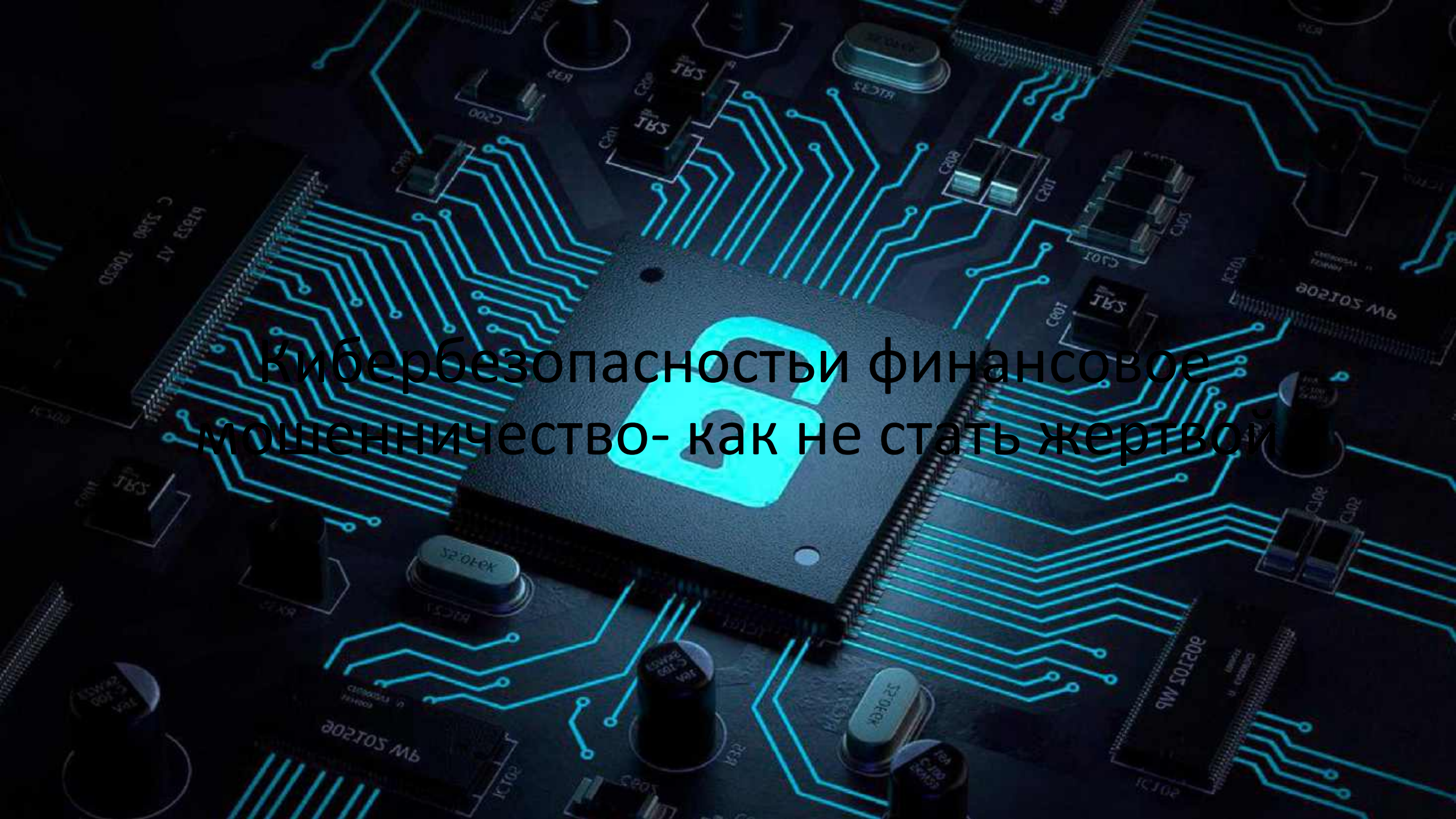


Кибербезопасностьи финансовое мошенничество- как не стать жертвой

Социальная инженерия – угроза №1

- Социальная инженерия в настоящее время – самый актуальный тип мошенничества.

- **более 90%** фактов хищения – с использованием социальной инженерии

- **30 млн в сутки** - количество попыток телефонного мошенничества в отношении россиян в 2024 по сравнению с 5 млн в 2022.

почему это случилось?

Сильное душевное волнение вследствие:

- самоустранения от реалий современной жизни, самонадеянности или отсутствие сбережений
- Отсутствия знаний о методах социальной инженерии, IP-телефонии, технологии DeepFake
- доверия к *значимому «титулу» (*предоставление ему критичной информации, осуществление иных действий)
- незнания технологии работы банков, правоохранительных или иных гос. структур
- Недостаточных навыков критического мышления

- Желаниелегкогозаработка

Последствия действий телефонных мошенников

	2020	2021	2022-2023	2024
Объекты посягательства	сбережения	сбережения	сбережения	сбережения
		кредиты	кредиты	кредиты
			жилье	жилье
				Акты терроризма

- 99% звонков с подменой номера
- Все больше фактов мошенничества - с использованием кредитных средств

- Каждая сотая жертва лишается единственного жилья

КАК МОШЕННИКИ ПОЛУЧАЮТ ДОСТУП К СРЕДСТВАМ ЛЮДЕЙ?

