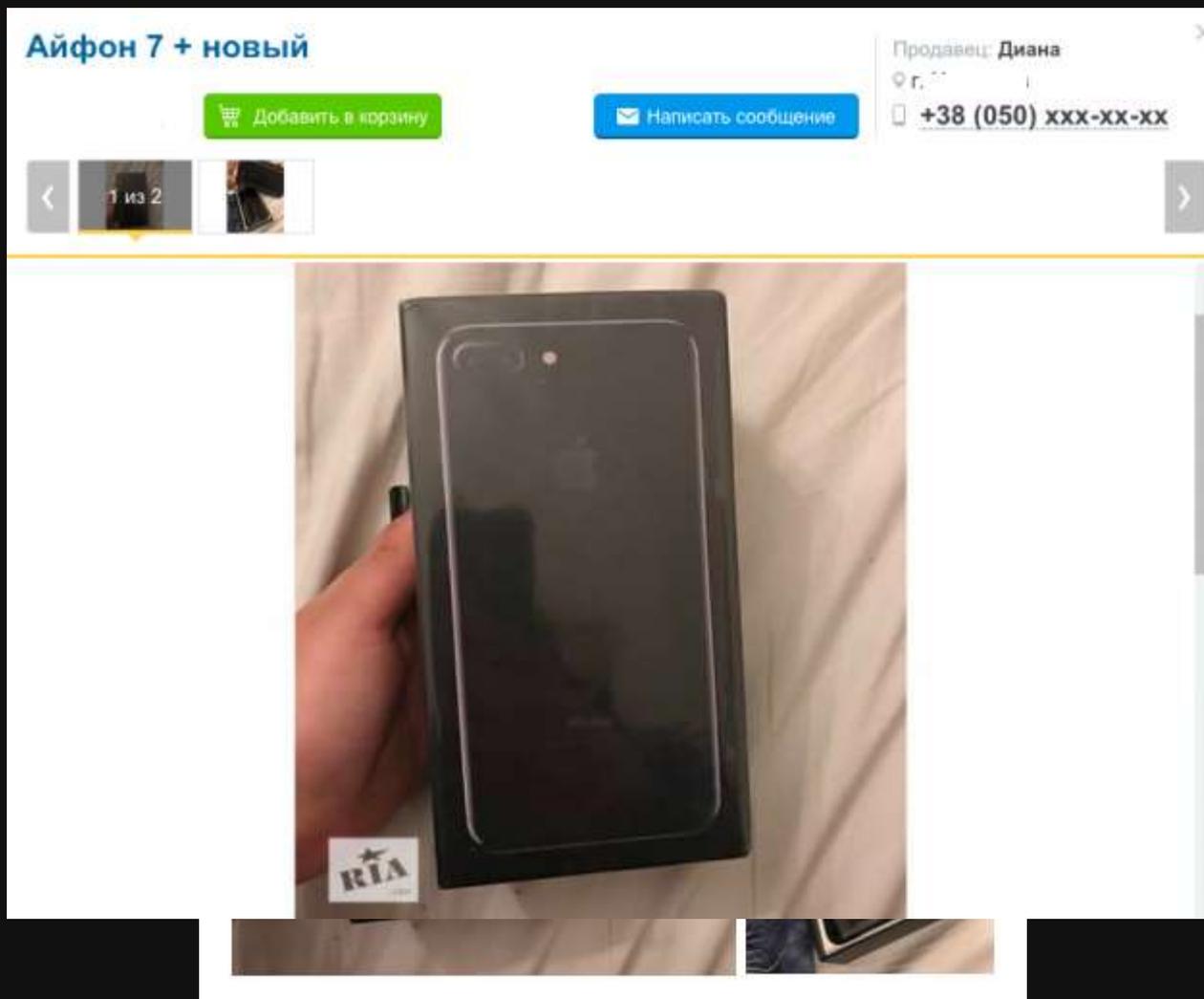
# Случай 6: Лотереи, розыгрыши призов

Последнее время в сети увеличились многочисленные предложения поучаствовать в «бесприигрышной» лотерее, получить приз или пройти опрос за вознаграждение



