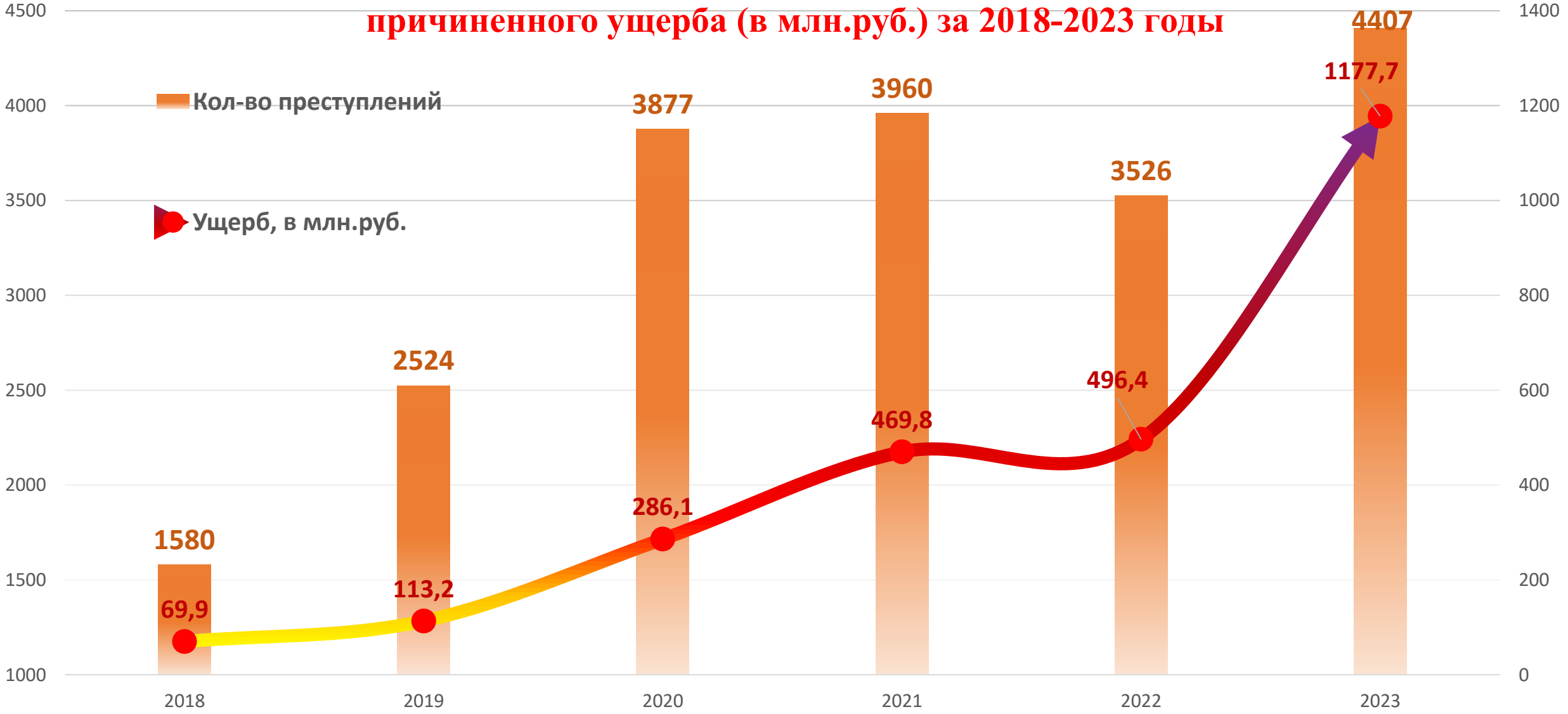
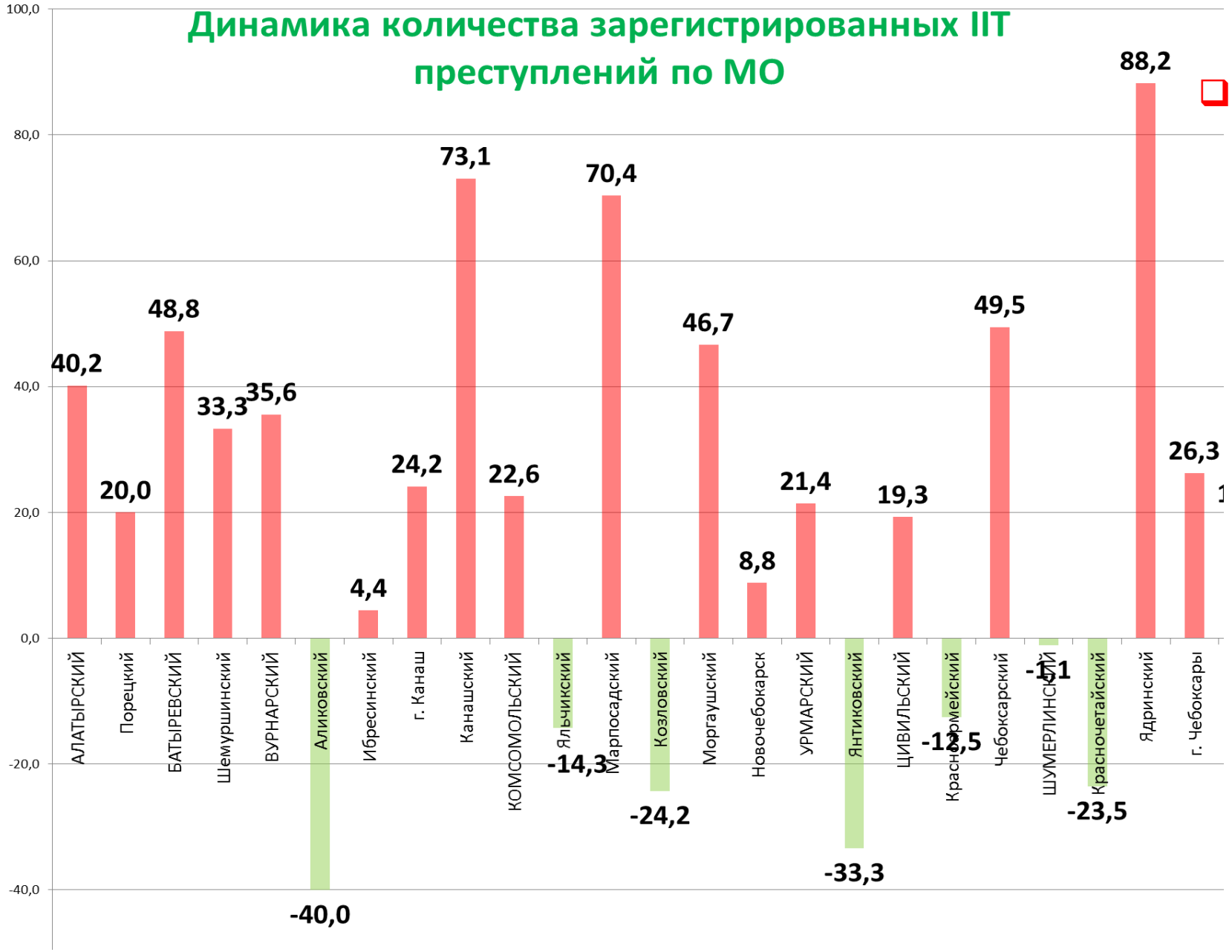
Как защититься от мошенников