Получают несанкционированный доступ к онлайн-банкингу путем:

- вирусного заражения мобильных устройств (вирусные ссылки в SMS, MMS, установка приложений из непроверенных источников и т.п.)
- получения критичной информации по карте (фишинговые сайты/ взлом настоящих сайтов компаний).

Вступают в непосредственный контакт с целью:

получить важную информацию, дающую доступ к банковским счетам или личному кабинету в интернет - порталах, позволяющих в т.ч совершать сделки от имени граждан (Госуслуги и т.п.) и похитить имущество жертвы

заставить жертву отправить деньги на счета преступников, оформить сделку по передаче своего имущества самостоятельно

Некоторые варианты социальной инженерии с целью хищения денежных средств, завладения имуществом

SMS-мошенничество, фишинговые письма

Мошенничество в социальных сетях, в т.ч. с предложением «легкого заработка»

QR-коды в общественных местах,

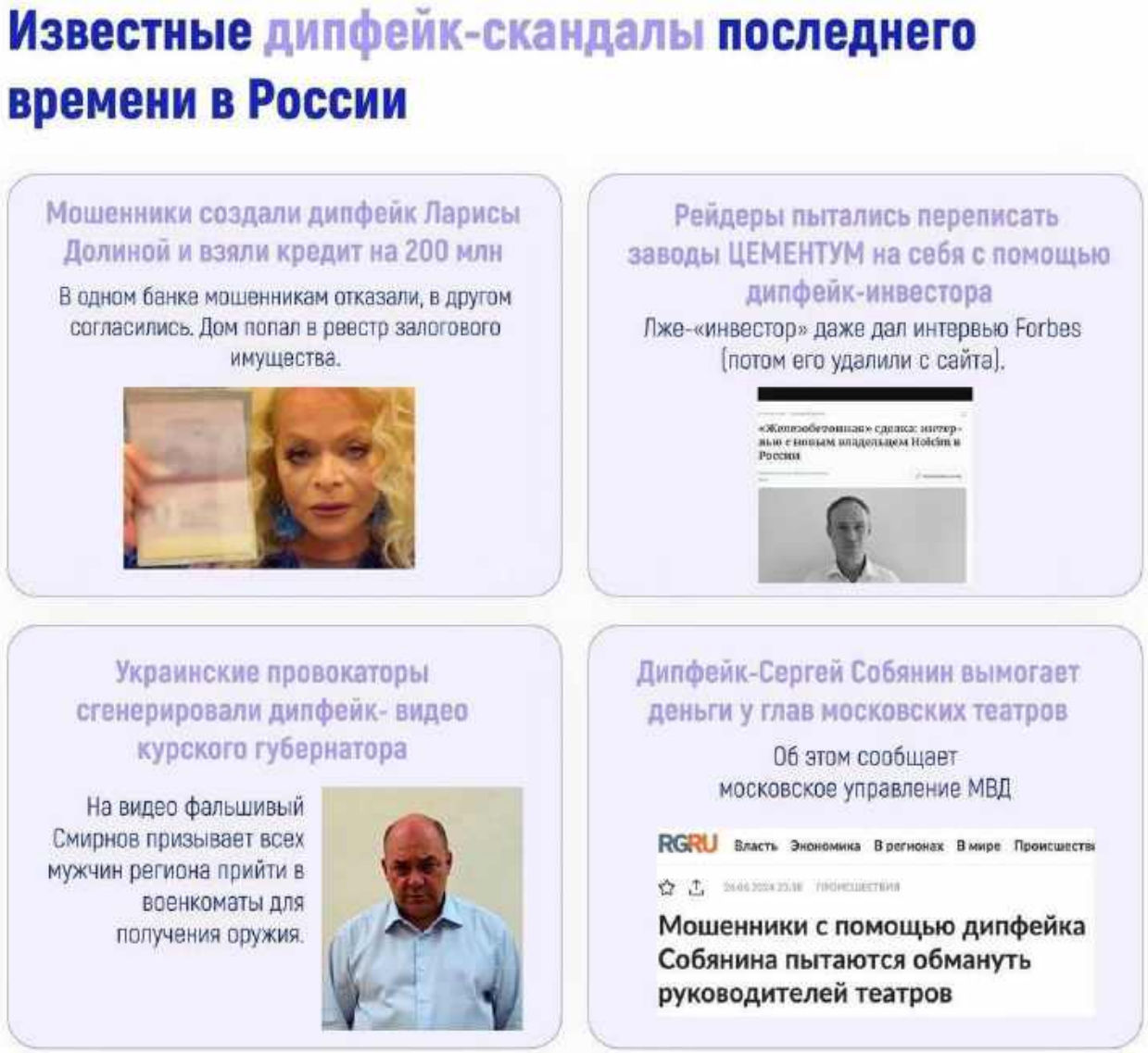
Телефонное мошенничество (социальная инженерия): - аватарке виден логотип известного банка или эмблема МВД (ФСБ, Следственного комитета и т.п.), или другие легко узнаваемые логотипы, присылают якобы фото документов и удостоверений и т.п.