## Случай 7: Группы в социальных сетях

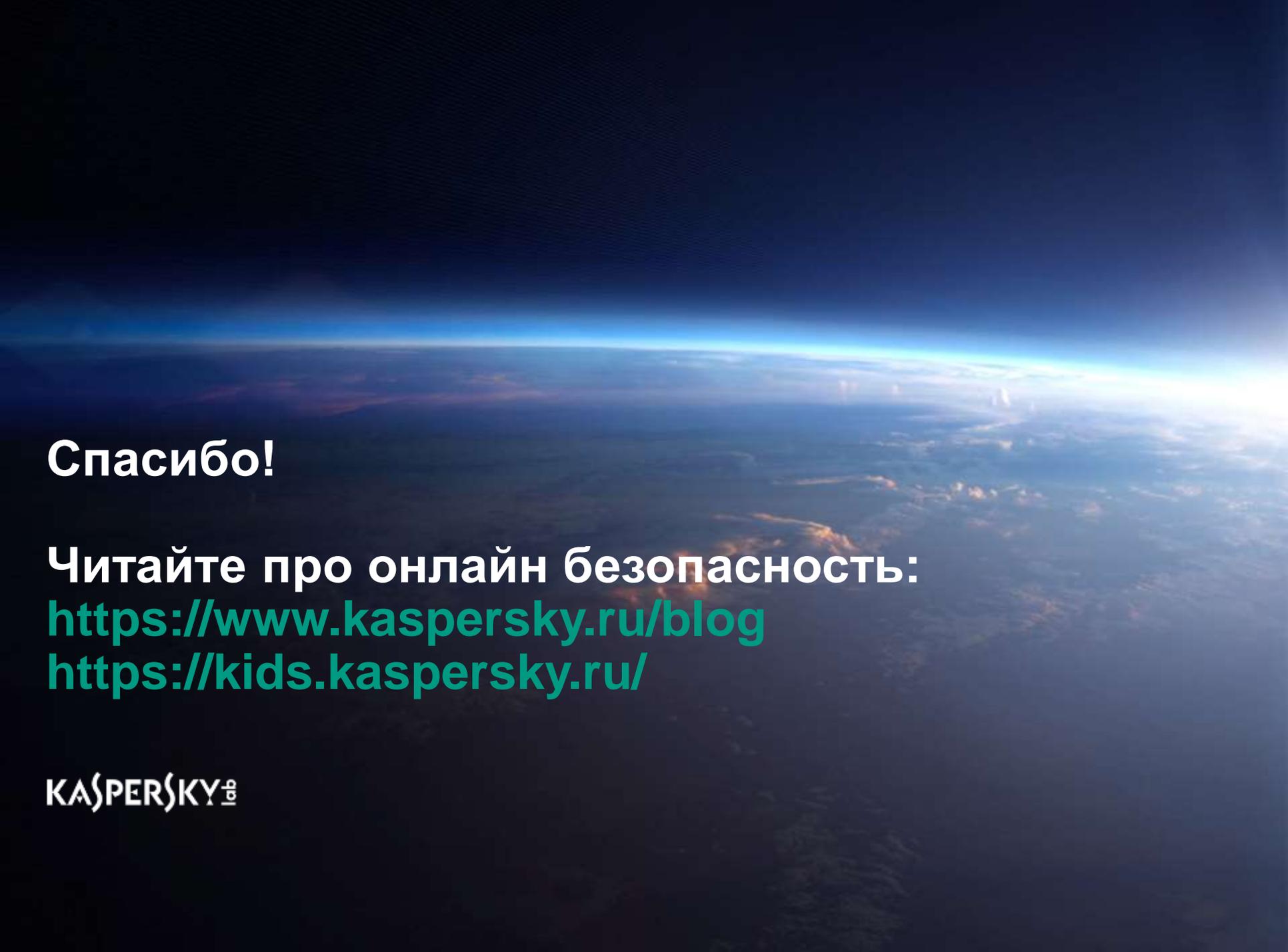
В группах «Отдам даром» участники предлагают обменять или просто подарить ненужные вещи. Чтобы получить бесплатную вещь, участник сообщества делает репост интересующей записи. После определённого времени даритель сам выбирает человека из списка поделившихся и договаривается о сделке.



# Как защититься от онлайн мошенничества? Советы!

# Простые правила

- Необходимо следовать принципам безопасного поведения в интернете и не переходить по ссылкам, присланным в подозрительных или непонятных сообщениях электронной почты или через мессенджеры.
- Не загружать вложенные файлы из сообщений электронной почты, которых вы не ожидали.
- Обеспечить надежной защитой свои пароли и не сообщать их никому.
- Не сообщать никому свои персональные данные - будь то по телефону, лично или в сообщении эл. почты.
- Внимательно анализировать адрес сайта (URL), на который была переадресация. В большинстве случаев фишинга, несмотря на то, что сайт выглядит идентично настоящему, URL-адрес может отличаться от оригинального (например, заканчиваться на .com вместо .gov).
- Поддерживать свой браузер обновленным и своевременно устанавливать обновления интернет безопасности программ.



**Спасибо!**

**Читайте про онлайн безопасность:**

<https://www.kaspersky.ru/blog>

<https://kids.kaspersky.ru/>

**KASPERSKY** 