



По словам источников «Денег», расценки у торгующих информацией небольшие. Например, при пробивке клиентов Сбербанка злоумышленники по номеру телефона предлагают узнать наличие счета в банке за 99 руб., за 2,5 тыс. руб. — полный номер банковской карты, за 2 тыс. руб. — выписку операций за один месяц, за 8–10 тыс. руб. — кодовое слово, за 5–6 тыс. руб. — паспортные данные владельца, включая прописку и т. д.

Повод для звонка

Поводы для звонка у представителя банка могут быть самые разные. Самый популярный, но далеко не единственный — это мошенническая операция по счету. Однако во всех случаях злоумышленник обязательно постарается выяснить номер карты, дату ее выпуска, код подлинности cvv2/cvc2, паспортные данные владельца карты, коды верификации.

«Есть мнение — если забить в телефон номер банка, то при звонке с подменой номера вы всегда отличите банк от мошенников. Это не так, — утверждает Лука Сафонов. — Если вы забили номер кредитной организации как „Мой банк“, то при мошенническом звонке „Мой банк“ и высветится».

Впрочем, нередко мошенники звонят и с похожих номеров. Например, мошеннический звонок с 8-800 часто определяется как звонок из Бангла-

деш. Порой даже номера телефонов подменяются на номера частных лиц, которые случайно оказались похожи на телефон того или иного банка.

По словам Луки Сафонова, в большинстве случаев мошенники используют «скрипты» обзвона, основанные на реальном скрипте банка, используя ловушки и приемы скрытой манипуляции. «Например, всем известно, что не надо сообщать девичью фамилию матери, — рассказывает Лука Сафонов. — Но легко сообщают фамилию девушки по материнской линии, а это и есть искомый вопрос». Впрочем, бывают и уникальные, но в то же время эффективно работающие скрипты. Чаще всего, отмечает Лука Сафонов, во время разговора слышен характерный шум колл-центра, что также направлено на повышение доверия граждан. «Это может быть как запись реального колл-центра, так и колл-центр мошенников», — отметил эксперт. При реальном звонке колл-центра звук колл-центра не слышен из-за специального шумопоглощающего оборудования.

Наряду с мошенническими звонками с подменой номера злоумышлен-

ники активно используют и СМС. Весьма распространенный вариант — жертва получает сообщение якобы от банка о том, что его карта заблокирована. При этом мошенническое СМС может прийти с номера, похожего до степени смешения на телефон банка. Например, от имени Сбербанка мошенники посылали СМС не с 900, а с 900. Или не от Tinkoff, а от Tinkoff. Однако главное отличие мошеннического СМС от реального — переписка с «банком» будет начата в новом диалоговом окне.

Кто все рассказывает

Стандартное заблуждение граждан — «уж я-то точно не попадусь на звонок мошенника», уверяют эксперты. Если судить по сообщениям жертв социальной инженерии, чаще всего они называли данные своих карт в несколько измененном состоянии — либо чрезвычайно расслабленном, либо взвинченном. Например, призналась одна дама, ей позвонили в день рождения, когда была куча гостей, праздник, и она все назвала лишь потому, чтобы «быстрее решить проблему». Еще одна

У МЕНЯ ЗАЗВОНИЛ ТЕЛЕФОН...

ЛУКА САФОНОВ,
руководитель лаборатории
практического анализа
защищенности компании
«Инфосистемы Джет»

Около полудня раздался звонок с прямого московского номера, мне сообщили мое ФИО и год рождения, заявили, что в данный момент с моей карты пытаются снять деньги. Для того чтобы эта операция не была произведена и все мои карты не заблокировали на 14 дней, мошенник просил подтвердить мои данные и что карта находится у меня. На фоне был шум, имитирующий колл-центр.

М. — Вам необходимо привязать двухфакторную авторизацию на ваш телефон.

Я. — Она у меня активирована.

М. — Да, я вижу, но произошла попытка списать с вашей карты 15 тыс. руб. неким Николаем Алексеевичем, последние цифры номера телефона 2186. Иначе все ваши карты будут заблокированы на 14 дней.

Я. — Ок. Что нужно делать?

М. — Давайте пройдем идентификацию — по номеру счета, через онлайн-помощника или по номеру карты. Да, 28.12.18 вам должно было приходиться СМС с номера 900 о том, что скоро будет необходимо обновить двухфакторную авторизацию. Далее были попытки перевести меня на «робота» якобы для подтверждения блокировки мошеннической операции — «специалист» «переключил» меня на голосового помощника, который механическим голосом попросил ввести номер моего счета (на минутку, это более десяти цифр, и на память такое мало кто помнит) — естественно, этот тест я с треском «провалил». После этого меня «переключило» на специалиста, и он предложил «ручную верификацию».

В такой схеме может быть два варианта — у мошенника есть напарник, который параллельно звонит в банк со всеми вашими данными и назовет кодовое слово, которое выманит первый мошенник, либо эти данные будут использованы для других схем. Также может использоваться «проверка» посредством «СМС», когда вы, не кладя трубку, сообщите мошеннику содержимое СМС, что позволит ему совершить денежный перевод с вашего счета или карты или вообще даст возможность доступа ко всем средствам через мобильный банк или приложение.

В моем случае злоумышленник хотел узнать реквизиты карты для совершения с ней мошеннических действий (даже если у вас настроено СМС-подтверждение, это не всегда уберет от списания — в интернете полно сервисов без 3D-Secure, достаточно просто знать реквизиты вашей карты).

Главное отличие мошеннического СМС от реального — переписка с «банком» будет начата в новом диалоговом окне