- видеозвонки через мессенджер – имитация звонка из офиса банка, подразделения полиции (ФСБ и т.п.) с последующими аналогичными действиями. -

использование курьеров для доставки фиктивных писем, получения денег.

Технология DeepFake

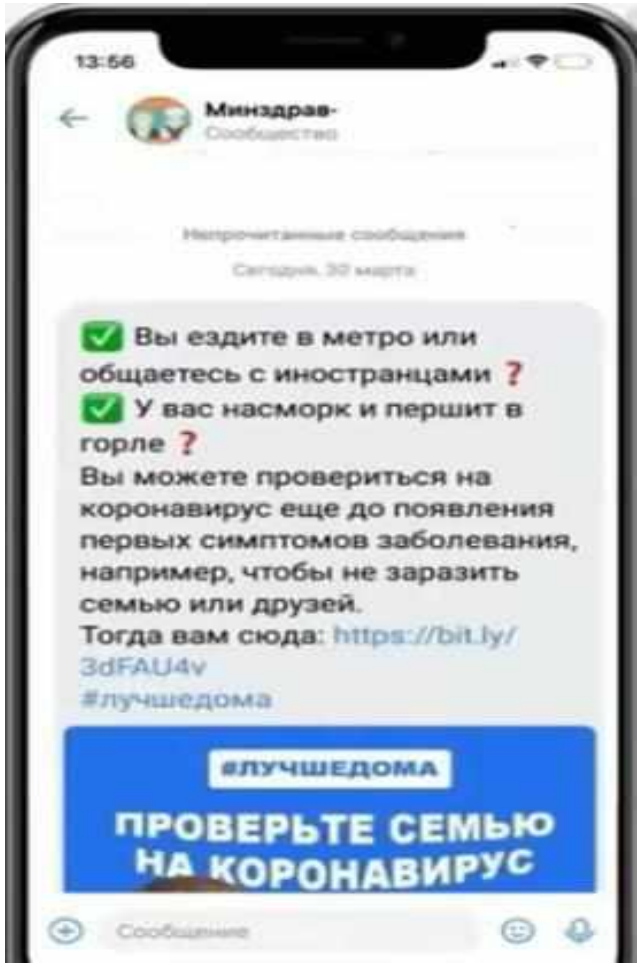
звонки через мессенджер. При таком звонке на



Примеры мошенничества в сети интернет

Компрометация реквизитов карты через фишинговые сайты

- Мошенники создают в интернет фишинговые сайты (сайт под видом сайта реальных компаний) для сбора персональных данных клиентов и критичной банковской информации.
- Еще мошенники размещают в интернет на разных сайтах объявления о продаже товара (услуг) по «выгодным» для покупателей ценам (условиям).
- При проявлении заинтересованности «продавец» (мошенник) **направляет покупателю ссылку на сайт для оплаты** товара (фактически – на фишинговый сайт).
- Человек заходит на фишинговый сайт и вводит реквизиты своей банковской карты.
- Мошенник, получив данные карты, совершает покупки в интернет-сервисах, где нет подтверждения одноразовыми паролями, на всю сумму, имеющуюся на карте либо переводит средства на свои карты.



Примеры мошенничества в сети интернет

Предложение быстрого обогащения

множество объявлений в интернет **о быстром и легком заработке**. Но зачастую в таких случаях внезапно разбогатеть удается только самим махинаторам:

- вложить деньги в «сверхприбыльный проект» (спойлер — в финансовую пирамиду).
- предлагают «быстро заработать», просто зарегистрировавшись на сомнительном сайте и выполняя задания или делая букмекерские ставки. Для вывода «заработка» надо «оплатить комиссию». В итоге - деньги вместе с данными карты оказываются в руках махинаторов.
- «быстро заработать» по объявлениям в мессенджерах/социальных сетях - работа «курьером»: За данную работу можно получить процент от полученных денег, а также **<u>судимость</u>**

Некоторые предлоги, с которыми обращаются мошенники к жертве

САМЫЕ ЧАСТЫЕ СЛУЧАИ

- «Попытка хищения средств или имущества», «попытка получения кредита» и необходимость «переоформления кредита для перекрытия суммы (в т.ч. под залог недвижимости)» , «оформление подконтрольной сделки с объектом недвижимости», дальнейший перевод денег на «спец.счет», «безопасный счет» и т.п., иные счета, указанные преступниками.