Динамика зарегистрированных преступлений в Чувашской Республике с использованием информационных-телекоммуникационных технологий и причиненного ущерба (в млн.руб.) за 2018-2023 годы





- **Результаты мониторингового опроса граждан Российской Федерации, посвящённому телефонному мошенничеству (*Всероссийский центр изучения общественного мнения от 20.02.2024*)**

- 67% россиян за последние полгода-год получали звонки от телефонных мошенников,

- 17% россиян за последние полгода-год получали СМС-сообщения, от телефонных мошенников.

IT преступления – угроза №1

- **более 90%** фактов хищения – с использованием IT

- **15 млн в сутки** - количество попыток телефонного мошенничества в отношении россиян в 2023 году по сравнению с 5 млн в 2022.

Ос

Характеристика потерпевших *(пол, возраст, профессия)*

- женщины - 57,2%, - мужчины - 42,8%,

ВОЗРАСТ:

- до 25 лет – 16,1% ,
- от 25 до 34 – 17,0% ,
- от 35 до 44 – 22,1% ,
- от 45 до 54 – 18,9% ,
- от 55 до 64 – 14,1% ,
- свыше 65 – 11,8% .

Образовательные, медицинские и иные организации, в отношении работников и учащихся которых в течение 2023 года совершены бесконтактные мошенничества и кражи денежных средств с банковских карт граждан

- **Чувашский государственный университет им. И.Н. Ульянова – 68,**
- **Чувашский государственный педагогический университет им. И.Я. Яковлева – 16,**
- **БУ «Городская клиническая больница № 1» – 15,**
- **Чебоксарский кооперативный институт – 9,**
- **БУ «Республиканская психиатрическая больница» – 8,**
- **Чувашский государственный аграрный университет – 7,**
- **Чебоксарский институт (филиал) Московского политехнического университета – 7,**
- **БУ «Республиканская клиническая больница» – 7.**

Наиболее подвержены преступным посягательствам

Динамика объектов посягательств преступников

	2020	2021	2022	2023
Объекты посягательства	сбережения	сбережения	сбережения	сбережения
		кредиты	кредиты	кредиты
			жилье	жилье
				акты терроризма

- 99% звонков с подменой номера
- 25% фактов мошенничества - с использованием кредитных средств
- Каждый сотый потерпевший лишается жилья

В 2023 году количество совершенных подростками мошенничеств увеличилось в 2,5 раза *(+155,6%; с 9 до 23):*

- *г. Чебоксары – на 220,0% (с 5 до 16),*
- *г. Новочебоксарск – на 200% (с 1 до 3),*
- *Шумерлинский МО – 2,*
- *Мариинско-Посадский МО -1,*
- *г. Канаш - по 1.*

Сведения о преступлениях, совершенных несовершеннолетними с использованием ИТТ в 2023 году:

Ст. 158 ч. 3 УК РФ «Кража» – 8 *(Алатырский МО, Мариинско-Посадский МО, Чебоксарский МО, Канашский МО, г. Чебоксары -3).*

Ст. 159 УК РФ «Мошенничество» - 18 *(г.Новочебоксарск -3, Шумерлинский МО – 2, г. Канаш -1, г. Чебоксары – 12, в т.ч. Ленинский район – 8, Калининский район- 3, Московский район – 1).*

Ст. 207 УК РФ «Ложное сообщение об акте терроризма»– 4 *(Калининский район г. Чебоксары).*

Ст. 228, 228.1 УК РФ (в сфере незаконного оборота наркотиков) – 41 *(Чебоксарский МО – 2, г. Чебоксары – 39, в т.ч. Ленинский район – 3, Калининский район- 6, Московский район – 30).*

Ст. 242.1 УК РФ «Распространение порнографии» – 1 *(г. Чебоксары).*

Ст. 272 КУК РФ «Неправомерный доступ к компьютерной информации» – 1 *(г. Канаш).*

Ст. 137 УК РФ «Нарушение неприкосновенности частной жизни» – 1 *(Московский район г. Чебоксары).*

Ст. 138.1 УК РФ (Незаконный оборот спецтехсредств) – 1 *(Ленинский район г. Чебоксары).*

«ТОП» 5 способов мошенничества граждан

1. Преступники представляются сотрудниками банков и правоохранительных органов, сообщают о попытках оформления кредитов на ваше имя и завладения деньгами.

