

# Социальная инженерия разрастается. Новый способ украсть у вас деньги

В ходу у мошенников — социальная инженерия, как верный способ втереться в доверие и с помощью психологических уловок заставить жертву добровольно расстаться с деньгами.

В России появился новый способ мошенничества, при котором злоумышленники получают доступ к интернет-банкингу россиян. Они представляются сотрудниками банков (чаще — сотрудниками службы безопасности банка) и сообщают о попытке взлома приложения мобильного банка. Чтобы предотвратить это, лжесотрудник банка просит жертву установить на смартфон приложение, которое позволит получить удаленный доступ к его устройству. Зловредное приложение чаще всего представляют как «специальный антивирус» или «программу для удалённой помощи».

После того, как жертва установит указанное приложение на смартфон, мошенники получают доступ ко всем возможностям учётной записи пользователя: переводить и снимать средства, изменять информацию в учётной записи, подавать заявки на кредиты и многое другое.

Указанный способ мошенничества относится к **социальной инженерии**, которая представляет из себя совокупность методов получения доступа к конфиденциальной информации, паролям и банковским данным. Социальная инженерия всегда основана на особенностях психологии людей. Как правило, необходимая информация выуживается из жертвы в ходе личного разговора, поэтому мошенникам важно установить доверительный личный контакт с жертвой, применить техники внушения и воздействия на психику. Например, надавить и поставить жертву в ограниченные временные рамки; убедить, что решение нужно принять прямо сейчас, в противном случае деньги с банковской карты или счёта будут украдены.



Другой, более распространённый на сегодняшний день, способ обмана в рамках социальной инженерии — звонки жертвам, опять же, якобы от сотрудника банка с сообщением о подозрительной транзакции, которую некие люди пытаются провести по карте. Чтобы «спасти» своего клиента от подозрительного платежа, мошенники просят указать код из СМС от банка, после чего средства попавшихся на удочку мошенников жертв выводятся на подконтрольные злоумышленникам счета.

Помимо личного диалога к методам социальной инженерии относится фишинг — рассылка электронных писем или сообщений якобы от официального банка или платёжной системы. В письме содержится форма для ввода персональных данных (пин-кодов, логина и пароля и так далее) или ссылка на страницу, где располагается такая форма. Опять же, мошенники давят на психологию: сообщают в письме любую тревожную информацию о банковских счетах жертвы.

Техника троянского коня — тоже из ряда социальной инженерии, основанная на любопытстве. В письме жертве предлагается обновить антивирус или получить денежное вознаграждение. Иногда приходит сообщение с текстов вроде «смотри, здесь твоё фото». Во вложении находится вредоносная программа, которая используется для сбора информации.

Есть и обратная инженерия, когда жертва первая выходит на контакт с мошенниками. Такое происходит в случаях, когда злоумышленники распространяют телефоны «службы поддержки».

Интересно, что методы социальной инженерии применяют не только охотники за чужими деньгами, но также политики и кандидаты в выборные должности, сотрудники спецслужб. Даже рядовые люди, которых нельзя назвать мошенниками, также, сами того не ведая, используют методы социальной инженерии.

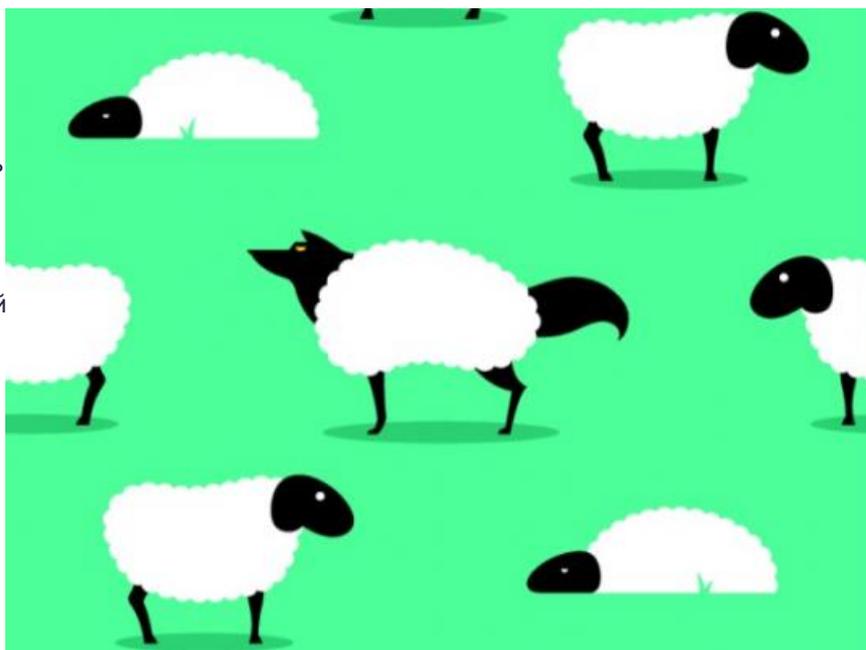
Самое обидное, что очень многие попадают в расставленные мошенниками ловушки.