- **«Оказание помощи полиции (прокуратуре, следственному комитету и т.п.), участие в спецоперации по в поимке злоумышленников в банке» для «задержания работников банка с поличным».**

- **«расследование по факту финансирования ВСУ» и компенсация отправленных сумм путем оформления кредитов или снятие со вкладов и направления денег на спец.счет.**

- «Родственник «попал в беду» и надо «срочно направить или передать деньги для «решения вопроса», для «операции». «Нужны деньги для проверяющих из вышестоящей организации».

- «Блокировка карты», «проблемы» с личным кабинетом на сайте Госуслуг, продление услуг оператора мобильной связи и т.п. и «необходимость» подтверждения реквизитов (номера карт, пароли, поступившие смс, введение кодов на телефоне и т.п.) для «разблокировки» и др.

- «Компенсации» («страховки») за перенесенные заболевания, выплаты «в связи с СВО», перерасчет пенсии и т.п.

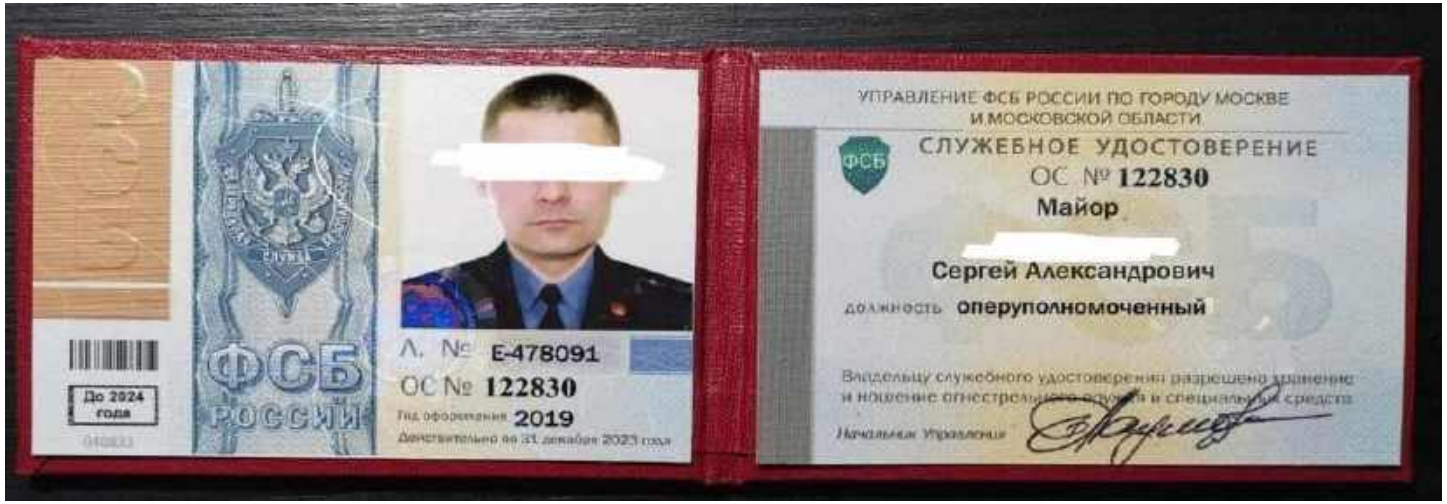
Как они нас обманывают?

Принципиальная схема социальной инженерии

1. «Задавить авторитетом» с использованием технологии подмены номера и специфической терминологии
2. Вывести жертву из душевного равновесия (страх, эйфория)
3. Закрепить, подтвердить «достоверность» информации из «другого источника» в т.ч. с использованием фиктивных документов
4. Нагнетание «срочности»
5. Запрет на общение с другими лицами, инструктаж о «легенде»
6. Длительное удержание жертвы «на телефоне»
7. управление по телефону действиями жертвы Дополнения:
8. Воздействие с отлагательным эффектом: разделение звонков от «разных источников» по времени

9. Побуждение к совершению теракта, хулиганских, иных противоправных действий
10. Имитация «похищения» человека (с хищением денег у жертвы) и вымогательство денег (у родственников)

Некоторые примеры «документов», направленных мошенниками жертве



Федеральная Служба безопасности
Российской Федерации

17.08.2022 № 30/1-р-2022

ПОВЕСТКА

(к вызову на допрос в качестве свидетеля)

Уважаемая

В соответствии с частью 8 статьи 162 УПК РФ уведомляю Вас, что с 17.08.2022 срок предварительного следствия по уголовному делу №280127052 части 3 статьи 159 УПК РФ (Мошенничество с превышением должностных полномочий), продлевается до 22.08.2022. Гражданин Г. , была назначена личная встреча в УФСБ России по Чувашской Республике, г. Чебоксары, ул. К. Маркса, д. 43 (каб. 28), и в связи с поступлением служебной переписки с ПАО "Сбербанк", назначается визит в 13 часов 00 минут для предоставления результатов следствия и дачи показаний со стороны потерпевшей.

