

Лжебанки — это мошеннические организации, которые в интернете выдают себя за банки. Они выманивают у людей деньги якобы за банковские онлайн-услуги и под разными предлогами заставляют наивных клиентов совершить несколько платежей. Рассказываем, как не стать их жертвой.



Как мошенники завлекают клиентов?

- Массово рассылают на электронные адреса потенциальных клиентов письма с многообещающими предложениями. Обманщики гарантируют более выгодные условия, чем в остальных банках и микрофинансовых организациях, более быстрое и комфортное обслуживание.
- Обзванивают потенциальных клиентов с предложениями взять кредит по сниженной ставке.
- Находят жертв через так называемые «онлайн-сервисы по подбору кредита», на которых потребитель заполняет единую заявку на кредит — и она рассыпается по разным банкам и микрофинансовым организациям.



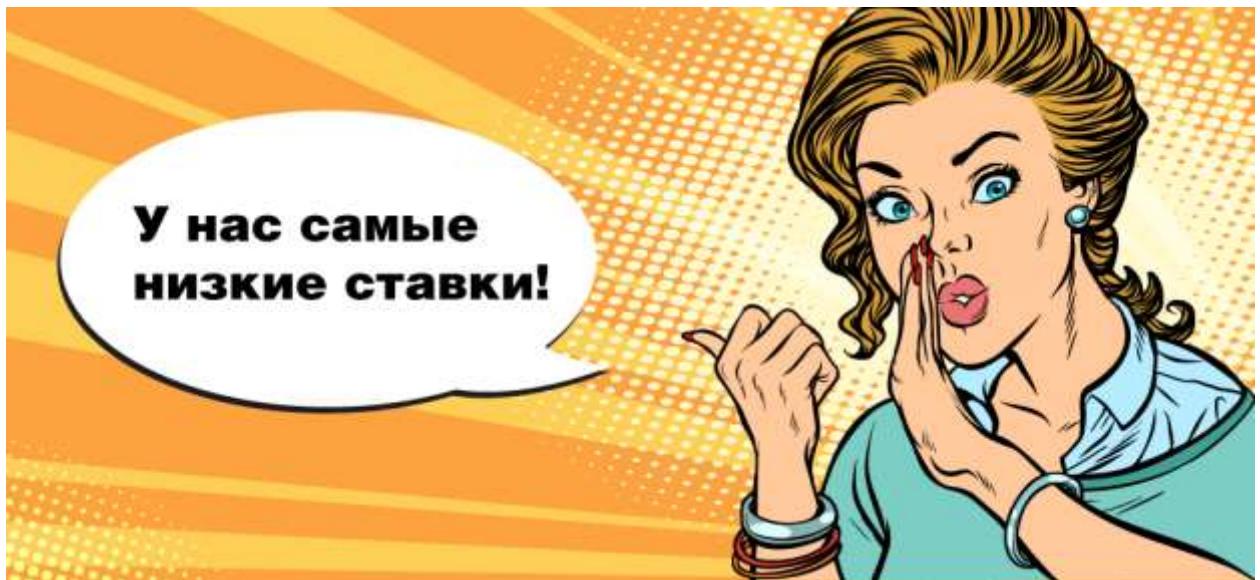
«Я嘗試過在幾家銀行申請貸款，但都被拒絕了。我打算去找另一個人借錢，突然接到一個神秘電話。一個女孩自稱是某家銀行的員工，說我的申請已經被批准了...»

Будьте бдительны, не наступайте на чужие грабли!

Как лжебанки выманивают деньги?

Мошенники просят что-то оплатить под разными предлогами. Например:

- «Кредит одобрен, но в вашем регионе нет нашего представительства, поэтому надо оплатить комиссию за перевод денег».
- «Для получения кредита необходимо оформить страховку, ее нужно оплатить заранее».



Сумма страховки обычно указывается в процентах от суммы кредита (например, 1,5%). Это убеждает клиента в том, что все правдоподобно. Деньги за страховку просят перевести на банковскую карту одного из крупных российских банков. Это якобы должно увеличить доверие потенциального заемщика.

После того как клиент оплатил страховку, ему звонит другой представитель лжебанка. Он представляется сотрудником службы безопасности и просит совершить еще несколько переводов. Для этого он придумывает разные предлоги. Например, говорит, что нужно оплатить доставку кредитки или договора кредитования, уплатить какой-то налог и тому подобное.

Получив деньги, мошенники перестают выходить на связь.

Как распознать лжебанки?

Обратите внимание на сайт такой организации: на первый взгляд он похож на веб-страницу настоящего банка. Но, присмотревшись, вы поймете: перед вами мошенники.

1. Фиктивная лицензия. Мошенники размещают на сайте якобы отсканированную копию лицензии, чтобы вы им доверились. Но при сверке со справочником Банка России

вы либо не найдете такой банк по регистрационному номеру документа, либо обнаружите, что номер принадлежит другому банку.

2. Сомнительное название. Название сайта мошенников может быть очень похоже на адрес настоящего банка. Они могут копировать логотипы и дизайн сайтов банков, которые когда-то работали, но лопнули. Так мошенники пытаются вас запутать.

3. Плохой дизайн. Качество дизайна у таких сайтов обычно низкое. Цель мошенников — заработать на вас, а не тратиться на хороший дизайн. Часть разделов меню — «Руководство», «Наши офисы», «Контакты» — может и вовсе не открываться.

4. Нет отчетности. Вы вряд ли найдете на сайте открытую информацию о работе организации, которую обязаны публиковать банки на своих сайтах: уставные документы, финансовую отчетность.

И еще: чаще всего лжебанки не имеют юридического лица и вообще какой-либо правовой формы. А значит, вычислить мошенников будет практически невозможно.



Как обезопасить себя от лжебанкиров?

1. Проверяйте лицензию банка в справочнике регулятора. Если такая компания есть в списке, убедитесь, что адрес сайта организации и адрес официального сайта банка, который указан в реестре, совпадают. Позвоните в банк по телефону на официальном сайте и попросите подтвердить одобрение кредита.

2. Не оставляйте свои персональные данные на сомнительных сайтах и не передавайте их «онлайн-сервисам по подбору кредита». Далеко не все ресурсы могут защитить вашу конфиденциальную информацию.

3. Помните, что настоящий банк никогда не предложит вам сделать денежный перевод через другой банк, тем более проводить операцию через карточный счет.