Л.С. Сагдеева, учитель экономики

МБОУ «Гимназия 25», город Кемерово

Кемеровская область – Кузбасс

Д.Д. Чумакова, учитель математики

МБОУ «Гимназия 25», город Кемерово

Кемеровская область – Кузбасс

**Мошенничество в социальных сетях:**

**как распознать обман и защитить себя**

*Аннотация:* В статье рассматриваются распространенные схемы мошенничества в социальных сетях: фишинг, фальшивые магазины, инвестиционные аферы, ложные благотворительные сборы и романтические обманы. Даются практические рекомендации по распознаванию мошеннических аккаунтов, проверке информации и защите персональных данных. Описаны признаки обмана, способы безопасных платежей и действия в случае, если вы уже стали жертвой аферистов. Материал поможет пользователям соцсетей избежать финансовых потерь и сохранить конфиденциальность.

*Ключевые слова:* мошенничество в соцсетях; фишинг; фальшивые магазины; благотворительный скам; инвестиционные аферы; романтические мошенники; защита от обмана; безопасность в интернете; кибербезопасность.

*Abstract:* The article examines common fraud schemes in social networks: phishing, fake stores, investment scams, false charity fees and romantic deceptions. Practical recommendations are given on recognizing fraudulent accounts, verifying information, and protecting personal data. It describes the signs of fraud, secure payment methods and actions in case you have already become a victim of scams. The material will help users of social networks avoid financial losses and maintain confidentiality.

*Keywords:* social media fraud; phishing; fake stores; charity scam; investment scams; romantic scams; protection from deception; Internet security; cybersecurity.

**Введение**

Социальные сети прочно вошли в нашу жизнь, став не только площадкой для общения, но и пространством для бизнеса, благотворительности и финансовых операций. Однако вместе с удобством и возможностями появились и новые риски – мошеннические схемы, которые с каждым годом становятся все более изощренными.

По данным Федеральная служба государственной статистики[[1]](#footnote-1) и РБК[[2]](#footnote-2) мошенники украли у россиян не менее ₽ 295 млрд. в 2024 году. В мае прошлого года был установлен рекорд по числу звонков — 20 млн. в сутки.

При этом социальные сети остаются одной из самых популярных площадок для киберпреступников – здесь они легко находят доверчивых пользователей, играя на их эмоциях и неосведомленности.

В этой статье мы подробно разберем:

Какие виды мошенничества наиболее распространены в социальных сетях; как работают современные аферисты и какие психологические приемы используют; по каким четким признакам можно распознать обман; какие меры безопасности помогут защитить себя и своих близких.

Эта информация будет полезна всем активным пользователям социальных сетей – от подростков до людей старшего поколения. Зная основные схемы мошенников и правила цифровой гигиены, вы сможете безопасно пользоваться соцсетями и не стать очередной жертвой киберпреступников.

"Предупрежден – значит вооружен" – эта древняя мудрость как никогда актуальна в цифровую эпоху. Давайте вместе разберемся, как защитить себя в социальных сетях.

**Основная часть**

Социальные сети стали неотъемлемой частью нашей жизни: мы общаемся, работаем, совершаем покупки и даже помогаем друг другу через платформы вроде Facebook, Instagram, ВКонтакте, Telegram и TikTok. Однако вместе с удобством пришли и мошенники, которые используют доверие пользователей в корыстных целях.

Фишинговые ссылки, фальшивые конкурсы, поддельные благотворительные сборы, инвестиционные аферы — все это может привести к потере денег, данных и даже доступа к аккаунту. Как распознать мошеннические предложения и страницы? Как не стать жертвой обмана? Разбираемся в этой статье.

**1. Основные виды мошенничества в социальных сетях**

Разберем основные виды мошенничества в социальных сетях:

*1.1. Фишинг и кража данных*

Мошенники создают поддельные страницы, имитирующие официальные сайты банков, госуслуг или популярных сервисов (например, "Вход в Instagram через Facebook"). Пользователя просят ввести логин, пароль или данные карты, после чего злоумышленники получают доступ к аккаунту или деньгам.

Примеры:

"Ваш аккаунт заблокирован! Перейдите по ссылке для восстановления".

"Вы выиграли приз! Введите данные карты для получения".

*1.2. Фальшивые магазины и продажи*

В соцсетях появляются группы и аккаунты, предлагающие товары по заниженным ценам (технику, одежду, билеты). После предоплаты продавец исчезает.

Как распознать: нет реальных отзывов; контакты скрыты или указан только Telegram; оформлен новый аккаунт с малым количеством подписчиков.

*1.3. Ложные благотворительные сборы*

Мошенники используют фото больных детей или пострадавших в катастрофах, собирая деньги на "лечение" или "помощь". Часто эти истории выдуманы или украдены у реальных фондов.

Как проверить: искать оригинальный сбор через официальные благотворительные платформы; проверять реквизиты (настоящие фонды не просят переводы на частные карты).

*1.4. "Быстрые деньги": финансовые пирамиды и инвестиционные аферы.*

Предложения вроде:

"Вложи 5000 ₽ и получай 50 000 ₽ в месяц!"

"Тайный курс по заработку в TikTok без вложений".

Обычно это схемы, где первые участники получают выплаты за счет новых жертв, а затем организаторы исчезают.