Постановил

Ходатайствовать перед руководителем следственного отдела Следственного комитета при Прокуратуре Российской Федерации по г. Брянск о продлении сроков предварительного расследования по уголовному делу №280127052 под надзором капитана УФСБ: Смолин С. А..

В соответствии с ч.1 ст 144 УПК РФ, Вам надлежит прибыть 22 августа 2022 года к 13 ч. 00 мин. в УФСБ г. Чебоксары по адресу: ул. К. Маркса, д. 43, (каб. 28) для дачи объяснений по материалам проверочного сообщения о преступлении от Центрального банка зарегистрированного в книге №1 регистрации сообщений о преступлениях за дело №64.

При себе необходимо иметь паспорт или другой документ удостоверяющий личность. При наличии причин препятствующий явке по вызову, Вам необходимо заранее увеличить капитана УФСБ заказным письмом по указанному выше адресу.

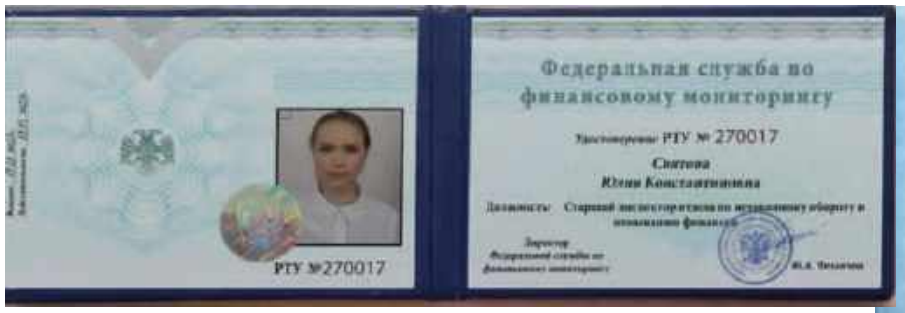
Майор УФСБ Чувашской Республике
Российской Федерации и
Приволжском федеральном округе Ю.М. Ланко

Ф.И.О.:

Дата: Подпись:

АП № 077

с использованием материалов ПАО Сбербанк



с использованием материалов ПАО Сбербанк

с использованием материалов
ПАО


МВД РОССИИ

НВК № 012398

Действительно

Личный № А-144913 по 20 марта 2026

ГЛАВНОЕ УПРАВЛЕНИЕ МВД РОССИИ
ПО МОСКОВСКОЙ ОБЛАСТИ

СЛУЖЕБНОЕ УДОСТОВЕРЕНИЕ № 012398

Подполковник внутренней службы
Александров
Юрий Николаевич

должность Комитет
Экономической безопасности
ГУ МВД

Владелец удостоверения имеет право на постоянное ношение и хранение табельного огнестрельного оружия и специальных средств

Начальник (заместитель)

20 марта 2020


СЛЕДСТВЕННОЕ УПРАВЛЕНИЕ
СЛЕДСТВЕННОГО КОМИТЕТА
РОССИЙСКОЙ
ФЕДЕРАЦИИ

МОО №937258

Действительно

Личный № ЕВ - 034913 по 23 апреля 2024 г.

СЛЕДСТВЕННОЕ УПРАВЛЕНИЕ
по Московской области

СЛУЖЕБНОЕ УДОСТОВЕРЕНИЕ МОО №937258

Старший лейтенант
Жураковский
Валентин Владимирович

Следователь

Владелец удостоверения имеет право на постоянное ношение и хранение табельного огнестрельного оружия и специальных средств

Начальник (заместитель)

Мещанинов В.И


МВД РОССИИ

МОО №576214

Действительно

Личный № ЕВ - 034913 по 27 марта 2022 г.

ГЛАВНОЕ УПРАВЛЕНИЕ МВД РОССИИ
ПО ТЮМЕНСКОЙ ОБЛАСТИ

СЛУЖЕБНОЕ УДОСТОВЕРЕНИЕ МОО №576214

Майор полиции
Филатов
Дмитрий Николаевич

Следователь

Владелец удостоверения имеет право на постоянное ношение и хранение табельного огнестрельного оружия и специальных средств

Начальник (заместитель)

27 марта 2017 г.


МВД РОССИИ

МКВ № 159777

Действительно

Личный № Б-117342 по 20 апреля 2023

Главное управление
МВД РОССИИ по Чувашской Республике

СЛУЖЕБНОЕ УДОСТОВЕРЕНИЕ МКВ № 159777

Капитан полиции
Волков
Михаил Олегович

должность следователь

Владелец удостоверения имеет право на постоянное ношение и хранение табельного огнестрельного оружия и специальных средств

Министр (заместитель)

20 апреля 2020


МВД РОССИИ

КРД № 076000

Действительно

Личный № Б-901216 по 15 февраля 2021 г.

ГЛАВНОЕ УПРАВЛЕНИЕ МВД РОССИИ
ПО КРАСНОДАРСКОМУ КРАЮ

СЛУЖЕБНОЕ УДОСТОВЕРЕНИЕ КРД № 076000

Старший лейтенант полиции
Донской
Олег Владимирович

должность дознаватель

Владелец удостоверения имеет право на постоянное ношение и хранение табельного огнестрельного оружия и специальных средств

Начальник (заместитель)

15 февраля 2017 г.


