

Мошенничество в соцсетях: как защитить себя?

Социальные сети давно стали не только местом для общения и развлечений, но и очень удобной площадкой для разных мошенников. Фальшивые розыгрыши, поддельные аккаунты компаний и даже сообщения от близких — все это может обернуться потерей денег и персональных данных.

Какие схемы используют мошенники

Фейковые страницы брендов и магазинов

Мошенники копируют логотипы, оформление и даже сайты известных компаний, обещая некие акции, лотереи, подарки или нереально низкие скидки. Когда пользователь заинтересуется предложением, его попросят перейти по ссылке и ввести данные карты и документов. А дальше он остается без денег, а его персональные данные оказываются в руках у мошенников, и они могут делать с ними все что угодно — оформлять кредиты, использовать в преступных схемах или шантажировать.

Реальный кейс: в ноябре прошлого года полиция Шымкента задержала 22-летнего жителя Тараза и двух его сообщников из Алматы и Шымкента. Они создали в соцсетях фейковый аккаунт магазина брендовой обуви и сумок — копировали фотографии и карточки товаров из реальных маркетплейсов и торговых площадок. Покупателей мошенники просили оплатить товар и доставку через денежные переводы или удаленные счета. Разумеется, заказов люди не дождались, потому что «продавцы» их просто заблокировали. Но покупатели не стали мириться с обманом, пошли в полицию, и аферистов нашли.

Как защитить себя:

- проверяйте, аккаунт магазина: наличие «галочки», ссылки на сайт, контакты, реальный адрес;
- изучайте отзывы на магазины на независимых площадках;
- не переходите по подозрительным ссылкам и не вводите данные карты;
- никогда не оплачивайте переводом или на карту неизвестному человеку — используйте только официальные сайты и приложения.

Сообщения от «друзей»

Пожалуй, самая популярная схема у мошенников, потому что не требует долгих действий, и можно играть на эмоциях людей, которые искренне готовы помочь друзьям и близким. Все происходит так: человеку в мессенджере соцсети приходит сообщение с просьбой занять денег или проголосовать за дочь, внука или племянницу в каком-то конкурсе. Но на самом деле, аккаунт взломан, и с потенциальной жертвой общаются мошенники. Как только вы переходите по вредоносной ссылке, все ваши данные оказываются у мошенников благодаря специальному приложению или вирусу, которые автоматически устанавливаются на ваш телефон, ноутбук, компьютер.

Реальный кейс: как мы уже говорили, этот способ очень полюбился мошенникам, и количество пострадавших просто не счесть — так их много. Например, только в прошлом году правоохранительные органы зарегистрировали в Казахстане более 4 000 случаев мошенничеств через соцсети и мессенджеры, в которых аферисты прикидывались близкими потенциальных жертв.

Как защитить себя:

- если близкий просит деньги или присылает ссылку — позвоните лично и уточните информацию;
- не переходите по сомнительным ссылкам, даже если они пришли от знакомых и родных;
- установите двухфакторную аутентификацию в соцсетях и мессенджерах.

Фальшивые розыгрыши и лотереи

В соцсетях нередко можно встретить посты с рекламой розыгрышей и лотерей, обещающих баснословные выигрыши. И, конечно, любой, кто напишет в такой аккаунт, сразу же станет победителем. Но есть одна загвоздка: вас попросят оплатить «комиссию» за приз. А дальше вы не увидите ни выигрыша, ни своих вложенных денег.

Реальный кейс: в конце 2024 года полиция арестовала жителя Атырауской области, который говорил доверчивым гражданам в соцсетях, что он представитель лотереи и они выиграли призы. Но для получения выигрыша мошенник просил перевести ему деньги — якобы для страховки. А жертв он искал под своими же постами о лотерее: выходил на них и писал о призах. Общий ущерб составил 140 тысяч тенге, но на самом деле, конечно, таких кейсов гораздо больше, просто далеко не все они доходят до полиции и судов.

Как защитить себя:

- никогда не забывайте, что честные лотереи и розыгрыши не требуют оплаты «комиссий» или «страховок»;
- проверяйте организатора: есть ли у него лицензия или официальный сайт, изучите отзывы на независимых площадках;
- не отправляйте личные данные и реквизиты ради «выигрыша».

Фейковые вакансии

Также достаточно популярный способ мошенничества в соцсетях. Как правило, такие объявления выглядят очень заманчиво: «Работа онлайн: 5 000 тенге за час, делать почти ничего не нужно». А заинтересованных кандидатов мошенники просят оплатить «регистрацию» или «обучение», после чего исчезают.

Реальный кейс: в марте этого года казахстанцы стали получать по WhatsApp предложения устроиться на работу в маркетплейс Ozon. Якобы работать нужно удаленно и всего лишь 30-60 минут в день, а за ее выполнение обещали платить от 20 до 50 тысяч тенге. При этом ни подробного описания вакансии, ни конкретных условий работы указано не было, а приходили сообщения вообще от номера с кодом Великобритании.

Конечно, все это оказалось происками мошенников, и до сих пор люди периодически получают в мессенджеры подобные предложения. При чем тем людям, которые заинтересовались, писали с просьбой перечислить определенную сумму под предлогом агентского взноса, проверки карты или поднятия уровня продавца. Но реальный маркетплейс никогда не берет деньги с кандидатов при трудоустройстве.

Как защитить себя:

- не верьте вакансиям и компаниям, которые предлагают «легкие деньги за пару часов работы»;
- никогда не переводите деньги за «регистрацию» или «обучение»;
- проверяйте работодателя: официальный сайт, контакты, отзывы.

Love scam или «романтические схемы»

Мошенники знакомятся с жертвой в соцсетях и стараются вызвать у нее как можно большую эмоциональную привязанность, чтобы манипулировать в будущем. Как только аферист понимает, что жертва «готова», начинает выпрашивать деньги — на переезд, оформление документов, лечение и так далее. И после того, как средства поступят, «возлюбленный» резко пропадет отовсюду.

Реальный кейс: весной этого года жительница Акмолинской области познакомилась в соцсетях с аферистом, который выдавал себя за миротворца ООН. При общении мужчина заявил, что готов приехать в Казахстан и жениться, но попросил 550 долларов под предлогом оформления отпуска. Женщина перечислила деньги, но потом с ней связались якобы представители ООН и потребовали дополнительную сумму — теперь уже на перелет. Здесь акмолинка уже поняла, что ее обманули, и обратилась в полицию.

Как защитить себя:

- не доверяйте людям, которые слишком быстро говорят о чувствах — они чаще всего оказываются абыззерами или мошенниками;
- никогда не отправляйте деньги «интернет-партнерам», даже если они просят «на билет» или «лечение»;
- проверьте фото и данные собеседника через поисковики — это действительно может помочь.

Что делать, если вы стали жертвой мошенников?

1. Срочно заблокируйте карту и сообщите в банк, что вас обманули мошенники.
2. Сделайте скриншоты переписки и страниц мошенников.
3. Сообщите о произошедшем в техподдержку соцсети и напишите заявление в полицию.

Сегодня быть бдительными в соцсетях так же важно, как и в реальной жизни. С каждым днем мошенники становятся все изощреннее, но если вы знаете их схемы и модели поведения, то вы сможете сохранить свои деньги и персональные данные.