*1.5. Романтические аферы (скам "под любовь")*

Мошенники создают фальшивые профили привлекательных людей, втираются в доверие и затем просят деньги "на билет", "лечение" или "бизнес".

Признаки: отказ от видеозвонков; быстрое признание в чувствах; просьбы о финансовой помощи.

**2. Способы и приемы распознать мошеннический аккаунт или группу.**

 1. Проверьте дату создания страницы

Фейковые аккаунты часто создаются недавно (менее года назад), а на стене мало постов или они скопированы из других источников.

2. Обратите внимание на контент: нет личных фото (только стоковые изображения); однотипные посты с призывами перейти по ссылке; подозрительные комментарии (боты, спам).

3. Изучите подписчиков и активность

У мошеннических групп тысячи подписчиков, но мало лайков и репостов. Фальшивые страницы часто добавляют в друзья случайных людей.

4. Проверяйте ссылки

Фишинговые сайты могут выглядеть как "instagrarn.com" вместо "instagram.com". Официальные компании редко используют сокращатели ссылок (bit.ly, clck.ru).

5. Анализируйте поведение собеседника

Давление: "Срочно отправьте деньги, иначе счет заморозят!"

Избегание вопросов: "Не могу показать документы, это конфиденциально".

**3. Защитите себя от мошенников.**

 1. Включите двухфакторную аутентификацию

Это защитит аккаунт от взлома даже при утечке пароля.

2. Не переходите по подозрительным ссылкам, особенно из личных сообщений или незнакомых чатов.

3. Проверяйте информацию. Ищите отзывы о магазине или проекте. Звоните на официальные номера компаний (не тем, что указаны в сообщении).

4. Не переводите деньги незнакомцам, даже под предлогом "срочной помощи".

5. Пользуйтесь безопасными платежами. Покупки — только через гаранты (например, "Авито Доставка"). Благотворительность — через проверенные фонды.

Если вдруг вы стали жертвой мошенников, то немедленно заблокируйте мошенника и сообщите о нем в социальных сетях. Поменяйте пароли от аккаунтов и банковских карт. Обратитесь в банк, если успели перевести деньги — иногда транзакцию можно отменить. Подайте заявление в полицию (ст. 159 УК РФ — мошенничество).

**Заключение**

Социальные сети — это не только площадка для общения и развлечений, но и пространство, где мошенники активно используют человеческое доверие в своих целях. Они постоянно совершенствуют схемы обмана, адаптируясь к новым технологиям и психологическим уловкам. Однако, зная их методы и соблюдая простые правила цифровой безопасности, можно значительно снизить риски и защитить себя от финансовых и эмоциональных потерь.

Мошенники в соцсетях постоянно придумывают новые схемы обмана, но их объединяет одно — они играют на доверии и эмоциях. Будьте бдительны: проверяйте информацию, не торопитесь переводить деньги и учитесь распознавать фейки.

Мошенничество в соцсетях многообразно: от фишинга и фальшивых магазинов до финансовых пирамид и романтических афер — злоумышленники используют любые способы, чтобы завладеть вашими деньгами или данными.

Важно понимать, как работают эти схемы, чтобы вовремя распознать обман.

Ключевые признаки мошенничества

Анонимность: у фейковых аккаунтов нет реальных фото, мало друзей, а дата создания — недавняя.

Давление: срочные просьбы перевести деньги, угрозы («аккаунт заблокируют», «ребенку нужна операция»).

Неофициальные каналы связи: переводы на частные карты, общение только в Telegram или WhatsApp.

Слишком выгодные предложения: «Заработайте 100 000 ₽ в день без усилий!» — такого не бывает.

Интернет может быть безопасным, если пользоваться им с умом!

**Список литературы**

1. Kaspersky Lab. Социальная инженерия: как мошенники манипулируют пользователями в соцсетях. [Электронный ресурс]. URL: https://www.kaspersky.ru (дата обращения: 01.04.2025).
2. Конникова, М. Искусство обмана: Социальная инженерия и человеческая психология. М.: Альпина Паблишер.
3. МВД РФ. Отчет о киберпреступлениях в России за 2022 год. [Электронный ресурс]. URL: https://мвд.рф (дата обращения: 01.04.2025).
4. РБК. Мошенничество: [Электронный ресурс] // https://www.rbc.ru/life/news/67c701169a79471c14b76fa5 (Дата обращения: 17.04.2025).
5. Роскачество. Как распознать мошенников в соцсетях: руководство для пользователей. [Электронный ресурс]. URL: https://rskrf.ru (дата обращения: 19.04.2025).
6. Уголовный кодекс РФ. Статья 159. Мошенничество. [Электронный ресурс]. URL: http://www.consultant.ru (дата обращения: 30.04.2025).
7. Федеральная служба государственной статистики: [Электронный ресурс] // www.gks.ru (Дата обращения: 17.04.2025).
8. Центральный банк РФ. Рекомендации по защите от финансового мошенничества. [Электронный ресурс]. URL: https://cbr.ru (дата обращения: 19.04.2025).
1. Федеральная служба государственной статистики: [Электронный ресурс] // [www.gks.ru](http://www.gks.ru) (Дата обращения: 17.04.2025). [↑](#footnote-ref-1)
2. РБК. Мошенничество: [Электронный ресурс] // <https://www.rbc.ru/life/news/67c701169a79471c14b76fa5> (Дата обращения: 17.04.2025). [↑](#footnote-ref-2)