СЛЕДСТВЕННЫЙ
КОМИТЕТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

МКВ № 771560

СЛУЖЕБНОЕ УДОСТОВЕРЕНИЕ МКВМ 771560

Организационная структура мошеннического call-центра

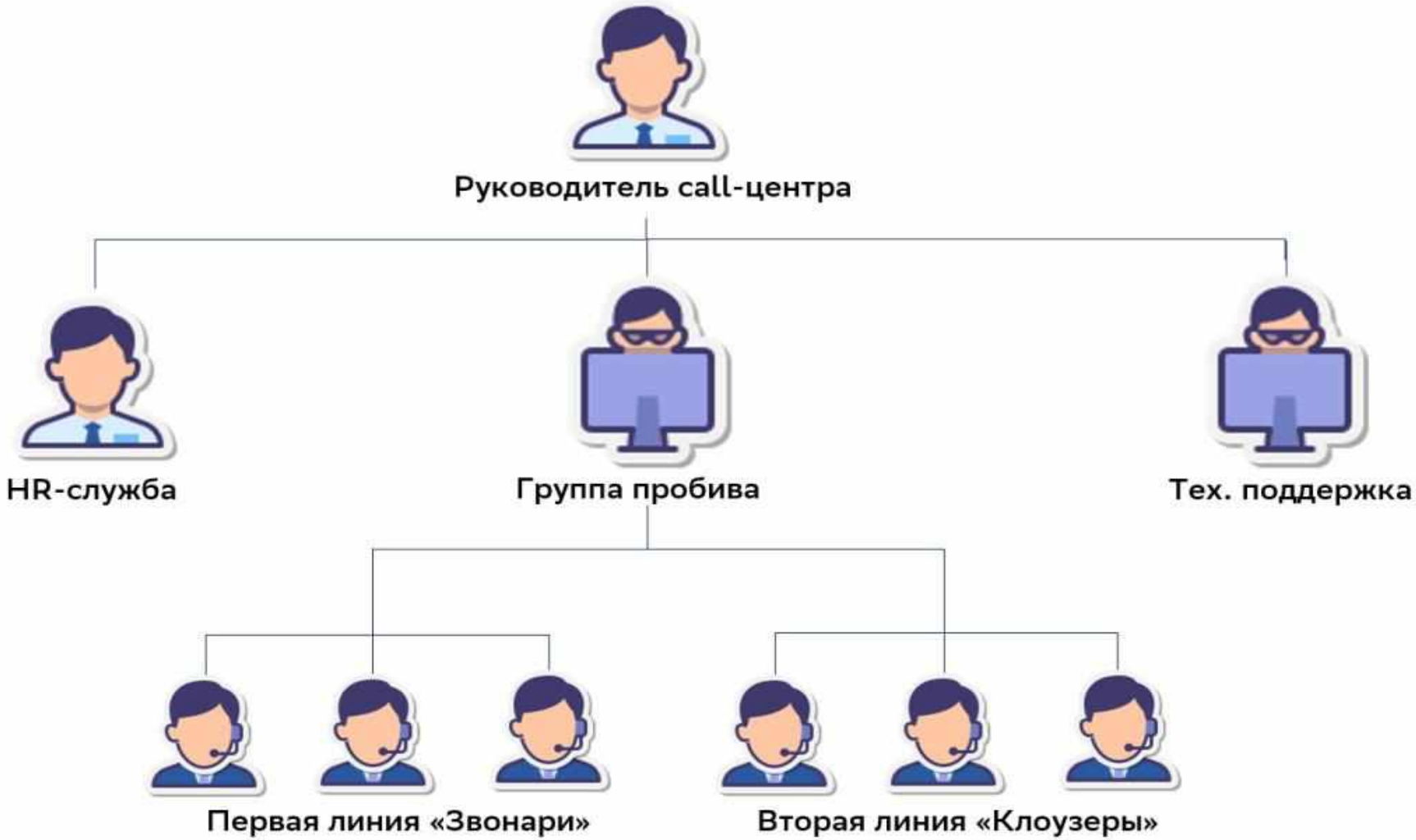
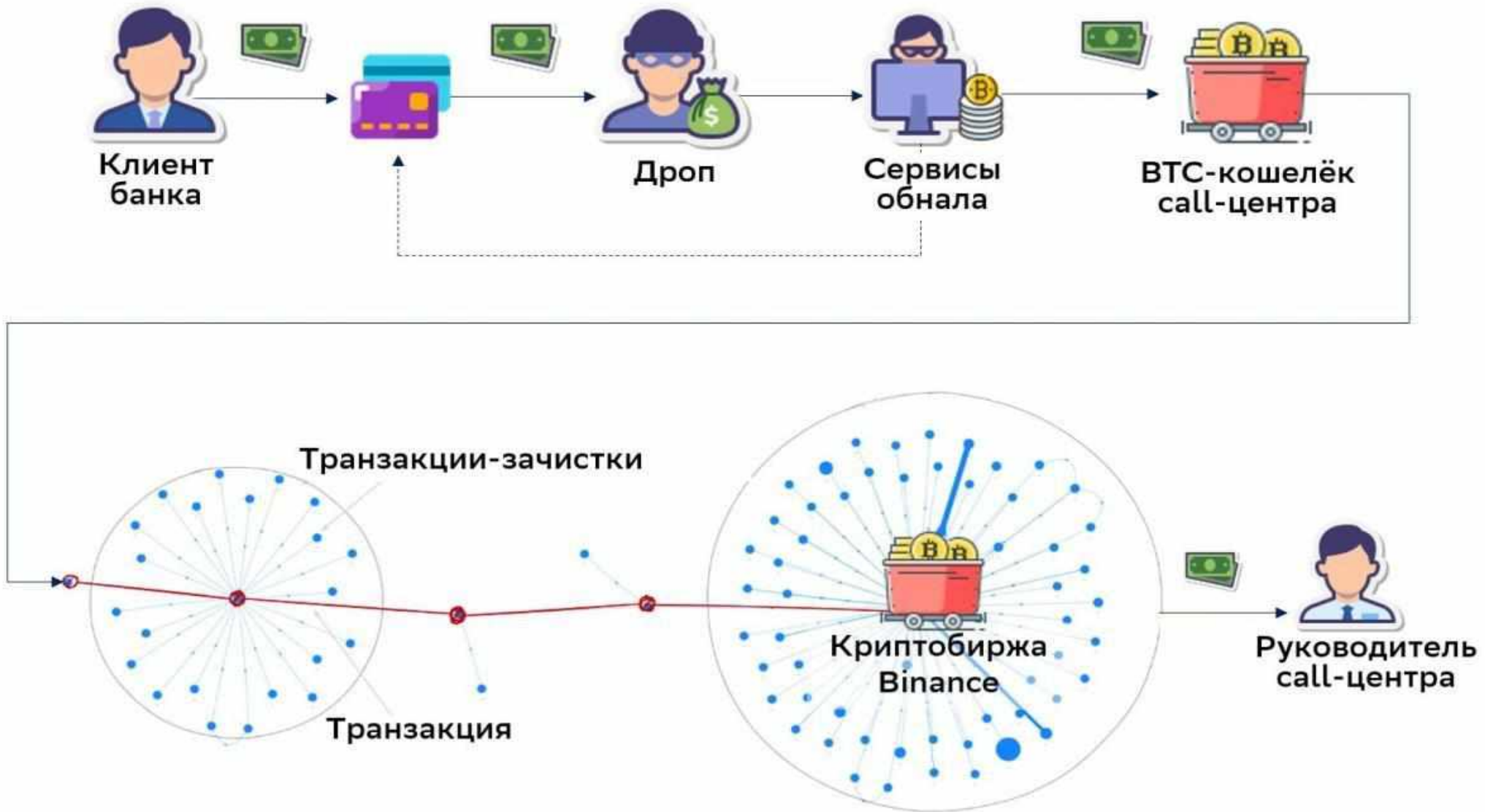


