

# Антивирус для кошелька

**О мошеннических схемах, казалось бы, знают все. Однако злоумышленники придумывают все новые схемы обмана. Нынешняя сложная социально-экономическая ситуация для них благодатная пора. Вместе с экспертами разбираемся, как максимально обезопасить себя.**



Практически ни одна мошенническая схема не обходится без применения социальной инженерии. Методы игры на слабостях и страхах обычного человека позволяют преступникам найти беспроигрышный подход, чтобы добиться желаемого – похитить деньги, персональные данные, продать бесполезное, ввести в заблуждение относительно истинного умысла своих действий.

На какие уловки мошенников можно попасться сейчас, рассказывает эксперт Центра финансовой грамотности НИФИ Минфина России Ольга Дайнеко.

**Искажение реального положения вещей.** Мошенник убеждает, что все деньги обесценятся/заморозятся "из-за обвала рубля и западных санкций". Любые предложения "спасти" накопления – обман. Если внезапно возникший "финансовый аналитик", знакомый со связями или лжегосслужащий уговаривают немедленно перевести деньги на якобы безопасный счет, поменять деньги на новые, обменять валюту по старому курсу – это мошенник, ваши "спасенные" деньги окажутся у него.

Подобные предложения часто транслируются через соцсети, мессенджеры или электронную почту. В заманчивых сообщениях нередко используют имена известных людей, якобы цитаты из законодательства, мошенники нагнетают ситуацию и пугают последним вагоном (сейчас или завтра будет поздно).

Все это – элементы социальной инженерии, нацеленные на то, чтобы потенциальная жертва поддавалась панике и не имела возможности и времени оценить такое предложение здраво, собрать дополнительную информацию. Спасение одно – бежать подальше и помнить, что любые финансовые решения нельзя принимать под сторонним эмоциональным давлением, в спешке, поддавшись панике.

**Помощь ближнему.** Беженцы, больные дети, голодные животные – все те, кому необходима помощь, не оставляют равнодушными многих людей. И это нормально. Но именно на этих чувствах построен лжефандрайзинг. Как обезопасить себя от удочки "на жалость"? Помогать лишь в том случае, если информация достоверна: личное знакомство с нуждающимся в помощи или наличие официального подтверждения беды.

Нельзя доверять смазанным фото неких документов или душещипательным историям в соцсетях. Лучшее оказывать помощь тем, кого знаешь лично, или официальным благотворительным организациям.

**Родственник в беде.** Звонок или сообщение "из органов" или от "родственника" о том, что близкий человек совершил административное или уголовное правонарушение (сбил пешехода, участвовал в несанкционированном митинге и т.п.) и нужно заплатить, чтобы не завели дело. Этот старый способ, известный многим.

Аферисты чаще выбирают для таких новостей пожилых людей. Желание спасти близкого человека, страх и растерянность – все это может лишить здравомыслия и не дать критически оценить ситуацию. Нужно объяснять своим пожилым родственникам, что любую информацию необходимо сначала проверять.

**Покупка дешево.** Не следует верить сообщениям о срочной распродаже товаров в связи с закрытием магазина или

ликвидацией. Часто такие предложения поступают в форме рассылки, в которой содержится ссылка для перехода на фейковый ресурс. В надежде купить телефон или компьютер по "выгодной" цене можно вовсе остаться без денег на счете. Помните, никто не будет торговать себе в убыток.

Никогда не нужно переходить по присланным ссылкам – именно так можно занести на свой девайс вирус, похищающий личные данные. Ссылка также может выглядеть как картинка или кнопка.

К подобным схемам часто прибегают мошенники на таких популярных сайтах, как avito: например, продавец срочно и дешево продает квартиру, потому что "уезжает из страны". Находит такой человек, как правило, не в городе покупателя, а в командировке, в больнице и т. п. Документы в наличии, но нужен аванс, обычно не слишком значительный – 1-3 % от стоимости, чтобы "я уже не предлагал никому".

Отправив аванс, можно попрощаться с деньгами. Все сделки купли-продажи заключаются очно, требуют письменного оформления, в том числе подтверждения внесения аванса.

**Заработок секретными способами или на криптовалюте.** Сценарий обычно такой: в "Телеграме" "известным хакером" создается канал, в котором сначала размещаются успешные схемы заработка, отчеты о баснословных доходах, лайфхаки. После привлечения подписчиков объявляется набор на "курс обучения", но мест ограниченное количество, разумеется, надо срочно записываться.

В стремлении обладать эксклюзивной информацией о заработке, люди переводят деньги, но получают либо бесполезные и общедоступные сведения, либо просто прощаются со своими средствами, потому что курс так и не состоялся.

Помните, "секретные" способы заработка не продаются (зачем о них рассказывать всем, если можно так хорошо зарабатывать). Более того, можно не только потерять деньги, но и свободу, если деятельность незаконна.

