RTM GROUP

Практикум по работе с банковскими хищениями: как противостоять интернет-мошенничеству

RTM TECHNOLOGIES — первая экспертная компания, специализирующаяся на проведении нормативных и нормативно - технических экспертиз в области ИБ и ИТ.

rtmtech.ru

СТАТИСТИКА ОПЕРАЦИЙ, СОВЕРШЕННЫХ БЕЗ СОГЛАСИЯ КЛИЕНТОВ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ ЗА 2019 ГОД

Всего украдено 6426,5 млн рублей, из них:

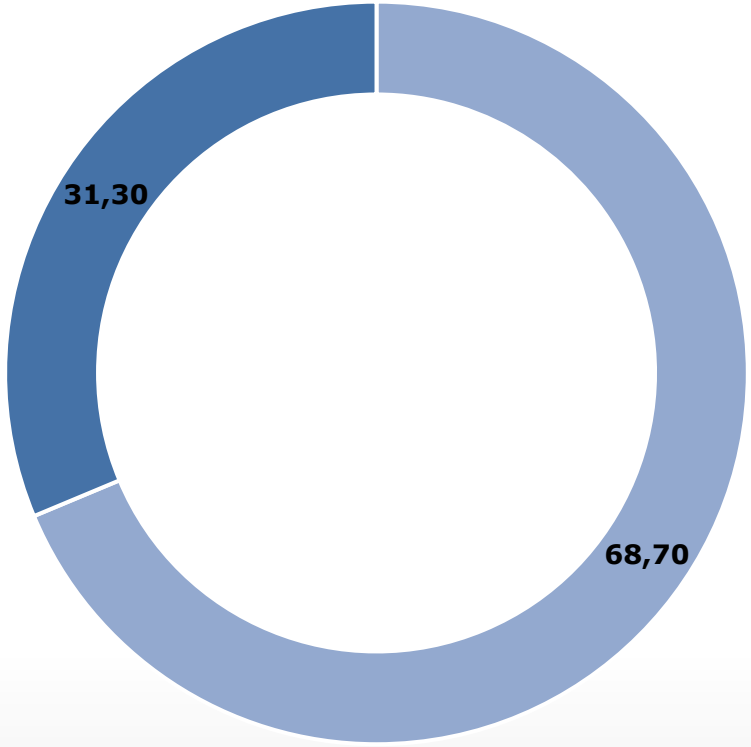
- **5723,5 млн рублей (физ. лица)**
- **701 млн рублей (юр. лица)**

Количество совершенных хищений - 576 566, в т.ч.:

- **571 957** единиц (**физ. лица**)
- **4 609** единиц (**юридические лица**)

Средняя сумма одной операции:

- **физ. лиц 10 тыс. рублей**
- **юр. лиц – 152 тыс. рублей**

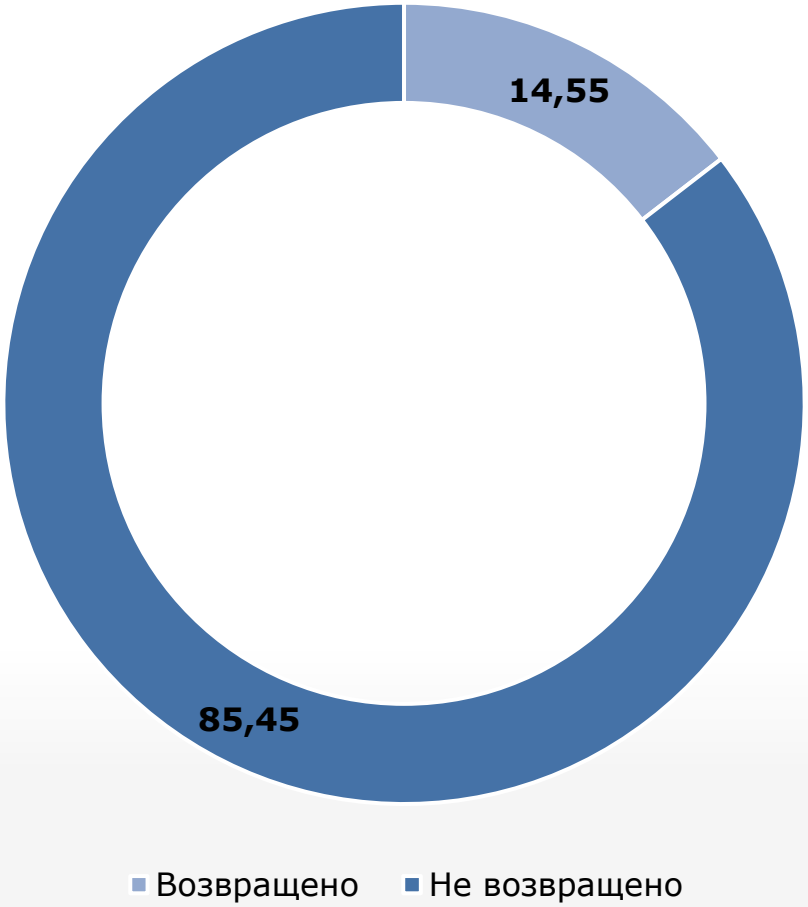


СТАТИСТИКА ОПЕРАЦИЙ, СОВЕРШЕННЫХ БЕЗ СОГЛАСИЯ КЛИЕНТОВ ФИНАНСОВЫХ ОРГАНИЗАЦИЙ ЗА 2019 ГОД

Банки возместили клиентам 935 млн руб.

(**15%** или **каждый 7-й похищенный рубль**):

- **869,9 млн рублей** (**физ. лица**)
- **65 млн рублей** (**юридические лица**)



СВЕДЕНИЯ БАНКА РОССИИ ОБ ИНЦИДЕНТАХ

В 2019 г. отчитывающиеся **операторы (ОПС и ОПДС)** направили в Банк России информацию о **973 инцидентах**, связанных с **несанкционированным доступом к их информационной инфраструктуре**, на общую **сумму 103,8 млн рублей**.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. КАК ОБМАНЫВАЮТ ФИЗИЧЕСКИХ ЛИЦ

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. КАК ЗАЩИТИТЬСЯ ФИЗИЧЕСКИМ ЛИЦАМ

Не доверять звонкам. **Никаким.**

Никому **НЕ СООБЩАТЬ РЕКВИЗИТЫ КАРТЫ и ДАННЫЕ SMS/PUSH**

НЕ ПЕРЕЗВАНИВАТЬ на номера, которые вам продиктовал «сотрудник банка».