Чаще всего мошенники звонят на сотовый телефон и представляются сотрудниками службы безопасности банка, полицейскими прокурорами, следователями и т.д. Они сообщают, что кто-то пытается похитить деньги с вашей банковской карты или оформить кредит на ваше имя, и для решения проблемы просят перевести сбережения на так называемый «безопасный» счет.

Нередко аферисты требуют получить кредит, пока это не сделали за вас, и также перевести уже заемные деньги на указанные ими счета. При этом они просят при посещении банка ни в коем случае не называть истинные причины обращения, так как в финансовом учреждении могут оказаться нечистые на руку сотрудники.

Другим способом хищения является требование установить на телефон специальное мобильное приложение, однако в случае его установки мошенники получают неограниченный доступ к паролям, персональным данным, банковским онлайн-сервисам.

В этой ситуации лучше всего сразу положить трубку, а если сомневаетесь, перезвоните в банк по телефону, указанному на обратной стороне карты.

Некоторые предлоги, с которыми обращаются мошенники

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 СВУ»**
- - **подключение специальных программ, препятствующих оформлению кредитов или снятию со вкладов и направления денег на спец.счет.**
- - 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, у 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, некачественные товары, **выплаты** «в связи с СВО» и т.п., «вступление в **наследство**», **получение вознаграждений**, приза, подарков.

Подвиды телефонного мошенничества:

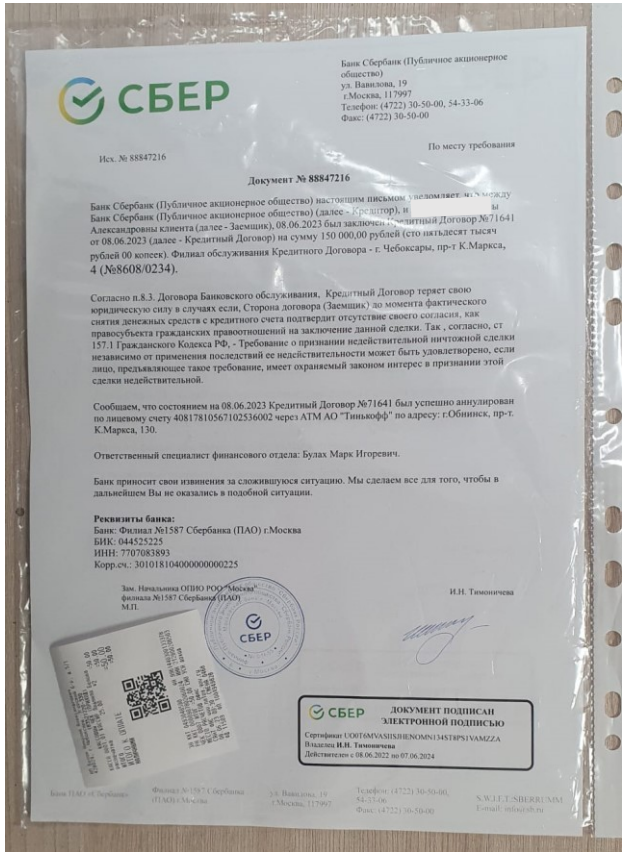
- звонки через мессенджер. При таком звонке **на аватарке виден логотип известного банка или эмблема МВД (ФСБ, Следственного комитета, Центрбанка и т.п.), или другие легко узнаваемые логотипы.** В качестве доказательств злоумышленники присылают якобы договора кредитования или материалы уголовного дела. Также просят набрать определенный номер, если пользователь выполняет требования, то хакеры получают доступ к его учетной записи.

- **видеозвонки через мессенджер –** имитация звонка из офиса банка (подразделения правоохранительных органов и т.п.), **спектакль** с последующими аналогичными действиями.

- использование курьеров для доставки фиктивных писем, получения денег.

- Технология DeepFake – компьютерные программы по переносу изображения и голоса объекта, значимого для потерпевшего, на изображение и голос преступника, и побуждение жертвы к действиям от имени значимого объекта .

Некоторые примеры «документов», направленных мошенниками потерпевшим



СБЕР

Банк Сбербанк (Публичное акционерное общество)
ул. Вавилова, 19
г.Москва, 117997
Телефон: (4722) 30-50-00, 54-33-06
Факс: (4722) 30-50-00

Исх. № 88847216

По месту требования

Документ № 88847216

Банк Сбербанк (Публичное акционерное общество) настоящим письмом уведомляет, что между Банк Сбербанк (Публичное акционерное общество) (далее - Кредитор), и [redacted] Александровны клиента (далее - Заемщик), 08.06.2023 был заключен [redacted]итный Договор №71641 от 08.06.2023 (далее - Кредитный Договор) на сумму 150 000,00 рублей (сто пятьдесят тысяч рублей 00 копеек). Филиал обслуживания Кредитного Договора - г. Чебоксары, пр-т К.Маркса, 4 (№8608/0234).

