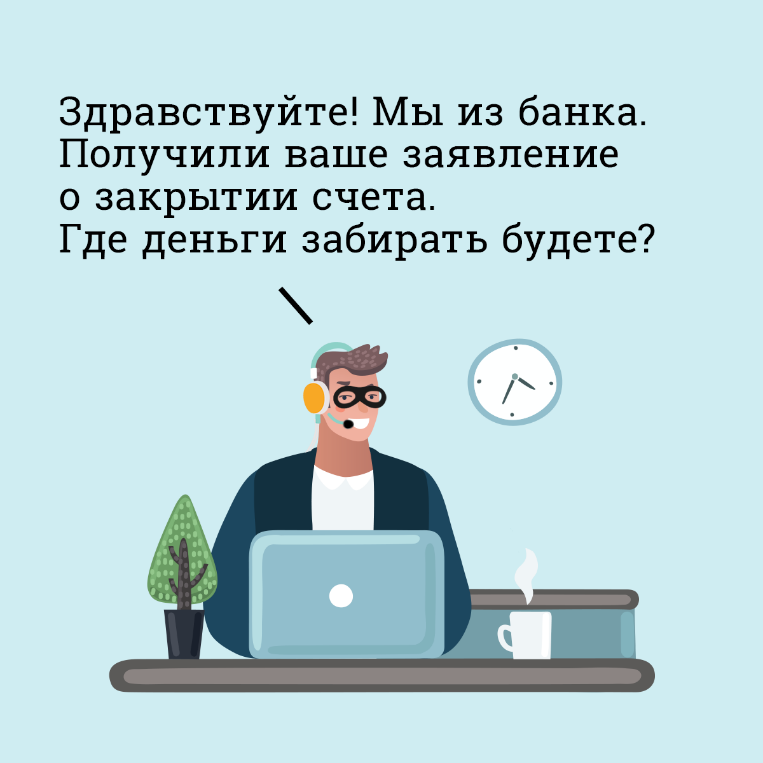
**Не отдавайте свои деньги мошенникам**

«Я из службы безопасности вашего банка, мы зафиксировали подозрительную операцию по вашему счету». С этой фразы в различных ее вариациях начинается «работа» телефонного мошенника, единственная цель которого — заставить вас отдать ему деньги.

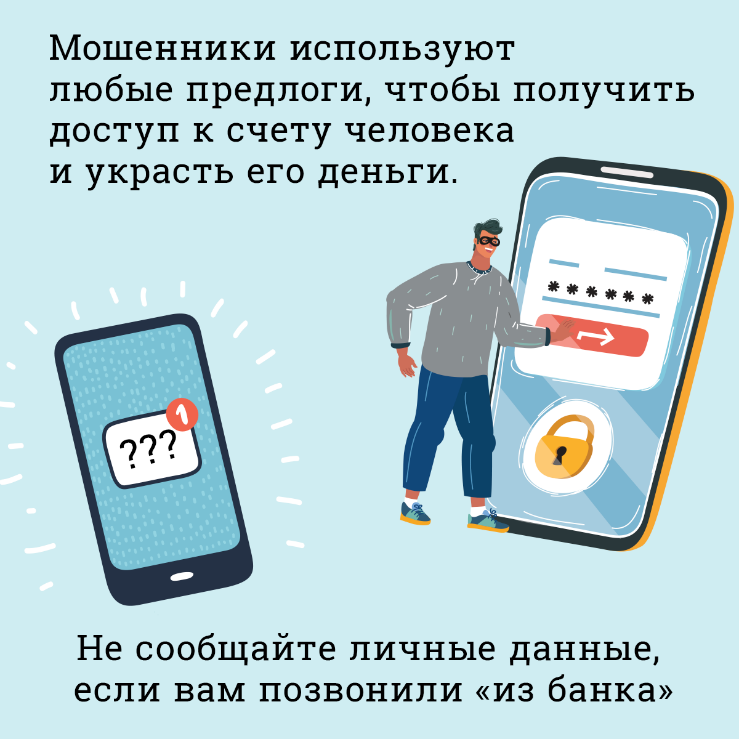


Несмотря на то, что осведомленность людей о таких мошенниках за последнее время значительно выросла, злоумышленникам по-прежнему удается обманывать граждан, усыпляя их бдительность — за 2020 год более 60% всех несанкционированных операций по банковским картам и счетам произошли с использованием социальной инженерии.