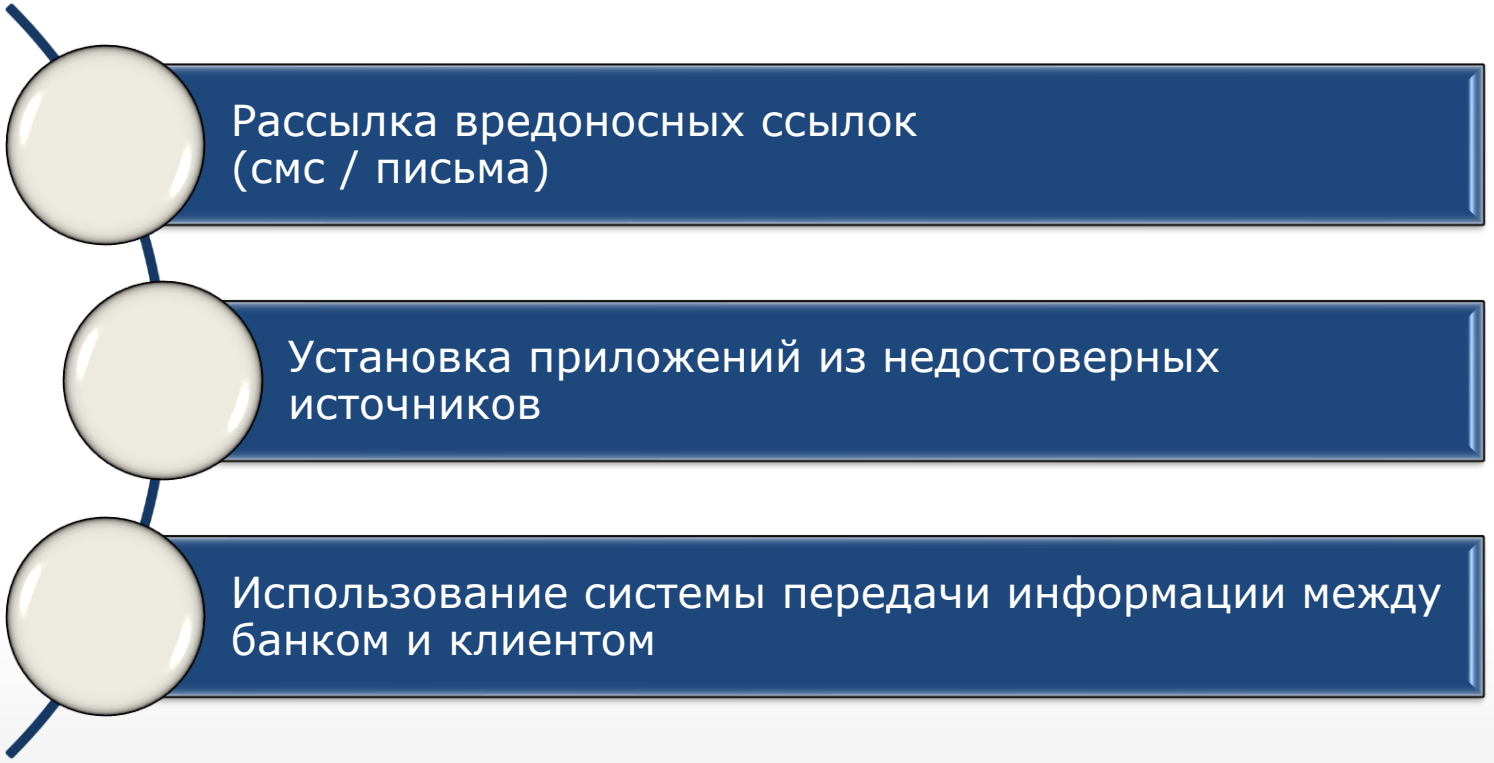
СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. КАК ОБМАНЫВАЮТ ЮРИДИЧЕСКИЕ ЛИЦА

- Рассылка писем, ориентированных на получение конфиденциальной информации
- Звонки банков / контролирующих органов

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ. КАК ЗАЩИТИТЬСЯ ЮРИДИЧЕСКИМ ЛИЦАМ