Согласно п.8.3. Договора Банковского обслуживания, Кредитный Договор теряет свою юридическую силу в случаях если, Сторона договора (Заемщик) до момента фактического снятия денежных средств с кредитного счета подтвердит отсутствие своего согласия, как правосубъекта гражданских правоотношений на заключение данной сделки. Так , согласно, ст 157.1 Гражданского Кодекса РФ, - Требование о признании недействительной ничтожной сделки независимо от применения последствий ее недействительности может быть удовлетворено, если лицо, предъявляющее такое требование, имеет охраняемый законом интерес в признании этой сделки недействительной.

Сообщаем, что состоянием на 08.06.2023 Кредитный Договор №71641 был успешно аннулирован по лицевому счету 40817810567102536002 через АТМ АО "Тинькофф" по адресу: г.Обинск, пр-т. К.Маркса, 130.

Ответственный специалист финансового отдела: Булах Марк Игоревич.

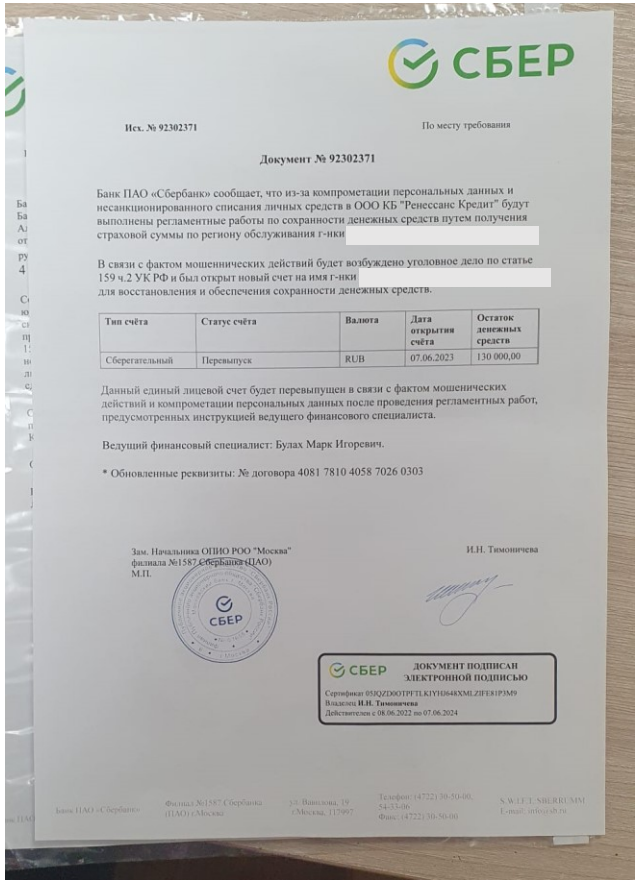
Банк приносит свои извинения за сложившуюся ситуацию. Мы сделаем все для того, чтобы в дальнейшем Вы не оказались в подобной ситуации.

Реквизиты банка:
Банк: Филиал №1587 Сбербанка (ПАО) г.Москва
БИК: 044525225
ИНН: 7707083893
Корр.сч.: 30101810400000000225

Зам. Начальника ОПИО РОО "Москва" филиала №1587 Сбербанка (ПАО)
М.П.

И.Н. Тимончева

СБЕР ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат C0OT6MVASIISBHEOMN134ST8PS1VAMZZA
Владелец И.Н. Тимончева
Действителен с 08.06.2022 по 07.06.2024



СБЕР

Исх. № 92302371

По месту требования

Документ № 92302371

Банк ПАО «Сбербанк» сообщает, что из-за компрометации персональных данных и несанкционированного списания личных средств в ООО КБ "Ренессанс Кредит" будут выполнены регламентные работы по сохранности денежных средств путем получения страховой суммы по региону обслуживания г-ники [redacted]

В связи с фактом мошеннических действий будет возбуждено уголовное дело по статье 159 ч.2 УК РФ и был открыт новый счет на имя г-ники [redacted] для восстановления и обеспечения сохранности денежных средств.

Тип счёта	Статус счёта	Валюта	Дата открытия счёта	Остаток денежных средств
Сберегательный	Перевыпуск	RUB	07.06.2023	130 000,00

Данный единый лицевой счет будет перевыпущен в связи с фактом мошеннических действий и компрометации персональных данных после проведения регламентных работ, предусмотренных инструкцией ведущего финансового специалиста.

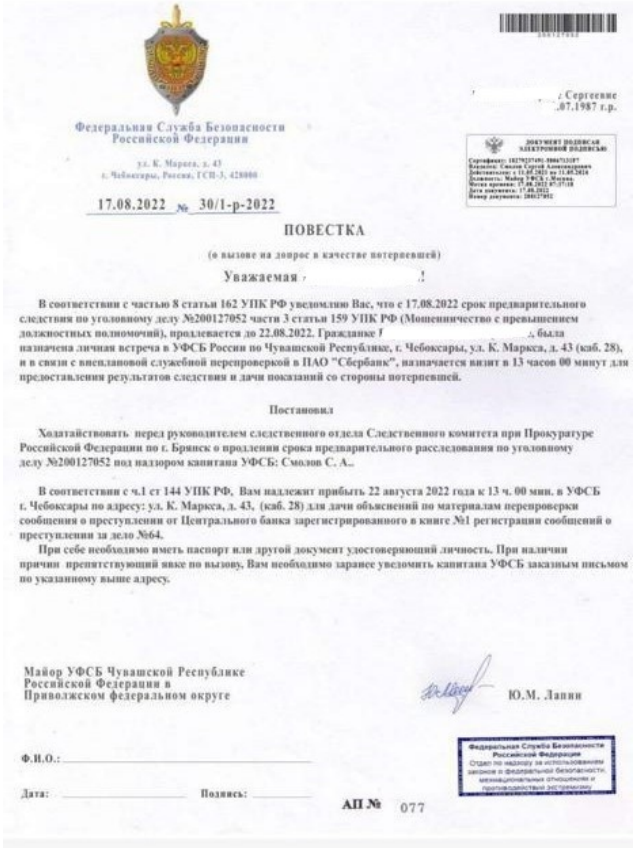
Ведущий финансовый специалист: Булах Марк Игоревич.