*«Анализ результатов нашего исследования показал, что в 48% случаев мошенник с легкостью получает доступ к устройству пользователя. Из практики скажу, когда мы общались с банками, для меня было удивительно, что пользователь легко верит в такие легенды — ведь надо зайти в магазин приложений, скачать программу, сказать человеку по телефону определенный код — это может занимать от 10 до 30 минут», —* рассказала менеджер по развитию бизнеса Kaspersky Fraud Prevention Екатерина Данилова (цитата по РИА Новости).

Напомним, в апреле Smartbabr рассказывал о появлении целого букета способов мошенничества на коронавирусной ниве. По принципу «кому война, а кому — мать родная». Тут и лжедезинфекторы квартир; и чудо-препараты от Covid-19; и традиционные подставные сайты со средствами индивидуальной защиты, которые исчезают сразу после оплаты.

Примечательно, что способы мошенничества, связанные с коронавирусом, регулярно пополняются. Среди новинок мошеннической мысли — платные услуги по проведению анализа на коронавирус; продажа



несуществующих товаров и услуг (очиститель воздуха, убивающий вирус, вызывающий Covid-19); продажа пропусков для выхода из дома; предложение получить льготы или выплаты на период самоизоляции.

Подробнее о «коронавирусном» мошенничестве:

[«Коронавирусное» мошенничество: способы отъёма денег](#)

Автор: Алиса Беглова © SmartBabr НАУКА И ТЕХНОЛОГИИ, ИНТЕРНЕТ И ИТ, МИР 👁 9494 19.05.2020, 19:10  
👤 1

URL: <https://babr24.com/?IDE=273432> Bytes: 5240 / 4749 Версия для печати

👍 [Порекомендовать текст](#)

Поделиться в соцсетях:

Также читайте эксклюзивную информацию в соцсетях:

- [Телеграм](#)

- [ВКонтакте](#)

Связаться с редакцией Бабра:

[newsbabr@gmail.com](mailto:newsbabr@gmail.com)



Автор текста: **Алиса Беглова**,  
обозреватель.

На сайте опубликовано **257**  
текстов этого автора.

#### НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: [@babr24\\_link\\_bot](#)

Эл.почта: [newsbabr@gmail.com](mailto:newsbabr@gmail.com)

#### ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: [bratska.net.net@gmail.com](mailto:bratska.net.net@gmail.com)

#### КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь

Телеграм: [@bur24\\_link\\_bot](#)

эл.почта: [bur.babr@gmail.com](mailto:bur.babr@gmail.com)

Иркутск: Анастасия Суворова

Телеграм: [@irk24\\_link\\_bot](#)

эл.почта: [irkbabr24@gmail.com](mailto:irkbabr24@gmail.com)

Красноярск: Ирина Манская

Телеграм: [@kras24\\_link\\_bot](#)

эл.почта: [krsyar.babr@gmail.com](mailto:krsyar.babr@gmail.com)

Новосибирск: Алина Обская

Телеграм: [@nsk24\\_link\\_bot](#)

эл.почта: [nsk.babr@gmail.com](mailto:nsk.babr@gmail.com)

Томск: Николай Ушайкин

Телеграм: [@tomsk24\\_link\\_bot](#)

эл.почта: [tomsk.babr@gmail.com](mailto:tomsk.babr@gmail.com)

Прислать свою новость

#### ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"

Телеграм: [@babrobot\\_bot](#)

эл.почта: [equatoria@gmail.com](mailto:equatoria@gmail.com)

## СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

---

эл.почта: [babrmarket@gmail.com](mailto:babrmarket@gmail.com)

[Подробнее о размещении](#)

[Отказ от ответственности](#)

[Правила перепечаток](#)

[Соглашение о франчайзинге](#)

[Что такое Бабр24](#)

[Вакансии](#)

[Статистика сайта](#)

[Архив](#)

[Календарь](#)

[Зеркала сайта](#)