- Применение принципа четырех глаз
- Осведомленность сотрудников организации

ПЕРЕХВАТ УПРАВЛЕНИЯ УСТРОЙСТВОМ. КАК ОБМАНЫВАЮТ ФИЗИЧЕСКИХ ЛИЦ

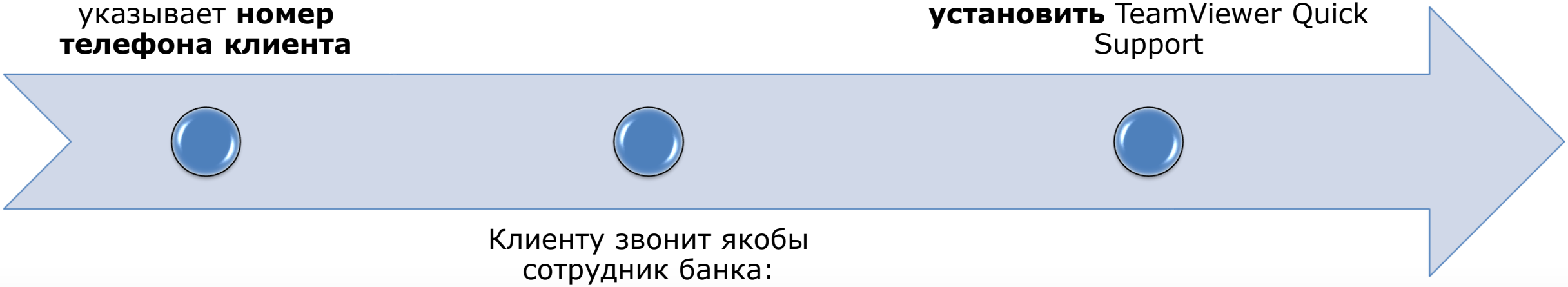


СЦЕНАРИЙ АТАКИ С ИСПОЛЬЗОВАНИЕМ TEAMVIEWER REMOTE CONTROL

Мошенник подает **заявку на кредит** на **сайте Банка** и указывает **номер телефона клиента**

Клиенту звонит якобы сотрудник банка: **интернет-банк взломан** с помощью **вирусного ПО**; кто-то **пытается оформить кредит**; **срочно сбросить пароль**

«**Сотрудник банка**» **лично проведёт** действия по **отмене** оформленного **кредита** и **сбросит пароль**: **необходимо установить** TeamViewer Quick Support

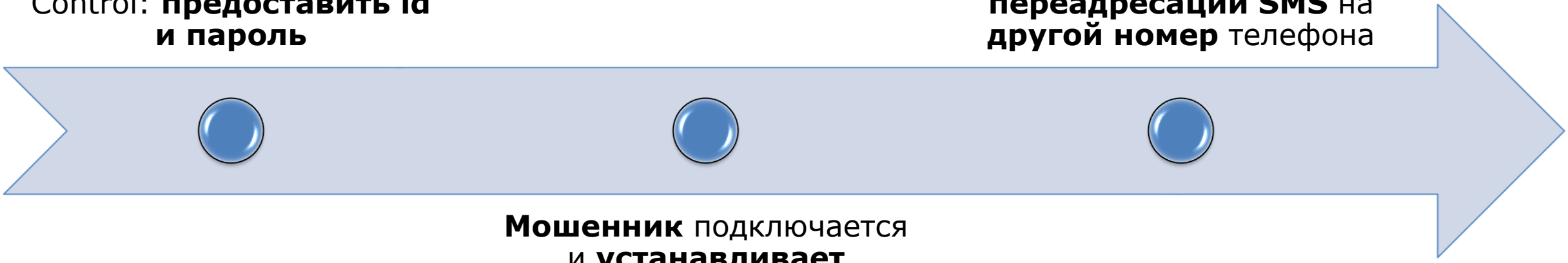


СЦЕНАРИЙ АТАКИ С ИСПОЛЬЗОВАНИЕМ TEAMVIEWER REMOTE CONTROL

Если **у клиента** уже **установлен** Remote Control: **предоставить id и пароль**

Мошенник подключается и **устанавливает кейлоггер**; информация **клиенту** – **вредоносная программа** успешно **удалена**

Клиента просят **проверить** в **личном кабинете сотового оператора**, нет ли **переадресации SMS** на **другой номер** телефона