* Обновленные реквизиты: № договора 4081 7810 4058 7026 0303

Зам. Начальника ОПИО РОО "Москва" филиала №1587 Сбербанка (ПАО)
М.П.

И.Н. Тимончева

СБЕР ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат 03QZD0OTPTTLKIYH0648XMLZIFE81P3M9
Владелец И.Н. Тимончева
Действителен с 08.06.2022 по 07.06.2024



Федеральная Служба Безопасности Российской Федерации

ул. К. Маркса, д. 43
г. Чебоксары, Россия, ГСП-3, 428000

17.08.2022 № 30/1-р-2022

ПОВЕСТКА

(о вызове на допрос в качестве потерпевшей)

Уважаемая [redacted]!

В соответствии с частью 8 статьи 162 УПК РФ уведомляю Вас, что с 17.08.2022 срок предварительного следствия по уголовному делу №200127052 части 3 статьи 159 УПК РФ (Мошенничество с превышением должностных полномочий), продлевается до 22.08.2022. Гражданке [redacted], была назначена личная встреча в УФСБ России по Чувашской Республике, г. Чебоксары, ул. К. Маркса, д. 43 (каб. 28), и в связи с внеплановой служебной перепроверкой в 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 срока предварительного расследования по уголовному делу №200127052 под надзором капитана УФСБ: Смолов 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 перепроверки сообщения о преступлении от Центрального банка зарегистрированного в книге №1 регистрации сообщений о преступлении за дело №64.

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

Майор УФСБ Чувашской Республике
Российской Федерации в
Приволжском федеральном округе

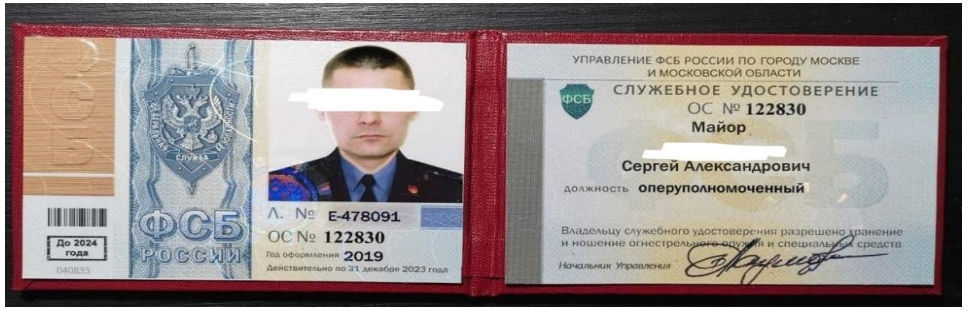
Ю.М. Лапин

Ф.И.О.: _____

Дата: _____ Подпись: _____

АП № 077

Федеральная Служба Безопасности Российской Федерации



УПРАВЛЕНИЕ ФСБ РОССИИ ПО ГОРОДУ МОСКВЕ И МОСКОВСКОЙ ОБЛАСТИ

СЛУЖЕБНОЕ УДОСТОВЕРЕНИЕ

ОС № 122830

Майор

Сергей Александрович

должность оперуполномоченный

Владельцу служебного удостоверения разрешено хранение и ношение огнестрельного оружия и специальных средств

Начальник Управления

ФСБ РОССИИ

Л. № Е-478091

ОС № 122830

Год оформления 2019

Действительно по 31 декабря 2023 года

До 2024 года

040833

ЦЕНТРАЛЬНЫЙ БАНК РФ

ЦА № 12482

(личная подпись)

Действительно до 31 декабря 2023

УДОСТОВЕРЕНИЕ ЦА № 12482

[redacted]

Дмитрий Геннадьевич

Ведущий специалист

Внутрибанковской службы безопасности

Центрального Банка Российской Федерации

Отдела по борьбе с мошенничеством

Руководитель Службы безопасности

ВНУТРИБАНКОВСКОЙ СЛУЖБЫ БЕЗОПАСНОСТИ ЦЕНТРАЛЬНОГО БАНКА РОССИЙСКОЙ ФЕДЕРАЦИИ

№331

«ТОП» 5 способов мошенничества граждан

2. Поступают звонки (не редко пожилым людям) с информацией о ДТП (ином происшествии) с участием их близких и необходимостью передать деньги для решения возникших проблем.

Вам звонят с незнакомого номера и тревожным голосом сообщают, что ваш родственник или знакомый попал в аварию, за решетку, в больницу, и теперь, чтобы решить проблему, нужна крупная сумма денег. По такой схеме работают мошенники!

Позвоните родственникам, чтобы проверить полученную информацию.

«ТОП» 5 способов мошенничества граждан

3. Продавцы товаров через сайты бесплатных объявлений просят перечислить предоплату, оставляя покупателей ни с чем. И наоборот, при попытке продать товар через Интернет, покупатели просят назвать реквизиты банковской карты для зачисления денег и похищают сбережения.

Огромное количество мошенничеств совершается с использованием сайтов бесплатных объявлений при покупке-продаже товаров. Преступники размещают объявления о продаже товара, как правило, по цене ниже рыночной, просят перевести предоплату или полную его стоимость, но желаемое вы так и не получите. И наоборот, если вы сами разместили объявление о продаже чего-либо, вам могут позвонить и попросить назвать реквизиты карты для перевода денег за товар или пройти по ссылке для получения денежных средств, а затем похищают все содержимое вашего счета.