Рисунок 15. Организационная структура call-центра «Бердянск»

с использованием материалов ПАО Сбербанк

Схема обналичивания похищенных денег


Клиент банка
Дроп
Сервисы обнала
BTC-кошелёк call-центра
Транзакции-зачистки
Транзакция
Криптобиржа Binance
Руководитель call-центра

с использованием материалов ПАО Сбербанк

ЧТО ДЕЛАТЬ?

ЧТО ДЕЛАТЬ?

✈НИЧЕГО НЕ ДЕЛАТЬ!

- ✈**не сообщать вообще никаких сведений**
- ✈**не совершать никаких действий с деньгами и имуществом**
- ✈**не устанавливать никаких программ**
- ✈**не нажимать никаких кнопок на телефоне или ином гаджете**
- ✈ **и т.п.**

Самые простые правила финансовой безопасности

Если Вам позвонили с неизвестного номера,
и стали рассказывать о проблемах с Вашими деньгами, имуществом:

- **Отнеситесь с недоверием к звонку неизвестного Вам** абонента**, успокойтесь и критически оцените информацию**
- **Вспомните, что мошенники существуют (независимо от нашего желания), что возможна подмена номера, изображения и голоса, видеозвонок**
- **Вспомните, технологию работы банков и правоохранительные органов и иных госструктур**
- **Не совершайте никаких действий**
- **Сразу прервите разговор и лично перезвоните или зайдите в ближайший филиал** банка (подразделение полиции и др.) .

ЧТО ДЕЛАТЬ?