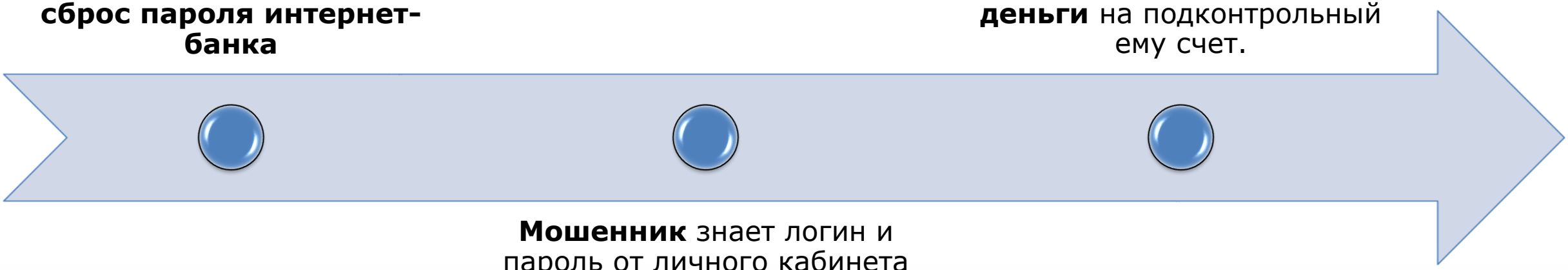


СЦЕНАРИЙ АТАКИ С ИСПОЛЬЗОВАНИЕМ TEAMVIEWER REMOTE CONTROL

Мошенник инициирует **сброс пароля интернет-банка**

Мошенник знает логин и пароль от личного кабинета мобильного оператора, **устанавливает переадресацию SMS** на подконтрольный ему номер; номер карты, CVV, логин и пароль от интернет-банка.

Мошенник получает кредит наличными **на карту клиента** и **выводит деньги** на подконтрольный ему счет.



ПЕРЕХВАТ УПРАВЛЕНИЯ УСТРОЙСТВОМ. КАК ЗАЩИТИТЬСЯ ФИЗИЧЕСКИМ ЛИЦАМ

- Установить антивирусную программу. Регулярно ее обновлять
- Не устанавливать приложения из неизвестных источников, в т.ч. взломанные игры
- Проверять разрешения, запрашиваемые приложениями
- Не устанавливать мобильный банк на то же устройство, куда приходят SMS-подтверждения
- Не использовать мобильное банковское приложение при подключении к общедоступной точке Wi-Fi

ПЕРЕХВАТ УПРАВЛЕНИЯ УСТРОЙСТВОМ. КАК ОБМАНЫВАЮТ ЮРИДИЧЕСКИЕ ЛИЦА

- Переход по ссылкам из писем / открытие вложений
- Неправильно организованная (отсутствующая) политика информационной безопасности
- Неосведомленность сотрудников о возможных угрозах
- Противоправные действия сотрудников организации

ПЕРЕХВАТ УПРАВЛЕНИЯ УСТРОЙСТВОМ. КАК ЗАЩИТИТЬСЯ ЮРИДИЧЕСКИМ ЛИЦАМ

- Выделенный компьютер для работы с системами дистанционного банковского обслуживания
- Установка ограничений на проведение операций
- Двойной контроль платежных поручений
- Эффективная антивирусная защита
- Применение технических мер защиты информации
- Применение организационных мер защиты информации
- Осведомленность сотрудников организации

ВЗЯТИЕ КРЕДИТА. КАК ОБМАНЫВАЮТ ФИЗИЧЕСКИХ ЛИЦ

- Звонок мошенников с переводом на робота
- Установка удаленного приложения
- Звонок мошенников с отправкой СМС с официального номера
- Звонок мошенников - необходимо взять "зеркальный кредит"

ВЗЯТИЕ КРЕДИТА. ПРИМЕР ОФОРМЛЕНИЯ «ЗЕРКАЛЬНОГО КРЕДИТА»

Звонит сотрудник банка и говорит, что уже **взят или прямо сейчас оформляется** крупный **займ / кредит**.

Необходимо **войти** в **личный кабинет** и **оформить** так называемый зеркальный **кредит**, чтобы **аннулировать действия мошенников**.