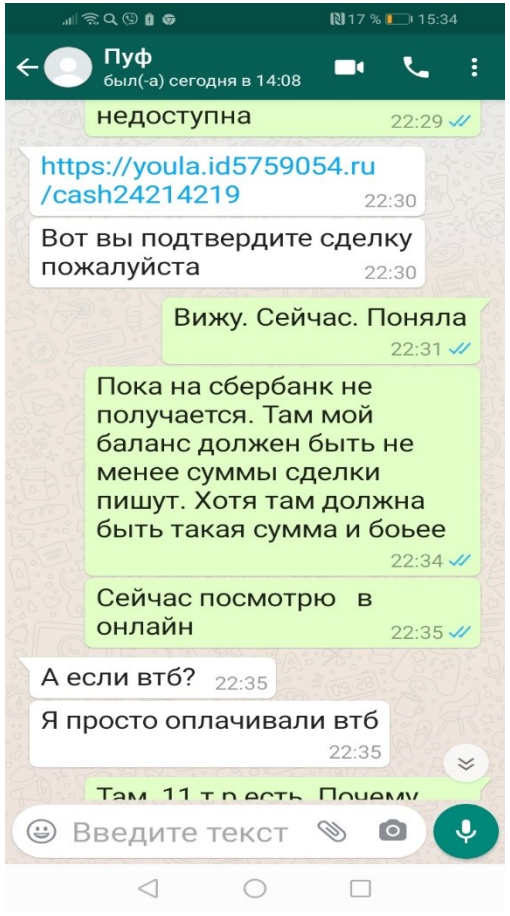
Как себя обезопасить? В первой ситуации не следует переводить деньги, если вы не уверены, что вас не обманут. Да, существуют известные продавцы с надежной репутацией, но к ним никак не относятся люди, разместившие частные объявления в Интернете.

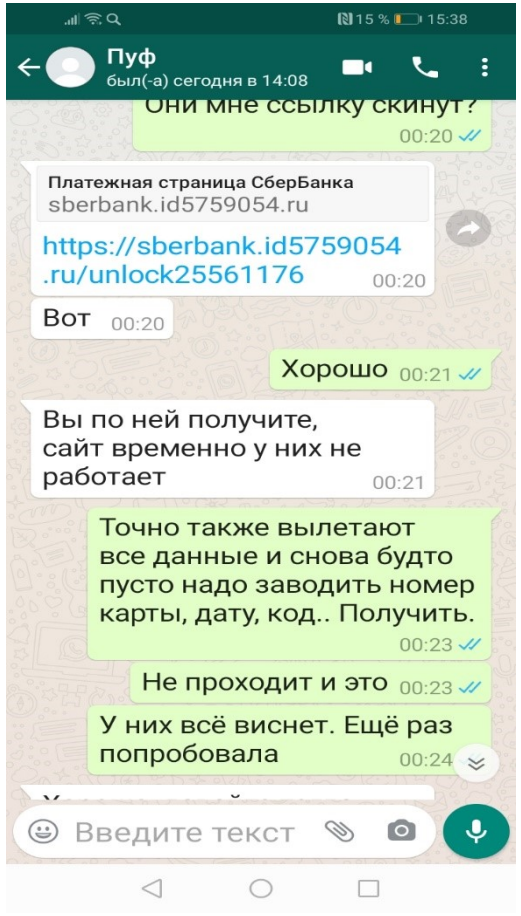
При покупке-продаже товара через популярные сайты бесплатных объявлений можно воспользоваться специализированной услугой доставки, но для этого внимательно изучите правила ее оформления и ни в коем случае не переходите к общению в мессенджеры, где вам могут выслать ссылку или QR-код для последующего хищения денежных средств, а также храните в тайне свои почту, коды из уведомлений и смс.

И если вы сами продаете товар и хотите получить за него деньги, достаточно будет назвать номер телефона, привязанный к вашей карте.

И все! Никаких кодов, паролей и реквизитов карты!

Компрометация реквизитов карты путем перехода по присланным гиперссылкам (фактически переход на фишинговый сайт)





- Мошенники размещают в интернет (на сайтах Юла, Авито, БлаБлаКар и т.п.) 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).
- Клиент проходит по ссылке, попадает на фишинговый сайт, где вводит реквизиты своей банковской карты.
- Мошенник, получив данные карты клиента, в режиме он-лайн совершает покупки в интернет-сервисах, либо переводит средства на свои карты.

«ТОП» 5 способов мошенничества граждан

4. Предприимчивым жителям республики предлагают заработать на инвестициях и вкладах, валютных и криптобиржах, обещая нереально высокие проценты.

Предложения заработать на фондовых биржах или акциях крупных нефтегазодобывающих компаний человека без соответствующих знаний должны сразу насторожить. К объявлениям и рекламе в Интернете, предлагающим сверхприбыли от инвестирования, нужно относиться очень критично. Сверхбольшими процентами, которые обещают мошенники, можно назвать те, что в два и более раза превышают средний процент по банковским вкладам.

К тому же серьезные брокеры, такие как банки, крупные фонды, не станут гарантировать доход от вложений в биржевые инструменты, ведь на фондовом рынке бывают как взлёты, так и падения.

Если есть интерес к этому виду деятельности, обращайтесь только к надежным брокерам. И начинать стоит с очень небольшой суммы, которую не жалко потерять в случае неудачи.