Если Вы все же успели сообщить какие-то сведения о себе, своих счетах, назвать код из СМС и т.п.:

- **немедленно прервать разговор**
- **срочно позвонить в Банк по номеру, указанному на Вашей карте, или зайти в ближайший филиал банка, сообщить о случившемся и немедленно инициировать блокировку своих карт, счетов, прекращение каких-либо сделок от Вашего имени.**
- **сообщить о данном звонке и о случившемся в полицию (сохранив номер звонившего)**

Вопросы к аудитории

-У кого установлен платный антивирус на телефон с ОС Android?

-У кого в мессенджере Telegram включена функция «Облачный пароль» (двухшаговая проверка в WhatsApp)?

-У кого включена блокировка SIM-карты (необходимость вводить PIN-код после перезагрузки телефона или установки SIM-карты в новое устройство)?

ОСНОВНЫЕ ПРАВИЛА ФИНАНСОВОЙ БЕЗОПАСНОСТИ (финансовая гигиена)

ПРИ ИСПОЛЬЗОВАНИИInterNet

1. **Проверять адресную строку интернет-ресурса и содержимое сайта (для выявления признаков фишингового сайта);**

2. **Использовать двухфакторную (многофакторную) идентификацию (логин, пароль, код в sms-сообщении) для входа на интернет – порталы, содержащие критически важную информацию, дающую доступ к банковским счетам или к личному кабинету в интернет - порталах, позволяющих совершать сделки от имени граждан (Госуслуги и т.п.);**

3. **Никому ни при каких условиях (даже родственникам) не сообщать пароли для доступа к своим личным кабинетам, коды в sms-сообщениях, поступившие на телефон;**

4. **Не размещать в соц.сетях персональную информацию, особенно номера счетов, карт, пароли и т.п.;**

5. **при получении от «контакта» в соц.сети просьбы о финансовой помощи, перезвонить лично по известному Вам телефону, для проверки реальности просьбы.**

с использованием материалов ПАО Сбербанк

ПРИ ОБРАЩЕНИИ С БАНКОВСКИМИ КАРТАМИ

ОСНОВНЫЕ ПРАВИЛА ФИНАНСОВОЙ БЕЗОПАСНОСТИ (финансовая гигиена)

1. **Никому ни при каких условиях не сообщать номер карты, CVV-коды, PIN-коды, содержание SMS от банка (иных структур).**
2. **Не указывать номера карт, CVV-коды, PIN-коды, содержание SMS от банка (иных структур) в переписке, сообщениях, объявлениях и т.п.**
3. **Ограничить посторонним доступ к карте. Расплачиваться всегда самостоятельно.**
4. **Не подключать номера чужих телефонов к своей карте.**
5. **При оплате покупок в интернет-магазинах использовать отдельную карту, на которую зачислять только необходимую для расчетов сумму.**
6. **Никогда не писать PIN-коды на карте или не хранить номер PIN-кода рядом с картой.**
7. **При получении SMS-сообщений о списании денег, которые Вы не совершали, немедленно звонить в банк и блокировать свои счета.**
8. **При утрате карты или компрометации PIN-кода или иных реквизитов карты немедленно звонить в банк и блокировать свои счета.**

ОСНОВНЫЕ ПРАВИЛА ФИНАНСОВОЙ БЕЗОПАСНОСТИ (финансовая гигиена)

1. **Блокировать доступ к телефону, планшету, компьютеру и SIM-карте путем установки паролей, пин-кодов, иными способами и не сообщать их никому.**

с использованием материалов ПАО Сбербанк

ПРИ ОБРАЩЕНИИ С МОБИЛЬНЫМИ УСТРОЙСТВАМИ

2. **Поддерживать в актуальном состоянии антивирусную защиту мобильных телефонов, планшетов, компьютеров для исключения вирусного заражения и возможности удаленного управления Вашим компьютером преступниками.**

3. **Не открывать сообщения (MMS, фото, видео и т.п.), полученные от неизвестных Вам номеров, и не переходить по полученным от них ссылкам.**

4. **Не совершать каких-либо действий по указанию звонящего, под какими бы предлогами абонент это не просил. При малейших сомнениях прервать общение по телефону и перезвонить по номеру, указанному на карте либо обратиться в офис банка.**

ОСНОВНЫЕ ПРАВИЛА ФИНАНСОВОЙ БЕЗОПАСНОСТИ (финансовая гигиена)

5. **При утрате телефона, SIM-карты или смене номера телефона, к которым были привязаны системы мобильного банкинга, в обязательном порядке проинформировать банк для блокировки функции мобильного банкинга на утраченном (замененном) номере телефона.**

6. **При получении сообщений даже от знакомых абонентов с просьбами о переводе денег, перезванивать только по известным Вам телефонам и уточнять достоверность информации.**

7. **При работе в интернет помнить про фишинговые сайты и способы их выявления.**

с использованием материалов ПАО Сбербанк

8. **Для работы на интернет-ресурсах, содержащих персональные данные или финансовые приложения, использовать многофакторную идентификацию (логин, пароль, смс-подтверждение), никому ни под какими предлогами их не сообщать.**