Преступники, как правило, примерно понимают, какие люди поддадутся влиянию, а какие – нет. К сожалению, сегодня практически невозможно не попасть в списки к таким мошенникам – мы сами нередко оставляем в открытом доступе информацию о себе: об имущественном положении, семье, отдыхе, заработке, заполняем анкеты в магазинах и точках продаж и многое другое.

Кроме того, злоумышленники постоянно придумывают новые уловки, меняют схемы обмана, а иногда возвращаются к старым, хорошо забытым способам. Предусмотреть их все невозможно, но это и не нужно. Абсолютное большинство методов преступников разобьются о банальную внимательность, осторожность, критическое мышление, базовые принципы финансовой безопасности и понимание, на каких чувствах и слабостях обычно играют мошенники.

**Открытие счетов в "надежных иностранных банках".** Такое мошенничество появилось не сегодня, сменились лишь аргументация – теперь жертве предлагают таким образом скрыть доходы и накопления в "далеких валютных офшорах".

Схема обмана: мошенники запускают страницу веб-сайта якобы "банка", организуют горячую линию кредитной организации. Открыть счет предлагается только удаленно и жертву убеждают в надежности тем, что находятся вне контроля мегарегулятора – Банка России, ИФНС и прочих надзорных органов.

Результат "открытия" таких счетов – гарантированное хищение личных и персональных данных (в том числе – реальных банковских) плюс кража денежных средств.

Какую информацию требуют аферисты? Данные паспорта – по словам "представителя банка" эта информация необходима для присвоения индивидуального кода счета (без имени), данные существующих банковских счетов/карт). Мошенники предупреждают, что для безопасности деньги на новый "счет" будут поступать через посредника.

Вводя в заблуждения клиента в процессе переговоров, они говорят, что могут потребоваться смс-или пуш-уведомления (для "подтверждения транзакции" на созданный "счет"). Каждый раз мошенники могут придумывать новые уловки с одной целью – добраться до сбережений жертвы. Однако далее наступает череда проблем: что-то идет не так, "нужно немного подождать", сложности с переводом ввиду санкций, проверка платежа, необходимость открыть еще один "резервный счет" и т.д.

Как обезопасить себя? Важно вовремя сказать себе "стоп", а лучше при первых словах собеседника о "безопасных счетах" положить трубку.

Помните – высокотехнологичное мошенничество имеет сложный алгоритм доказательства совершения противоправных действий. Кроме того, зачастую все посредники мошеннических действий находятся вне досягаемости правоохранительных структур, вне их юрисдикции и вернуть украденные деньги будет практически невозможно.

Существуют непреложные правила цифровой гигиены. Они актуальны в любое время, но сейчас особенно. Используя эти общие рекомендации, можно противостоять любым мошенническим атакам. Это касается и финансовых услуг, и покупок каких-либо товаров в интернете.

- Не совершайте никаких операций с картой или счетом под диктовку человека по телефону или посредством иных видов связи.
- Не принимайте в спешке решения, связанные с финансами, пока не разберетесь в ее сути. Посоветуйтесь с родными или друзьями.
- Помните о фишинге! Не переходите по ссылкам в письмах или сообщениях от неизвестных адресов. Проверяйте подлинность и защищенность сайтов, когда совершаете оплату или переводы. Нужно обратить внимание на название сайта в адресной строке. Мошенники регистрируют домены похожие на адреса официальных сайтов известных брендов, но с едва заметными ошибками. Следите, чтобы в начале адресной строки на сайте размещался символ черного "замочка". Сайт безопасен если "замочек" закрыт.
- Заведите отдельную карту для онлайн-покупок и перечисляйте на нее суммы, необходимые для конкретной покупки.
- Ни при каких обстоятельствах не передавайте платежные данные, пароли и коды подтверждений третьим лицам, кем бы они не представлялись!

Информация предоставлена  
Центром финансовой грамотности  
Ульяновской области.

## 8 полезных советов, как сохранить деньги

Общемировой тренд сейчас – растущая инфляция. Это значит, что на ту же сумму можно купить меньше товаров, чем годом ранее. Как сохранить свои сбережения?

- Положить деньги на депозит. Российские банки сейчас предлагают рекордную доходность по рублевым депозитам.
- Завести накопительный счет. Альтернатива банковскому вкладу – накопительный счет. На него можно переводить зарплату, а затем тратить ее по чуть-чуть.
- Не усердствовать с погашением кредита. В условиях инфляции гасить досрочно невыгодно.
- Возьмите льготную ипотеку. Ставки по ипотеке сейчас неподъемные. При этом лучше отдать предпочтение покупке квартиры в уже сданном доме.
- Вложитесь в свое образование и образование детей. Можно начать изучать, например, китайский язык по еще довольно выгодным тарифам. Многие учебные платформы пока не повышали цены.
- Купите нужные вещи, приобретение которых откладывали. Если давно помышляли о покупке стиральной машины взамен той, что доживает свои последние дни, сейчас самое время.
- Инвестируйте в здоровье. Нет лучшего способа спасти деньги от инфляции, чем потратить их на самое дорогое.