**Инженеры человеческих душ**

Под термином «социальная инженерия» скрывается банальная психологическая атака на человека. Мошенники настолько умело сочетают известные им данные клиента банка и психологические приемы, что люди сами отдают им свои деньги.

Обращаясь к человеку по имени-отчеству, называя обрывки информации о его банковских картах и счетах, лжесотрудники банков вызывают к себе доверие, которое подкрепляют малопонятными, зачастую абсурдными терминами и профессиональными выражениями. Следующий шаг мошенника — вызвать у собеседника сильные эмоции, которые помешают жертве рационально мыслить и критически оценивать ситуацию. Чаще всего — это страх: ваши деньги в опасности. Взломали ваш личный кабинет на сайте банка, с вашей карты совершается денежный перевод неизвестному лицу, от вашего имени поступила заявка на получение кредита. И в этот момент мошенник переходит к последней фазе: еще не поздно все исправить, нужно лишь совершить несколько простых действий. Однако если следовать этим указаниям злоумышленника, результат будет диаметрально противоположным — деньги будут потеряны по-настоящему.



**Что нужно мошеннику, чтобы получить ваши деньги**

Вариантов развития событий несколько. «Спаситель» ваших денег может требовать сообщить ему данные для доступа в мобильный и Интернет-банк, трехзначный CVV или CVC-код (указаны на оборотной стороне карты), срок действия платежной карты, одноразовые пароли из СМС. Даже части этой информации будет достаточно, чтобы мошенник смог перевести ваши деньги на другой счет или оплатить с помощью вашей карты покупки дорогостоящих товаров в интернет-магазине.

«Сотрудники банков не имеют права запрашивать у вас коды и пароли, поэтому вам необходимо самостоятельно произвести операцию» — это начало другого сценария, где мошенник под видом заботы о сохранности ваших средств будет требовать перевести все деньги на «безопасный» счет через онлайн-банк или отправит вас к ближайшему банкомату, где все в итоге закончится тем же самым — переводом денег на счет злоумышленника. Причем сделано это будет вашими же руками. В прошлом году интерес мошенников сместился с текущих расчетных счетов клиентов банков на депозиты. Злоумышленники стараются украсть за один звонок как можно больше денег. Запомните – сотрудники банков никогда не попросят вас под различными предлогами перевести средства на другие счета.

**Что делать, чтобы не отдать свои деньги мошеннику**

«Чем выше осведомленность людей о способах дистанционной кражи денег, тем более сложными и изощренными становятся новые сценарии телефонных мошенников, — рассказывает управляющий отделением по Ленинградской области Северо-Западного ГУ Банка России Сергей Григорьев. — Поэтому не пытайтесь самостоятельно определить, настоящий сотрудник банка вам звонит или мошенник, не сравнивайте ситуацию с уже известными и описанными сценариями. Просто положите трубку, если разговор кажется вам подозрительными. Затем вручную наберите номер телефона вашего банка (он указан на всех банковских картах) и узнайте, действительно ли что-то угрожает вашим сбережениям».



Можно описать десяток известных на сегодняшний день вариантов действий мошенников, но завтра появятся новые. Например, злоумышленники научились подделывать официальные телефонные номера банков и других организаций, стали удлинять цепочки взаимодействия, так что теперь звонят «сотрудники» государственных учреждений, полиции, а уже затем якобы переключают человека на представителя банка. Поэтому самый эффективный способ не отдать свои деньги преступникам — не дать им шанса убедить вас. Запомните, если в разговоре вас торопят, не дают времени подумать, заставляют действовать здесь и сейчас, когда речь идет о деньгах на вашем счете – это признак мошенничества.