«ТОП» 5 способов мошенничества граждан

5. Поступают сообщения из взломанных аккаунтов с просьбой одолжить деньги

Нередко мошенники взламывают аккаунты в соцсетях и под видом ваших знакомых просят одолжить деньги. Прежде чем перечислять средства на указанный счет, перезвоните знакомому. Наверняка у него все хорошо, не считая того, что его аккаунт взломали. Для защиты от такого рода мошенников не рекомендуется также переходить по ссылкам от незнакомых людей. Установите дополнительную защиту своего аккаунта, например, необходимость введения пароля при входе с другого устройства.

Еще раз запомните! Мошенники могут использовать различные уловки: представляться сотрудниками банков, правоохранительных органов, работодателями, Вашими близкими, придумывать что угодно! Их главная цель - получить от вас деньги или реквизиты банковской карты! В случае сомнений, обратитесь в полицию.

Иные варианты мошенничеств с целью хищения денежных средств, завладения имуществом

- **SMS-мошенничество, фишинговые письма** – рассылка сообщений (писем) от имени солидной организации (соц.служба, банки, правоохранительные структуры, судебные приставы, инвестиционные компании, госучреждения, мобильные операторы и т.п.) с вложенными гиперссылками, пройдя по которым жертва или загружает ПО (в т.ч. вирусное), позволяющее удаленно управлять своим гаджетом, или попадает на фишинговый сайт, где вводит критичные реквизиты, позволяющие совершать действия с деньгами или имуществом.

- **Мошенничество в социальных сетях –** взлом (копирование) аккаунтов пользователя соц.сети с последующей рассылкой от его имени сообщений контактам жертвы с просьбой переслать деньги или иную критичную информацию, переписка с «продавцом» («покупателем») , который пересылает фишинговую ссылку на «сайт» для получения критичных реквизитов, позволяющих совершать действия с деньгами или имуществом.

- **Мошенничество в Интернет** – использование фишинговых сайтов, где жертва вводит критичные реквизиты, позволяющие совершать действия с деньгами или имуществом.

- **QR-коды в общественных местах**, при переходе по которым гражданам обещают «гарантированные» выплаты. Когда человек сканирует QR-код, он попадает в чат-бот в мессенджере. Далее выясняется, что ему якобы положена выплата. Однако под предлогом оформления пособий мошенники запрашивают персональные данные, которые они используют для хищения денег с банковской карты.

Как они обманывают? Принципиальная схема мошенничеств

1. **«Задавить авторитетом»:** весомый «сотрудник банка», «правоохранительных органов», госслужащий (уверенный или сочувствующий голос), использование **технологии подмены номера** (IP-телефония и т.п.), **специфической терминологии** (псевдобанковской: «спецсчет», «защищенный счет», «объединенный счет ЦБ» и т.п., правоохранительной («следователь», «потерпевший, «уголовное дело», «допрос», «спецоперация», «ответственность за разглашение тайны следствия, банковской тайны или конфиденциальной информации», «арест» и т.п.);
2. **Вывести из душевного равновесия (страх, эйфория):** (угроза потери денег, имущества, угроза стать невольным должником по кредиту, беда с родственником, выигрыш, социальная выплата, компенсация и т.п.);
3. **Закрепить, подтвердить «достоверность» информации из «другого источника» -** дополнительным звонком «значимого сотрудника из другого ведомства», предложением **перепроверить достоверность номера** абонента через интернет, направлением **фотографии «служебного удостоверения», «письма банка»**, «повестки», любого иного документа «официального документа» (в т.ч. с реальной доставкой фиктивных документов);
4. **Нагнетание «срочности»,** необходимости «незамедлительности» действий под угрозой невозможности предотвратить последствия в случае промедления.
5. **Запрет на общение с другими лицами** под угрозой «уголовной ответственности за разглашение конфиденциальной информации», «тайны следствия», «банковской тайны», **инструктаж о «легенде»** для окружающих (в т.ч работников банка, полиции) и т.п.
6. **Удержание непрерывно длительное время на телефоне по несколько часов или дней** (якобы для контроля и недопущения разглашения тайны следствия, гос.тайны, банковской тайны и т.п.)
7. По мере «созревания жертвы» **управление по телефону её действиями: по переводу денег** на номера мобильных телефонов, интернет-кошельки, передаче наличных денег сообщникам и т.п., получение реквизитов банковских карт, PIN-кода, sms и т.п., п**обуждение к установке** «специальных защитных программ», введению «специальных защитных или проверочных кодов» и т.п., периодически повторяя действия по п.п.1-5 для поддержания необходимого для преступника состояния жертвы;

Почему это случилось?

- **самоустранение от реалий** современной жизни, **самонадеянность**, отсутствие актуальных знаний о современной криминальной ситуации в стране и мире **(***новости не смотрю и не читаю, т.к. там только одна чернуха и вранье, мне это не интересно и не надо, я сам все знаю); у меня все равно денег нет, поэтому мне это не грозит.*
- **Отсутствие знаний** **о методах** социальной инженерии, о технологиях подмены номеров (например, IP-телефония и т.п.), технологиях подмены изображения и голоса;
- **доверие** **к** *значимому «титулу», присланным фотографиям и документам (строгий голос, убедительные фразы, номер телефона гос.органа, который указан в интернете, «солидные» бланки «документов», внешне легкое и «приемлемое» решение возникшей ситуации, «угроза наказания» за раскрытие информации посторонним или отказ от выполнения требований и т.п.),*
- **состояние** **сильного душевного волнения** **от полученной информации** (*страх потерять деньги, эйфория от возможности заработать быстро и много, опасение за своих близких или за здоровье и т.п.);*
- **незнание технологии работы** банков, правоохранительных или иных гос. структур**: предоставление критичной информации, осуществление иных действий** *(операции со своими счетами, оформление кредитов, передача или пересылка денег, установка каких-либо приложений на телефон (планшет, компьютер) и т.п.)* по указанию звонящего;
- **Недостаточные навыки критического мышления**: **не задумываемся, почему должны верить абоненту?** *(Почему нельзя посоветоваться даже с близкими людьми? Зачем переводить куда-то уже снятые наличные деньги? и т.п.);*