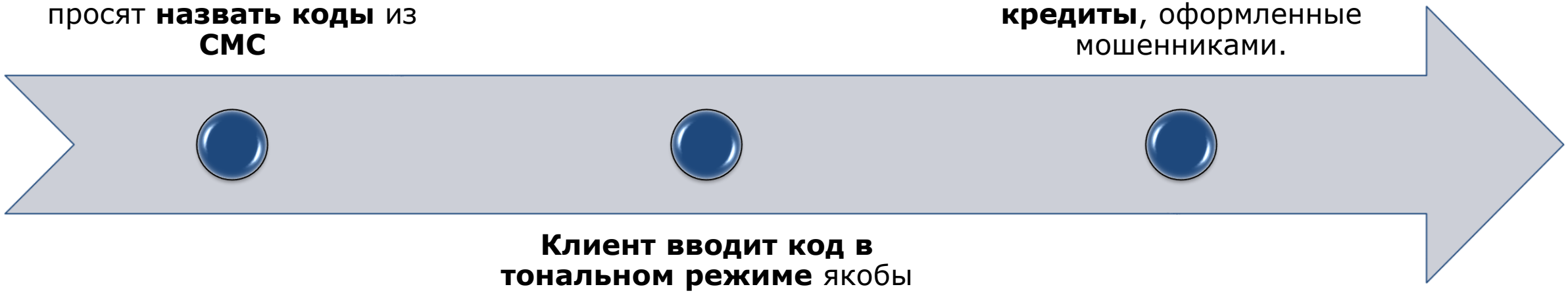
Полученную сумму необходимо либо сразу же **перевести на резервный счет**, либо вначале **обналичить** через безопасный банкомат банка партнера, после чего **перевести деньги на резервный счет**

ВЗЯТИЕ КРЕДИТА. ПРИМЕР ОФОРМЛЕНИЯ КРЕДИТА ПРИ ОБЩЕНИИ С РОБОТОМ БАНКА

Звонок «сотрудник банка»: на клиента якобы **оформляются** незаконные **кредиты**, **для** их **отмены** просят **назвать коды** из **СМС**

Клиент вводит код в тональном режиме якобы **в автоматизированной банковской системе**

Со счета **списываются собственные средства клиента**, а также **онлайн-кредиты**, оформленные мошенниками.



ВЫВОДЫ

- Осведомленность
- Многофакторная аутентификация
- Разделение факторов между устройствами
- Оперативное реагирование на обращения
- Antifraud системы

НАМ ДОВЕРЯЮТ

УПРАВЛЕНИЕ
ФЕДЕРАЛЬНОЙ СЛУЖБЫ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПО КРАСНОДАРСКОМУ КРАЮ

БЛАГОДАРСТВЕННОЕ ПИСЬМО

МУЗАЛЕВСКОМУ
Фёдору Александровичу

От имени УФСБ России по Краснодарскому краю выражаем Вам благодарность за активное участие в деятельности по обеспечению информационной безопасности Российской Федерации, высокий уровень профессионализма, оперативное и качественное проведение компьютерно-технических исследований.

Начальник УФСБ России
по Краснодарскому краю
генерал-майор С.Б. Захарихин
«27» октября 2020 года

БЛАГОДАРСТВЕННОЕ ПИСЬМО

Отдел "К" БСТМ УМВД России по Липецкой области
выражает благодарность экспертному учреждению
ООО "РТМ ТЕХНОЛОГИИ" и лично ведущему эксперту
Музалевскому Федору Александровичу
за регулярное содействие в раскрытии киберпреступлений,
оперативное и качественное проведение компьютерно-технических
судебных экспертиз, а также оказание консультаций в области
информационной безопасности.

Начальник отдела «К»
подполковник полиции А.В. Лялякин

СПАСИБО ЗА ВНИМАНИЕ!

Музалевский Федор Александрович

Директор технического департамента RTM Group

Волокитин Сергей Анатольевич

Ведущий эксперт компьютерно-технического направления RTM Group

8 800 201-20-70

info@rtmtech.ru

https://rtmtech.ru

GroupRTM

rtm.group

@GroupRtm

rtm.group.Russia

t.me/kurilka_ib