САМЫЕ ПРОСТЫЕ ПРАВИЛА БЕЗОПАСНОСТИ

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

- **Отнестись с недоверием к звонку неизвестного Вам абонента.**
- **Успокоиться и критически оценить информацию (почему должен ему верить? Почему мне нельзя посоветоваться даже с близкими людьми, теми, кого я знаю и кому доверяю, зачем переводить куда-то уже снятые наличные деньги, как я могу убедиться, что полученные мной по телефону изображения документов – не подделка** (ведь при современном уровне компьютерной техники можно сфабриковать любой документ) **и т.п.);**
- **Вспомнить, что мошенники существуют (независимо от нашего желания), что возможна подмена номера на любой номер, в т.ч. на номер, указанный на официальном интернет-портале ведомства (технология IP-телефонии** и т.п.), возможна подмена изображения и голоса (технология DeepFake и т.п.).
- **Вспомнить, что ни банки, ни правоохранительные органы и иные госструктуры: никогда не требуют** от Вас информацию, **не требуют куда-то переводить** Ваши деньги или получать кредиты, **не просят** передать деньги кому-либо, **не используют** каких-либо номеров, кроме официальных, или интернет-кошельки, **не привлекают** клиентов к оперативно-розыскным и следственным мероприятиям, **не направляют** фотографии своих удостоверений, не общаются по несколько часов непрерывно по телефону и т.п.
- **Не совершать никаких действий** по указанию звонящего, под какими бы предлогами это не просил (угрожал): **не переводить деньги, не оформлять кредиты, никаких программ не устанавливать, не переходить по гиперссылке, никакие кнопки не нажимать, ни сообщать поступившее на телефон содержание SMS, никакие коды не вводить и т.п.**
- **Сразу прервать разговор. В случае сомнений лично перезвонить** в Банк (полицию, иную структуру) по официальному номеру, указанному на Вашей карте (найденному лично Вами по официальным справочникам и т.п.) или лично **зайти в ближайший филиал** банка (подразделение полиции и др.).

Почему необходимо прервать разговор?

- «Сбросив» звонок, Вы разрываете IP-соединение с преступником. Преступники «боятся потерять» контакт. Попытка перезвонить на номер звонившего будет неудачной, т.к. используются подменные номера.
- -Преступники подготовлены (обучены) ответить на любой вопрос (имеют «скрипты», интернет, хакерские программы). Задавая вопросы, можно убедить себя, что действительно разговариваешь с тем, за кого выдает себя преступник.
- Ваш номер (в отместку) могут использовать в технологии IP-телефонии для звонка в правоохранительные органы об угрозе теракта и т.д.;
- Ваш голос может быть использован для модуляции иного «поддельного», дискредитирующего Вас, сообщения или для звонка Вашим контактам от Вашего имени с целью мошенничества.
- При продолжении разговора со стороны преступников может последовать требование денег под различными угрозами.

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.

Что делать если Вы все же успели сообщить какие-то сведения о себе, своих счетах и т.п.?

- **немедленно прервать разговор**, не брать телефон при повторных звонках, или (если ответили) не вступать в разговор, несмотря ни на какие уговоры, угрозы и т.п.

- **лично перезвонить в Банк** по номеру, указанному на Вашей карте, **или зайти в ближайший филиал банка, сообщить о поступившем звонке**. При наличии сомнений заблокировать свои карты.

- **Лично перезвонить в структуру, от имени которой обращался мошенник** по официальному номеру, найденному лично Вами по официальным справочникам и т.п. или лично **зайти в ближайшее подразделение госоргана** (подразделение правоохранительных органов, финансовая организация, администрация, госуслуги, мобильный оператор и др., от имени которого поступил звонок) .

- для большей уверенности и поддержки лучше дополнительно **позвонить своим близким** (детям, родным, знакомым)

- **сообщить о данном звонке в полицию** (сохранив номер звонившего, переписку и т.д.).

ОСНОВНЫЕ ПРАВИЛА ФИНАНСОВОЙ БЕЗОПАСНОСТИ (финансовая гигиена)

ПРИ ИСПОЛЬЗОВАНИИ InterNet

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.

ОСНОВНЫЕ ПРАВИЛА ФИНАНСОВОЙ БЕЗОПАСНОСТИ (финансовая гигиена)

ПРИ ОБРАЩЕНИИ С БАНКОВСКИМИ КАРТАМИ

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)

ПРИ ОБРАЩЕНИИ С МОБИЛЬНЫМИ УСТРОЙСТВАМИ

1. Блокировать доступ к телефону, планшету, компьютеру путем **установки паролей, пин-кодов,** иными способами и не сообщать их никому.
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.
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.
8. Для работы на интернет-ресурсах, содержащих персональные данные или финансовые приложенния, **использовать многофакторную идентификацию** (логин, пароль, смс-подтверждение), никому ни под какими предлогами их не сообщать.

БЕРЕГИТЕ СЕБЯ
И НЕ ПОПАДАЙТЕСЬ НА УЛОВКИ МОШЕННИКОВ

Материалы по профилактике мошенничества

Телеграмм-канал «Вестник киберполиции России»